[redacted]

Installation of certificate on controller for WebUI, Captive Portal and 802.1X authentication

Contents

Introduction

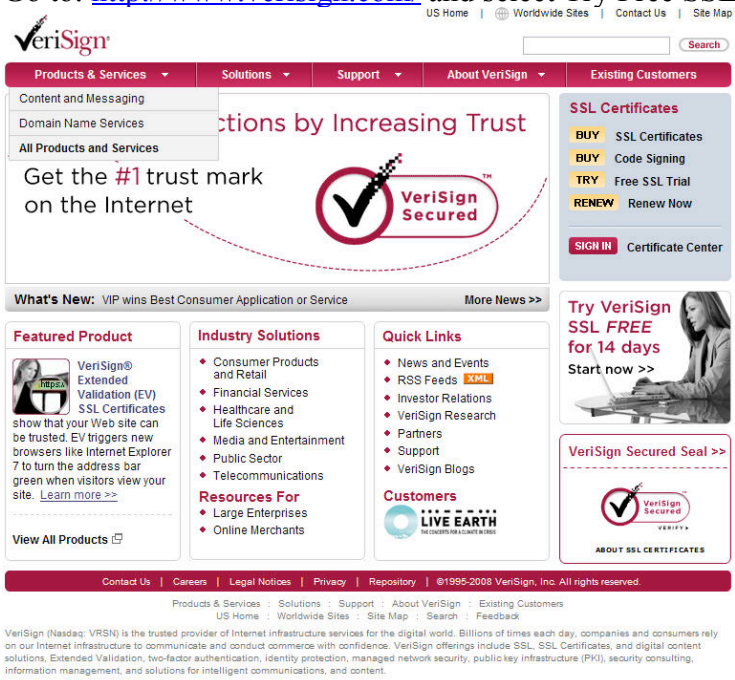
All Aruba controllers are shipped with a default certificate which is used by WebUI, captive portal as well as dot1x termination.
The Common Name (CN) of this cert is securelogin.arubanetworks.com.
Aruba Networks includes the cert in ArubaOS to allow customers to be up and running quickly. Using a default cert is not safe from a security point of view and is not recommended for long-term production. Customers are advised to purchase their permanent certs from a well known CA such as VeriSign, GeoTrust, etc.

This document explains how to install a trial certificate from VeriSign on an Aruba controller.

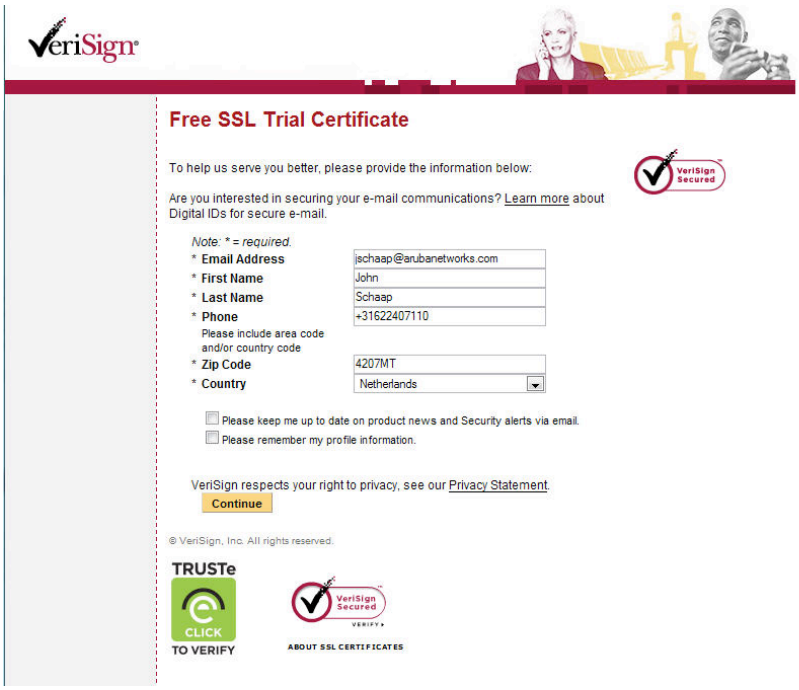
You do not need to go through the procedure of adding the Test Root CA when you purchase a certificate at VeriSign. These certificates are already trusted by your PC.

Get the trial certificate from Verisign

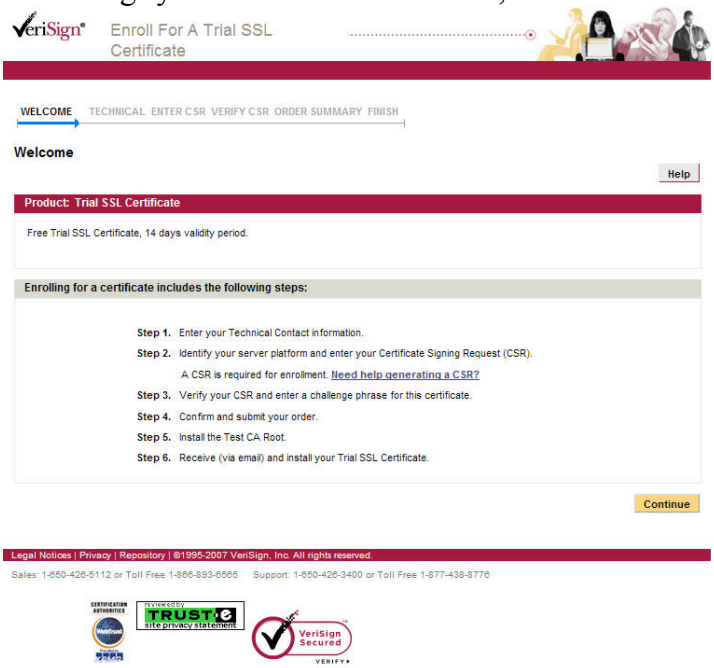
Go to: http://www.verisign.com/ and select Try Free SSL Trial



Complete the following form



This brings you to the welcome screen, click continue



Complete the following form and click continue

VeriSign® Enroll For A Trial SSL Certificate

WELCOME TECHNICAL ENTER CSR VERIFY CSR ORDER SUMMARY FINISH

Enter Technical Contact information for this certificate

The Technical Contact receives and manages the certificate and is notified for renewal.

Help

*Required field

Product: Trial SSL Certificate

Free Trial SSL Certificate, 14 days validity period.

Technical Contact

* First Name:	John
* Last Name:	Schaap
* Title:	Systems Engineer
* Company:	Aruba Networks
* Address1:	Algolweg 11A
Address2:	
* City:	Amersfoort
* State/Province:	ZH
* ZIP/Postal Code:	3821BG
* Country:	Netherlands
* Telephone:	+31622407110
Fax:	
* Email:	jschaap@arubanetworks.com

☐ Save my contact information for future certificate enrollments.

☐ Please keep me up to date on product news and security-related information.

Continue

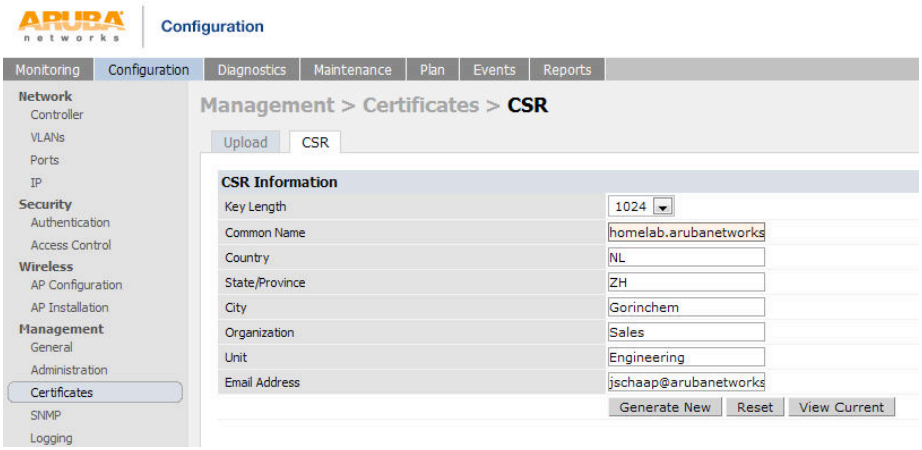
Sales: 1-650-426-5112 or Toll Free 1-866-893-6565 Support: 1-650-426-3400 or Toll Free 1-877-438-8776

CERTIFICATION AUTHORITIES WebTrust AICPA

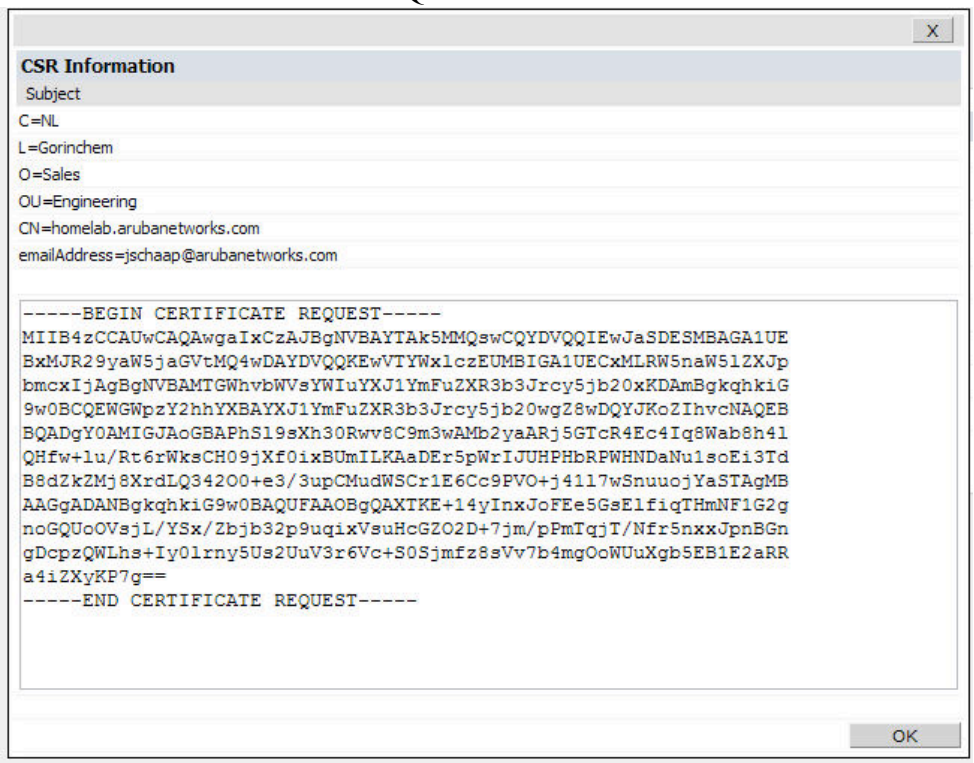
reviewed by TRUSTe site privacy statement

VeriSign Secured VERIFY

Go to the controller and configure it to generate a new CSR. The CN (Common Name) should be the same as the name of the controller. Click “Generate New” after entering all the details

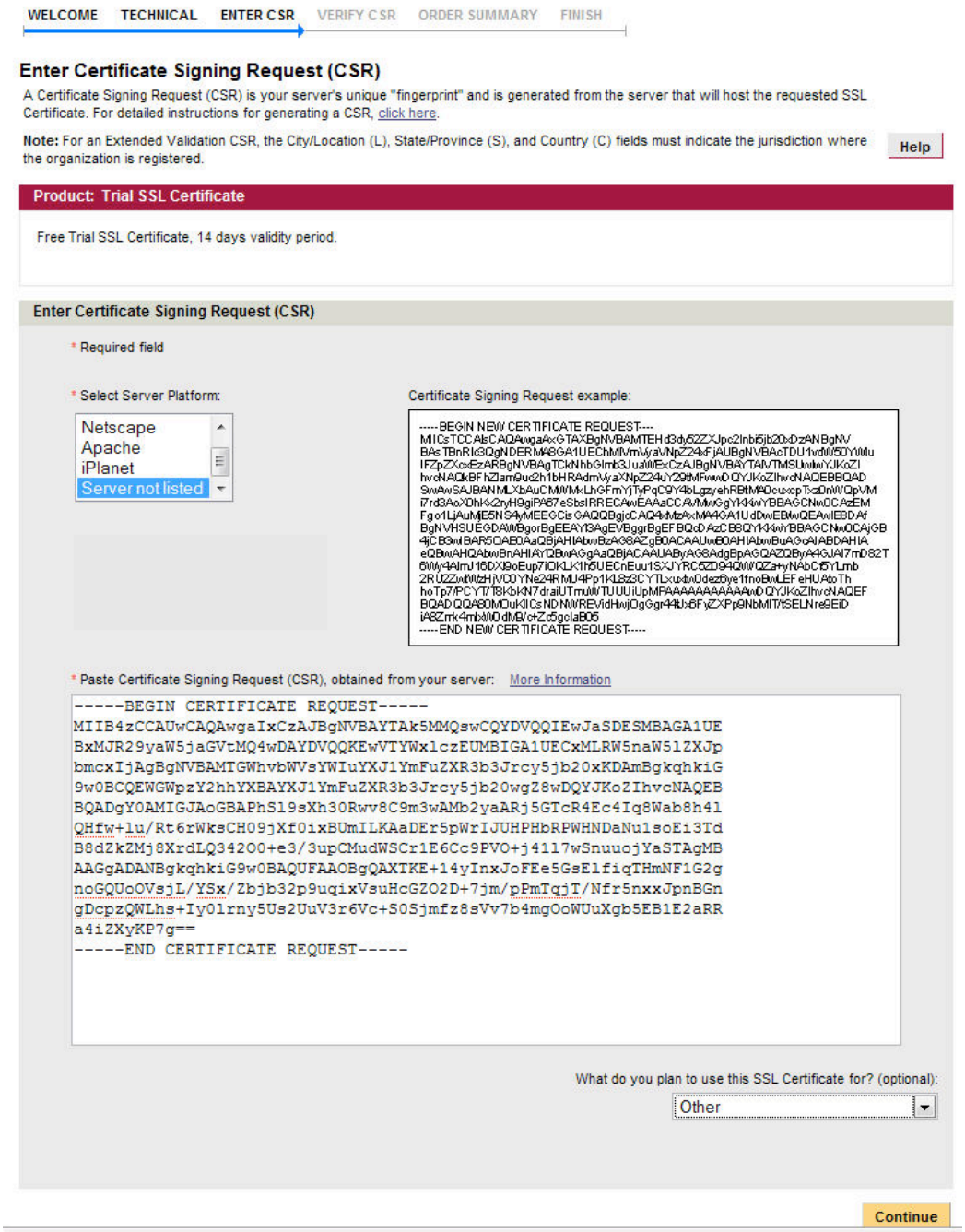


Click “View Current” to see your CSR and copy everything including
-------BEGIN CERTIFICATE REQUEST-------- and
-------END CERTIFICATE REQUEST-------




```
-----BEGIN CERTIFICATE REQUEST-----
MIIB4zCCAUwCAQAwgaIxCzAJBgNVBAYTAk5MMQswCQYDVQQIEwJaSDESMBAGA1UE
BxMJR29yaW5jaGVtMQ4wDAYDVQQKEwVTYWxlczEUMBIGA1UECxMLRW5naW51ZXJp
bmcxIjAgBgNVBAMTGWhvbWVsYWIuYXJ1YmFuZXR3b3Jrcy5jb20xKDAmBgkqhkiG
9w0BCQEWGWpzY2hhYXBAYXJ1YmFuZXR3b3Jrcy5jb20wgZ8wDQYJKoZIhvcNAQEB
BQADgY0AMIGJAoGBAPhS19sXh30Rwv8C9m3wAMb2yaARj5GTcR4Ec4Iq8Wab8h41
QHfw+lu/Rt6rWksCH09jXf0ixBUmILKAaDEr5pWrIJUHPHbRPWHNDaNu1soEi3Td
B8dZkZMj8XrdLQ342O0+e3/3upCMudWSCr1E6Cc9PVO+j4117wSnuuojYaSTAgMB
AAGgADANBgkqhkiG9w0BAQUFAAOBgQAXTKE+14yInxJoFEe5GsElfiqTHmNF1G2g
noGQUoOVsjL/YSx/Zbjb32p9uqixVsuHcGZO2D+7jm/pPmTqjT/Nfr5nxxJpnBGn
gDcpzQWLhs+Iy01rny5Us2UuV3r6Vc+S0Sjmfz8sVv7b4mgOoWUuXgb5EB1E2aRR
a4iZXyKP7g==
-----END CERTIFICATE REQUEST-----
```

Paste the text that you copied in the previous step into the CSR window. Select “Server not listed” and “Other” as use for the SSL certificate. Then click continue.



Verify your CSR info and make up a challenge phrase

VeriSign® Enroll For A Trial SSL Certificate

WELCOME TECHNICAL ENTER CSR VERIFY CSR ORDER SUMMARY FINISH

CSR information

Confirm your Certificate Signing Request (CSR) information and enter a challenge phrase. Help

Product: Trial SSL Certificate

Free Trial SSL Certificate, 14 days validity period.

CSR information

The requested certificate will include the following details from the CSR :

Common Name: **a800.homelab.arubanetworks.com**
Organization: Sales
Organizational Unit: Engineering
City/Location: Amsterdam
State/Province: ZH
Country: NL

Change CSR

Challenge phrase

Create a new challenge phrase (password) for your SSL certificate. **Do not lose the challenge phrase!** The challenge phrase is used the next time you renew this certificate or in case you revoke or make changes to the certificate.

* Required field

* Challenge Phrase:
* Re-enter Challenge Phrase:
* Reminder Question:

Continue

Sales: 1-650-426-5112 or Toll Free 1-866-893-6565 Support: 1-650-426-3400 or Toll Free 1-877-438-8776

Verify your order summary and click Accept

VeriSign® Enroll For A Trial SSL Certificate

WELCOME TECHNICAL ENTER CSR VERIFY CSR ORDER SUMMARY FINISH

Order summary & acceptance

Please review and confirm your order information, and accept the terms of the Subscriber Agreement to complete your order. Help

Product: Trial SSL Certificate

Free Trial SSL Certificate, 14 days validity period.

CSR information

The requested certificate will include the following details from the CSR :

Common Name: **a800.homelab.arubanetworks.com**
Organization: Sales
Organizational Unit: Engineering
City/Location: Amsterdam
State/Province: ZH
Country: NL

Change CSR

Contact and payment information

Technical Contact

Edit

John Schaap
Systems Engineer
Aruba Networks
Algolweg 11A
Amersfoort ZH
NL
3821BG
Telephone 31622407110
Email: jschaap@arubanetworks.com

Privacy Statement

By clicking **Accept & Purchase**, you confirm that you have carefully read, understood, and accept to become bound by the terms and conditions of the Subscriber Agreement, including VeriSign's Privacy Statement. In particular, you agree to VeriSign transferring your enrollment information to third parties in accordance with the Privacy Statement. Please note that you can change your preferences by visiting VeriSign communication preferences.

Subscriber Agreement

Printable Version

```
VeriSign Test Certification Authority
Certification Practice Statement

YOU MUST READ THIS VERISIGN TEST
CERTIFICATION AUTHORITY PRACTICE STATEMENT
("TEST CPS") CAREFULLY. BY CLICKING "ACCEPT"
BELOW AND/OR REQUESTING, USING, OR RELYING
UPON A TEST CERTIFICATE OR THE TEST CA ROOT
CERTIFICATE (AS THESE TERMS ARE DEFINED
BELOW), YOU AGREE TO BE BOUND BY THE TERMS OF
THIS TEST CPS, AND TO BECOME A PARTY TO THIS
```

Decline Accept

You will see that you trial order is complete and soon you will receive an email with your signed certificate

VeriSign® Enroll For A Trial SSL Certificate

WELCOME TECHNICAL ENTER CSR VERIFY CSR ORDER SUMMARY FINISH

Thank you for completing your order!

VeriSign is processing your Trial SSL Certificate request. Your Trial SSL Certificate and installation instructions will be sent to you via email within the next hour.

Your order number is: **318790472**

You can print this page as proof of purchase.

Print Help

Product: Trial SSL Certificate

Free Trial SSL Certificate, 14 days validity period.

CSR information

You are enrolling for an SSL Certificate for a800.homelab.arubanetworks.com. Make sure this domain matches the URL your Web site visitors connect to. If this information is incorrect, contact Customer Support at 1-877-438-8776 or 1-650-426-3400.

Common Name: a800.homelab.arubanetworks.com

Organization: Sales

Organizational Unit: Engineering

City/Location: Amsterdam

State/Province: ZH

Country: NL

What is the status of my order?

Visit the Order Status page at any time to check the current status of your order. Additionally, your technical and Organizational Contacts will soon receive an Order Confirmation email to help track the progress of your order. You can visit the Order Status page by clicking the link below and bookmark the page to check the status of your order at any time.

Check Order Status

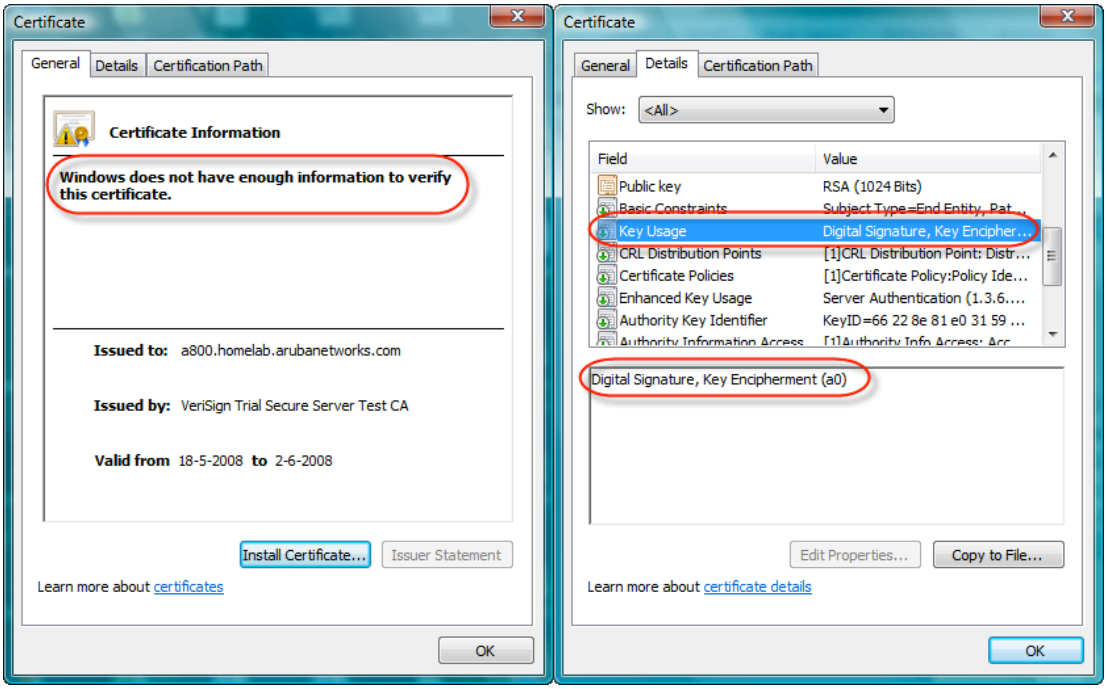
Sales: 1-650-426-5112 or Toll Free 1-866-893-6565 Support: 1-650-426-3400 or Toll Free 1-877-438-8776

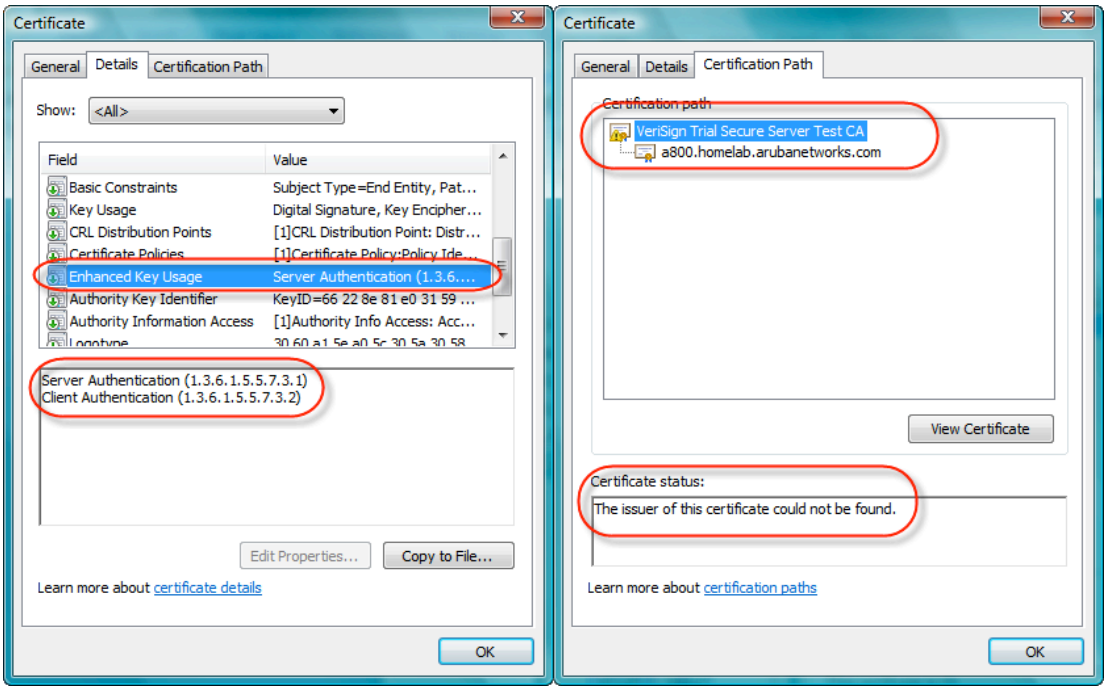
This is an example of the signed certificate that you receive in the email from Verisign


```
Thank you for your interest in VeriSign!

-----BEGIN CERTIFICATE-----
MIIFYDCCBEigAwIBAgIQVZATlk6S7kX5BJgwtucVSDANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNl
cnZlciBUZXN0IENBMB4XDTA4MDUxNzAwMDAwMFoXDTA4MDUzMTIzNTk1OVowgbQx
CzAJBgNVBAYTAk5MMQswCQYDVQQIEwJaSDESMBAGA1UEBxQJR29yaW5jaGVtMQ4w
DAYDVQQKFAVTYWxlczEUMBIGA1UECxQLRW5naW5lZXJpbmcxOjA4BgNVBAsUMVRl
cm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMpMDUx
IjAgBgNVBAMUGWhvbWVsYWIuYXJ1YmFuZXR3b3Jrcy5jb20wgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAPhSl9sXh30Rwv8C9m3wAMb2yaARj5GTcR4Ec4Iq8Wab
8h4lQHfw+lu/Rt6rWksCH09jXf0ixBUmILKAaDEr5pWrIJUHPHbRPWHNDaNu1soE
i3TdB8dZkZMj8XrdLQ342O0+e3/3upCMudWSCr1E6Cc9PVO+j41l7wSnuuojYaST
AgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIFoDBDBgNVHR8EPDA6
MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJlLWNybC52ZXJpc2lnbi5jb20vU1ZSVHJp
YWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUwMTAvBggrBgEFBQcC
ARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EwHQYDVR0lBBYw
FAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8GA1UdIwQYMBaAFGYijoHgMVndKn+rRsU2
AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
dmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZSU2VjdXJlLWFpYS52
ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYIKwYBBQUHAQwEYjBg
oV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQUS2u5KJYGDLvQUjib
KaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9nbzEuZ2lm
MA0GCSqGSIb3DQEBBQUAA4IBAQA/iVAMx1DoluSgae9dDRslc/1uDBB7moKFswwh
vLwXD7bbRJsOOSfwcMTnmxsDYqbJD2ELqLCzFrpxuFVa5cKDtXHO+iGEjJ6VAq4E
bfzY/GHmznWbzuoh3Z+/TYxF7kHnQw7pRb0ML9BDyFn0279OdvPaKfOpzNNnmV7e
PV51OcxrXXIn5ll8Egx5ZktoVWuBNCvbeQB8lrMskO66/AfaGaQo2Aiu9R8zC7j3
Qg70Tmw1Yj4oBMu7VdBZGe0baRGkjReGe40ea6IVrRY+N2k+9vPRxYURqgIhalJR
miza5YcUbcUq8oOUBwtR+fp2o5Ol9Rd/sQaFjCQQHdKLcDr3
-----END CERTIFICATE-----
```

Create a new file and call it your-server-certificate.cer. Open the file with Notepad and paste the text above including -------BEGIN CERTIFICATE-------- and -------END CERTIFICATE-------
In this file.
You can double click the file in Windows and it will show you the certificate.
You will see that a default Windows PC will not trust the certificate and the Verisign Trial Secure Server Test CA.





You will need to follow the procedure below to install the special Test CA Root on each computer that you will be using during the test.

http://www.verisign.com/ssl/buy-ssl-certificate/free-ssl-certificate-trial/test-root-ca/trialcainstall.html

Free Trial SSL Certificate

Test Root CA Instructions

In order to test the use of a trial certificate, you must install a special Test CA Root on each browser that you will be using in the test. (This requirement is to prevent fraudulent use of test certificates. When you purchase a regular SSL Certificate, your users will not have to go through this step.)

Note: Some servers require you to install the Trial Root CA certificate onto the server prior to installing the SSL certificate. Please refer to your Server vendor for further information.

Trial Root Certificates

Secure Site Trial Root CA Certificate >>

This Root CA Certificate is used during the testing phase of the Trial VeriSign Secure Site SSL Certificate. This will need to be installed into each browser that will be used to test the SSL Certificate.

Installation Instructions

For Microsoft Browsers

1. Click on the "Secure Site Trial Root Certificate" link above.
2. Save the certificate into a file with a .cer extension.
3. Open a Microsoft IE Browser.
4. Go to Tools > Internet Options > Content > Certificates
5. Click Import. A certificate manager Import Wizard will appear. Click Next.
6. Browse to the location of the recently stored root (done in step 2). Select ALL files for file type.
7. Select the certificate and click Open.
8. Click Next.
9. Select "Automatically select the certificate store based on the type of the certificate". Click Ok.
10. Click Next then Finish.
11. When prompted and asked if you wish to add the following certificate to the root store, click Yes.

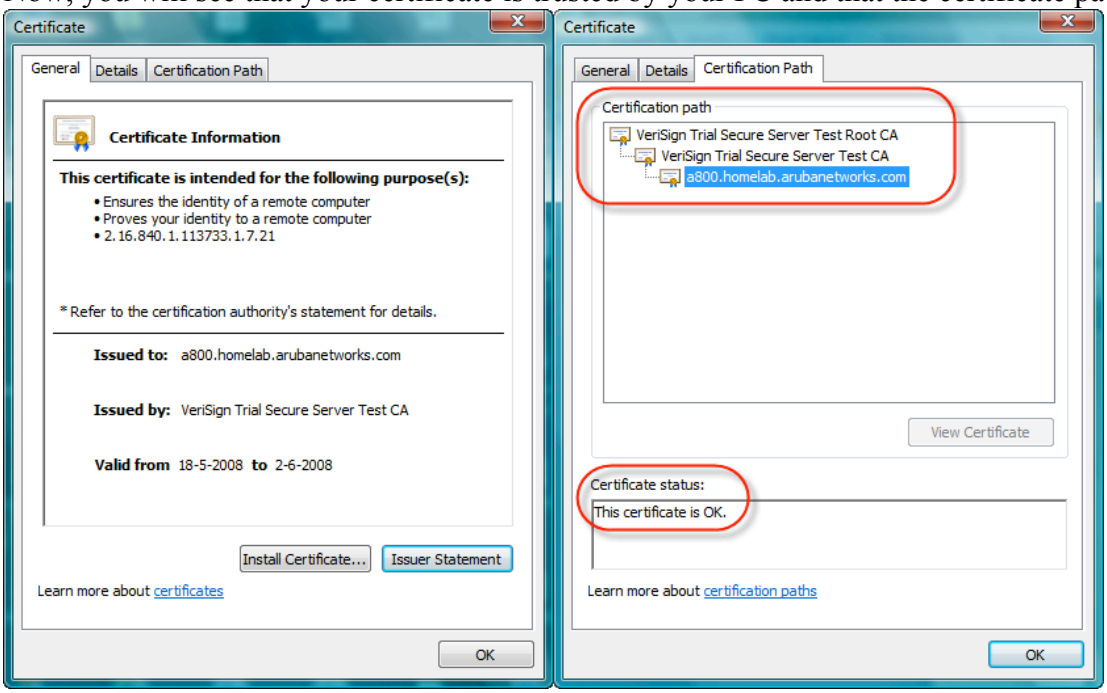
For Netscape Browsers

1. Click on the "Secure Site Trial Root Certificate link" above.
2. Save the certificate into a file with a .cer extension.
3. Open a Netscape browser.
4. Go to Edit > Preferences > Privacy & Security > Certificates > Manage Certificates > Authorities.
5. Click Import
6. A dialog box appears that says, "Are you willing to accept this Certificate Authority for the purposes of certifying other Internet sites, email users, or software developers?". Check "Trust this CA to identify web sites". Click Next.
7. Click Ok.

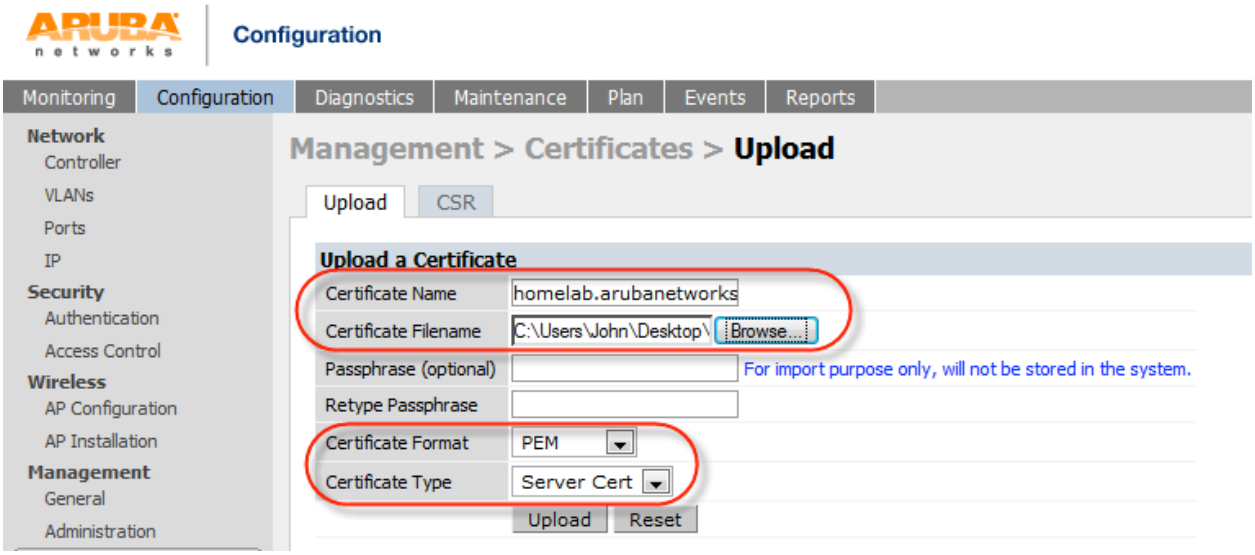
For Firefox Browsers

1. Click on the "Secure Site Trial Root Certificate link" above.
2. Save the certificate into a file with a .cer extension.
3. Open a Firefox browser.
4. Go to Tools > Options > Advanced > View Certificates >Authorities.
5. Click Import.
6. Select the Trial Root certificate > click Open.
7. A dialog box appears that says, "Do you want to trust 'VeriSign Trial Secure Server Test Root CA' for the following purposes?". Check "Trust this CA to identify web sites".
8. Click OK.

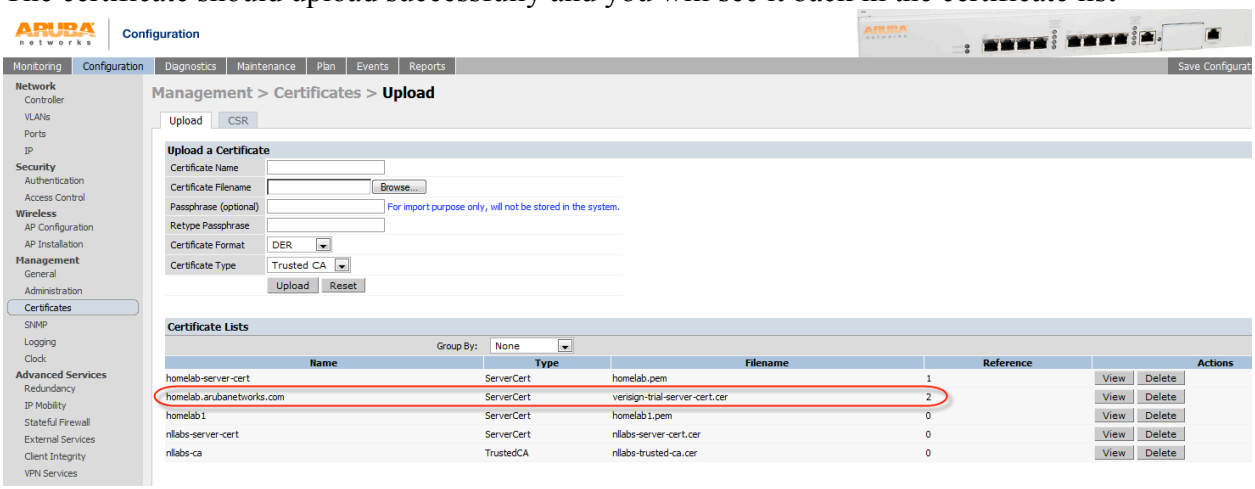
Now, you will see that your certificate is trusted by your PC and that the certificate path is OK



Go to Configuration -> Management -> Certificate and select Upload and upload your certificate in PEM format and as server certificate type

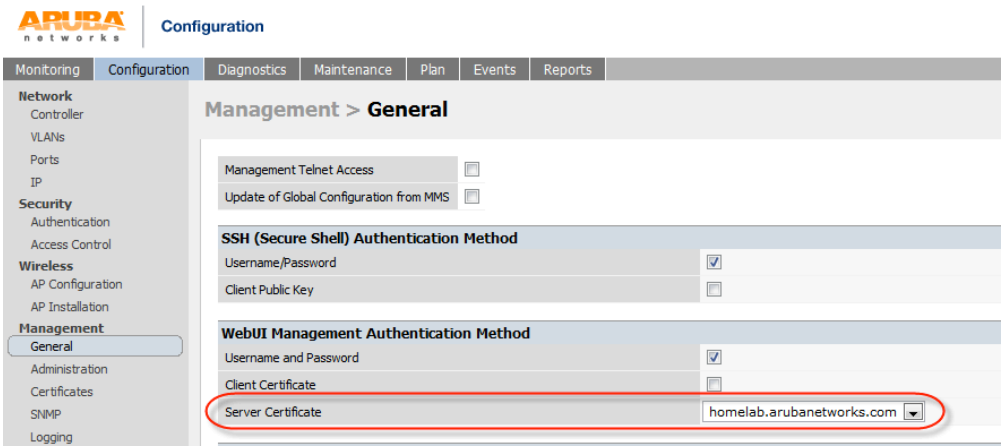


The certificate should upload successfully and you will see it back in the certificate list

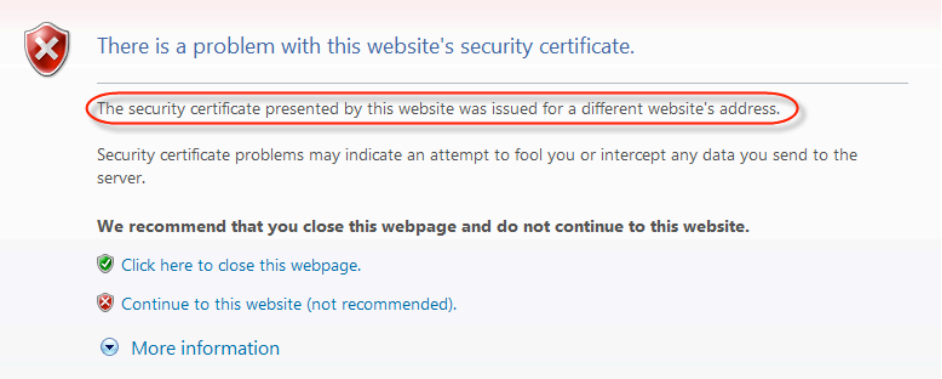


Use certificate for WebUI management

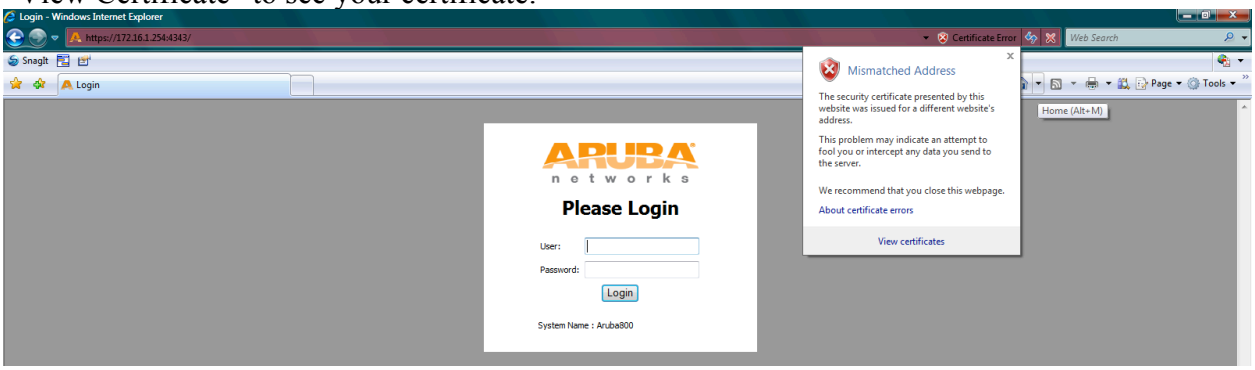
Go to Configuration -> Management -> General and select you certificate as server certificate for WebUI Management Authentication. This will restart the webserver so wait for 30 seconds before connecting



Open IE7 and connect to the controller. You will see the following warning. That is because the IP address of my controller is not known by the DNS name used in the certificate

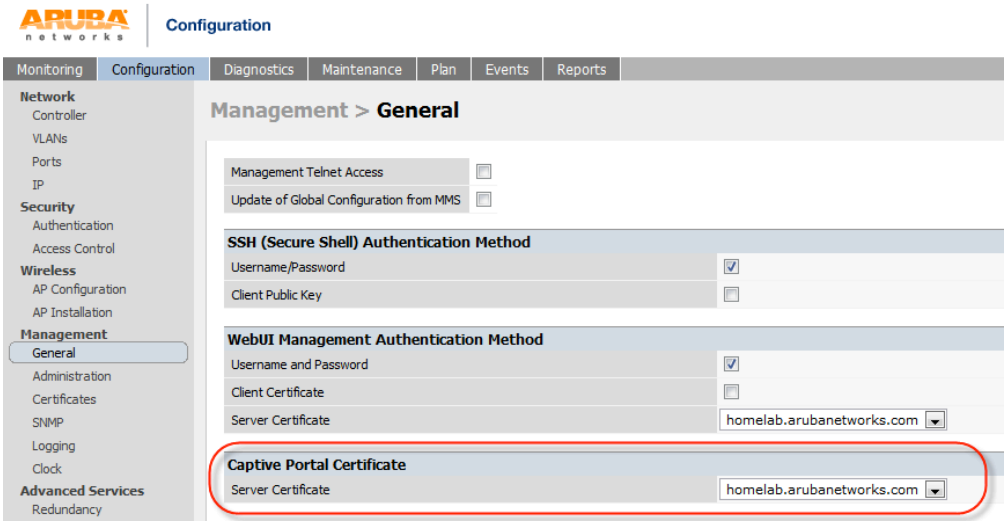


Click "Continue to this website" In the browser you can click on "Certificate Error" and click "View Certificate" to see your certificate.

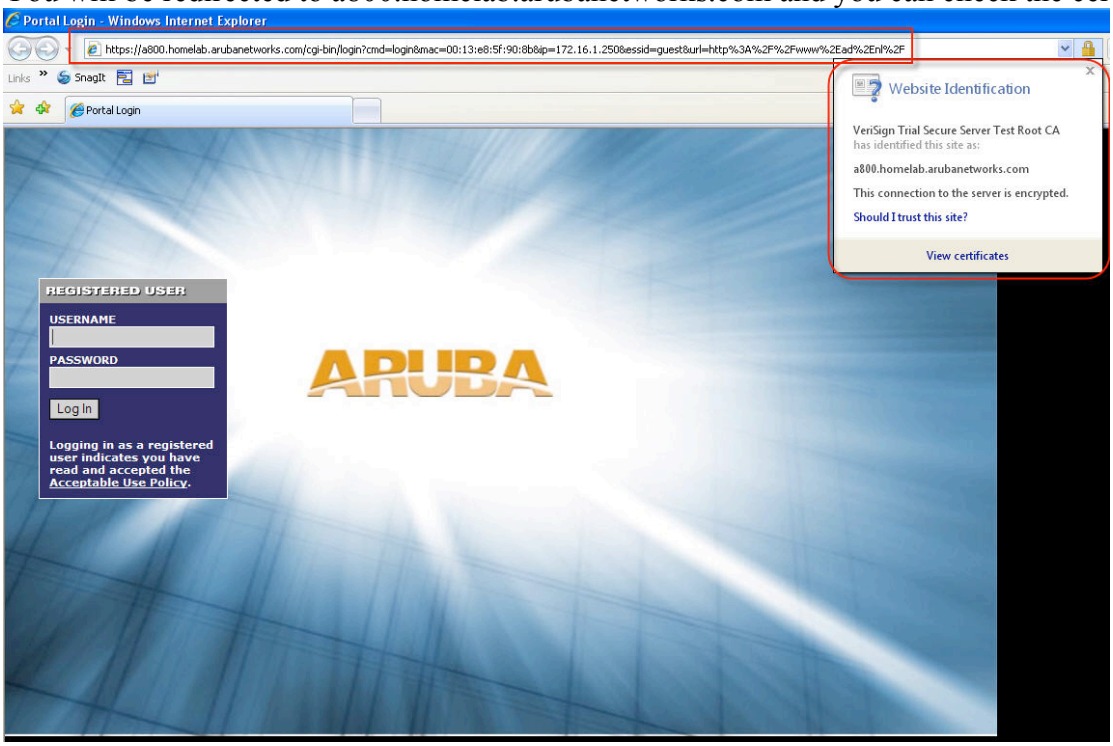


Use certificate for Captive Portal

Normally the default captive portal will redirect you to securelogin.arubanetworks.com but this will change to whatever you used as CN in your certificate.
In this case it will be a800.homelab.arubanetworks.com
Go to Configuration -> Management -> General and select you certificate as server certificate for Captive Portal.



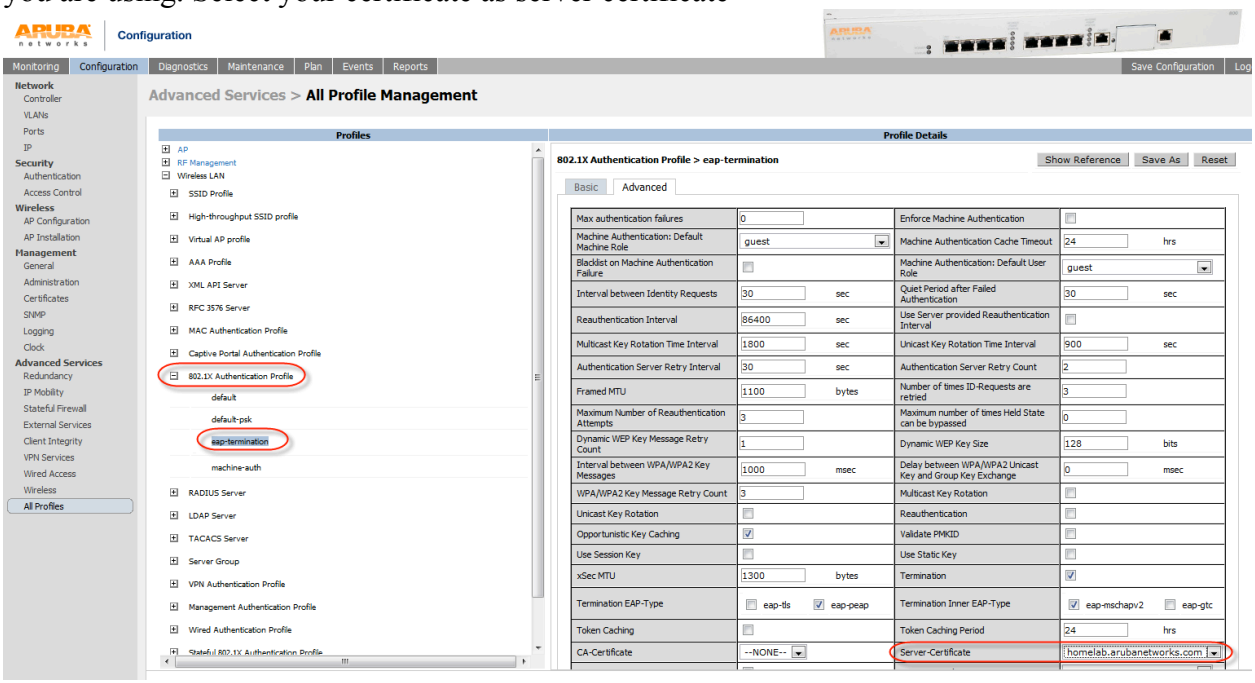
You will be redirected to a800.homelab.arubanetworks.com and you can check the certificate.



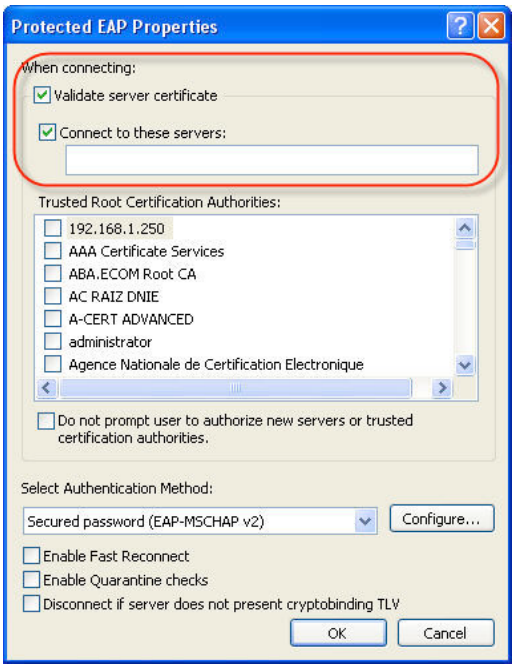
Use certificate for dot1x eap—termination WZC

WZC (Windows XP Professional SP3)

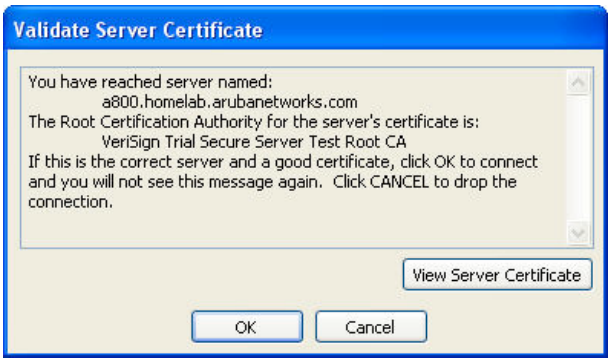
Go to Configuration -> All Profiles -> 802.1X Authentication Profile and select the profile that you are using. Select your certificate as server certificate



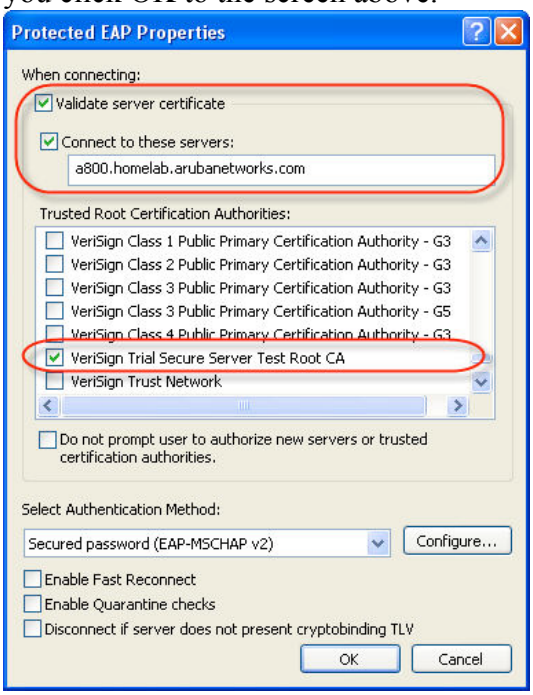
First check if the connection is established without checking the server certificate. When everything works as expected then you can select “Validate server certificate” and “Connect to these servers”



You will see the following pop-up screen when you connect again



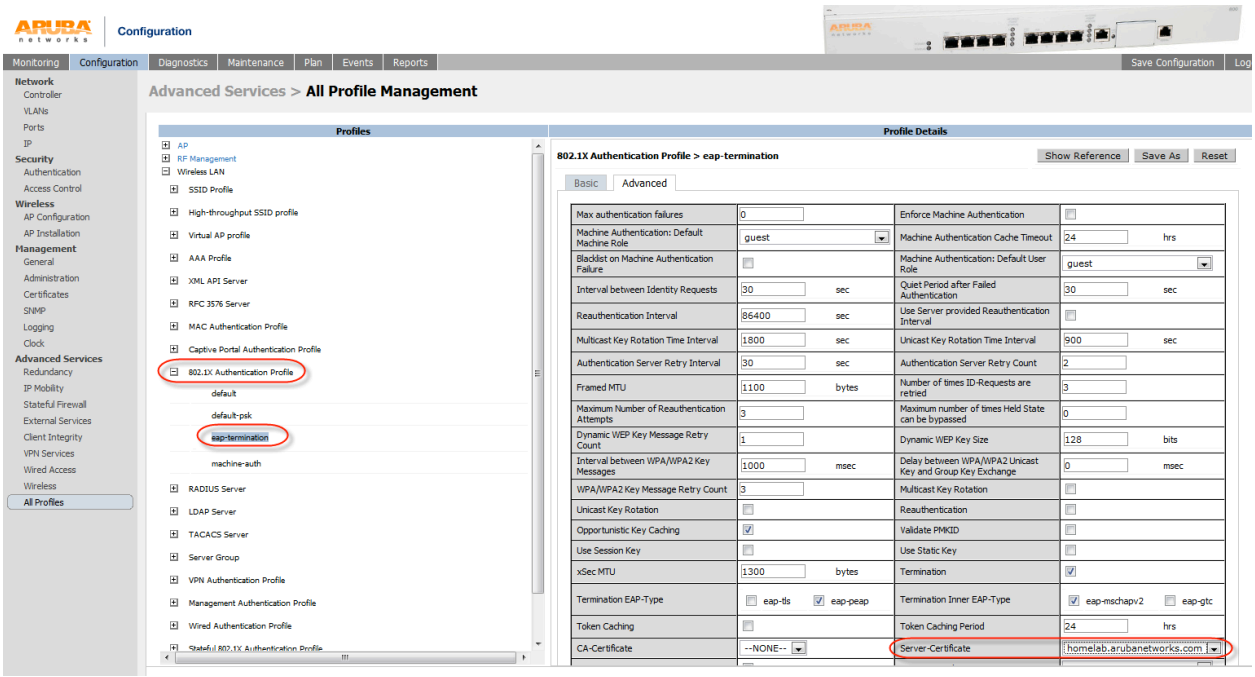
Windows will automatically change the Protected EAP Properties to the settings below when you click OK to the screen above.



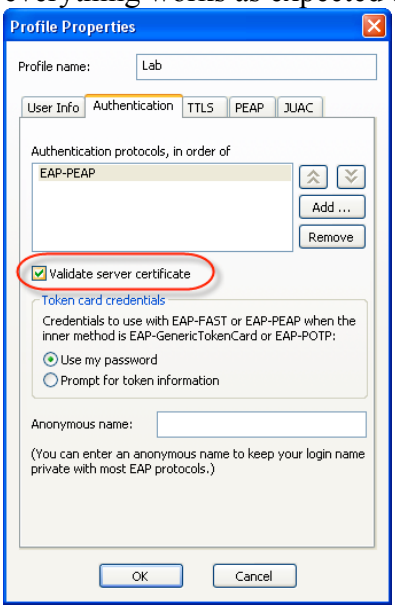
Use certificate for dot1x eap—termination Odyssey

Juniper Odyssey Access Client (version 4.70.10697.0)

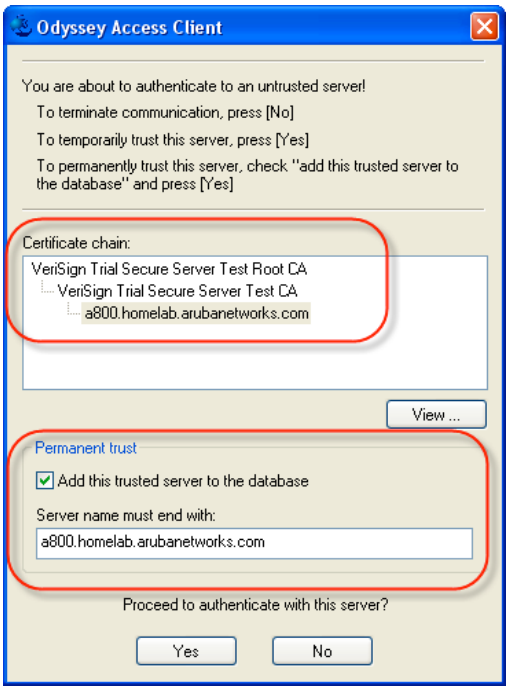
Go to Configuration -> All Profiles -> 802.1X Authentication Profile and select the profile that you are using. Select your certificate as server certificate



First check if the connection is established without checking the server certificate. When everything works as expected then you can select "Validate server certificate"



Odyssey will show a pop-up screen asking you if you trust this untrusted server. You can view the certificate and add permanent trust.


Odyssey Access Client
You are about to authenticate to an untrusted server!
To terminate communication, press [No]
To temporarily trust this server, press [Yes]
To permanently trust this server, check "add this trusted server to the database" and press [Yes]
Certificate chain:
VeriSign Trial Secure Server Test Root CA
VeriSign Trial Secure Server Test CA
a800.homelab.arubanetworks.com
View ...
Permanent trust
Add this trusted server to the database
Server name must end with:
a800.homelab.arubanetworks.com
Proceed to authenticate with this server?
Yes
No

Troubleshooting

The easiest way to check if your certificate is OK and if the laptop that you want to use trusts the certificate is to use the certificate for the WebUI and use Internet Explorer to access the controller. IE will tell you when something is wrong and you can then correct the problem.

For example IE will tell you :

- "The security certificate presented by this website was not issued by a trusted certificate authority". This means that your PC does not trust the CA that issued the certificate.

- "The security certificate presented by this website was issued for a different website's address". This means that the DNS address in the certificate does not match the controllers IP address. In a lab environment this is OK and you can use this certificate for eap-termination, captive portal and WebUI.

The following shows a client trying to authenticate but there is something wrong with the trust of the certificate. Authentication stops with "station-term-start"

```
(Aruba800) #show auth-tracebuf count 20

Auth Trace Buffer
----------------


May 16 19:58:13  cert-downloaded      *  00:0b:86:52:b8:10  00:00:00:00:00:00//tmp/certmgr/ServerCert/homelab1  -  -
May 16 19:59:06  station-up          *  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                        -  -  wpa2 aes
May 16 19:59:06  station-term-start    *  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                        10  -
May 16 19:59:06  eap-term-start      ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination            -  -
May 16 19:59:06  station-term-start    *  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                        10  -
```

The following shows a client which successfully sets up the TLS tunnel so the certificate is OK

```
(Aruba800) #show auth-tracebuf count 20

Auth Trace Buffer
----------------


May 16 19:58:13  cert-downloaded      *  00:0b:86:52:b8:10  00:00:00:00:00:00//tmp/certmgr/ServerCert/homelab1  -  -
May 16 19:59:06  station-up          *  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                        -  -  wpa2 aes
May 16 19:59:06  station-term-start    *  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                        10  -
May 16 19:59:06  eap-term-start      ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination            -  -
May 16 19:59:06  station-term-start    *  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                        10  -
May 16 19:59:06  client-finish       ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination            -  -
May 16 19:59:06  server-finish       <-  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination            -  61
May 16 19:59:21  server-finish-ack    ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination            -  -
```

Just for reference a complete successful authentication including MS-CHAPv2 and the key exchange.

```
May 16 19:58:13  cert-downloaded      *  00:0b:86:52:b8:10  00:00:00:00:00:00//tmp/certmgr/ServerCert/homelab1  -  -
```

```
May 16 19:59:06  station-up           *  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                          -  -    wpa2 aes
May 16 19:59:06  station-term-start    *  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                       10  -
May 16 19:59:06  eap-term-start       ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination             -  -
May 16 19:59:06  station-term-start    *  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                       10  -
May 16 19:59:06  client-finish        ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination             -  -
May 16 19:59:06  server-finish        <-  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination             -  61
May 16 19:59:21  server-finish-ack    ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination             -  -
May 16 19:59:21  inner-eap-id-req     <-  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination             -  35
May 16 19:59:21  inner-eap-id-resp    ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination             -  -    employee1
May 16 19:59:21  eap-mschap-chlg      <-  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination             -  67
May 16 19:59:21  eap-mschap-response  ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                          7  49
May 16 19:59:21  mschap-request       ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                          7  -    employee1
May 16 19:59:21  mschap-response      <-  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/Internal                 -  -    employee1
May 16 19:59:21  eap-mschap-success   <-  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination             -  83
May 16 19:59:21  station-data-ready    *  00:16:ce:2c:b2:80  00:00:00:00:00:00                       10  -
May 16 19:59:21  station-data-ready_ack *  00:16:ce:2c:b2:80  00:00:00:00:00:00                       10  -
May 16 19:59:21  eap-mschap-success-ack->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                          -  -
May 16 19:59:21  eap-tlv-rslt-success <-  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination             -  43
May 16 19:59:21  eap-tlv-rslt-success ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                          -  2
May 16 19:59:21  eap-success          <-  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30/eap-termination             -  4
May 16 19:59:21  wpa2-key1            <-  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                          -  117
May 16 19:59:21  wpa2-key2            ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                          -  117
May 16 19:59:21  wpa2-key3            <-  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                          -  151
May 16 19:59:21  wpa2-key4            ->  00:16:ce:2c:b2:80  00:0b:86:a0:ab:30                          -  95
```