Installing an SSL Certificate Provided by a Certificate Authority (CA) on the vWLAN Appliance

Date: 2/18/2011
Revision: 1.0

Introduction

This document explains how to install an SSL certificate provided by a Certificate Authority (CA) such as VeriSign on the vWLAN Appliance or vWLAN Virtual Appliance (VMware).

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:

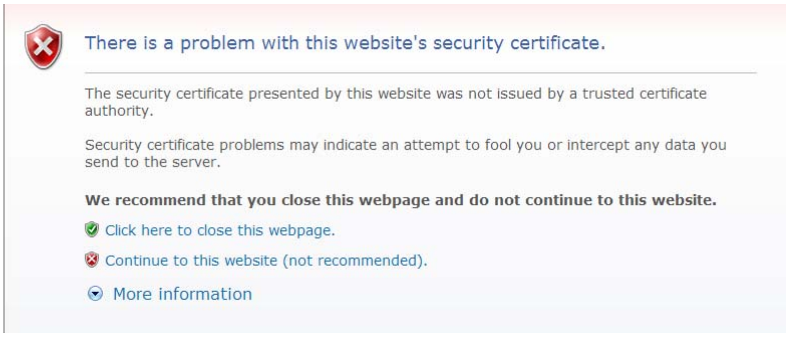
- All supported platforms running current software image/patches. Current software image/patches and release notes available at support.bluesocket.com for download.

Background Information

By default the vWLAN Appliance uses a pre-installed self-signed SSL certificate to encrypt web based login transactions. The vWLAN Appliance 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 CA. This is because the Bluesocket self-signed certificate is not in the browsers list of trusted root certificate authorities and Bluesocket is not a CA. Below is an example of what the error will look like when using Microsoft Internet Explorer 8 (IE8).



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

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

1. Continue to use the default Bluesocket self-signed certificate on the vWLAN Appliance and install the Bluesocket self-signed certificate on each client in the browser's list of trusted root certificate authorities.
2. Install an SSL certificate provided by a CA such as VeriSign on the vWLAN Appliance that is already in the client's list of trusted root certificate authorities. This method does not require installing a certificate on each client.

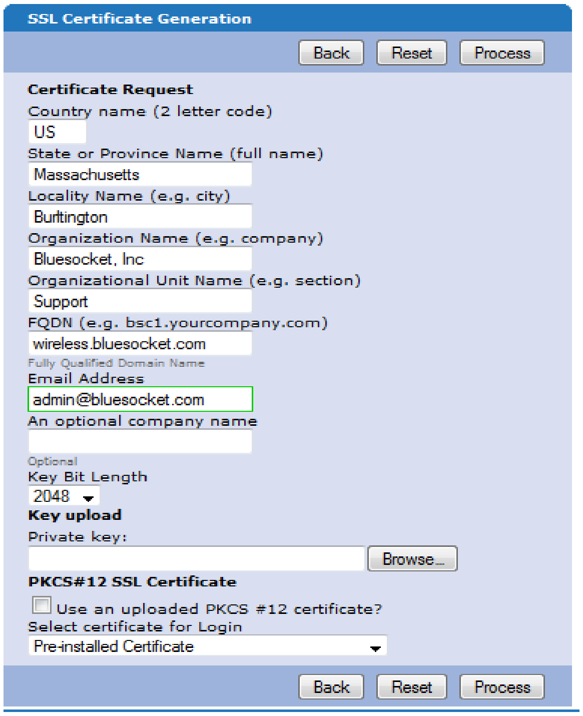
This document explains the second method of how to install an SSL certificate provided by a CA on the vWLAN Appliance. When shopping for an SSL certificate it important to look for a CA with 99.9% + browser recognition if all possible. Some lower cost CA's provide 99% browser recognition which might result in compatibility issues with certain browsers.

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 vWLAN Appliance**
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 vWLAN Appliance**
8. **Click to apply changes (restart web server)**

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

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



Certificate Request

Country name (2 letter code)
US

State or Province Name (full name)
Massachusetts

Locality Name (e.g. city)
Burltington

Organization Name (e.g. company)
Bluesocket, Inc

Organizational Unit Name (e.g. section)
Support

FQDN (e.g. bsc1.yourcompany.com)
wireless.bluesocket.com
Fully Qualified Domain Name

Email Address
admin@bluesocket.com

An optional company name

Optional

Key Bit Length
2048

Key upload

Private key:

PKCS#12 SSL Certificate

□ Use an uploaded PKCS #12 certificate?

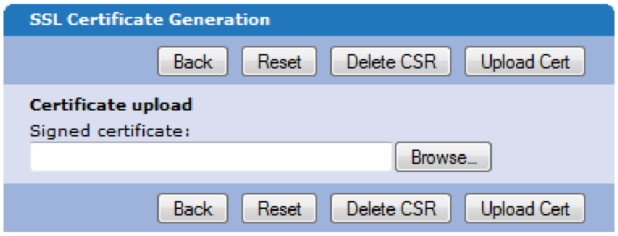
Select certificate for Login
Pre-installed Certificate

- **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 of the certificate**.** The Common Name is the Host + Domain Name. For example if the hostname of the vWLAN Appliance is wireless(Platform>Interfaces>Network>Hostname) and your domain name is bluesocket.com

(Platform>Interfaces>Network>Default Domain). You should enter wireless.bluesocket.com. *Alternatively if you are purchasing a wild card certificate to install on multiple vWLAN Appliances, enter an asterisk (*) instead of the hostname. For example *.bluesocket.com. ***If you are using Internal 802.1x Authentication in addition to Web Based Authentication** or will be in the future, it is NOT recommended to install a wildcard certificate. Microsoft clients will not be able authenticate via Internal 802.1x if they are configured to validate the certificate. Not validating the certificate is a potential security risk.

- **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 2048 or 1024. As of the end of 2010, most CA's now require a minimum of a 2048 bit CSR.

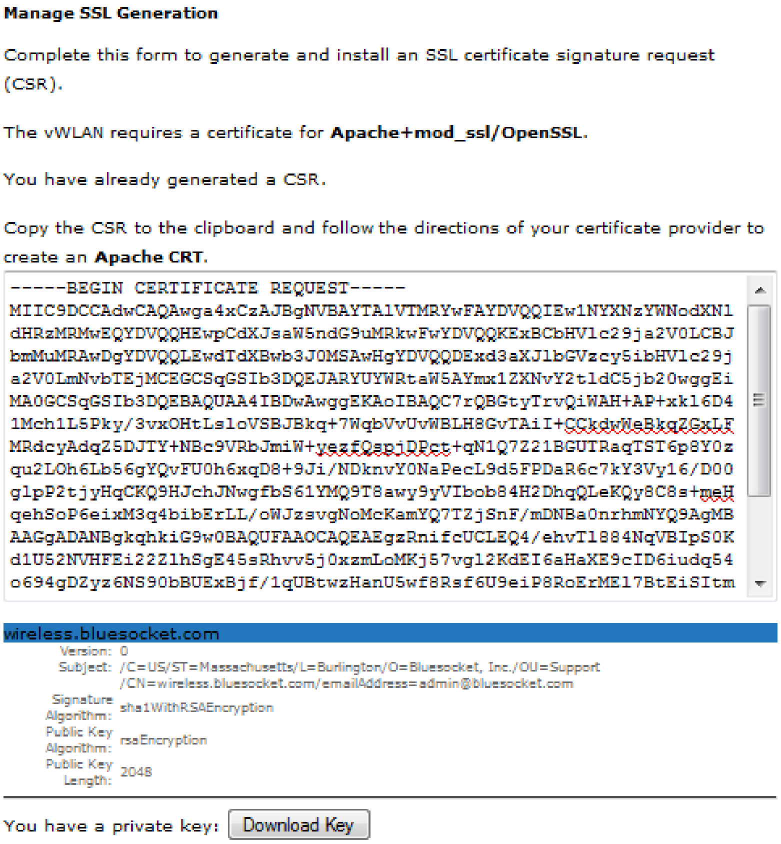
A public/private key pair has now been created. The private key is stored locally on the vWLAN Appliance. The public key, in the form of a Certificate Signing Request (CSR) will be used for certificate enrollment. The CSR will be displayed on the right hand side of the page in text format. A link to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



SSL Certificate Generation

Certificate upload

Signed certificate:



Manage SSL Generation

Complete this form to generate and install an SSL certificate signature request (CSR).

The vWLAN requires a certificate for **Apache+mod_ssl/OpenSSL**.

You have already generated a CSR.

Copy the CSR to the clipboard and follow the directions of your certificate provider to create an **Apache CRT**.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC9DCCAdwCAQAwga4xCzAJBgNVBAYTAlVTMRYwFAYDVQQIEw1NYXNzYWNodXNl
dHRzMRMwEQYDVQQHEwpCdXJsaW5ndG9uMRkwFwYDVQQKExBCbHVlc29ja2V0LCBJ
bmMuMRAwDgYDVQQLEwdTdXBwb3J0MSAwHgYDVQQDExd3aXJlbGVzcy5ibHVlc29j
a2V0LmNvbTEjMCEGCSqGSIb3DQEJARYUYWRtaW5AYmx1ZXNvY2tldC5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7rQBGtyTrvQiWAH+AP+xkl6D4
1Mch1L5Pky/3vxOHtLsloVSBJBkq+7WqbVvUvWBLH8GvTAiI+CCkdwWeBkqZGxLF
MRdcyAdqZ5DJTY+NBc9VRbJmiW+yezfQspjDPct+qN1Q7Z21BGUTRaqTST6p8Y0z
qu2LOh6Lb56gYQvFU0h6xqD8+9Ji/NDknvY0NaPecL9d5FPDaR6c7kY3Vy16/D00
glpP2tjyHqCKQ9HJchJNwgfbS61YMQ9T8awy9yVIbob84H2DhqQLeKQy8C8s+meH
qehSoP6eixM3q4bibErLL/oWJzsvgNoMcKamYQ7TZjSnF/mDNBa0nrhmNYQ9AgMB
AAGgADANBgkqhkiG9w0BAQUFAAOCAQEAEgzRnifcUCLEQ4/ehvTl884NqVBIpS0K
d1U52NVHFEi22ZlhSgE45sRhvv5j0xzmLoMKj57vgl2KdEI6aHaXE9cID6iudq54
o694gDZyz6NS90bBUExBjf/1qUBtwzHanU5wf8Rsf6U9eiP8RoErMEl7BtEiSItm
```

wireless.bluesocket.com

Version: 0

Subject: /C=US/ST=Massachusetts/L=Burlington/O=Bluesocket, Inc./OU=Support /CN=wireless.bluesocket.com/emailAddress=admin@bluesocket.com

Signature Algorithm: sha1WithRSAEncryption

Public Key Algorithm: rsaEncryption

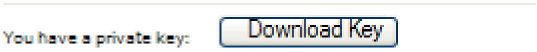
Public Key Length: 2048

You have a private key:

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.

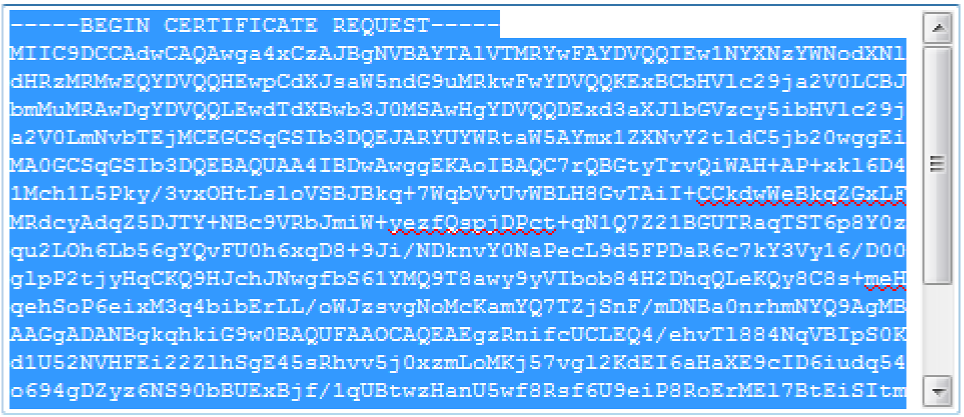
   Click Download Key to backup your private key



You have a 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 CA's enrollment form.



```
-----BEGIN CERTIFICATE REQUEST-----
MIIC9DCCAdwCAQAwga4xCzAJBgNVBAYTAlVTMRYwFAYDVQQIEw1NYXNzYWNodXNl
dHRzMRMwEQYDVQQHEwpCdXJsaW5ndG9uMRkwFwYDVQQKExBCbHVlc29ja2V0LCBJ
bmMuMRAwDgYDVQQLEwdTdXBwb3J0MSAwHgYDVQQDExd3aXJlbGVzcy5ibHVlc29j
a2V0LmNvbTEjMCEGCSqGSIb3DQEJARYUYWRtaW5AYmx1ZXNvY2tldC5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC7rQBGtyTrvQiWAH+AP+xkl6D4
1Mch1L5Pky/3vxOHtLsloVSBJBkq+7WqbVvUvWBLH8GvTAiI+CCkdwWeBkqZGxLF
MRdcyAdqZ5DJTY+NBc9VRbJmiW+yezfQspjDPct+qN1Q7Z21BGUTRaqTST6p8Y0z
qu2LOh6Lb56gYQvFU0h6xqD8+9Ji/NDknvY0NaPecL9d5FPDaR6c7kY3Vy16/D00
glpP2tjyHqCKQ9HJchJNwgfbS61YMQ9T8awy9yVIbob84H2DhqQLeKQy8C8s+meH
qehSoP6eixM3q4bibErLL/oWJzsvgNoMcKamYQ7TZjSnF/mDNBa0nrhmNYQ9AgMB
AAGgADANBgkqhkiG9w0BAQUFAAOCAQEAEgzRnifcUCLEQ4/ehvT1884NqVBIpS0K
d1U52NVHFEi22Z1hSgE45sRhvv5j0xzmLoMKj57vgl2KdEI6aHaXE9cID6iudq54
o694gDZyz6NS90bBUExBjf/1qUBtwzHanU5wf8Rsf6U9eiP8RoErME17BtEiSItm
```

v

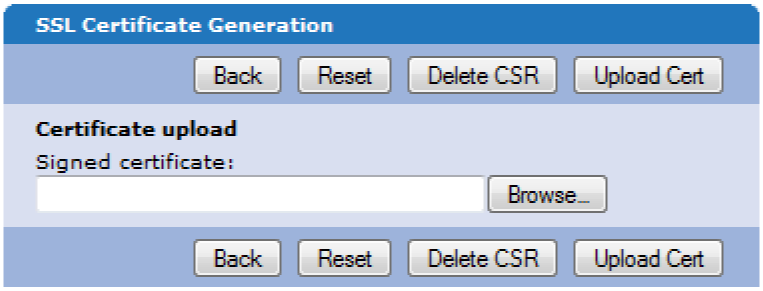
- Select apache mod ssl or apache as the server platform on your CA's enrollment form.
- Complete any remaining steps required by the CA.

4. Retrieve the certificate that the CA Produces

- The CA 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 format. 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 vWLAN Appliance

- Upon receipt of the certificate go back to the Provision>Logins>SSL Certificate>Current in the vWLAN Appliance.
- In the certificate upload box click browse, browse for the certificate file (.cer) then click upload cert.

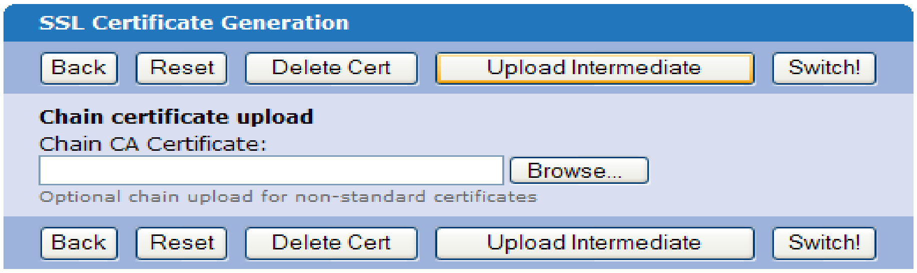


SSL Certificate Generation

Certificate upload

Signed certificate:

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



SSL Certificate Generation

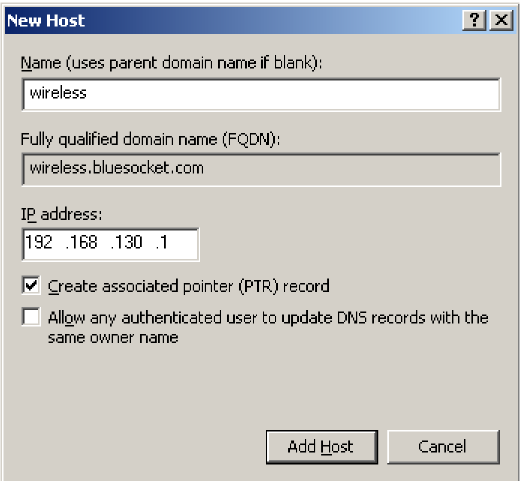
Chain certificate upload

Chain CA Certificate:

Optional chain upload for non-standard certificates

- If your CA requires more than one intermediate, you will need to obtain an intermediate certificate bundle for apache from the CA or create one with the contents of the two intermediate certificates and a text editor. Using a text editor such as Notepad, copy and paste in the contents of the primary intermediate certificate. Then copy and paste in the contents of the second intermediate certificate. In both cases you should include the BEGIN and END tags. Save the file as a .cer file, for example intermediatebundle.cer. After uploading your certificate, browse for the intermediate certificate bundle by clicking the browse button near the chain certificate upload field. Select the file and click upload intermediate.

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 network interface IP address of the vWLAN Appliance 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 2008 R2's DNS server.



New Host

Name (uses parent domain name if blank): wireless

Fully qualified domain name (FQDN): wireless.bluesocket.com

IP address: 192 .168 .130 .1

☑ Create associated pointer (PTR) record

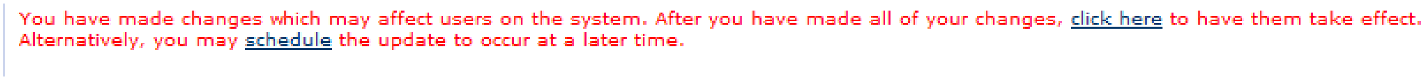
☐ Allow any authenticated user to update DNS records with the same owner name

- 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 network interface of the vWLAN Appliance.
    - Example: C:\>nslookup wireless.bluesocket.com (should return IP of vWLAN Appliance network interface)
    - Example: C:\>nslookup 192.168.130.1 (should return FQDN of vWLAN Appliance)

7. **Enable Redirect to hostname in the vWLAN Appliance**

    - Go to Platform>Admin>HTTP>Check the Redirect to hostname box>click save.
    - This will redirect users to the hostname rather than the network interface IP address. You must click to apply changes (restart web server) as indicated below for this to take effect as the vWLAN Appliance queries the PTR record during the web server restart process.

8. **Click to apply changes (restart web server).**



You have made changes which may affect users on the system. After you have made all of your changes, click here to have them take effect. Alternatively, you may schedule the update to occur at a later time.

- You will be prompted to "click here" for changes to take affect. Upon clicking, the vWLAN Appliances web server will restart. You will lose access to the vWLAN Appliances secure web based administrative console momentarily, clients will not be able to access the secure user login page momentarily, but clients who are already connected will not be disconnected. You can also go to Maintain>Restart>Advanced>Restart Web Server to restart the web server.
- The vWLAN Appliance queries the PTR during the web server restart and redirects users to what is received going forward.

High Availability

If you are running High Availability you must install an SSL certificate on each vWLAN Appliance. You can repeat the process above and generate a CSR on the secondary vWLAN Appliance using the unique FQDN of the secondary vWLAN Appliance, for example wireless2.bluesocket.com. This would require submitting two separate CSR's and purchasing two separate SSL certificates. *Alternatively you can purchase one wild card SSL certificate that can be installed on both vWLAN Appliances. If you are purchasing a wild card SSL certificate, when generating the CSR on the primary, in the FQDN field, enter an asterisk (*) instead of the hostname, for example *.bluesocket.com. You can then backup the private key on the primary vWLAN Appliance using the process outlined in step 2 above, and then restore it to the secondary vWLAN Appliance. To restore the private key to the secondary vWLAN Apppliance, go to Provision>Logins>SSL Certificate>Current>Key upload Private key, browse for and upload private key. You can then skip to step 5 above to complete the process of installing the wild card SSL certificate on the secondary vWLAN Appliance.

***If you are using Internal 802.1x Authentication** in addition to Web Based Authentication or will be in the future, it is NOT recommended to install a wild card certificate. Microsoft clients will not be able authenticate via Internal 802.1x if they are configured to validate the certificate. Not validating the certificate is a potential security risk.

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 vWLAN Appliance is in the list of trusted CAs that the client's browser supports.

Troubleshooting

I installed a cert provided by a trusted CA on the vWLAN Appliance but I am still receiving a certificate error:
I have verified the certificate is valid. I have verified that redirect to hostname is functioning and that the name in the url bar of the browser matches the common name of the certificate (FQDN). Why am I still receiving a certificate error from the browser indicating the certificate was not issued by a trusted certificate authority? Occasionally some browsers will give the error when others do not.

Examples of the browser error include:
IE: "The security certificate presented by this website was not issued by a trusted certificate authority".
Firefox: "The certificate is not trusted because the issuer certificate is unknown. (Error code: sec_error_unknown_issuer)".
Safari: "Authentication failed because the server certificate is not trusted."

You may not have installed a required chain/intermediate certificate. Check with your certificate authority if a chain/intermediate certificate is required. Go to logins>ssl certificate>current. Under chain certificate upload Chain CA Certificate: browse for and upload the chain/intermediate certificate obtained from the certificate authority.

Your CA might not provide support for the particular browser version you are using. Check with your CA to make sure they have support for the specific browser version you are using. Some CAs provide 99.9% + browser recognition while some other lower cost CA's provide 99% browser recognition and therefore might not have support for some browsers.

I have enabled redirect to hostname under admin>http of the vWLAN Appliance but clients are still being redirected to an ip address. I am receiving a certificate name mismatch error in the browser:

Examples of the browser error:
Internet Explorer: "The security certificate presented by this website was issued for a different website's address".
Firefox: "192.168.130.1 uses an invalid security certificate. The certificate is only valid for: vWLAN.bluesocket.com".
Safari: "This certificate is not valid (host name mismatch)"

Why is redirect to hostname not functioning and why am I receiving a certificate name mismatch error in the browser?

Redirect to hostname requires both an A record (forward) and PTR record (reverse) in your organizations DNS server for the vWLAN Appliances Fully Qualified Domain Name (FQDN) and the network interface IP address. The FQDN entered in your DNS server must match the common name (FQDN) you used when generating the CSR. Check to make sure you have BOTH these records in your organizations DNS server. If redirect to hostname is enabled and not functioning it is likely you are missing the PTR.

To test the PTR, perform an nslookup from the command prompt of a client for the network interface IP address. You should be returned the FQDN. Assuming the client is using the same DNS server configured on the network interface of the vWLAN Appliance. For example C:\>nslookup 192.168.130.1 assuming 192.168.130.1 is the network interface IP address. If not, add the PTR, test with nslookup to confirm, and then restart the web server (Maintain>Restart>Advanced>Restart Web Server). The vWLAN Appliance queries the PTR during the web server restart and redirects users to what is returned going forward. The name in the url bar of the browser must match the common name (FQDN) you used when generating the CSR or you will receive a certificate name mismatch error in the browser.

Check to make sure you only have one PTR record (reverse) in your organizations DNS server for the vWLAN Appliances network interface IP address. This entry should correspond to the Fully Qualified Domain Name (FQDN) of the vWLAN Appliance to match the CN of the certificate. For example when setting up AP discovery using DNS you might have added another corresponding PTR record however a PTR record is NOT required for AP discovery.