

# How to replace Aruba Default Certificate - April-MHC

## Why do you need to replace Aruba default certificate?

Have you ever tried to replace Aruba default certificate issued by GeoTrust DV SSL CA to securelogin.arubanetworks.com. You found many reasons to change and read many articles how to do it, but it seemed too many details, you gave up and forgot about it because things are still working.

Let's try it again, at least, for the benefit shows in figure 1, the problem with security certificate.

This article based on Windows 2012 ROOT-CA. Assuming you have - or you can request - a certificate from your ROOT-CA.

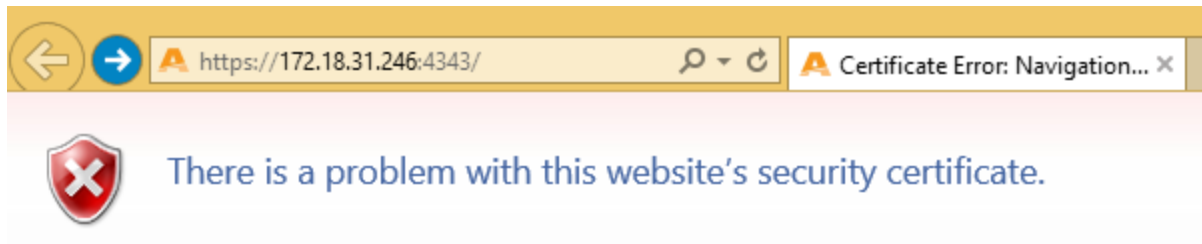


Figure 1: By replacing default certificate, you can get rid of this annoying security certificate problem.

## Getting the Certificate

Generate CSR at the controller

The screenshot shows the Aruba Mobility Controller web interface. The top navigation bar includes the Aruba Networks logo, the text "MOBILITY CONTROLLER | Aruba3600", and tabs for "Dashboard", "Monitoring", "Configuration" (which is active), "Diagnostics", and "Maintenance". A "Save Configuration" button is located on the right. On the left side, there is a sidebar menu with categories: "WIZARDS" (containing AP, Controller, Campus WLAN, Remote AP, WIP, AirWave), "NETWORK" (containing Controller, VLANs, Ports, Cellular Profile, IP), and "SECURITY" (containing Authentication, Access Control). The main content area is titled "Management > Certificates > CSR". Below this title are three tabs: "Upload", "CSR" (which is active), and "Revocation CheckPoint". The "CSR Information" section contains a form with the following fields: "CSR Type" (a dropdown menu set to "rsa"), "Key Length" (a dropdown menu set to "2048"), "Common Name" (a text box containing "172.18.31.246"), "Country" (a text box containing "US"), "State/Province" (a text box containing "NE"), "City" (a text box containing "OMAHA"), "Organization" (a text box containing "HOME"), "Unit" (a text box containing "LAB"), and "Email Address" (a text box containing "me@lab.net"). At the bottom of the form are three buttons: "Generate New", "Reset", and "View Current".

Figure 2: This step is straight forward. Make sure the **Common Name is the name you are using to access your controller**. In this lab, I use <https://172.18.31.246:4343>, so the CN is 172.18.31.246. Although the Key Length minimum is 1024, but the standard is 2048, many Root-CA are no longer support 1024.

## Request certificate

Click Generate New, and copy the text between -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- inclusive. Save to a text file.

HTTPS to your Root-CA

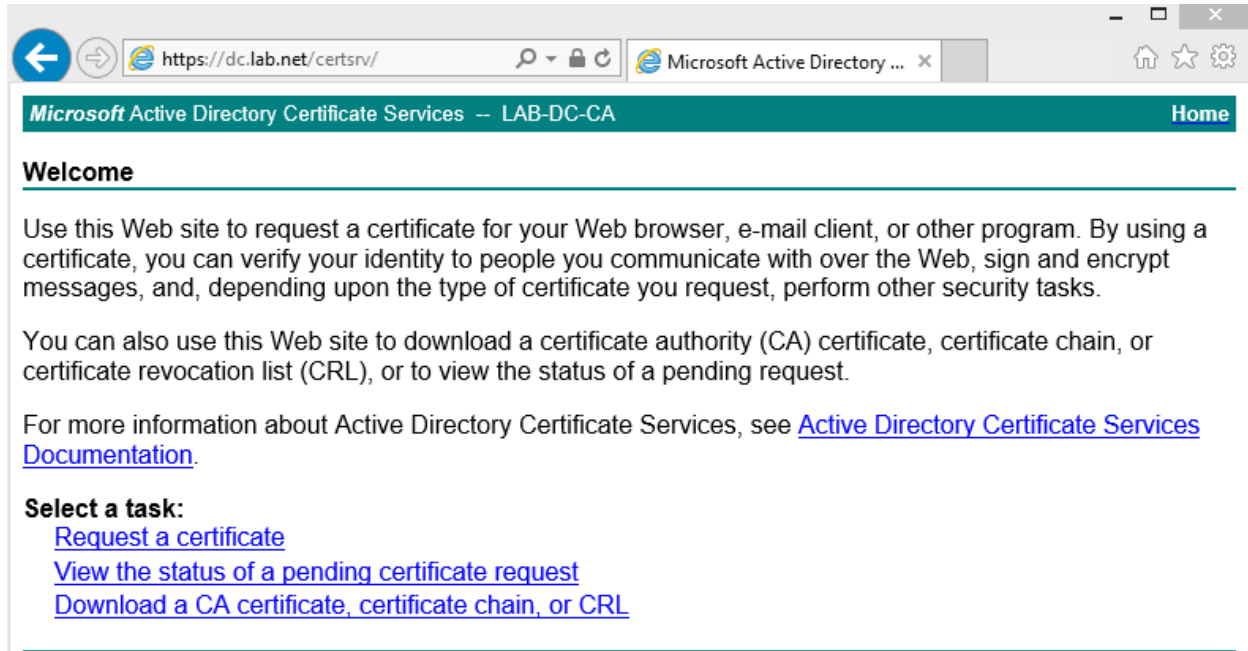


Figure 3: Https to Root-CA, click Request a certificate

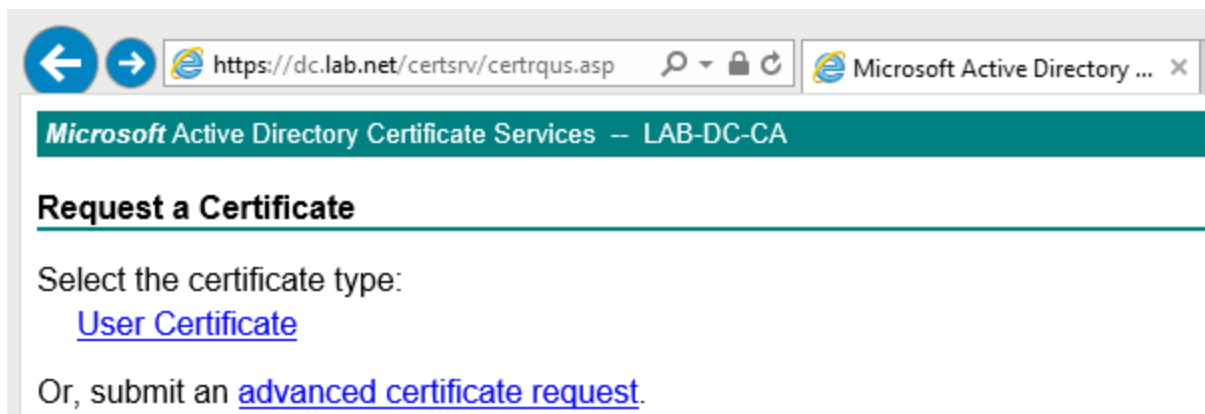


Figure 4: Click submit an "advanced certificate request"

← → <https://dc.lab.net/certsrv/certrqxt.asp> Microsoft Active Directory ...

Microsoft Active Directory Certificate Services -- LAB-DC-CA Home

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIICvzCCAacCAQAweljELMAkGA1UEBhMCVVMxCzAJ
DAVPTUFIQTENMAzGA1UECgwESE9NRTEMMAoGA1UE
NzIuMTguMzEuMjQ2MRkwFwYJKoZIhvcNAQkBFgpt.
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAYmXxU1jx
jm7KB6xFiMUUAeRwmhtey8akEoyueGAp3pynNjAv
-----
```

**Certificate Template:**

Web Server

**Additional Attributes:**

Attributes:

Submit >

Figure 5: Paste the CSR that you saved to txt file in figure 2 above to Saved Request, **change Certificate Template to Web Server**, click Submit.

← → <https://dc.lab.net/certsrv/certifnsh.asp> Microsoft Active Directory ...

Microsoft Active Directory Certificate Services -- LAB-DC-CA

### Certificate Issued

The certificate you requested was issued to you.

☒ DER encoded or ☐ Base 64 encoded


 [Download certificate](#)  
[Download certificate chain](#)

Figure 6: Keep default DER encoded, click "Download certificate", and save it. In my Root-CA, I configured the server to automatic assign certificate, so I can download the certificate right after I submit. Some root-CA requires you come back later to download after the administrator issue it.

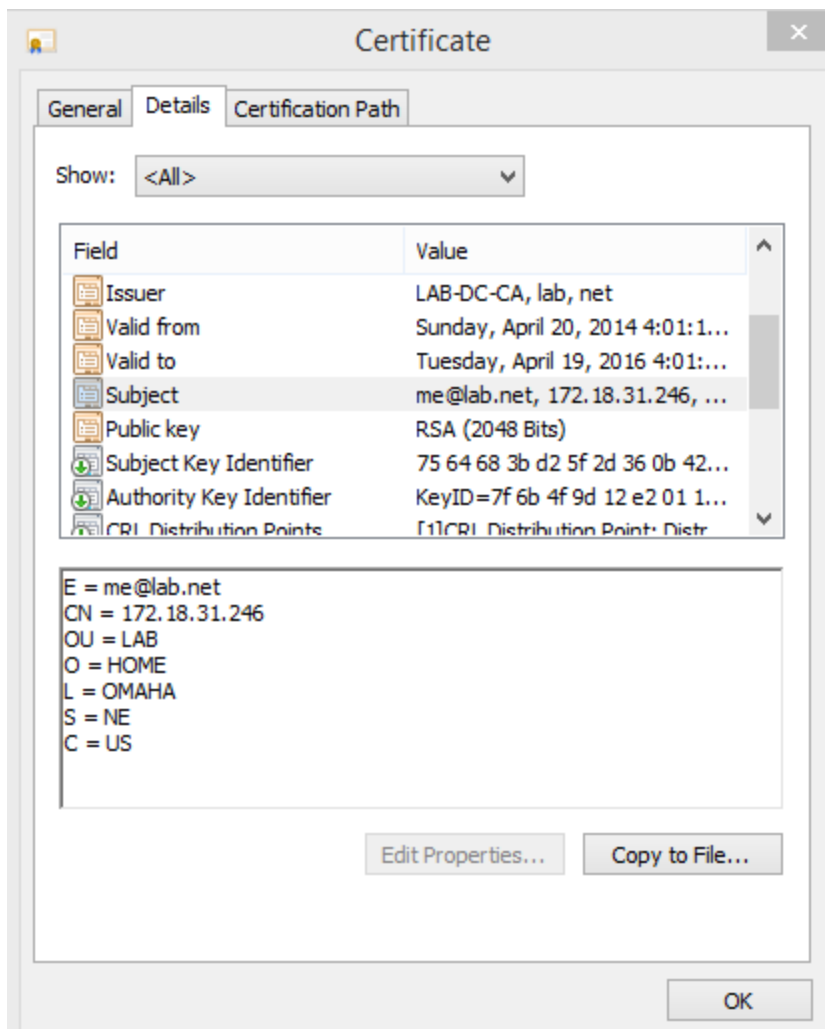


Figure 7: You can view the detail of certificate you just saved to ensure it is the right one

## Install Certificate to Controller

**Configuration** Diagnostics Maintenance Save Configuration

**Management > Certificates > Upload**

Upload CSR Revocation CheckPoint

**Upload a Certificate**

Certificate Name	<input type="text" value="WEB_SERVER2"/>
Certificate Filename	<input type="button" value="Choose File"/> <input type="text" value="certnew.cer"/>
Passphrase (optional)	<input type="text"/> For import purpose only,
Retype Passphrase	<input type="text"/>
Certificate Format	DER ▼
Certificate Type	Server Cert ▼

Figure 8: To install certificate to controller, click Management > Certificates > Upload. Give it a name, find the certificate you downloaded. Default name is download\certnew.cer

Configuration

Diagnostics

Maintenance

Save Configuration

Management > General

Management Telnet Access

☐

WebUI HTTPS Port (443) Access

☐

SSH (Secure Shell) Authentication Method

Username/Password

☒

Client Public Key

☐

WebUI Management Authentication Method

Username and Password

☒

Client Certificate

☒

Server Certificate

WEB\_SERVER2 ▾

WebUI Idle Logout Timer

User session timeout

900 (seconds)

Captive Portal Certificate

Server Certificate

WEB\_SERVER2 ▾

Configure Cipher LOW/MEDIUM/HIGH

Web Server Ciphers

High ▾

Figure 9: Configure controller to use new certificate for WebUI Management Authentication and Captive Portal. Click Apply, Save Configuration, and log out.

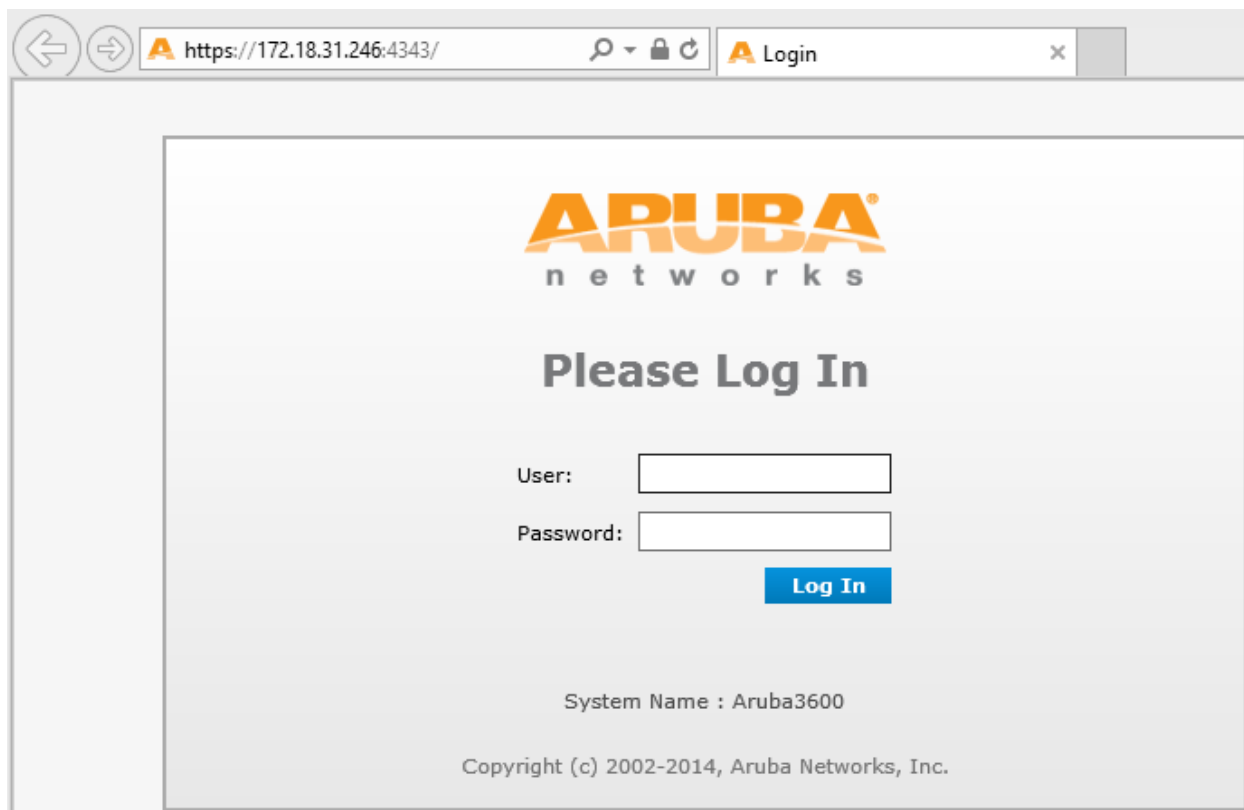


Figure 10: Log back to controller, no more Problem with Website Security Certificate