



## Installing and Renewing an SSL Certificate Provided by a Certificate Authority (CA) on the ADTRAN Bluesocket vWLAN

Date: 06/26/2014

Revision: 2.0

### Introduction

This document explains how to install and renew an SSL certificate provided by a Certificate Authority (CA) such as VeriSign on the vWLAN Appliance (Hardware) or vWLAN Virtual Appliance (VMware), hereinafter referred to as vWLAN, running software version 2.2.1 and later.

### 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.
- Platform administrative access to the vWLAN.

### Components Used

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

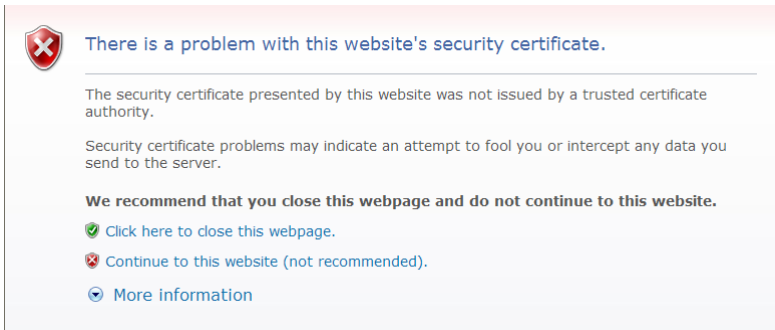
- All supported platforms running software version 2.2.1 and later.

### Background Information

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

- Clients connect to the secure user login page (Captive Portal) 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 9 (IE9).



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 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 that is already in the client's list of trusted root certificate authorities. This method does not require installing a certificate on each client.

## Installing an SSL Certificate

This document explains the second method of how to install an SSL certificate provided by a CA on the vWLAN. When shopping for an SSL certificate it is 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. After this document explains how to install an SSL certificate, it will then explain how to renew an SSL certificate seamlessly before it expires.

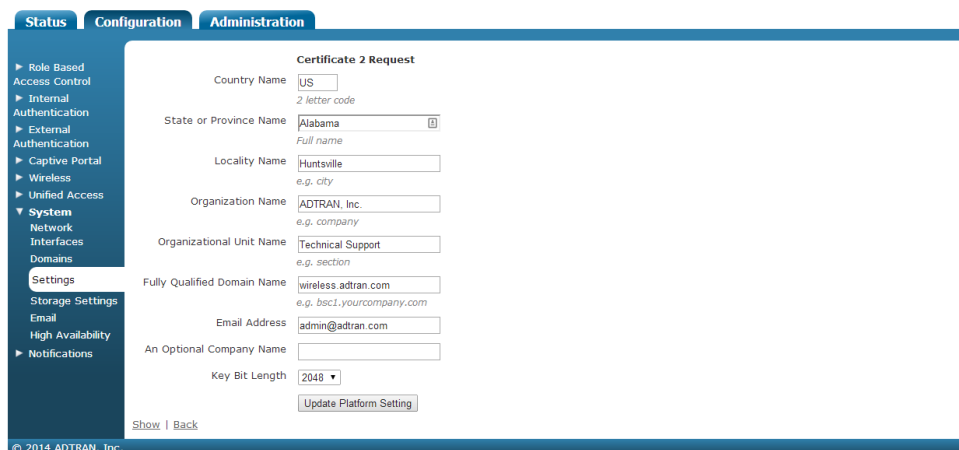
These are the steps to follow to install an SSL Certificate:

1. **Generate a CSR**
2. **Submit the CSR to the CA**
3. **Backup your private key**
4. **Retrieve the certificate that the CA Produces**
5. **Upload the certificate to the vWLAN**
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**
8. **Run Platform Tasks to apply changes**
9. **Allow HTTP outgoing to the OCSP and CRL URLs associated with the certificate in the un-registered role**

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

Go to Configuration>System>Settings>Platform and click the link to edit Certificate Signature Request (CSR). Click show to display the Certificate Request Form. Fill out the form.

- **Country Name:** Use the two-letter code without punctuation for country, for example: US or CA.
- **State or Province Name:** Spell out the state completely; do not abbreviate the state or province name, for example: Alabama
- **Locality Name:** The Locality field is the city or town name, for example: Huntsville
- **Organization Name:** 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: ADTRAN, Inc.
- **Organizational Unit Name:** 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. For example Technical Support Engineering
- **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 is wireless (Configuration>System>Network Interfaces>click the link to edit Public>Hostname), and your domain name is adtran.com, you should enter wireless.adtran.com. Alternatively if you are purchasing a wild card certificate to install on multiple vWLAN, enter an asterisk (\*) instead of the hostname. For example \*.adtran.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@adtran.com](mailto:admin@adtran.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.

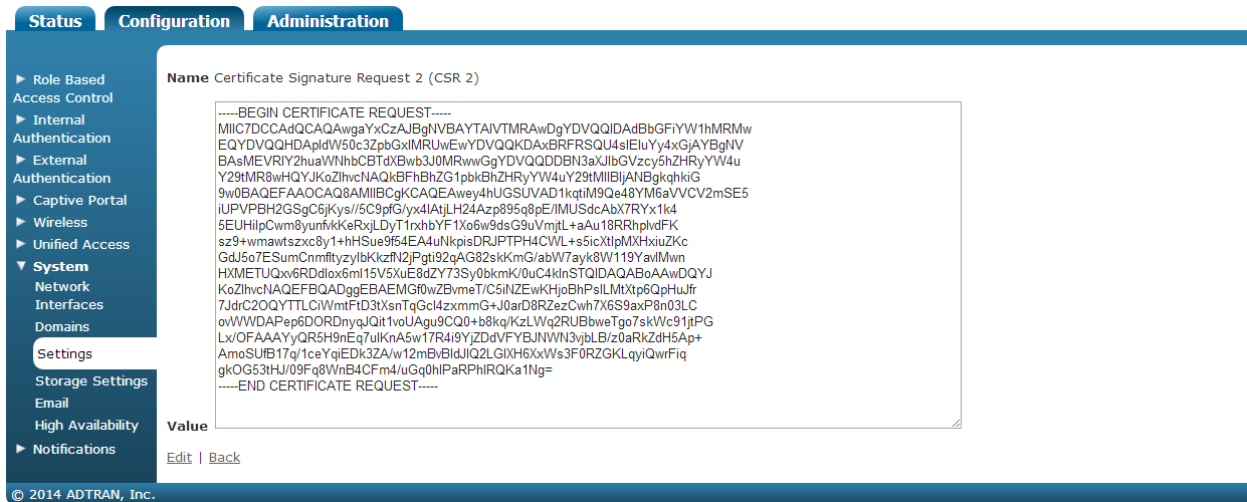


The screenshot shows the ADTRAN web interface with the 'Administration' tab selected. The left sidebar contains a navigation menu with 'System' expanded to 'Settings'. The main content area displays the 'Certificate 2 Request' form with the following fields:

- Country Name:  (2 letter code)
- State or Province Name:  (Full name)
- Locality Name:  (e.g. city)
- Organization Name:  (e.g. company)
- Organizational Unit Name:  (e.g. section)
- Fully Qualified Domain Name:  (e.g. bsc1.yourcompany.com)
- Email Address:
- An Optional Company Name:
- Key Bit Length:  (dropdown menu)

At the bottom of the form is an 'Update Platform Setting' button. The footer of the page reads '© 2014 ADTRAN, Inc.' and 'Show | Back'.

Click Update Platform Setting. A public/private key pair has now been created. The public key, in the form of a Certificate Signing Request (CSR) will be displayed. This will be used for certificate enrollment. The private key is stored locally on the vWLAN under Configuration>System>Settings>Platform> Certificate Private Key.

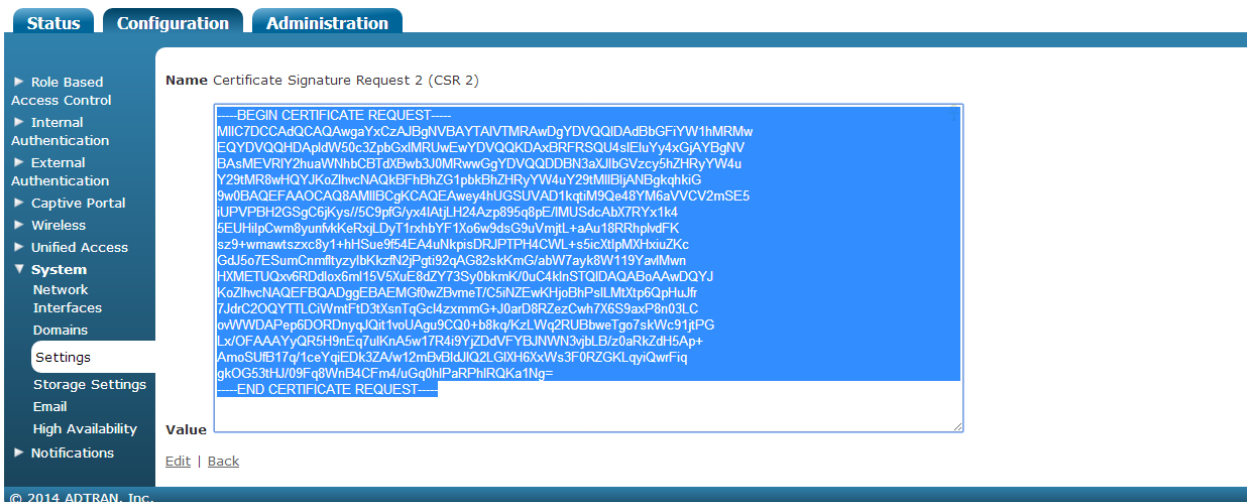


The screenshot shows the ADTRAN configuration interface with the 'System' tab selected. Under 'System', 'Settings' is chosen. The 'Certificate Signature Request 2 (CSR 2)' configuration is displayed. The 'Value' field contains the following CSR text:

```
-----BEGIN CERTIFICATE REQUEST-----
MIC7DCCAdQCAQAwgaxCzAIBgNVBAYTAiVMTMRwDgYDVQQIDAdBbGFYVW1hMRMw
EQYDVQQHDAdW50c3ZpbGxIMRUwEwYDVQQKDAxBRFRSQU4sEiUyY4xGAYBgNV
BAsMEVRlY2huaWNhbcBTdXBw3J0MRwwGgYDVQQDBN3aXJlbGVzcy5hZHRyYW4u
Y29tMR8wHQYJKoZIhvcNAQkBFhBhZG1pbkZhZHRyYW4uY29tMlIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBBgKCAQEAWey4hUGSUVAD1kqIM9Qe48YM6aVVCV2mSE5
iUPVPB2GSgC6jKys//5C9pG/yx4IAJLH24Azp895q8pE/IMUSdcAbX7RYx1k4
5EUHilpCwm8yunkKkeRqjLDyT1rxhbYF1Xo6w9dsG9uVmjL+aAu18RRhplvFK
sz9+wmawtszxc8y1+hHSue9f54EA4uNkpsDRJPTPH4CWL+s5icXtlpMXHxiuZKc
GdJ5o7ESumCnmfityzYlbKzfn2Jpgt92qAG82skKmG/abW7ayk8W119YavIMwn
HXMETUQxv6RDdlox6ml15V5XuE8dZY73Sy0bkmK/0uC4klnSTQIDAQABoAAwDQYJ
KoZIhvcNAQEFBQADggEBAEMGf0wZBvmeT/C5iNZEwKHjdBhPslMxTp6QpHuJfr
7JdrC2OQYTLTLCiWmtFtD3XsnTqGc4zxmG+J0arD8RZezCwh7X6S9axP8n03LC
ovWWDAPep6DORDnyqQit1voUAg9CQ0+b8kq/KzLWq2RUBbweTgo7skWc91jPG
Lx/OFAAAyYQR5H9nEq7ulKnA5w17R49yJZDdVfYBJNWN3jblB/z0aRkZdH5Ap+
AmoSUIB17q/1ceYqiEDk3ZA/w12mBvBlDjIQ2LGIxH6xW53F0RZGKlqyQwrFq
gkOG53tHJ/09Fq8WnB4CFm4/uGq0hPaRPhRQKa1Ng=
-----END CERTIFICATE REQUEST-----
```

## 2. 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. Select Apache+mod\_ssl/OpenSSL or Apache as the server platform on your CA's enrollment form. Complete any remaining steps required by the CA.



This screenshot is identical to the one above, but the CSR text in the 'Value' field is highlighted in blue, indicating it has been selected for copying.

### 3. Backup your private key

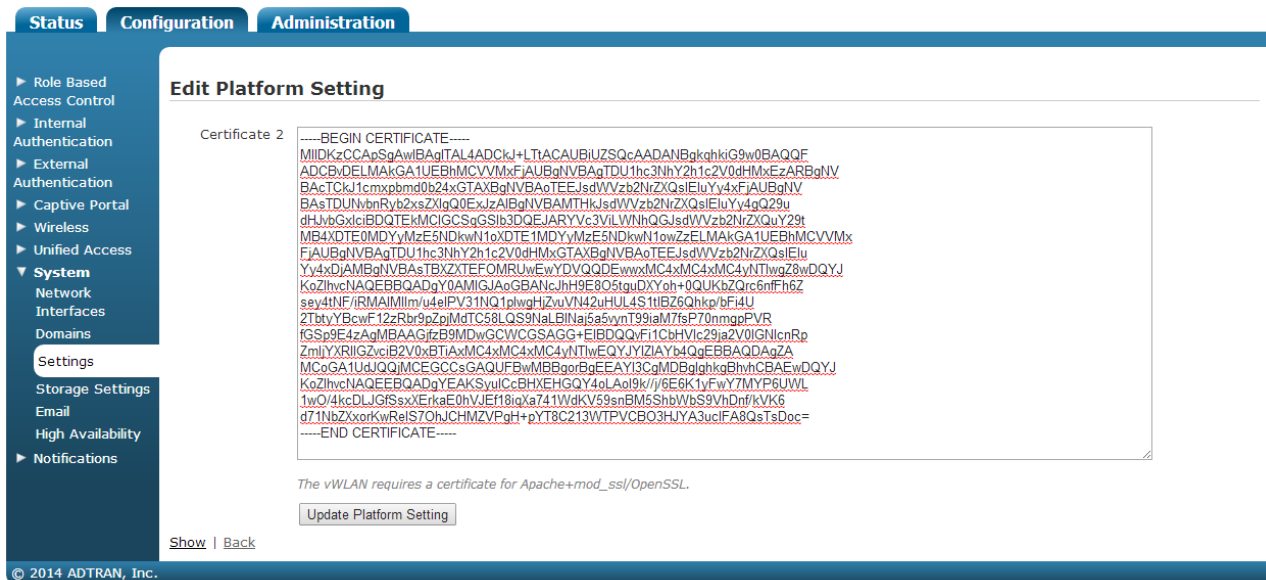
If the private key is lost or corrupted for any reason, the certificate will no longer work. For that reason, it is good practice to download the private key to a safe and secure place. Go to Configuration>System>Settings>Platform and click the link to edit Certificate Private Key. Copy and paste the text of the private key into a text editor such as Notepad and save with a .key extension. For example privatekey.key.

### 4. Retrieve the certificate that the CA Produces

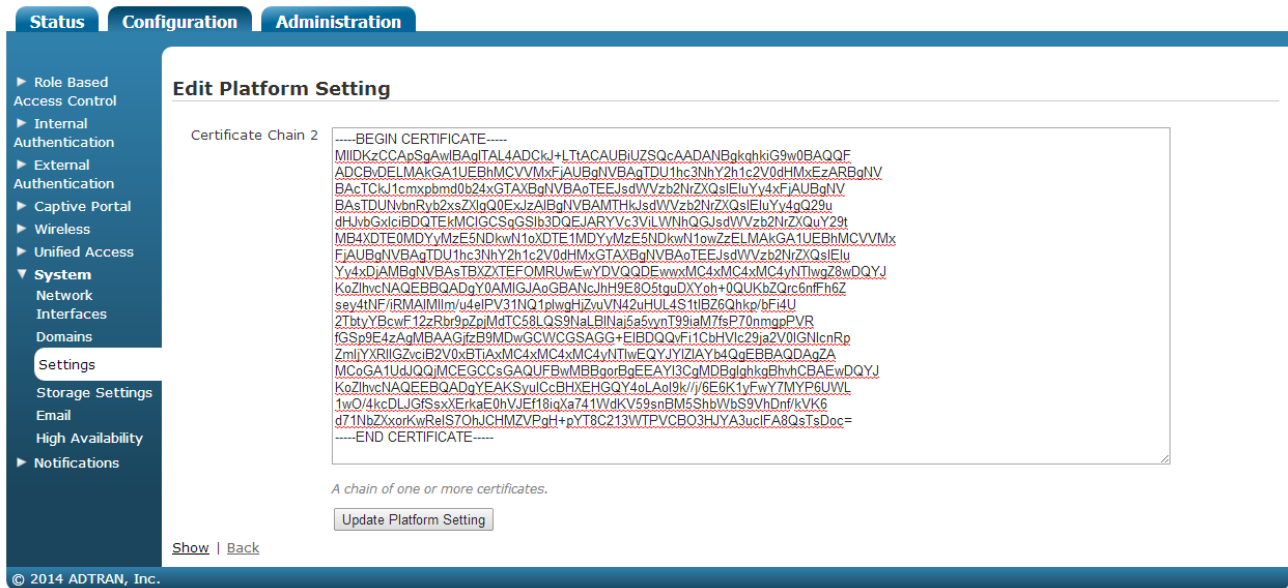
The CA will send you the certificate or instructions on how to obtain the certificate when authentication and processing is complete. Some certificate authorities may send the certificate in text format. Others may send a certificate file with an extension such as .cer, .crt, or .pem.

### 5. Upload the certificate to the vWLAN

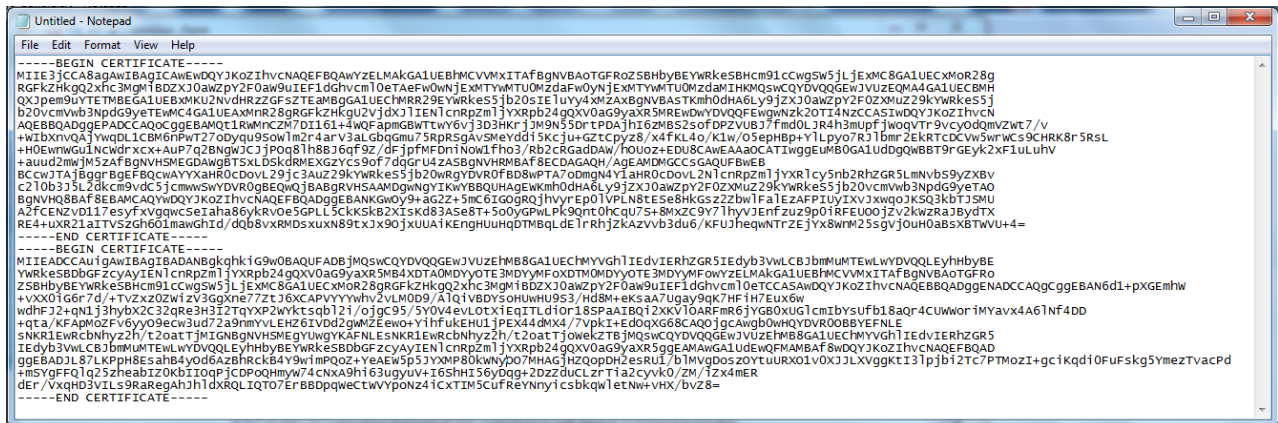
Upon receipt of the certificate go to Configuration>System>Settings>Platform>click the link to edit Certificate File. Copy and paste the text of the certificate into the Certificate File box. If you received a certificate file with an extension such as .cer, .crt, or .pem, you can open the file with a text editor such as Notepad. After copying and pasting the text of the certificate, click Update Platform Setting.



If you also have an optional intermediate certificate go to Configuration>System>Settings>Platform>click the link to edit Certificate Chain. Copy and paste the text of the intermediate certificate into the Certificate Chain box. Again if you received an intermediate certificate file with an extension such as .cer, .crt, or .pem, you can open the file with a text editor such as Notepad. After copying and pasting the text of the intermediate certificate, click Update Platform Setting.

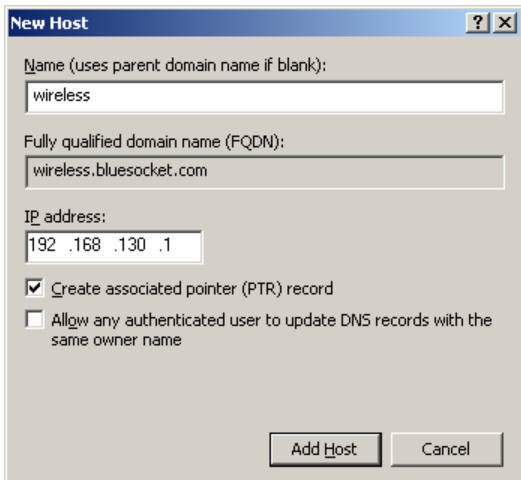


If your CA requires more than one intermediate certificate, you will need to obtain an intermediate certificate bundle for Apache from the CA or create one with the contents of the multiple intermediate certificates and a text editor. Using a text editor such as Notepad, copy and paste the contents of the primary intermediate certificate. Then copy and paste the contents of the secondary intermediate certificate and so on. In both cases you should include the BEGIN and END tags. Now paste into the Certificate Chain box as outlined above. Below is an example of two intermediate certificates “chained up” in Notepad.



## 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 IP address of the public network interface of the vWLAN 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.

A screenshot of the "New Host" dialog box in Windows DNS Manager. The dialog has a title bar with a question mark and a close button. It contains three text input fields: "Name (uses parent domain name if blank):" with "wireless" entered, "Fully qualified domain name (FQDN):" with "wireless.bluesocket.com" entered, and "IP address:" with "192 .168 .130 .1" entered. Below the fields are two checkboxes: "Create associated pointer (PTR) record" which is checked, and "Allow any authenticated user to update DNS records with the same owner name" which is unchecked. At the bottom are "Add Host" and "Cancel" buttons.

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 public network interface of the vWLAN.

Example:

```
C:\>nslookup wireless.bluesocket.com (should return IP of public network interface of vWLAN)
```

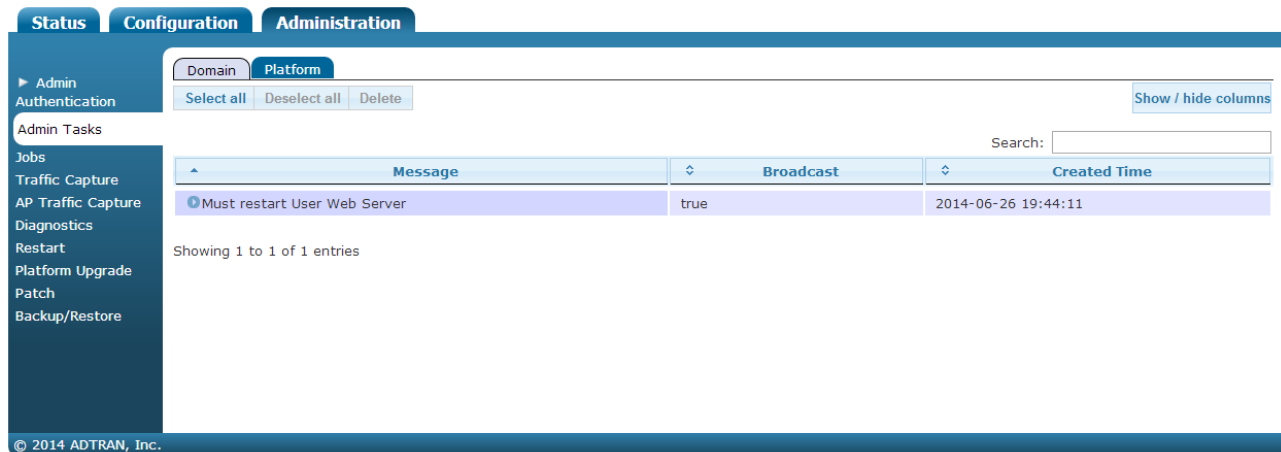
```
C:\>nslookup 192.168.130.1 (should return FQDN of vWLAN)
```

## 7. Enable Redirect to hostname in the vWLAN

Go to Configuration>System>Settings>Platform. Scroll down the list and click to edit "Redirect to hostname." Select "Enabled" in the drop-down menu and click Update Platform Setting to save. This will redirect users to the hostname rather than the public network interface IP address. You must Run Platform Tasks to apply changes (Restart admin and user web servers) as indicated below for this to take effect as the vWLAN queries the PTR record during the web server restart process.

## 8. Run Platform Tasks to apply changes.

Click Platform Tasks in the top menu. This will bring you to Administration>Admin Tasks>Platform where you will see a pending task to restart the user web server. Click the play button next to Must restart User Web server to restart the user web server. Clients will not be able to access the secure user login page (Captive Portal) momentarily but clients who are already connected will not be disconnected. Alternatively you can go to Administration>restart and restart the web server from there.



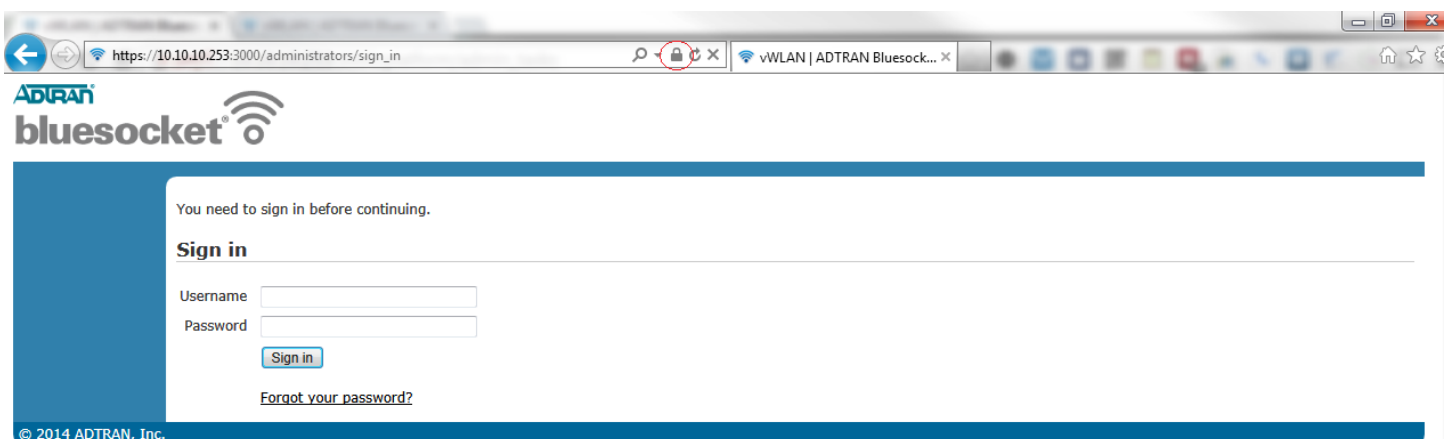
The screenshot shows the Administration interface with the following elements:

- Navigation tabs: Status, Configuration, Administration.
- Sub-navigation: Admin, Authentication, Admin Tasks, Jobs, Traffic Capture, AP Traffic Capture, Diagnostics, Restart, Platform Upgrade, Patch, Backup/Restore.
- Current view: Platform (under Admin Tasks).
- Buttons: Select all, Deselect all, Delete, Show / hide columns.
- Search: Search: [input field]
- Table columns: Message, Broadcast, Created Time.
- Table content:
 

Message	Broadcast	Created Time
Must restart User Web Server	true	2014-06-26 19:44:11
- Footer: © 2014 ADTRAN, Inc.

## 9. Allow HTTP outgoing to the OCSP and CRL URLs associated with the certificate in the un-registered role.

These URLs are used to check the validity of the certificate. Some browsers will not redirect to the login page if they cannot validate the certificate. To find the URLs associated with your certificate, in IE9 for example, click the lock to the right of the address bar and select View Certificates while on the sign in page of the vWLAN secure web based administrative console.

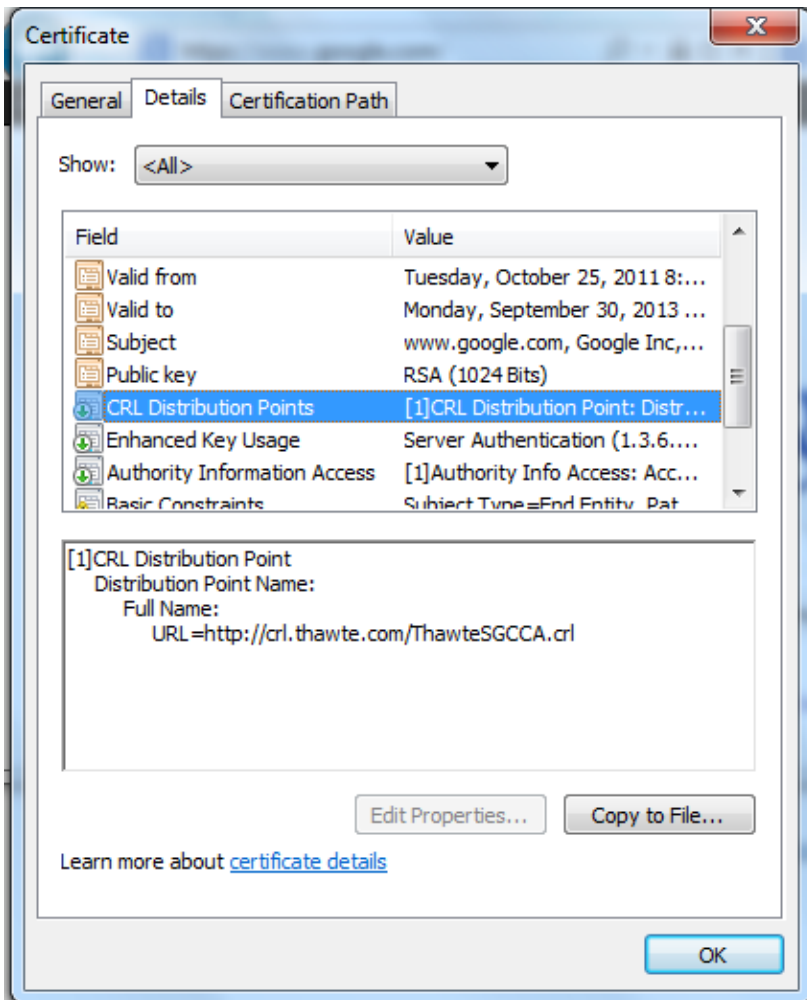


The screenshot shows the sign-in page with the following elements:

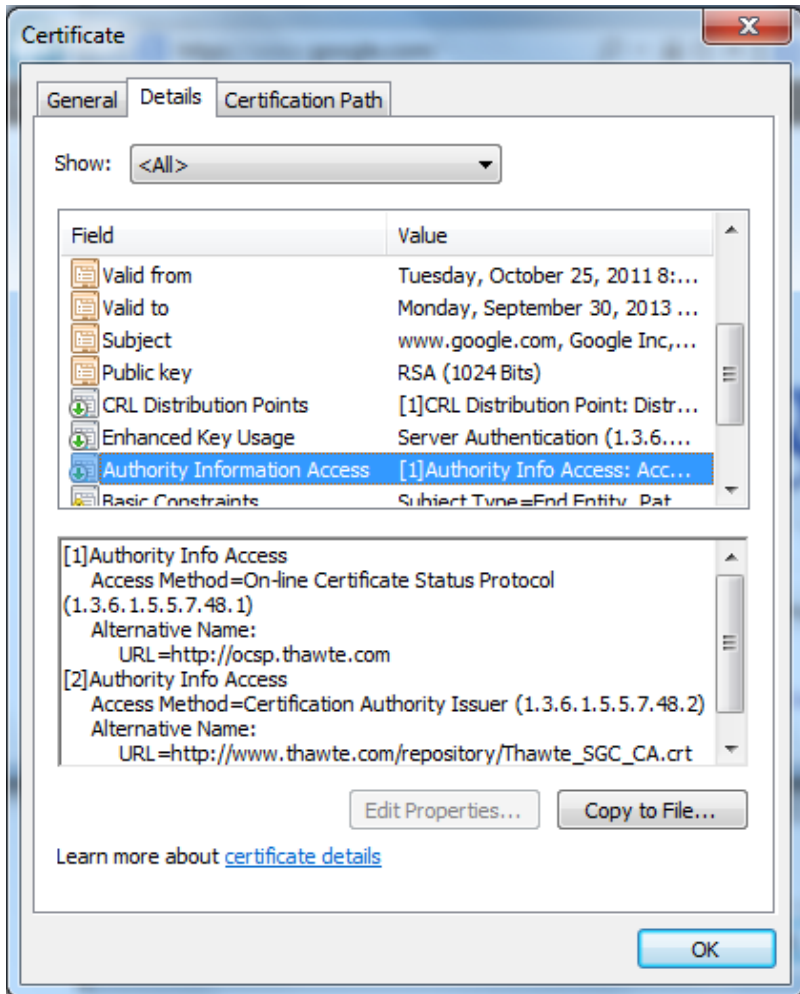
- Browser address bar: https://10.10.10.253:3000/administrators/sign\_in
- ADTRAN bluesocket logo
- Message: You need to sign in before continuing.
- Section: Sign in
- Form fields: Username [input], Password [input]
- Buttons: Sign in
- Link: [Forgot your password?](#)
- Footer: © 2014 ADTRAN, Inc.



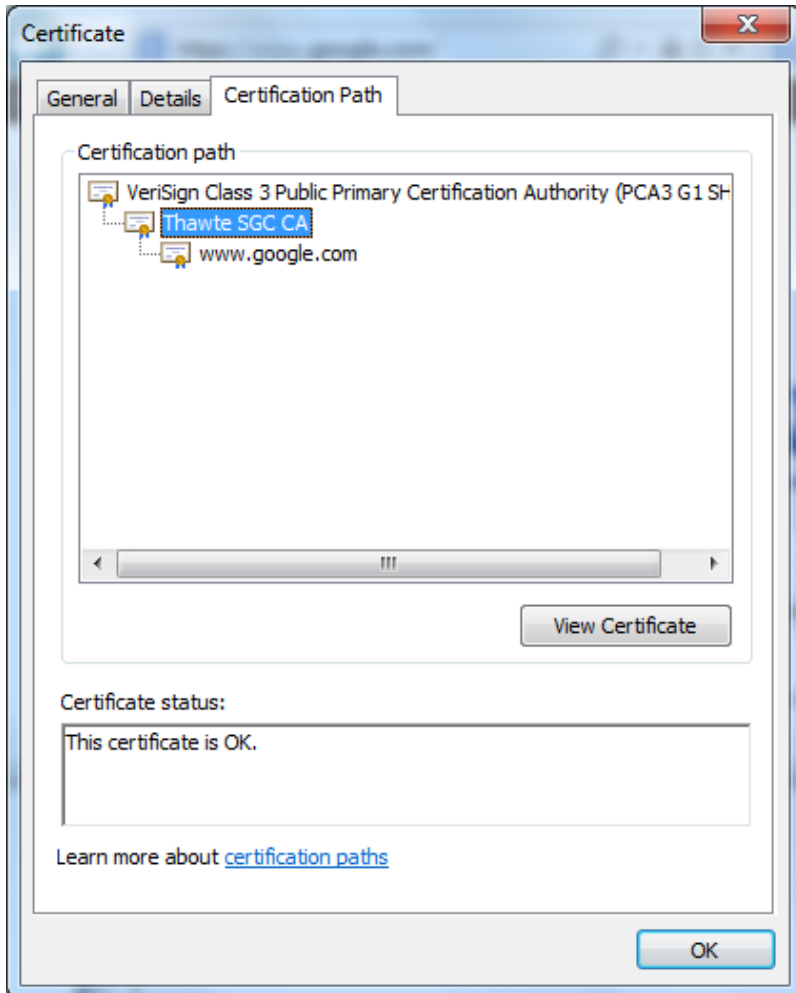
Now click the Details tab. Scroll down to the CRL Distribution Points field. There you will find the CRL URLs. For example [crl.thawte.com](http://crl.thawte.com).



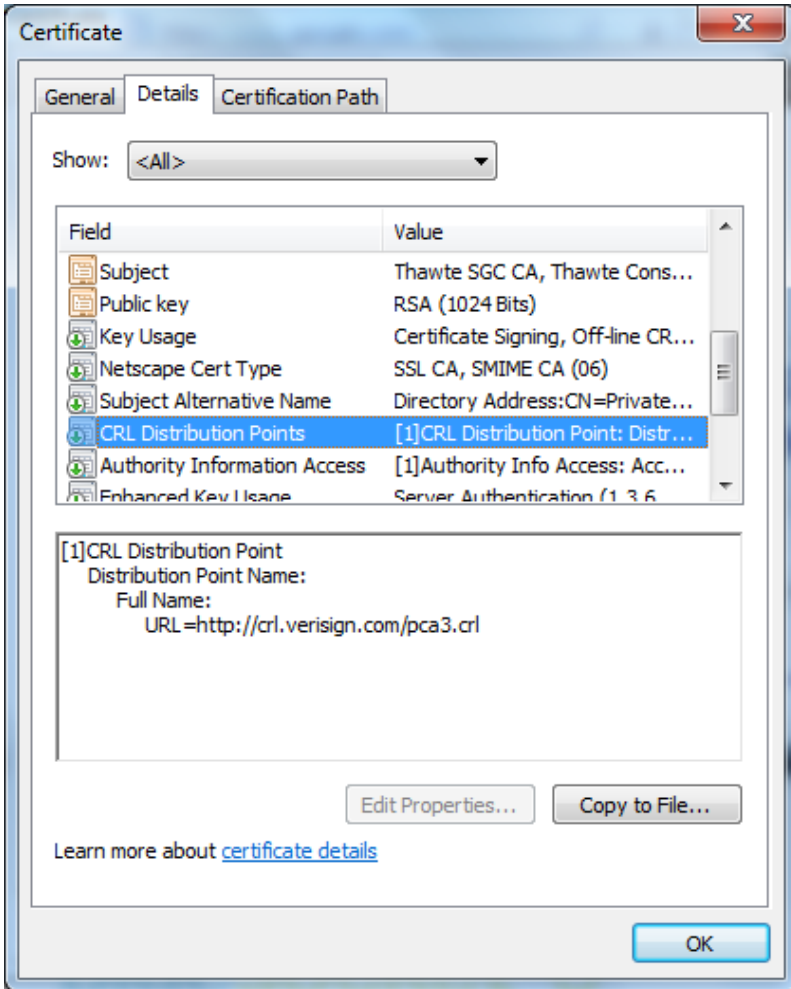
Now scroll down to the Authority Information Access field. There you will find the OCSP URL. For example ocsf.thawte.com. Depending on the certificate you may have one, both, or neither of these fields, but if you do have them, you should allow http outgoing to them in the un-registered role.



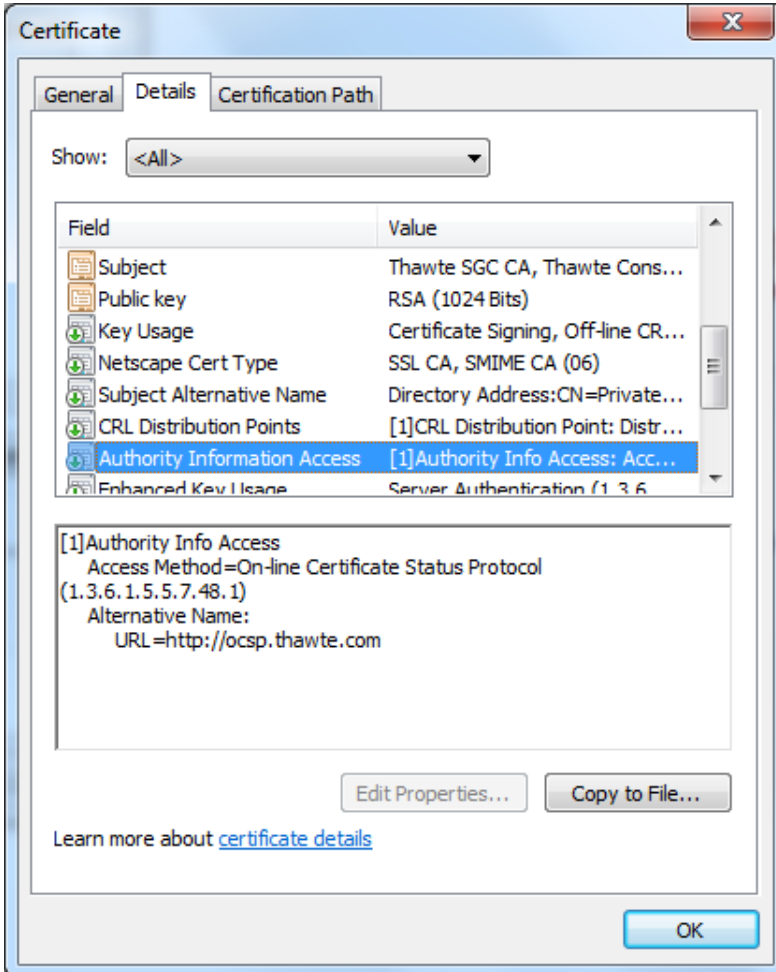
Make sure you repeat this process for all the certificates in the chain. Click the Certification Path tab and click the next certificate up in the chain. For example Thawte SGC CA. Now click view certificates.



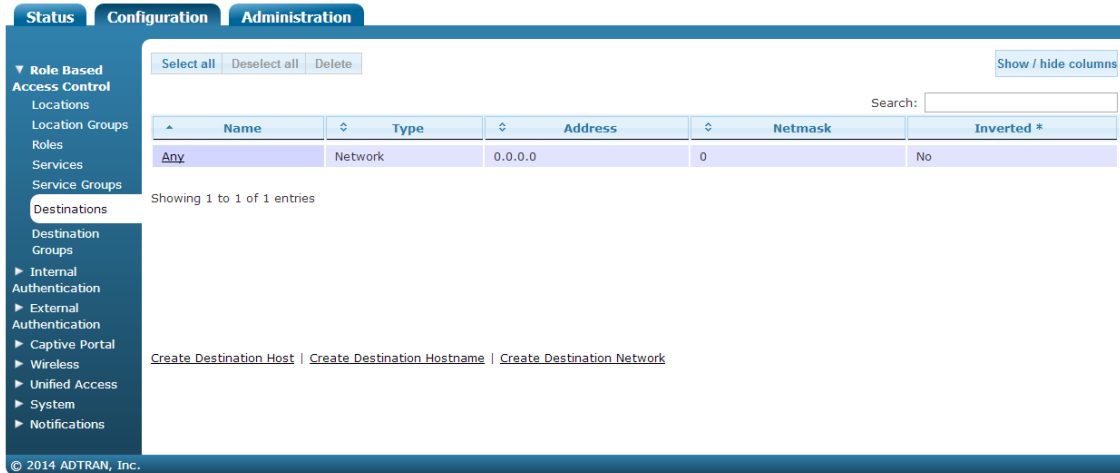
Now click the Details tab. Scroll down to the CRL Distribution Points field. There you will find the CRL URLs. For example `crl.verisign.com`.



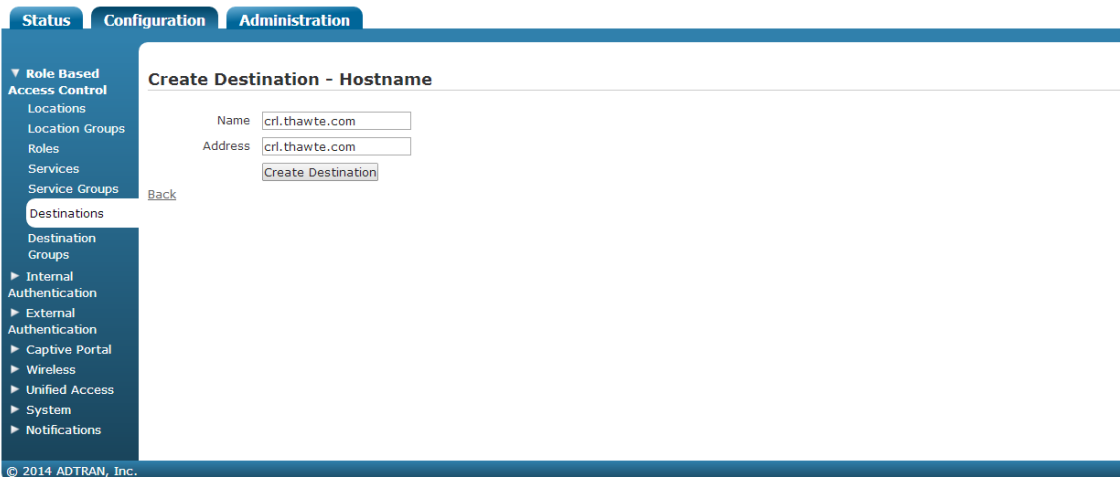
Now scroll down to the Authority Information Access field. There you will find the OCSP URL. For example ocsf.thawte.com. Again depending on the certificate you may have one, both, or neither of these fields. Continue gathering the URLs for all the certificates in the chain.



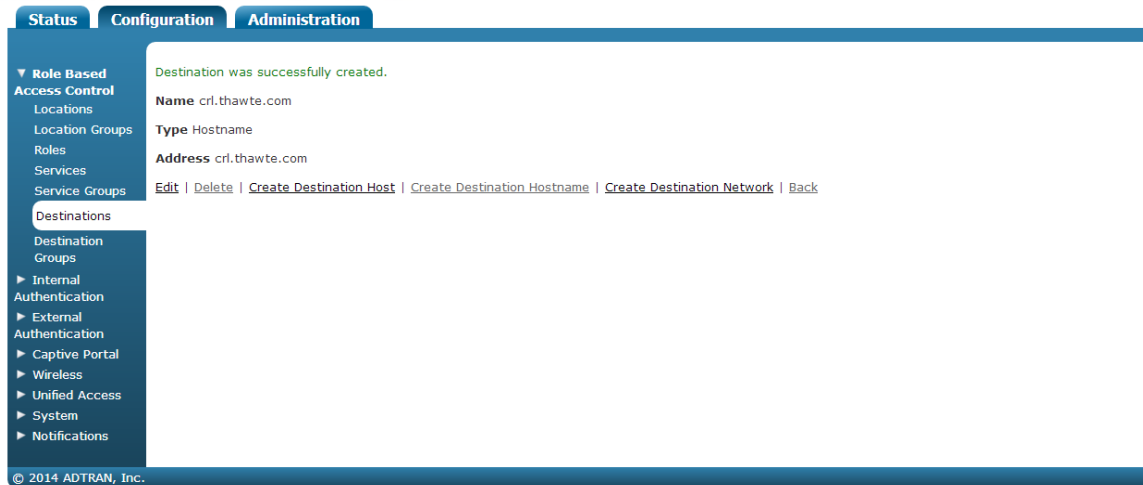
Once you have gathered the URLs for all of the certificates in the chain, go to Configuration>Role Based Access Control>Destinations and click Create Destination Hostname.



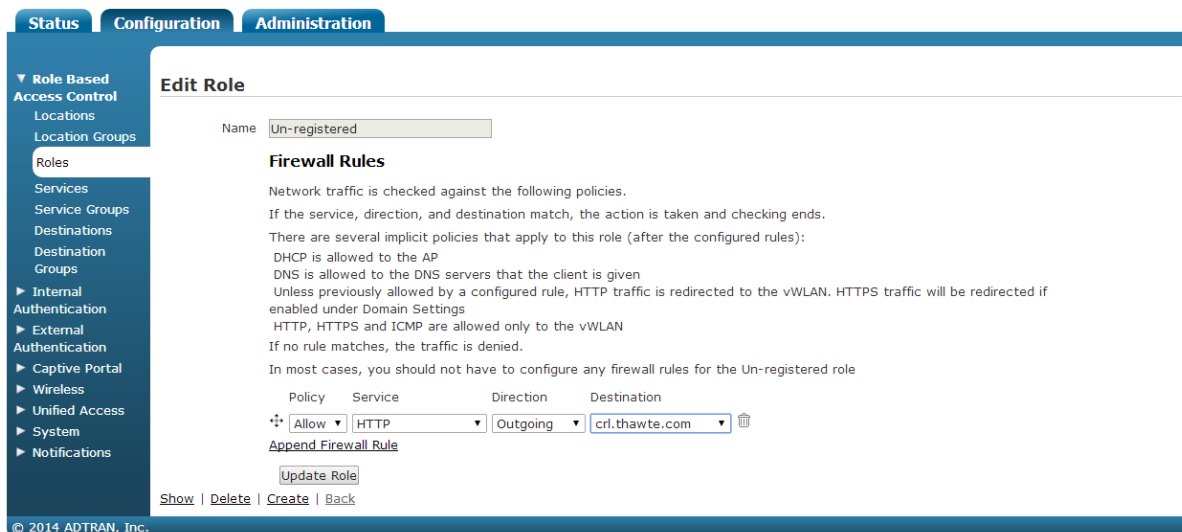
In the Name field, enter a friendly name for the destination hostname. In the Address field, enter the hostname in the URL. For example we entered `crl.thawte.com` in both fields here.



Repeat until all hostnames are added.



Now go to Configuration>Role Based Access Control>Roles>and click the link to edit the Un-registered role. Click append firewall rules and select Allow, HTTP, Outgoing, and select one of the destination hostnames added in the previous step. Repeat until there is a firewall rule allowing HTTP, Outgoing for all of the destination hostnames.



After updating the Un-registered role, click Domain Tasks in the top menu. This will bring you to Administration>Admin Tasks>Domain where you will see a pending task to apply the configuration to the APs. Click the play button next to Must apply configuration to APs. The APs will update the new firewall rules for Un-registered clients. All clients on modified APs will briefly lose connectivity while the change is applied and APs are in the “Updating” status. Therefore, you may wish to run this task during a maintenance window.

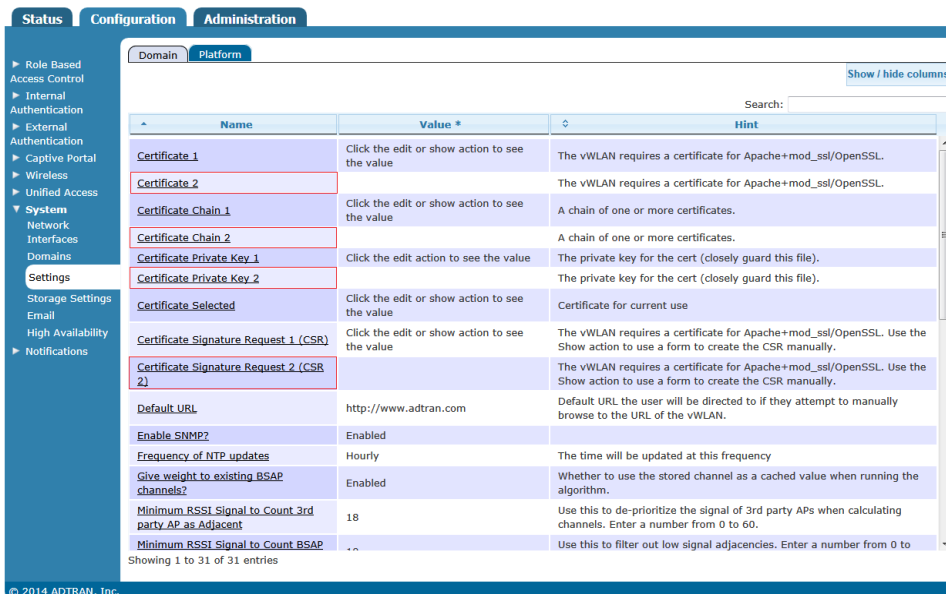
## High Availability

If you are running High Availability you must install an SSL certificate on each vWLAN. You can repeat the process above and generate a CSR on the secondary vWLAN using the unique FQDN of the secondary vWLAN, for example wireless2.adtran.com. This would require submitting two separate CSRs and purchasing two separate SSL certificates. Alternatively you can purchase one wild card SSL certificate that can be installed on both vWLANs. 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 \*.adtran.com. You can then copy the private key from the primary vWLAN using the process outlined in step 3 above, then paste it into the secondary vWLAN under Configuration>System>Settings>Platform>click the link to edit Certificate 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.

## Renewing an SSL Certificate

An SSL Certificate provided by a CA is only valid for a finite period of time. The vWLAN allows you to maintain 2 SSL certificates and select one for use. By having the ability to switch between certificates it is easy to renew an expiring certificate without impacting the production network.

To renew an SSL certificate, simply follow steps 1-5 of “Installing an SSL Certificate” above. The difference is that you will perform the steps entering values in the alternate certificate. For example, if you used Certificate Signature Request 1 (CSR), Certificate Private Key 1, Certificate 1, to enter the values for the current certificate, you would use Certificate Signature Request 2 (CSR), Certificate Private Key 2, Certificate 2, for your renewal.



Name	Value *	Hint
Certificate 1	Click the edit or show action to see the value	The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL.
Certificate 2		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL.
Certificate Chain 1	Click the edit or show action to see the value	A chain of one or more certificates.
Certificate Chain 2		A chain of one or more certificates.
Certificate Private Key 1	Click the edit action to see the value	The private key for the cert (closely guard this file).
Certificate Private Key 2		The private key for the cert (closely guard this file).
Certificate Selected	Click the edit or show action to see the value	Certificate for current use
Certificate Signature Request 1 (CSR)	Click the edit or show action to see the value	The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL. Use the Show action to use a form to create the CSR manually.
Certificate Signature Request 2 (CSR 2)		The vWLAN requires a certificate for Apache+mod_ssl/OpenSSL. Use the Show action to use a form to create the CSR manually.
Default URL	http://www.adtran.com	Default URL the user will be directed to if they attempt to manually browse to the URL of the vWLAN.
Enable SNMP?	Enabled	
Frequency of NTP updates	Hourly	The time will be updated at this frequency
Give weight to existing BSAP channels?	Enabled	Whether to use the stored channel as a cached value when running the algorithm.
Minimum RSSI Signal to Count 3rd party AP as Adjacent	18	Use this to de-prioritize the signal of 3rd party APs when calculating channels. Enter a number from 0 to 60.
Minimum RSSI Signal to Count BSAP	..	Use this to filter out low signal adjacencies. Enter a number from 0 to ..

Showing 1 to 31 of 31 entries



When you are ready to activate the new certificate, go to Configuration>System>Settings>Platform>click the link to edit Certificate Selected and choose the certificate you added.



You can skip step 6 (DNS Entries) if the hostname on the certificate has not changed. You can also skip step 7 as redirect to hostname should be already enabled. Further, you may skip step 9 if the CRL distribution points have not changed.

To implement the change to the new certificate, go to Platform Tasks in the top menu. This will bring you to Administration>Admin Tasks>Platform where you will see a pending task to restart the user web server. Click the play button next to Must restart User Web server to restart the user web server. Clients will not be able to access the secure user login page (Captive Portal) momentarily but clients who are already connected will not be disconnected. Alternatively you can go to Administration>restart and restart the web server from there.

If you have already renewed a certificate once, and both Certificate 1 and Certificate 2 values are populated, edit and delete the Certificate Signature Request (CSR), Certificate Private Key, Certificate, and Certificate Chain that are presently unused to make space for the next renewal.

## Verify

The next time that a client connects to the secure user login page (Captive Portal) 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 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 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 Configuration>System>Settings>Platform>click the link to edit Certificate Chain and copy and paste the intermediate certificate chain text 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 Configuration>System>Settings>Platform of the vWLAN 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 vWLANs Fully Qualified Domain Name (FQDN) and the IP address of the public network interface. 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 public network interface IP address. You should be returned the FQDN. Assuming the client is using the same DNS server configured on the public network interface of the vWLAN. For example C:\>nslookup 192.168.130.1 assuming 192.168.130.1 is the public network interface IP address. If not, add the PTR, test with nslookup to confirm, and then restart the web servers (Administration>Restart>restart admin and user web servers). The vWLAN 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 public network interface IP address. This entry should correspond to the Fully Qualified Domain Name (FQDN) of the vWLAN 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.

**I have an existing wild card SSL certificate for the Microsoft IIS server platform that I would like to use on the vWLAN. Can this be done?**

Yes, you must first export your IIS certificate into a PFX file. Use an application such as openssl to extract the private key and certificate. Next, go to Configuration>System>Settings>Platform>Certificate Private Key and paste the text of the private key. After you have pasted the text of the private key, go to Configuration>System>Settings>Platform>Certificate File and paste in the text of the certificate. This requires platform administrative access.