

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

## Contents

|  |    |
|--|----|
| Introduction.....                                      | 3  |
| Use certificate for WebUI management .....             | 17 |
| Use certificate for Captive Portal.....                | 18 |
| Use certificate for dot1x eap—termination WZC.....     | 18 |
| Use certificate for dot1x eap—termination Odyssey..... | 21 |
| Troubleshooting .....                                  | 23 |

## 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

US Home | Worldwide Sites | Contact Us | Site Map

**verisign**

Search

Products & Services | Solutions | Support | About VeriSign | Existing Customers

Content and Messaging  
Domain Name Services  
All Products and Services

**Get the #1 trust mark on the Internet**

**VeriSign Secured**

**SSL Certificates**

**BUY** SSL Certificates  
**BUY** Code Signing  
**TRY** Free SSL Trial  
**RENEW** Renew Now

**SIGN IN** Certificate Center

**What's New:** VIP wins Best Consumer Application or Service **More News >>**

**Featured Product**

VeriSign® Extended Validation (EV) SSL Certificates show that your Web site can be trusted. EV triggers new browsers like Internet Explorer 7 to turn the address bar green when visitors view your site. [Learn more >>](#)

[View All Products](#)

**Industry Solutions**

- Consumer Products and Retail
- Financial Services
- Healthcare and Life Sciences
- Media and Entertainment
- Public Sector
- Telecommunications

**Resources For**

- Large Enterprises
- Online Merchants

**Quick Links**

- News and Events
- RSS Feeds **RSS**
- Investor Relations
- VeriSign Research
- Partners
- Support
- VeriSign Blogs

**Customers**

**LIVE EARTH**

**Try VeriSign SSL FREE for 14 days**  
**Start now >>**

**VeriSign Secured Seal >>**



**ABOUT SSL CERTIFICATES**

Contact Us | Careers | Legal Notices | Privacy | Repository | ©1995-2008 VeriSign, Inc. All rights reserved.

Products & Services | Solutions | Support | About VeriSign | Existing Customers  
US Home | Worldwide Sites | Site Map | Search | Feedback

VeriSign (Nasdaq: VRSN) is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence. VeriSign offerings include SSL, SSL Certificates, and digital content solutions, Extended Validation, two-factor authentication, identity protection, managed network security, public key infrastructure (PKI), security consulting, information management, and solutions for intelligent communications, and content.

Complete the following form



## Free SSL Trial Certificate

To help us serve you better, please provide the information below:

Are you interested in securing your e-mail communications? [Learn more](#) about Digital IDs for secure e-mail.

Note: \* = required.

|   |  |
|---|--|
| * Email Address   | <input type="text" value="jschaap@arubanetworks.com"/> |
| * First Name  | <input type="text" value="John"/>                      |
| * Last Name   | <input type="text" value="Schaap"/>                    |
| * Phone   | <input type="text" value="+31622407110"/>              |
| <small>Please include area code and/or country code</small> |  |
| * Zip Code  | <input type="text" value="4207MT"/>                    |
| * Country   | <input type="text" value="Netherlands"/>               |



☐ Please keep me up to date on product news and Security alerts via email.

☐ Please remember my profile information.



VeriSign respects your right to privacy, see our [Privacy Statement](#).

[Continue](#)

© VeriSign, Inc. All rights reserved.

  
CLICK TO VERIFY ABOUT SSL CERTIFICATES

This brings you to the welcome screen, click continue



## Enroll For A Trial SSL Certificate

[WELCOME](#) [TECHNICAL](#) [ENTER CSR](#) [VERIFY CSR](#) [ORDER SUMMARY](#) [FINISH](#)

### Welcome

[Help](#)

**Product: Trial SSL Certificate**

Free Trial SSL Certificate, 14 days validity period.




**Enrolling for a certificate includes the following steps:**

- Step 1. Enter your Technical Contact information.
- Step 2. Identify your server platform and enter your Certificate Signing Request (CSR).  
A CSR is required for enrollment. [Need help generating a CSR?](#)
- Step 3. Verify your CSR and enter a challenge phrase for this certificate.
- Step 4. Confirm and submit your order.
- Step 5. Install the Test CA Root.
- Step 6. Receive (via email) and install your Trial SSL Certificate.

[Continue](#)

Legal Notices | Privacy | Repository | ©1995-2007 VeriSign, Inc. All rights reserved.

Sales: 1-850-426-5112 or Toll Free 1-866-893-6565    Support: 1-850-426-3400 or Toll Free 1-877-436-8776



Complete the following form and click continue



## 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:   
\* Last Name:   
\* Title:   
\* Company:   
\* Address1:   
Address2:   
\* City:   
\* State/Province:   
\* ZIP/Postal Code:   
\* Country:   
\* Telephone:   
Fax:   
\* Email:

- ☐ Save my contact information for future certificate enrollments.  
☐ Please keep me up to date on product news and security-related information.

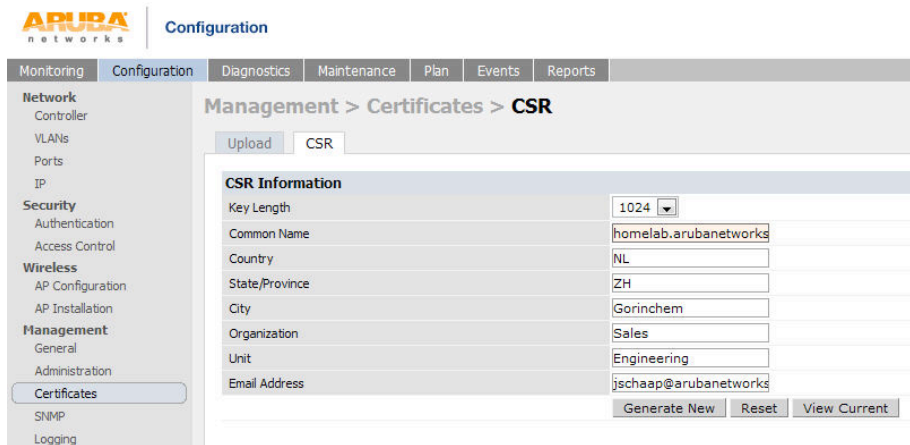
[Continue](#)

[Legal Notices](#) | [Privacy](#) | [Repository](#) | ©1995-2007 VeriSign, Inc. All rights reserved.

Sales: 1-850-426-5112 or Toll Free 1-866-893-8585 Support: 1-850-426-3400 or Toll Free 1-877-438-8778

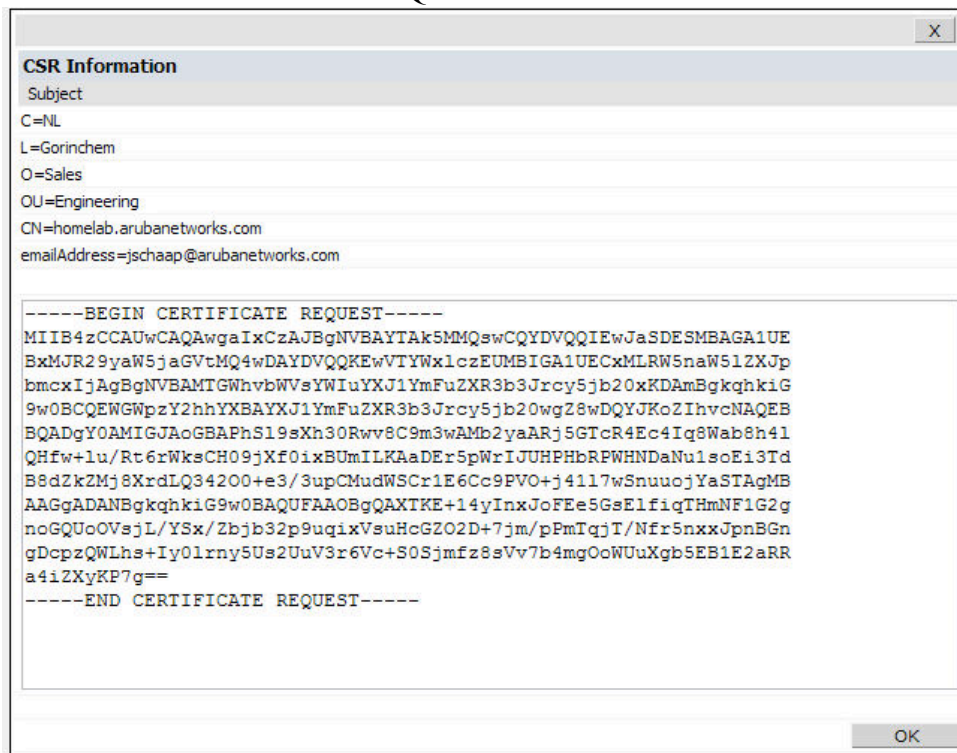


Go to the controller and configure it to generate a new CSR. The CN (Common Name) should be the same as the name of the controller. Click “Generate New” after entering all the details



The screenshot shows the Aruba Configuration interface. The left sidebar contains a navigation menu with categories like Network, Security, Wireless, Management, and Certificates. The main content area is titled 'Management > Certificates > CSR'. Below this title are two tabs: 'Upload' and 'CSR'. The 'CSR' tab is active, displaying a form for 'CSR Information'. The form includes fields for Key Length (set to 1024), Common Name (homelab.arubanetworks), Country (NL), State/Province (ZH), City (Gorinchem), Organization (Sales), Unit (Engineering), and Email Address (jschaap@arubanetworks). At the bottom of the form are three buttons: 'Generate New', 'Reset', and 'View Current'.

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



The screenshot shows a window titled 'CSR Information'. It displays the following details:

- Subject
- C=NL
- L=Gorinchem
- O=Sales
- OU=Engineering
- CN=homelab.arubanetworks.com
- emailAddress=jschaap@arubanetworks.com

Below these details is a text area containing the CSR text, which starts with '-----BEGIN CERTIFICATE REQUEST-----' and ends with '-----END CERTIFICATE REQUEST-----'. The text is as follows:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB4zCCAUAwCAQAwgaIx CzA JBgNVBAYTAk5MMQswCQYDVQQIEwJaSDESMBAGA1UE
BxMJR29yaW5jaGVtMQ4wDAYDVQQKEwVlYWx1czEUMBIGA1UECxmLRW5naW51ZXJp
bm90BCQEWGpZ2hhYXBAYXJ1YmFuZXR3b3Jrcy5jb20wZDQYJkoZIHvcNAQEB
BQADgY0AMIGJAoGBAPhS19sXh30Rwv8C9m3wAMb2yaARj5GTcR4Ec4Iq8Wab8h41
QHfw+lu/Rt6rWksCH09jXf0ixBUmILKAaDEr5pWrI JUHPHbRPWHNDaNu1soEi3Td
B8dZkZmJ8XrdLQ34200+e3/3upCMudWSCr1E6Cc9FVO+j4117wSnuuojYaSTAgMB
AAGgADANBgkqhkiG9w0BAQUFAAOBgQAAXTKE+14yInxJoFEe5GsElfiqTHmNF1G2g
noGQUoOVsjL/Ysx/Zbjb32p9uqixVsuHcGZ02D+7jm/pPmTqjT/Nfr5nxxJpnBGn
gDcpzQWLhs+Iy0lrny5Us2UuV3r6Vc+S0Sjmfz8sVv7b4mgOoWUuXgb5EB1E2aRR
a4i2XyKP7g==
-----END CERTIFICATE REQUEST-----
```

At the bottom right of the window is an 'OK' button.

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.

WELCOME
TECHNICAL
ENTER CSR
VERIFY CSR
ORDER SUMMARY
FINISH

## Enter Certificate Signing Request (CSR)

A Certificate Signing Request (CSR) is your server's unique "fingerprint" and is generated from the server that will host the requested SSL Certificate. For detailed instructions for generating a CSR, [click here](#).

**Note:** For an Extended Validation CSR, the City/Location (L), State/Province (S), and Country (C) fields must indicate the jurisdiction where the organization is registered.

Product: Trial SSL Certificate

Free Trial SSL Certificate, 14 days validity period.

### Enter Certificate Signing Request (CSR)

- \* Required field
- \* Select Server Platform:
 

Netscape
Apache
iPlanet
Server not listed

Certificate Signing Request example:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICsTCCABCAQAwAgAAxGATAGNVBAMTEHd3dyZSZXJpc2lnb5kzODzANBgNV
BAUwTmRlSGQgNERMA8GA1UEEChMVMVYyYjY2NDQ4FJAUBGNVBACDUIvdWw5ODYyMTU
IFZpZCwEZAARBNVBAGTCNNbGlm3uaMEKcZAJBgNVBAYTAUVTMSUwbyYKOZl
hvdiNAKBFhzian6uc2t1bHRAdmMyaXNpZ24uY29mfWw0QYIKoZIhvdAAGEBBQAD
SwAwSAJBANML3baUCMMVKLHoFYMYTFqC9r4BLgzehRBVM4OuoopTzdNM/QpVM
I7rd3aoXdhkZnyH9gIPAE7eStRIERCAwEAACAACAMwGvY144vYBBAGCNwOCACEM
Fgo1LiAutME5NS4MEEGCsGAQQBglcgAQ4MBzAAM4GA1UdEWBQAQEALBDAAt
BgNVHSUEGDAlMBgorBgEEAYISAgEVBggrBgEFBQCDAzCBQDY144vYBBAGCNwOCACjGB
4QCBOmlBAR5OAEOAaQBIAHAbwEzaGGAZGBOACAAUwBOAHIAbmBuAaGAIBDADAHIA
eQBWAHQAbwEbnAHIAeQBWAQGaGGAQBACAAUAByAGAgaGAgGAQQBggAgAQIDM28T
20Mw44ImU16DjXBUpTQCLK1KHUECnEuuiSXJYRCGDQ4ZWQZayNABCGYLmb
ZR1UZ2WWlMhHjVDDYNz4RMU4Pp14LSZSCYTLuzubDdezzyefnoBwLEF eHU4toTh
hoTp7PCYT/TbtkIN7draUTrmv/TUUUIUPMPAAAAAAAAAAAAQYIKoZIhvdNAQEF
BQADQQAOMDUklCSNDNI/NRevIdHwjDjGgr44b5FyZXPp9NbMITSELNreGEID
iAEZmk4mbMDdmB/czZ5golaBO5
-----END NEW CERTIFICATE REQUEST-----
```

- \* Paste Certificate Signing Request (CSR), obtained from your server: [More Information](#)

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB4zCCAUAwCAQAwgaIx CzAJBgNVBAYTAkSMQMqswCQYDVQQIEwJaSDESMBAGA1UE
BxmJR29yaW5jaGVtMQ4wDAYDVQQKEwtYXwx1czEUMBIGA1UECxMLRW5naW51ZXJp
bmciIjAgBgNVBAMTGWlnb5kzODzANBgNVBAYTAUVTMSUwbyYKOZl hvdiNAKBFhzia
n6uc2t1bHRAdmMyaXNpZ24uY29mfWw0QYIKoZIhvdAAGEBBQADSwAwSAJBANML3ba
UCMMVKLHoFYMYTFqC9r4BLgzehRBVM4OuoopTzdNM/QpVM I7rd3aoXdhkZnyH9gIP
AE7eStRIERCAwEAACAACAMwGvY144vYBBAGCNwOCACEM Fgo1LiAutME5NS4MEEGCs
GAQQBglcgAQ4MBzAAM4GA1UdEWBQAQEALBDAAtBgNVHSUEGDAlMBgorBgEEAYISAg
EVBggrBgEFBQCDAzCBQDY144vYBBAGCNwOCACjGB4QCBOmlBAR5OAEOAaQBIAHAbw
EzaGGAZGBOACAAUwBOAHIAbmBuAaGAIBDADAHIAeQBWAHQAbwEbnAHIAeQBWAQGa
GGAQBACAAUAByAGAgaGAgGAQQBggAgAQIDM28T20Mw44ImU16DjXBUpTQCLK1KHUE
CnEuuiSXJYRCGDQ4ZWQZayNABCGYLmb ZR1UZ2WWlMhHjVDDYNz4RMU4Pp14LSZSC
YTLuzubDdezzyefnoBwLEF eHU4toTh hoTp7PCYT/TbtkIN7draUTrmv/TUUUIUPMP
AAAAAAAAAAAAQYIKoZIhvdNAQEF BQADQQAOMDUklCSNDNI/NRevIdHwjDjGgr44b5
FyZXPp9NbMITSELNreGEID iAEZmk4mbMDdmB/czZ5golaBO5
-----END CERTIFICATE REQUEST-----
```

What do you plan to use this SSL Certificate for? (optional):

Other

Continue



## Verify your CSR info and make up a challenge phrase



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](#)

[Legal Notices](#) | [Privacy](#) | [Repository](#) | ©1995-2007 VeriSign, Inc. All rights reserved.

Sales: 1-850-426-5112 or Toll Free 1-866-893-6565 Support: 1-850-426-3400 or Toll Free 1-877-438-8776



## Verify your order summary and click Accept



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



[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](http://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](http://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](#)

[Legal Notices](#) | [Privacy](#) | [Repository](#) | ©1995-2007 VeriSign, Inc. All rights reserved.

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



Thank you for your interest in VeriSign!

-----BEGIN CERTIFICATE-----

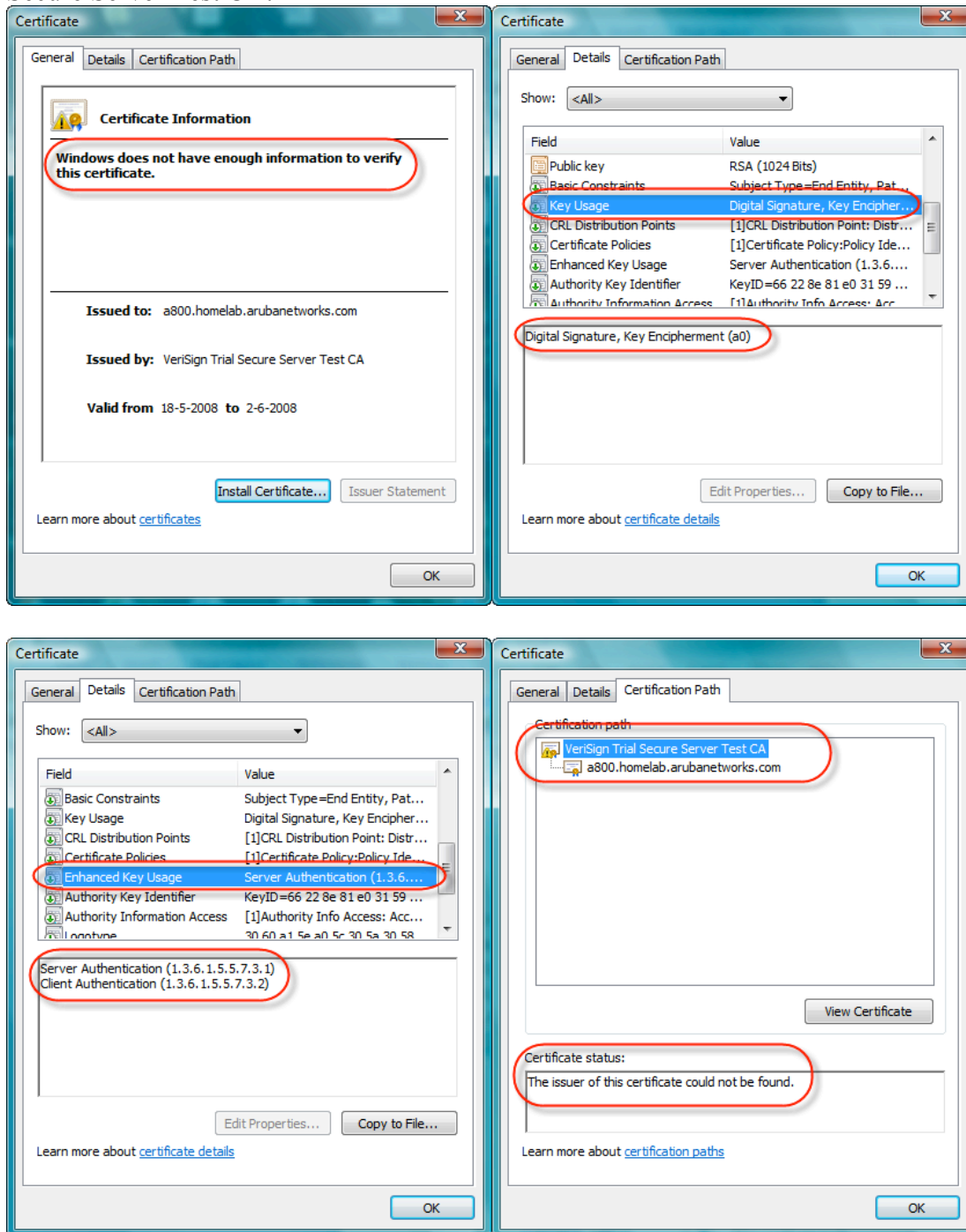
MIIFYDCCBEigAwIBAgIQVZATlk6S7kX5BJgtucVSDANBgkqhkiG9w0BAQUFADCB  
yzELMAkGA1UEBhMCVVMxZjZAVBgNVBAoTD1Zlcm1TaWduLCB3bmMuMTAwLgYDVQQL  
EydGb3I9VGvzdCBQdXJwb3NlcYBPbm5SLiAgTm8gYXNzdXJhbmlcy4xQjBABgNV  
BASToVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnb15jb20vY3Bz  
L3R1c3RlYSA0Yk9wNTETETMcGSA1UEAEMkVmVyaVYVnpZ24gVWJ3pVjdXJlIFNl  
cnZlcibuZUN0IENBMB4XDTA4MDUxNzAwMDAwMFoXDTA4MDUzMtIzNTk1OVowgbQx  
CzA3BGNVBAyTAk5MMQSwcQYDVQIIEwJaSDESMBAAGA1UEBxQ3R29yaW5jaGVTMQ4w  
DAYDVQQKFAVTVWxlcZEUmBIGA1UECXLRW5naW5lZXJpbm5lc0jA4BGNVBA5UMVR1  
cm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EgKGMPMDUx  
IjAgBgNVBAMUGWhvbVVsYWIuYXJ1YmFuZXR3b3Jrcy5jb20wgZ8wDQYJKoZIhvcN  
AQEBBQADgY0AMIGIAoGBAPhS19sXh30Rwv8C9m3wAmb2yaARj5GTCr4Ec4Iq8Wab  
8h41QHfw+lu/Rt6rWksCH09jXf0ixBUMILKAAder5pwrIJUHPHBRPWHNDaNU1soE  
i3TDB8dZKZMj8XRdLQ34200+e3/3upCMudWSCr1E6Cc9PV0+j4117wSnuuoJYaST  
AgMBAAGjggHXMIIBoZAJBgNVHRMEAjAAMASGA1UdDwQEAwIFoDBDBgNVHR8EPDA6  
MDignQA0hijOdhRwOi8vU1ZSU2VjdXJlLWwYb3c52ZXJpc2lnb15jb20vY1ZSVHQp  
YWwYMDA1LmNybDBKBGNVHSAEQzBBMD8GCMCSAGG+EUBBxUwMTAVBggrBgEFBQCC  
ARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EwHQYDVOR1BBYw  
FAYTKwYBBQUHAWEGCCsGAQUFBwMCMCB8GA1UdIwQYMBaAFGYIjoHgMVndKn+rRsU2  
AgZwJ4daMHGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au  
dmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZSU2VjdXJlLWwYb3c52  
ZXJpc2lnb15jb20vY1ZSVHQpYWwYMDA1LWwYb3c52ZXIwbgYTKwYBBQUHAWQYejBg  
oV6gXDBAMFgwVhYjAw1hZ2UvZ2lmcEeWzAHBgUrDgMCGGQUS2u5KJYGDlvQUjib  
KaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9nbzEuZ2lmc  
MA0GCsQsGIB3DQEBBQUAA4IBAQA/iVAMx1DoluSgae9dDRslc/1uDBB7moKf5wwh  
vLwXD7bBRJ3s00SfwmCTnmxsDYqBJD2ELqLCzFrpxuFVa5cKdTXHO+iEgjJ6VAAq4E  
bfz7/GhmznWBLzuoh3Z+/TyxF7kHnQw7pRb0ML9BDyFn02790dvpakfOpzNNnmV7e  
PV510cxrXXIn5118Egx5ZktoVwUBNCvbeQB8lrMsk066/AfaGaQo2AiurR8zC7j3  
Qg70Tmw1Yj4oBMu7VdBZGe0baRGkjReGe40ea6IVrRY+N2k+9vPRxYURqgIhalJR  
miza5YcUbcUq80OuBwtR+fp2o5019Rd/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.

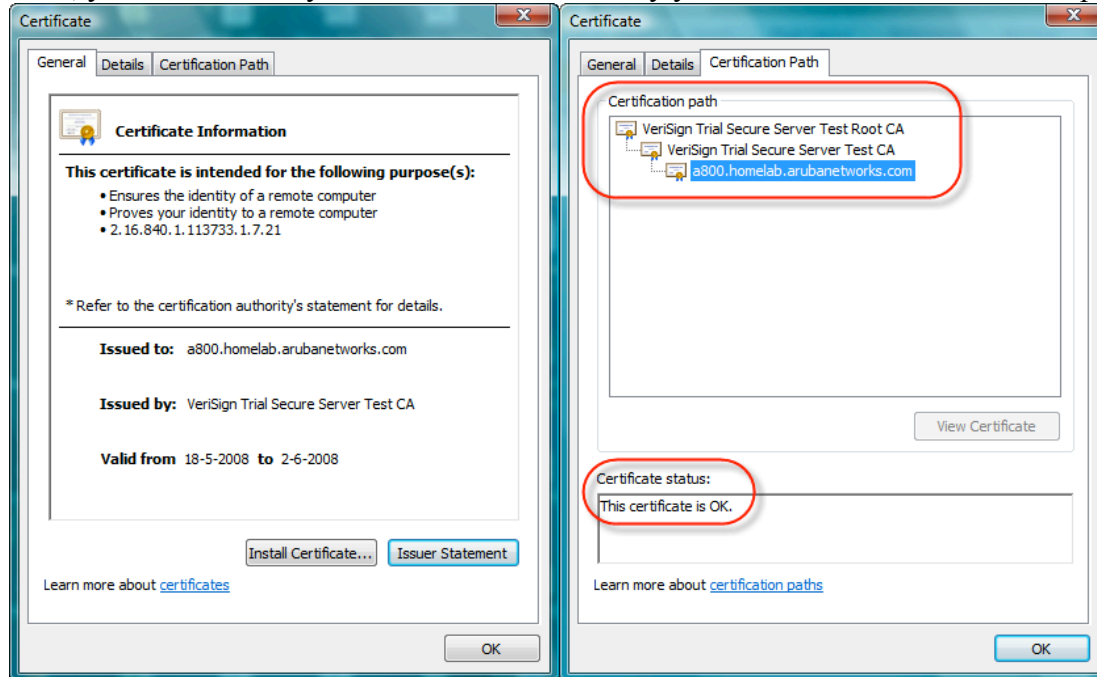
##### For Netscape Browsers

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.

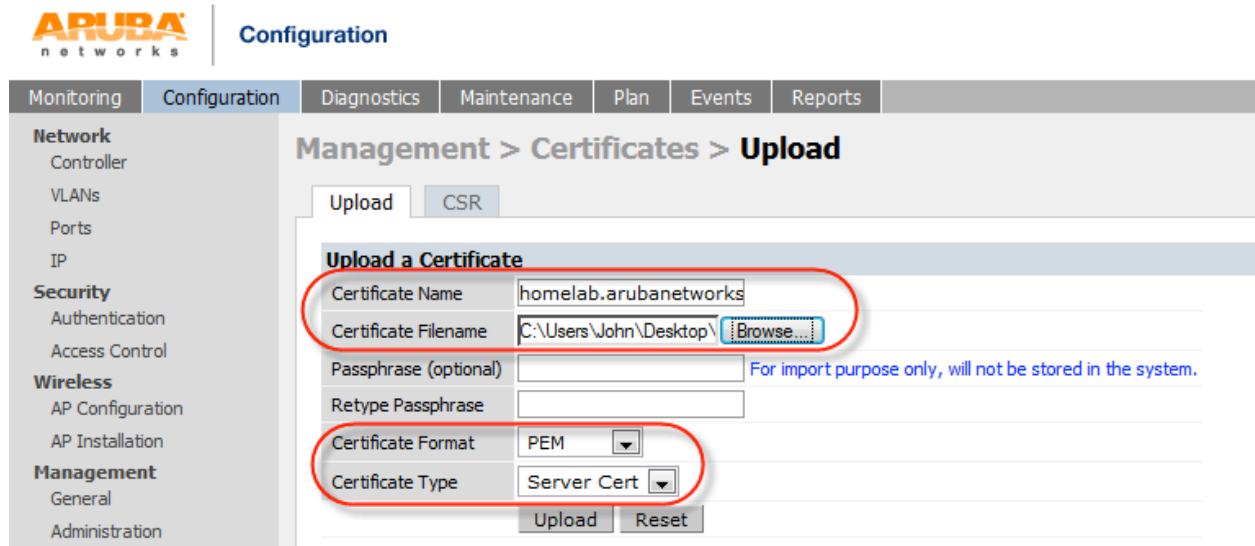
##### For Firefox Browsers

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

ARUBA networks Configuration

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Save Configuration

Management > Certificates > Upload

Upload CSR

**Upload a Certificate**

Certificate Name

Certificate Filename

Passphrase (optional)  For import purpose only, will not be stored in the system.

Retype Passphrase

Certificate Format

Certificate Type

**Certificate Lists**

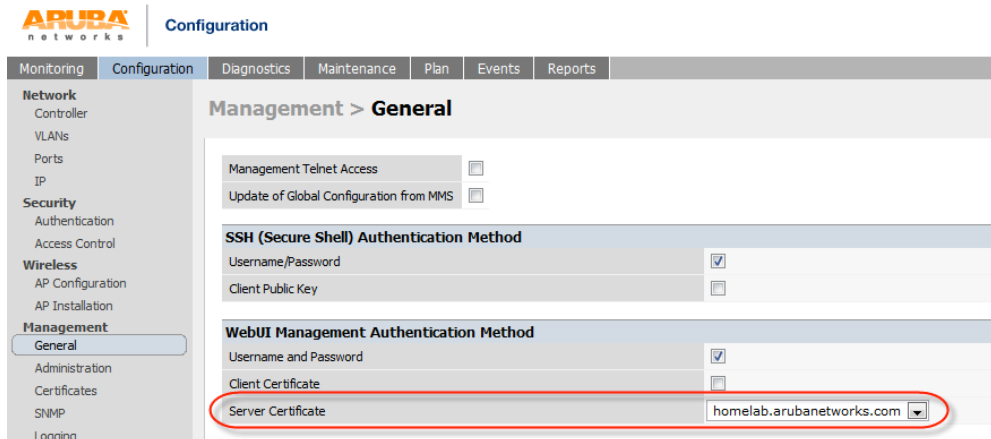
Group By:

| Name                      | Type       | Filename                      | Reference | Actions   |
|---------------------------|------------|-------------------------------|-----------|---|
| homelab-server-cert       | ServerCert | homelab.pem                   | 1         | <input type="button" value="View"/> <input type="button" value="Delete"/> |
| homelab.arubanetworks.com | ServerCert | version-trial-server-cert.cer | 2         | <input type="button" value="View"/> <input type="button" value="Delete"/> |
| homelab1                  | ServerCert | homelab1.pem                  | 0         | <input type="button" value="View"/> <input type="button" value="Delete"/> |
| nlabs-server-cert         | ServerCert | nlabs-server-cert.cer         | 0         | <input type="button" value="View"/> <input type="button" value="Delete"/> |
| nlabs-ca                  | TrustedCA  | nlabs-trusted-ca.cer          | 0         | <input type="button" value="View"/> <input type="button" value="Delete"/> |

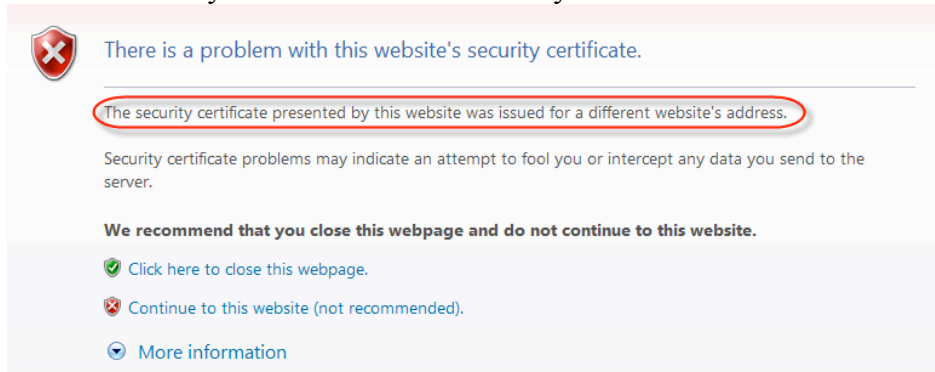


## Use certificate for WebUI management

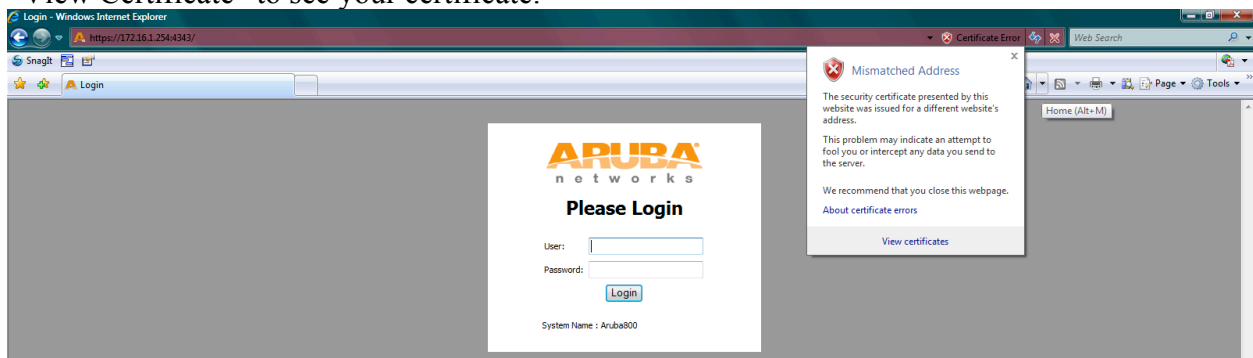
Go to Configuration -> Management -> General and select your certificate as server certificate for WebUI Management Authentication. This will restart the webserver so wait for 30 seconds before connecting



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.

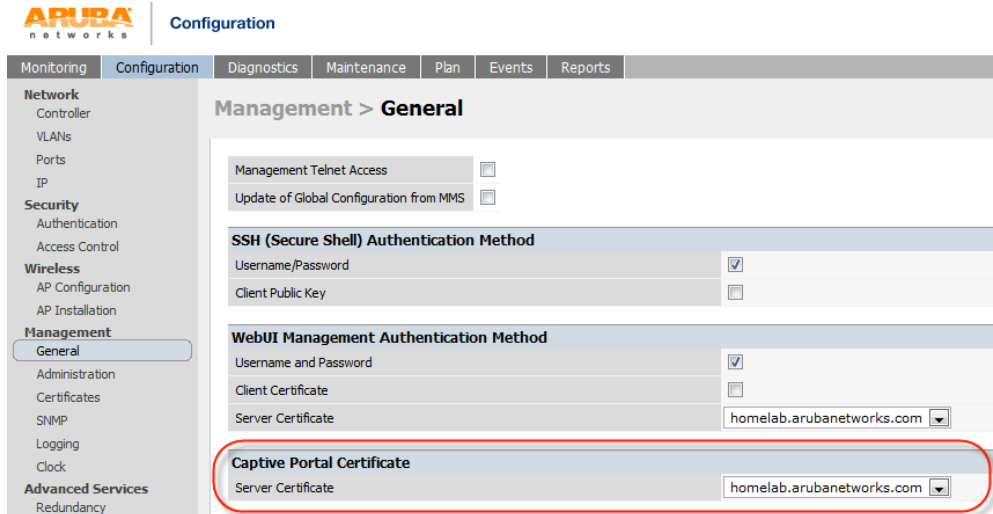


## Use certificate for Captive Portal

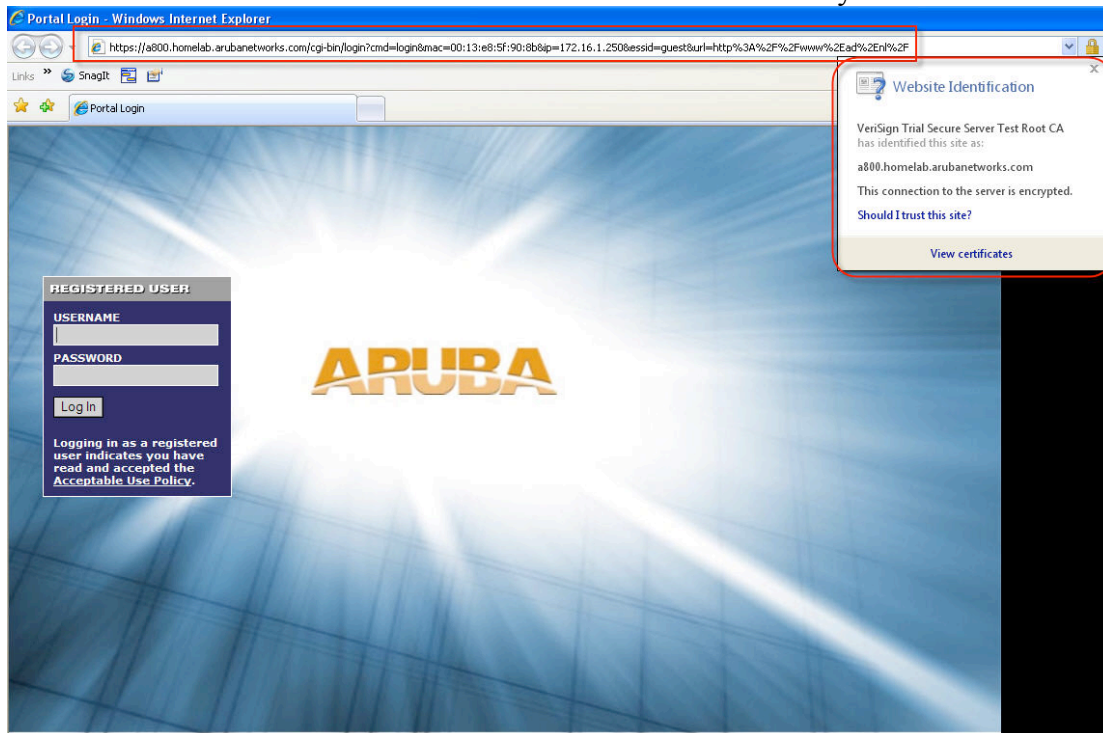
Normally the default captive portal will redirect you to `securelogin.arubanetworks.com` but this will change to whatever you used as CN in your certificate.

In this case it will be `a800.homelab.arubanetworks.com`

Go to Configuration -> Management -> General and select your 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

The screenshot shows the Aruba Configuration web interface. On the left, the 'Configuration' menu is expanded, and 'All Profiles' is selected. In the 'Profiles' list, the '802.1X Authentication Profile' is highlighted, and its sub-profile 'eap-termination' is selected. The 'Profile Details' tab is active, showing the 'Basic' configuration. The 'CA-Certificate' field is set to 'Server-Certificate' and 'homelab.arubanetworks.com'. The 'Server-Certificate' field is also highlighted with a red box.

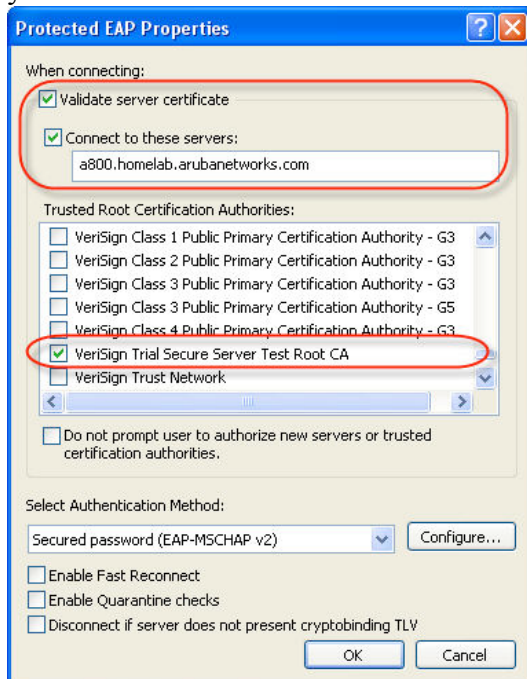
First check if the connection is established without checking the server certificate. When everything works as expected then you can select “Validate server certificate” and “Connect to these servers”

The screenshot shows the 'Protected EAP Properties' dialog box. The 'When connecting:' section has two checked options: 'Validate server certificate' and 'Connect to these servers:'. Below this, there is a list of 'Trusted Root Certification Authorities' with several entries. The 'Select Authentication Method:' dropdown is set to 'Secured password (EAP-MSCHAP v2)'. At the bottom, there are checkboxes for 'Enable Fast Reconnect', 'Enable Quarantine checks', and 'Disconnect if server does not present cryptobinding TLV'. The 'OK' button is highlighted.

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

The screenshot shows the Juniper Odyssey Configuration interface. On the left, the 'Configuration' menu is expanded, and 'All Profiles' is selected. In the 'Profiles' list, '802.1X Authentication Profile' is highlighted. The 'Profile Details' pane on the right shows the '802.1X Authentication Profile > eap-termination' configuration. The 'Basic' tab is active, and the 'Server-Certificate' is set to 'homelab.arubanetworks.com'. The 'CA-Certificate' is set to 'NONE'.

| 802.1X Authentication Profile > eap-termination           |   |
|---|---|
| Max authentication failures                               | 0   |
| Machine Authentication: Default Machine Role              | guest   |
| Bladlist on Machine Authentication Failure                | <input type="checkbox"/>  |
| Interval between Identity Requests                        | 30 sec  |
| Reauthentication Interval                                 | 86400 sec   |
| Multicast Key Rotation Time Interval                      | 1800 sec  |
| Authentication Server Retry Interval                      | 30 sec  |
| Framed MTU  | 1100 bytes  |
| Maximum Number of Reauthentication Attempts               | 3   |
| Dynamic WEP Key Message Retry Count                       | 1   |
| Interval between WPA/WPA2 Key Messages                    | 1000 msec   |
| WPA/WPA2 Key Message Retry Count                          | 3   |
| Unicast Key Rotation                                      | <input type="checkbox"/>  |
| Opportunistic Key Caching                                 | <input checked="" type="checkbox"/>   |
| Use Session Key   | <input type="checkbox"/>  |
| xSec-MTU  | 1300 bytes  |
| Termination EAP-Type                                      | <input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-peap     |
| Token Caching   | <input type="checkbox"/>  |
| CA-Certificate  | --NONE--  |
| Enforce Machine Authentication                            | <input type="checkbox"/>  |
| Machine Authentication Cache Timeout                      | 24 hrs  |
| Machine Authentication: Default User Role                 | guest   |
| Quiet Period after Failed Authentication                  | 30 sec  |
| Use Server provided Reauthentication Interval             | <input type="checkbox"/>  |
| Unicast Key Rotation Time Interval                        | 900 sec   |
| Authentication Server Retry Count                         | 2   |
| Number of times ID-Requests are retried                   | 3   |
| Maximum number of times Held State can be bypassed        | 0   |
| Dynamic WEP Key Size                                      | 128 bits  |
| Delay between WPA/WPA2 Unicast Key and Group Key Exchange | 0 msec  |
| Multicast Key Rotation                                    | <input type="checkbox"/>  |
| Reauthentication  | <input type="checkbox"/>  |
| Validate PMKID  | <input type="checkbox"/>  |
| Use Static Key  | <input type="checkbox"/>  |
| Termination   | <input checked="" type="checkbox"/>   |
| Termination Inner EAP-Type                                | <input checked="" type="checkbox"/> eap-mschapv2 <input type="checkbox"/> eap-gtc |
| Server-Certificate  | homelab.arubanetworks.com   |

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

The screenshot shows the 'Profile Properties' dialog box with the 'Authentication' tab selected. The 'Authentication protocols, in order of' list contains 'EAP-PEAP'. The 'Validate server certificate' checkbox is checked. The 'Token card credentials' section shows 'Use my password' selected. The 'Anonymous name' field is empty.

Profile name: Lab

Authentication protocols, in order of

- EAP-PEAP

☒ Validate server certificate

Token card credentials

Credentials to use with EAP-FAST or EAP-PEAP when the inner method is EAP-GenericTokenCard or EAP-POTP:

☒ Use my password

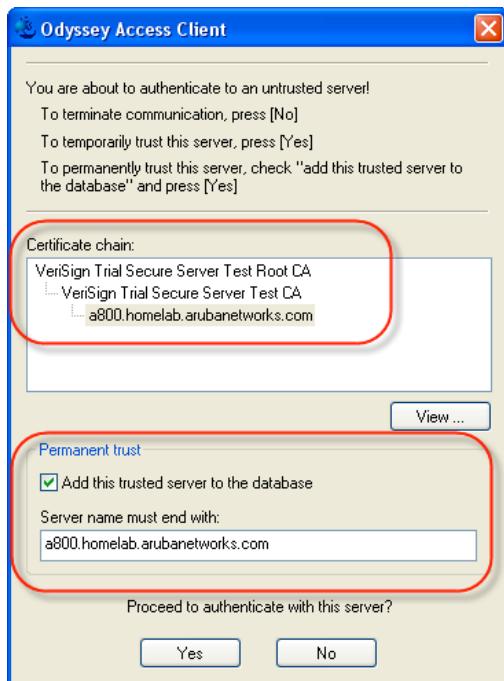
☐ Prompt for token information

Anonymous name:

(You can enter an anonymous name to keep your login name private with most EAP protocols.)

OK Cancel

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



## 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

```



