

Support Advisory:

ArubaOS Default Certificate Expiration

Issued October 10, 2013

This document, including the information it contains and the programs made available through the links that it includes, is provided to you on an "as is" basis. ARUBA AND ITS SUPPLIERS DO NOT WARRANT THAT SUCH INFORMATION OR THE FUNCTIONS CONTAINED IN SUCH PROGRAMS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PROGRAMS WILL BE UNINTERRUPTED OR ERROR-FREE. THE INFORMATION AND PROGRAMS ARE PROVIDED TO YOU WITH NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IN NO EVENT WILL ARUBA, ITS SUPPLIERS, OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE INFORMATION OR PROGRAMS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOST DATA, THAT MAY ARISE OUT OF YOUR USE OF OR FAILURE TO USE THE INFORMATION OR PROGRAMS, EVEN IF ARUBA OR SUCH OTHER ENTITIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING SHALL NOT BE DEEMED TO PRECLUDE ANY LIABILITY WHICH, UNDER APPLICABLE PRODUCTS LIABILITY LAW, CANNOT BE PRECLUDED BY CONTRACT.

This document is being provided to you pursuant to the provisions of your applicable software license agreement with Aruba, and the information and programs may be used only pursuant to the terms and conditions of such agreement. This Aruba Security Advisor constitutes Aruba Proprietary Information and should not be disseminated, forwarded or disclosed.

SUMMARY

The default "Server Certificate" in older ArubaOS releases installed on your Mobility Controllers and Mobility Access Switches will expire on November 21, 2013.

While this default certificate was never intended for production use, Aruba is aware that a number of our customers are using this certificate in the production networks typically for Administrative WebUI and securing the Captive Portal login screen in guest networks.

On Mobility Controllers running ArubaOS_6.1.3.8 or ArubaOS_5.0.4.12 and earlier, and Mobility Access Switches running ArubaOS_MAS_7.2.3.0 and earlier, customers using the default Server Certificate should expect to experience following issues when the default certificate expires on 11/21/2013.

1. Users connecting to Captive Portal or Controller's WebUI will receive a browser warning showing that the server certificate has expired.

Workaround: Users may bypass the warning (with varying degrees of difficulty depending on the browser) and continue on to use the system normally.

If EAP termination has been enabled for 802.1X, and the default certificate is being used as the server certificate, many client operating systems will refuse to continue the authentication process. This will result in an apparent network outage for these users. Client operating systems may or may not display a warning message to the user.

Workaround: Disable EAP termination on the controller or switch and let the clients complete EAP exchanges directly with the authenticator (RADIUS server) as long as the RADIUS Server has a Server Certificate installed whose Root/Issuing Certificate Authority is trusted by the clients.

SOLUTION

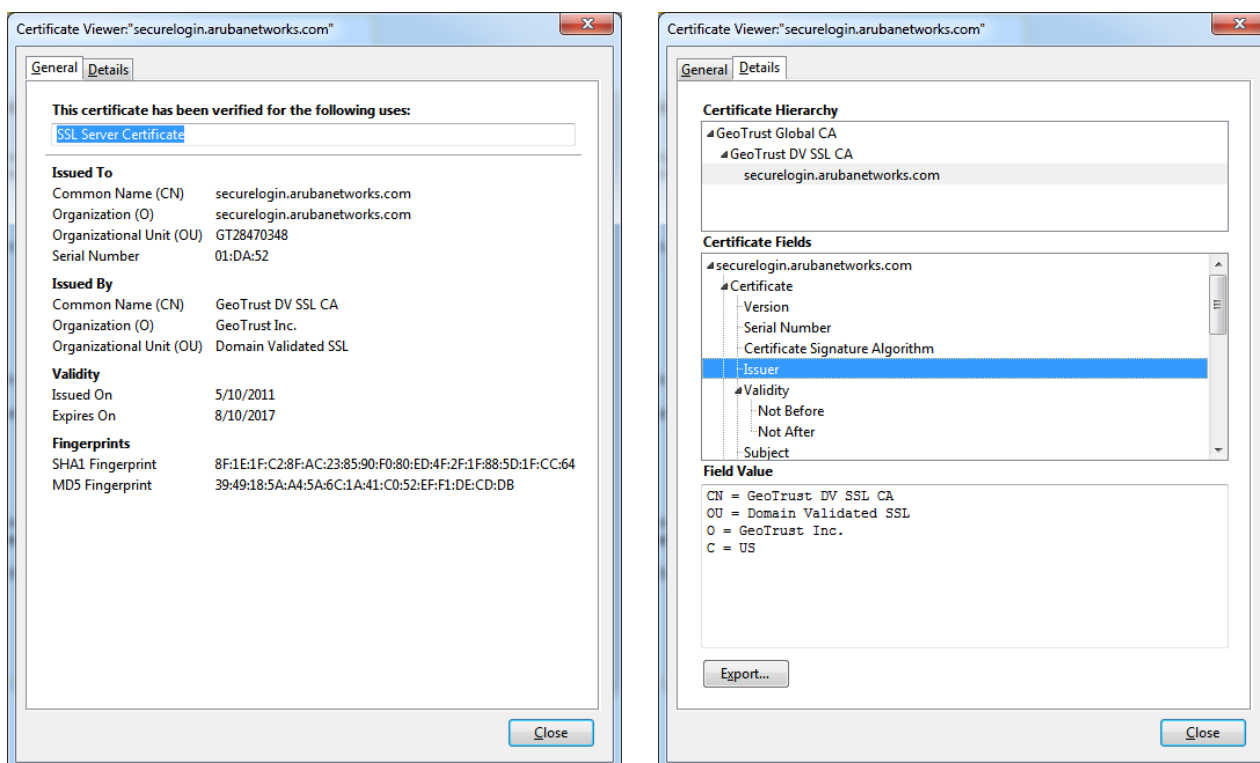
Aruba Networks recommends the following two options, in order of preference, to replace the default certificate installed on the controllers.

- **Option 1:** Replace the default certificate with a certificate issued by an internal certificate authority or a public certificate authority. *This option provides the greatest security*.
- **Option 2:** Upgrade ArubaOS software
 - On Mobility Controllers running :
 - 6.1.3.8 and earlier – upgrade to ArubaOS 6.1.3.9 or later
 - 5.0.4.12 and earlier – upgrade to ArubaOS 5.0.4.13 or later
 - On Mobility Access Switches running –
 - 7.2.3.0 and earlier – upgrade to ArubaOS 7.2.3.1 (available Oct 30, 2013)

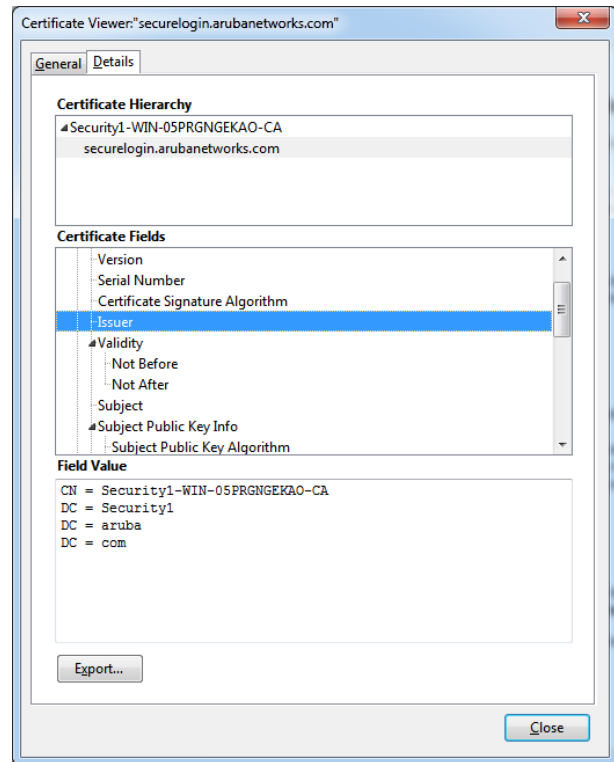
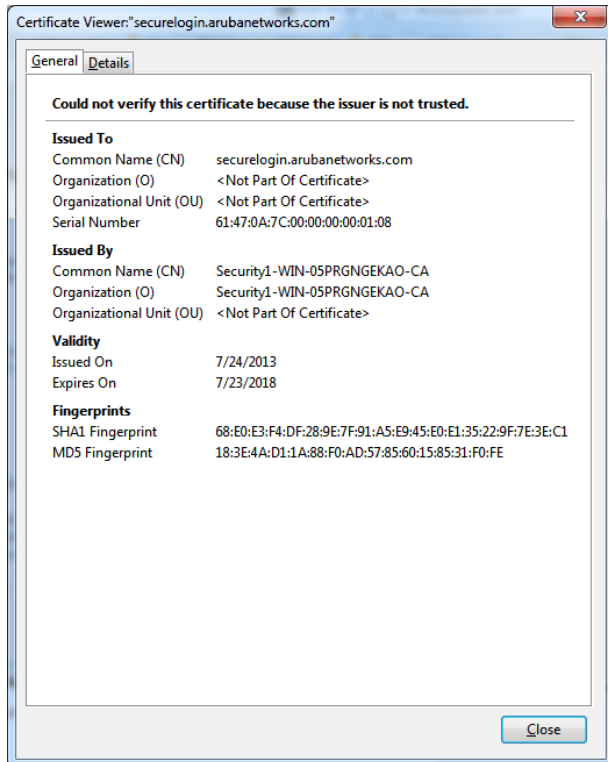
This option however, does not provide good security because all Aruba controllers have the same certificate and impersonation attacks are possible.

NOTE:

1. The new certificate for “securelogin.arubanetworks.com” in ArubaOS 6.x and ArubaOS 7.x is obtained from a public CA – GeoTrust DV SSL CA and is valid until August 11, 2017 (8/11/2017 4:40:59 AM GMT).



2. ArubaOS 5.x accepts only 1024-bit Server Certificate for Administrative WebUI. Since Public Certificate Authorities no longer issue a 1024-bit certificate, the new certificate included in ArubaOS 5.0.4.13 is a self-signed cert. Therefore, if the default server certificate is used and EAP-termination is enabled on the controller for 802.1x authentication, clients will not be able to verify the Server Certificate unless it is loaded into their Certificate Store/keychain.

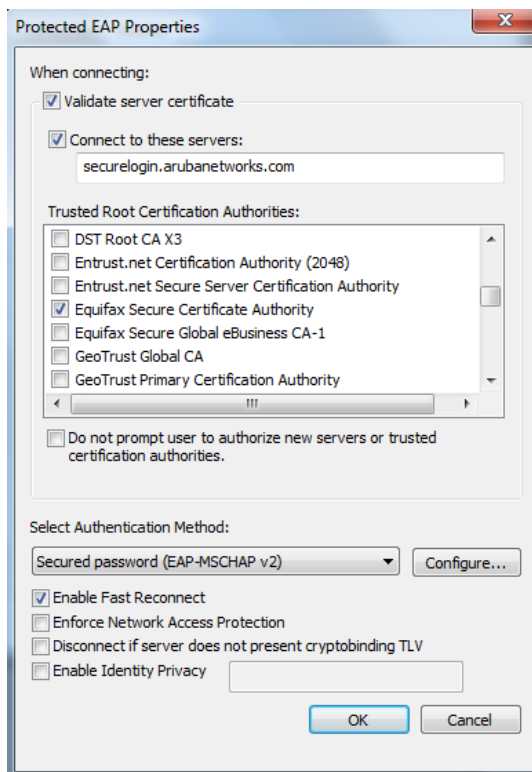


FAQ

Q_1: How does this expiring Server Certificate affect Aruba Instant?

A_1: The new Server Certificate is already included in Aruba Instant software versions starting with 6.1.3.4_3.1.0.0.

Q_2: What happens if I have configured 802.1X devices in my network to only trust the *securelogin.arubanetworks.com* certificate, or to only trust the Equifax Secure Certificate Authority?



A_2: These devices will need to be reconfigured after installation of a new certificate. If these are Windows devices, UNCHECK “Connect to these servers” and UNCHECK “Equifax Secure Certificate Authority” in the Trusted Root Certification Authorities. After connecting to the controller with the new certificate installed, Windows will update these settings by prompting the user.

Q_3: Is the certificate built into the TPM chip affected by this advisory?

A_3: No. All Aruba controllers that contain a Trusted Platform Module (TPM), including the M3, 3000 series, 600 series and 7200 series, contain a certificate unique to the controller that has been programmed at the factory. This certificate is not expiring and is not affected by this advisory. This certificate is used for Master-Local authentication, Control Plane Security (CPsec), and RAP authentication. It is not suitable for use as an SSL certificate since it was issued by Aruba's manufacturing CA, which is not trusted by browsers.

Q_4: How do I install a unique Server Certificate?

A_4: This is the recommended approach since it provides the best security. In this approach, the default certificate will remain on the controller, but you will load one or more new certificates and then configure the system to use the new certificate(s).

If your organization operates an internal certificate authority (CA) and all clients that will use the system already trust the internal CA, you may use the internal CA to issue a new certificate to the controller. This option is recommended for 802.1X EAP termination and WebUI administrative access to the controller. It can also be used for captive portal as long as the general public will not be accessing the system (since the internal CA will not be trusted, the general public would receive browser warnings.)

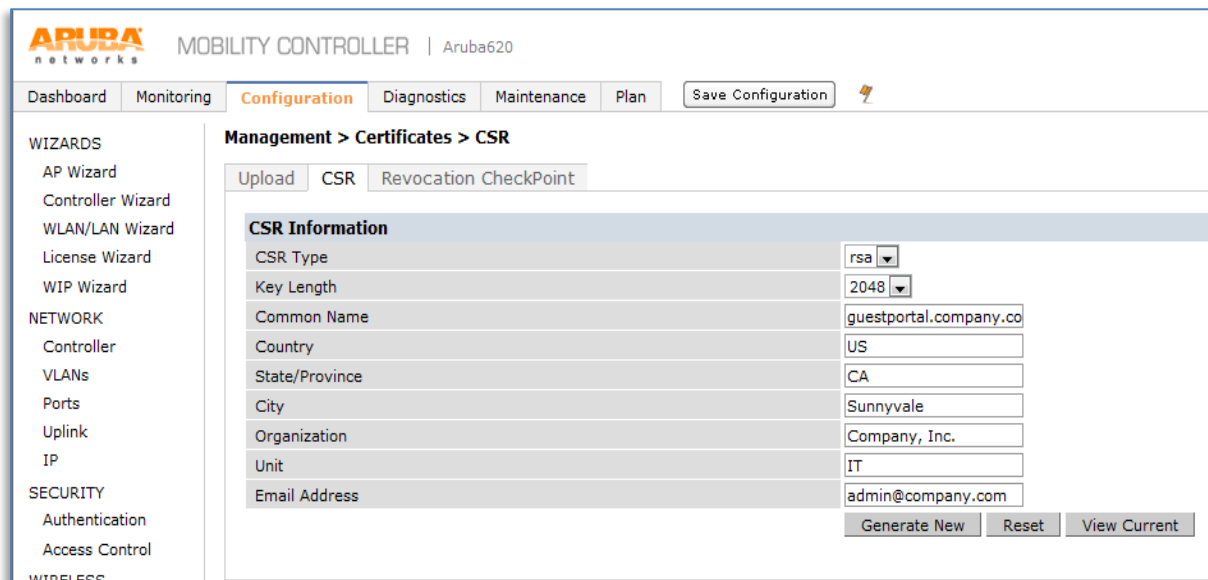
If presenting a captive portal page to computers owned by the general public, a certificate issued by a public CA (VeriSign, GeoTrust, Comodo, etc.) should be used so that browser warnings are not generated. You may choose to use a certificate issued by a public CA for WebUI administrative access to the controller and for 802.1X EAP termination as well, but use of a public CA instead of an internal CA provides no benefit in those cases.

Before requesting a certificate, decide whether you need a 1024-bit key, 2048-bit key, or 4096-bit key. Note that many public CAs no longer issue certificates with 1024-bit keys.

- If you are running ArubaOS 6.1 or greater, you may use a certificate with a 2048-bit key for any purpose. You may use a certificate with a 4096-bit key only for captive portal and WebUI. For WebUI or captive portal, performance is the greatest with smaller key sizes, but security is slightly reduced. To maximize compatibility, always use RSA unless you have a specific reason to use ECC.
- If you are running any release prior to 6.1, you may use a certificate with a 2048-bit or 4096-bit key only for captive portal and WebUI. 802.1X EAP termination supports only 1024-bit keys. For WebUI or captive portal, performance is the greatest with smaller key sizes, but security is slightly reduced.

The following instructions should be followed to obtain and install a server certificate.

1. Generate a Certificate Signing Request (CSR) from the controller by navigating to Configuration→Management→Certificates→CSR. Fill out the necessary fields. After clicking “Generate New”, the controller will generate a private key, which remains locked inside the controller, and a base64-encoded CSR. The CSR contains all the details needed for your CA to issue the certificate. The Common Name (CN) field should contain the full URL that web browsers will navigate to in order to reach the controller’s embedded web server. Take care to fill out the Common Name field correctly according to the purpose of the certificate:
 - a. For captive portal, the system will automatically issue HTTP redirects and spoof DNS responses to the captive portal client so that the browser appears to be connecting to the correct DNS name that matches the certificate common name. This is to ensure that browser warnings are not generated. If the certificate is only being used for captive portal, the name in the CN field is unimportant – but make sure it falls within your domain name so that a public CA will correctly authorize ownership of the certificate.
 - b. For WebUI, the CN field should match the address you use to manage the controller. This can be an IP address or a Fully Qualified Domain Name (FQDN).
 - c. For 802.1X EAP Termination, the CN field is not matched by the client against any other parameter. It is suggested that you choose a FQDN that is owned by your organization.



The screenshot shows the Aruba Mobility Controller web interface. The top navigation bar includes 'Dashboard', 'Monitoring', 'Configuration' (selected), 'Diagnostics', 'Maintenance', and 'Plan'. A 'Save Configuration' button is visible. The left sidebar lists various configuration categories: WIZARDS, NETWORK, SECURITY, and WIRELESS. The main content area is titled 'Management > Certificates > CSR'. Below this, there are tabs for 'Upload', 'CSR' (selected), and 'Revocation CheckPoint'. The 'CSR Information' section contains a form with the following fields:

- CSR Type: dropdown menu set to 'rsa'
- Key Length: dropdown menu set to '2048'
- Common Name: text input field containing 'guestportal.company.co'
- Country: text input field containing 'US'
- State/Province: text input field containing 'CA'
- City: text input field containing 'Sunnyvale'
- Organization: text input field containing 'Company, Inc.'
- Unit: text input field containing 'IT'
- Email Address: text input field containing 'admin@company.com'

 At the bottom right of the form are three buttons: 'Generate New', 'Reset', and 'View Current'.

2. Click on “View Current”. Copy the base64 text shown, and paste this into the certificate request window provided by your certificate authority.

CSR Information

Subject


C=US
L=Sunnyvale
O=Company Inc.
OU=IT
CN=guestportal.company.com
emailAddress=admin@company.com

-----BEGIN CERTIFICATE REQUEST-----

MIIC3DCCAcQCAQAwZyxCZAJBgNVBAYTA1VTMQswCQYDVQQLIEwJDQTESMBAGA1UEBxMJU3Vubnl2YWxlMRUwEwYDVQKEwDb21wYW55IEluYy4xCZAJBgNVBAsTAk1UMSAwHgYDVQQDExdndWVzdHBvcnRhC5jb21wYW55LmNvbTEgMB4GCSqGSIb3DQEJARYRYWRtaW5AY29tcGFueS5jb20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK AoIBAQDYnjrVx1b602pCu7vk6dVJWPSfSXUDI0k7Jvt94C7/zaM+iTbS5rrI0cAF UZj5bx68wAlStTdrMoN1V5SN9cmtFaSDLRrwCd2tGjZcP+/hC2mv39e+x1Y1SU0Z 1SSNc4aGTs0C19q50Ek1FwM1UAEIo9yr5IIo9pgCC1iRVAg2J02PewPVTdkHGx3t lMMhGcwz8JjgUeHk9QIVRTp4dwCzC16ICuH3rRhL8CV5/vee/RH/kbMwTNyM/iWi HniQFe9amj3l6j4lu5kuKHAhCEIPKLhNN1Wo5DYK/p5hEBATugw115hoTjKXmqQ NkH0oxD14lQoEyK0zAGDPwHG1455AgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEA Q8dX7ztuBQ3l08q3GcwVE1/e7MgbpphgyV1AHqfRxeFHI75kv4YAG7QcAWQJtGjR ZWpm/b9zim8aTJmrR1yAkWleQNX1Vfv8Ev365Sz1IggcOdwtOyrtrIBx+S8L18wj sozgILB8/soY855nzaqZzcIeCZcN4/w/bjkulAFm6gvbqdNAIcnsKGD1Zms45Xbw yZPmboDhM/9/KhMZ26J8i26vbv8r4vBvH2/hT4W/FQyqlmubJT8j4TSQHVHq9M5h

OK

- Once you have obtained the certificate, navigate to Configuration→Management→Certificates→Upload and upload the certificate to the controller. The certificate will most likely be provided to you in PEM or DER format – if you are not sure which format it is in, try PEM first and if an error message results, try DER. A PEM format certificate will be base64-encoded and will begin with the text “-----BEGIN CERTIFICATE-----”.


MOBILITY CONTROLLER | Aruba620

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Plan | Save Configuration

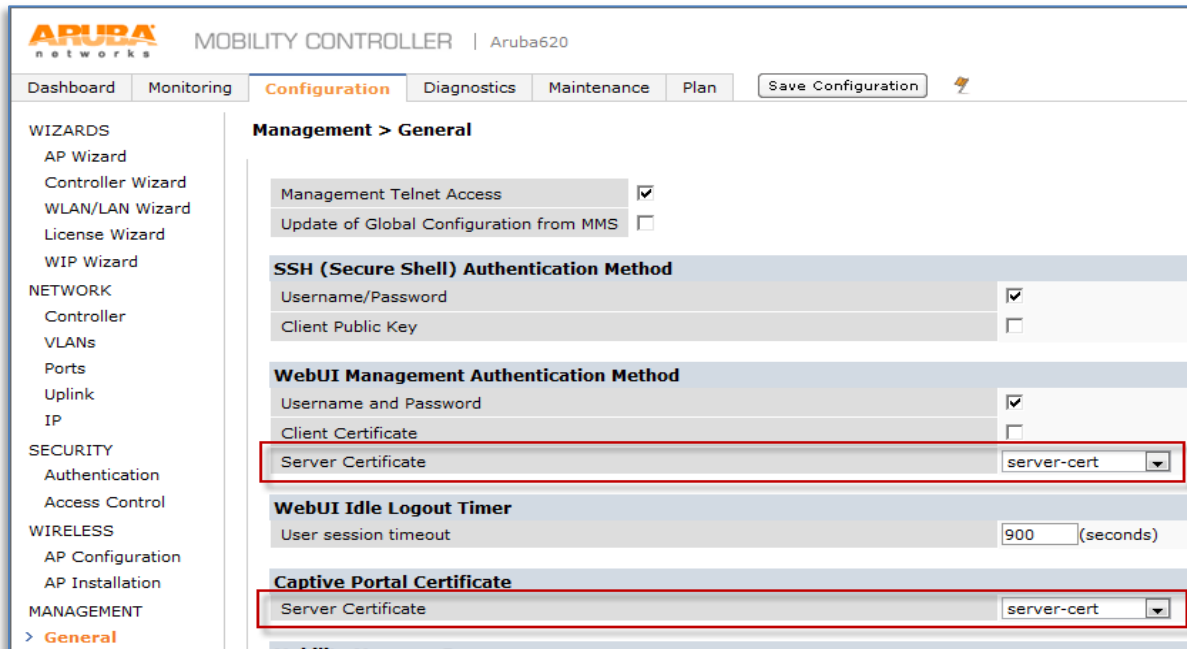
WIZARDS
AP Wizard
Controller Wizard
WLAN/LAN Wizard
License Wizard
WIP Wizard
NETWORK
Controller
VLANs
Ports
Uplink
IP

Management > Certificates > Upload
Upload | CSR | Revocation CheckPoint

Upload a Certificate

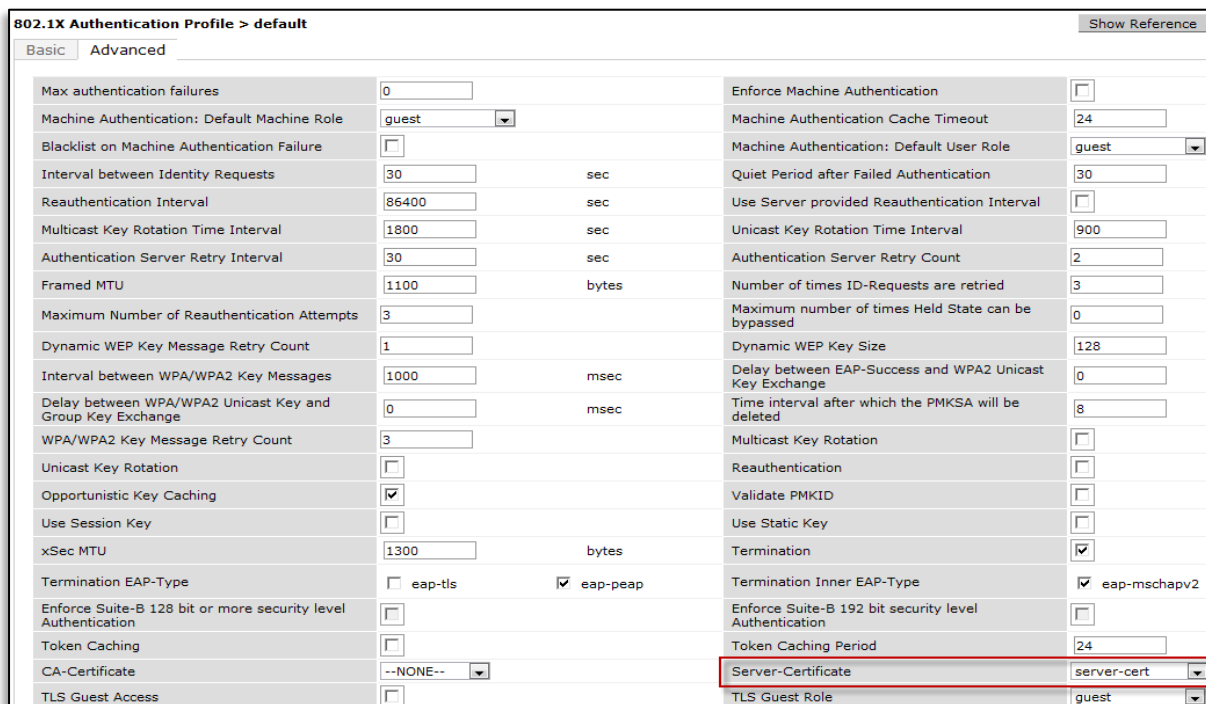
Certificate Name
Certificate Filename Browse...
Passphrase (optional) For import purpose only, will not be stored in the system.
Retype Passphrase
Certificate Format
Certificate Type
Upload Reset

- If you want to use the new certificate for captive portal, navigate to Configuration→Management→General and change the Captive Portal Server Certificate. If you want to use the new certificate for WebUI, configuration is found on the same screen under “WebUI Management Authentication Method”.



The screenshot shows the Aruba Mobility Controller configuration interface. The left sidebar lists various configuration categories: WIZARDS, NETWORK, SECURITY, WIRELESS, and MANAGEMENT. The 'General' tab is selected under MANAGEMENT. The main content area is titled 'Management > General'. It contains several sections: 'Management Telnet Access' (checked), 'Update of Global Configuration from MMS' (unchecked), 'SSH (Secure Shell) Authentication Method' (Username/Password checked, Client Public Key unchecked), 'WebUI Management Authentication Method' (Username and Password checked, Client Certificate unchecked, Server Certificate dropdown set to 'server-cert'), 'WebUI Idle Logout Timer' (User session timeout set to 900 seconds), and 'Captive Portal Certificate' (Server Certificate dropdown set to 'server-cert'). The 'Server Certificate' dropdowns are highlighted with red boxes.

- If you want to use the new certificate for EAP Termination, navigate to Configuration→Security→Authentication→L2 Authentication→802.1X Authentication Profile→Advanced and change the server certificate for all active 802.1X authentication profiles that use EAP Termination.



The screenshot shows the '802.1X Authentication Profile > default' configuration page, specifically the 'Advanced' tab. The page contains a table of configuration parameters. The 'Server-Certificate' parameter is highlighted with a red box and is set to 'server-cert'. Other parameters include 'Max authentication failures' (0), 'Machine Authentication: Default Machine Role' (guest), '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), 'Delay between WPA/WPA2 Unicast Key and Group Key Exchange' (0 msec), 'WPA/WPA2 Key Message Retry Count' (3), 'Unicast Key Rotation' (unchecked), 'Opportunistic Key Caching' (checked), 'Use Session Key' (unchecked), 'xSec MTU' (1300 bytes), 'Termination EAP-Type' (eap-peap checked), 'Enforce Suite-B 128 bit or more security level' (unchecked), 'Token Caching' (unchecked), 'CA-Certificate' (--NONE--), 'TLS Guest Access' (unchecked), 'Enforce Machine Authentication' (unchecked), 'Machine Authentication Cache Timeout' (24), 'Machine Authentication: Default User Role' (guest), 'Quiet Period after Failed Authentication' (30), 'Use Server provided Reauthentication Interval' (unchecked), 'Unicast Key Rotation Time Interval' (900), '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), 'Delay between EAP-Success and WPA2 Unicast Key Exchange' (0), 'Time interval after which the PMKSA will be deleted' (8), 'Multicast Key Rotation' (unchecked), 'Reauthentication' (unchecked), 'Validate PMKID' (unchecked), 'Use Static Key' (unchecked), 'Termination' (checked), 'Termination Inner EAP-Type' (eap-mschapv2 checked), 'Enforce Suite-B 192 bit security level Authentication' (unchecked), 'Token Caching Period' (24), and 'TLS Guest Role' (guest).