Support Advisory:
ArubaOS Default Certificate Expiration

Issued February 14, 2011

Summary

On June 29, 2011 the default SSL/TLS certificate “securelogin.arubanetworks.com” that is installed on all Aruba controllers will expire. While this default certificate was never intended for production use, Aruba is aware that a number of customers are using this certificate in production networks. These customers will need to replace the certificate. Affected customers have two options:

1. Replace the default certificate with a certificate issued by an internal certificate authority or a public certificate authority. This option is recommended and provides the greatest security.
2. Upgrade the ArubaOS image to a version number equal to or greater than 3.4.4.1, 5.0.3.2, 6.0.1.0, or 6.1.0.0. These software images contain a new default certificate that will replace the expiring certificate. This option does not provide good security, since all Aruba customers have access to the same certificate and impersonation attacks are possible.

Background

The ArubaOS operating system loaded on all Aruba Mobility Controllers contains a pre-loaded digital certificate with the name “securelogin.arubanetworks.com”. This certificate was issued by a public certificate authority (CA) that is trusted by most browsers and operating systems. By default the certificate is used for the controller’s management interface (WebUI), captive portal, and EAP termination. This certificate is intended for quickly setting up lab networks, demonstrations, and proof-of-concept deployments. As stated in the user guide, the default certificate is not intended for production deployment, since every Aruba controller contains the same certificate and this enables impersonation attacks. The following text summarizes the risks:

- Captive Portal: An attacker impersonating a captive portal login screen may be able to obtain the username and password of authorized users on the system. If captive portal is used only for guest access, this may not be deemed a serious security risk. If captive portal is used to authenticate internal users, this attack could cause more serious damage.
- Administrative WebUI: To carry out an impersonation attack against the controller’s administrative WebUI, the attacker would need to intercept traffic between a system administrator’s computer and the controller. This would typically require an insider attack, assuming administrative access is blocked from public networks. The risk is serious in this case, since a successful attack would allow an unauthorized person to obtain administrative credentials for the Aruba controller. The WebUI certificate should always be replaced, even if with a self-signed certificate that each system administrator must explicitly trust.
- 802.1X EAP Termination: This is the riskiest use of the default certificate, because an impersonation attack may be carried out over a wireless network, and a successful attack may reveal usernames and password hashes (providing material for an offline password cracking attempt) or allow the attacker to get a user connected to a hostile network while the user thinks he or she is connected to a trusted network. The default certificate should never be used for 802.1X.

Aruba is aware that some customers do use the default certificate in production, typically for securing the captive portal login screen in guest networks where ensuring the identity of the controller is not an important security consideration. The default certificate was valid for five years, and will expire on June 29, 2011. **If the network administrator does not replace the certificate, the following will occur:**

1. Users connecting to captive portal or WebUI pages will receive a browser warning showing that the server certificate has expired. Users may bypass the warning (with varying degrees of difficulty depending on the browser) and continue on to use the system normally.
2. 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.

This document outlines the procedures needed to update the default certificate, in order of preference:

Option 1: Install a unique server certificate
Option 2: Upgrade ArubaOS

Option 1: Install a Unique Server Certificate

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.

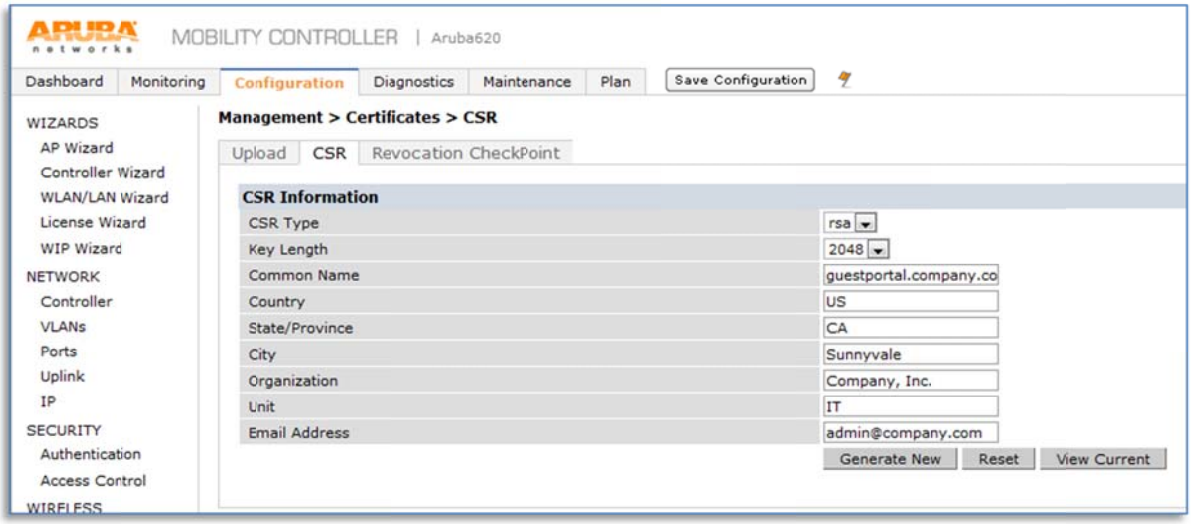
The following instructions should be followed to obtain and install a server certificate.

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

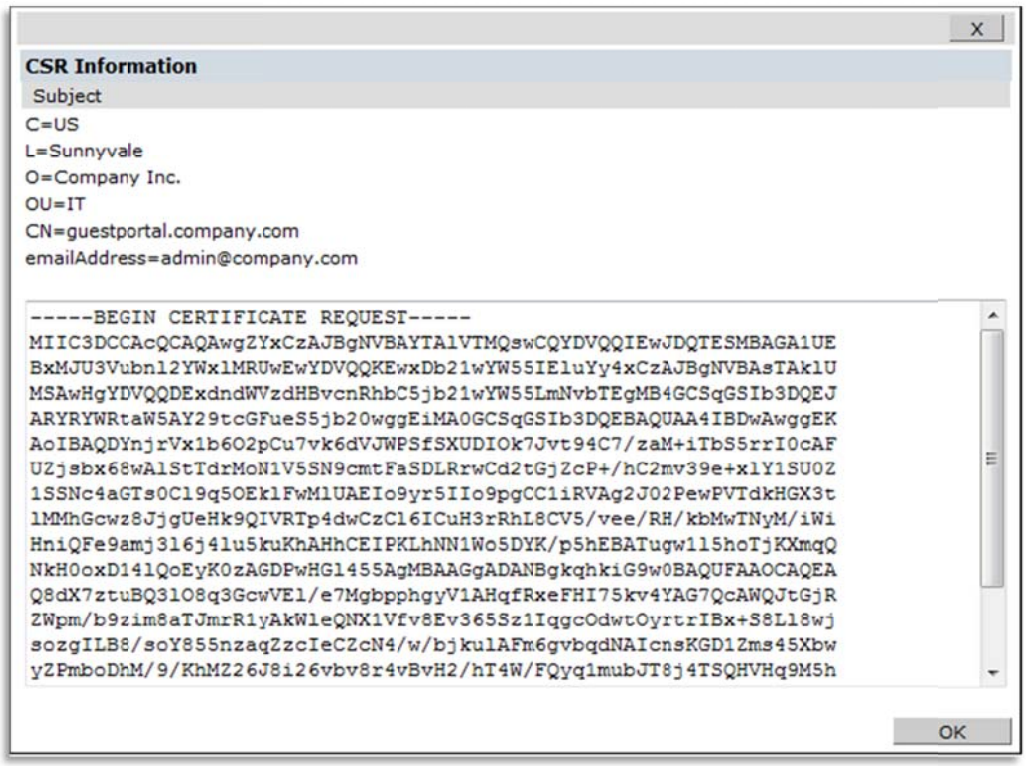
your domain name so that a public CA will correctly authorize ownership of the certificate.

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).

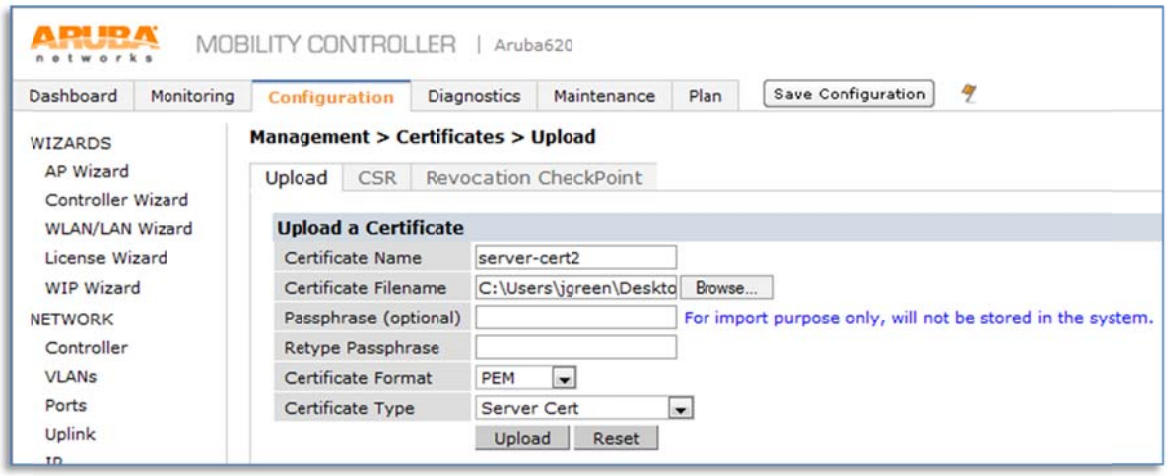
c. For 802.1X EAP Termination, the CN field is not matched by the client against any other parameter. It is suggested that you choose a FQDN that is owned by your organization.



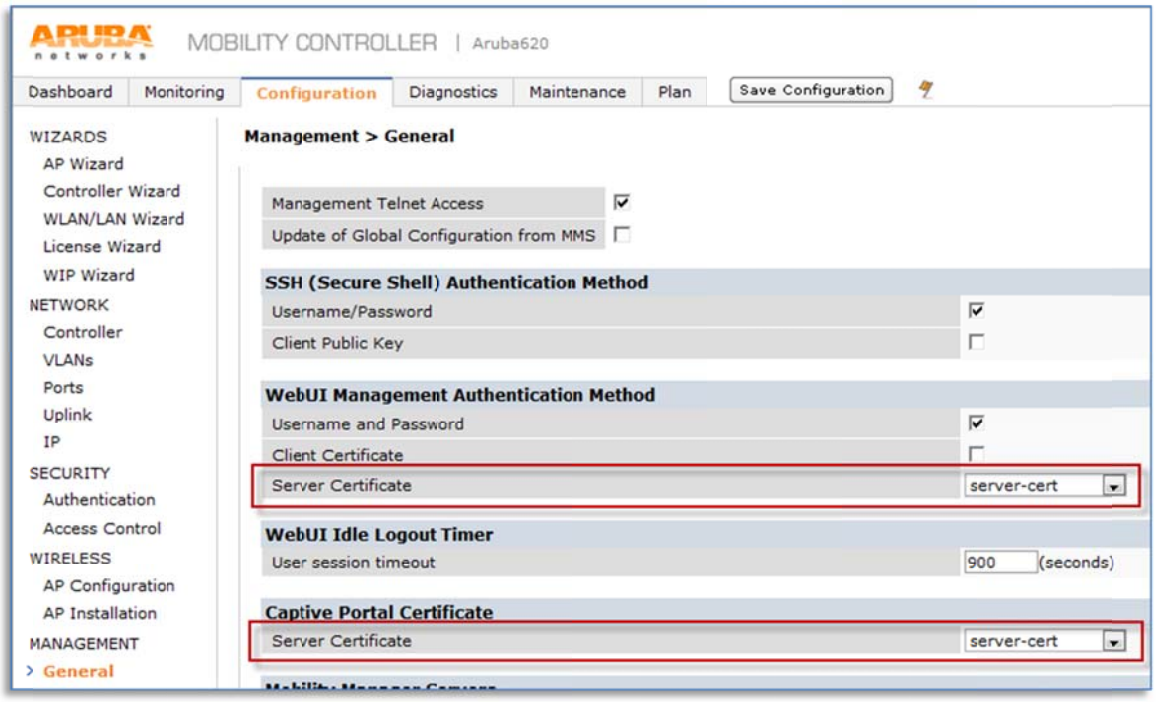
2. Click on “View Current”. Copy the base64 text shown, and paste this into the certificate request window provided by your certificate authority.



3. 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-----".

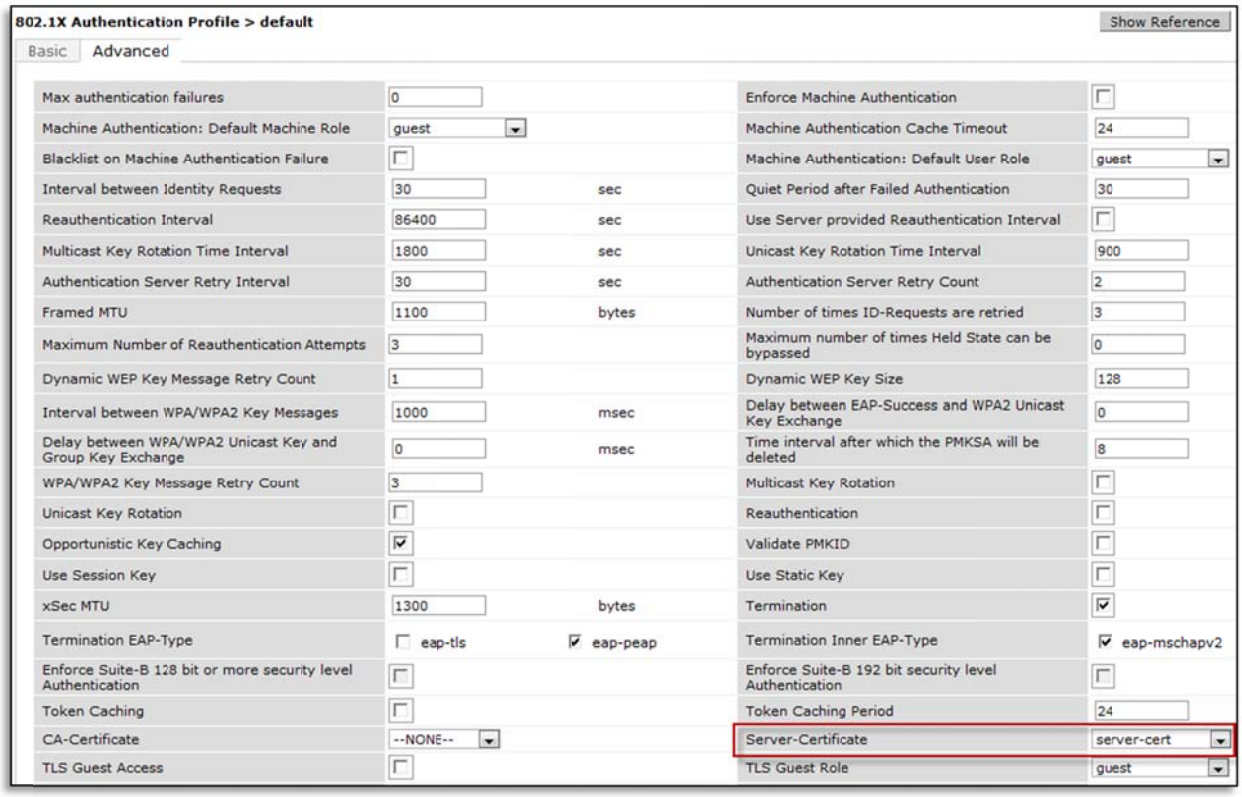


4. If you want to use the new certificate for captive portal, navigate to Configuration→Management→General and change the Captive Portal Server Certificate. If you want to use the new certificate for WebUI, configuration is found on the same screen under "WebUI Management Authentication Method".



5. 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.



Option 2: Upgrade ArubaOS

Aruba has obtained a new certificate labeled “securelogin.arubanetworks.com” from a public CA that replaces the old default certificate. The new certificate has an expiration date of November 21, 2013. This certificate is included as part of the following ArubaOS software releases:

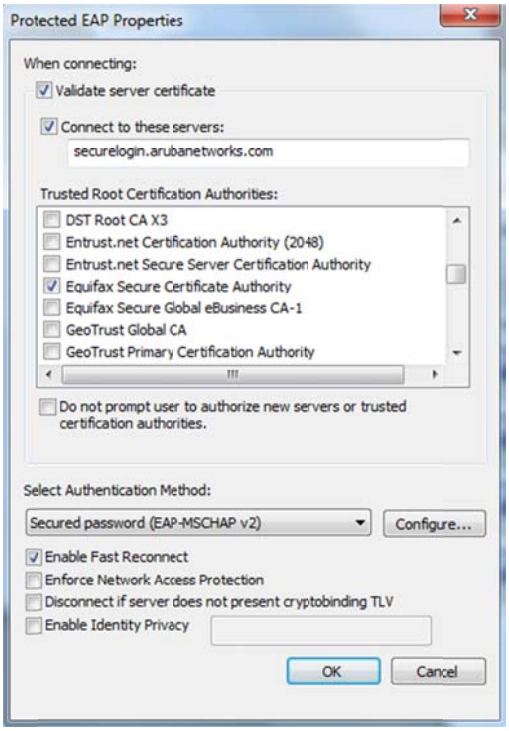
- 6.1 beginning with release 6.1.0.0
- 6.0 beginning with release 6.0.1.0
- 5.0 beginning with release 5.0.3.2
- 3.4 beginning with release 3.4.4.1
- All other ArubaOS releases dated later than June 1, 2011

After upgrading to one of the above listed releases, no further action is required to enable the certificate. If the system was previously configured to use the default certificate, it will automatically use the newly updated certificate.

While this option provides the same level of security given by the previous default certificate, it is not a good option where any security requirements exist. SSL/TLS security is provided by the certificate’s private key being kept secret. If the certificate’s private key becomes known, it is possible for an attacker to impersonate any server or website using that certificate without the knowledge of the end user. Because the same certificate and private key are installed on all Aruba controllers, an attacker need only reverse engineer a single software image to obtain the private key. While this process is non-trivial, it is certainly not beyond the means of a skilled and determined attacker. It is also possible for an attacker to simply purchase and use an Aruba controller for the purpose of conducting an impersonation attack.

FAQ

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

A: No. All Aruba controllers that contain a Trusted Platform Module (TPM), including the M3, 3000 series, and 600 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.