Aruba Support Advisory ARUBA-SA-20160908-01

ArubaOS Default Certificate Revocation

Confidentiality Level: Aruba Customers and Partners only | Rev-1.0909 (Sep 8, 2016)

SUMMARY

The ArubaOS operating system loaded on all Aruba Mobility Controllers and Mobility Access Switches contains a pre-loaded digital certificate with the name “securelogin.arubanetworks.com”. As is stated in the user guide, and multiple customer advisories and Airheads Community postings, the default certificate is not intended for production deployment since every Aruba controller or switch contains the same certificate. Aruba has always recommended customers to replace this default certificate with a certificate issued by a public Certificate Authority or by an internal (PKI) Certificate Authority.

While a majority of security conscious customers have taken our advice seriously and replaced the default certificate, Aruba is aware that there are still other customers that are using the default certificate in the production networks typically for Administrative WebUI, securing the Captive Portal login screen in guest networks and for dot1x authentication with EAP termination enable.

This default certificate (securelogin.arubanetworks.com) was issued by a GeoTrust certificate authority (CA) that is trusted by most browsers and operating systems. However, in light of the following articles, http://www.itnews.com.au/news/aruba-products-contain-compromised-https-certificate-436511 and http://www.darkreading.com/vulnerabilities---threats/cryptographic-key-reuse-remains-widespread-in-embedded-products/d/d-id/1326826, securelogin.arubanetworks.com has been revoked by GeoTrust.

This Support Advisory will also be posted under Announcements on the Aruba Support Site. It may be revised if needed. Kindly check back for updates.

PRODUCTS AFFECTED

- Mobility Controllers
- Mobility Access Switches - S1500, S2500 and S3500
- Instant APs (Captive Portal and 802.1x authentication with EAP termination)

PRODUCTS NOT AFFECTED

- ClearPass Policy Manager *(See notes for config changes if Captive Portal is offloaded to CPPM*)*
- Aruba Next Generation Access Switches – 2530, 2920, 2930F, 3810 and 5400R Series
- AirWave
- Meridian
- Aruba Central
- Mesh Routers
- Analytics and Location Engine

CALL TO ACTION

1. Users accessing the Controller/Switch's management WebUI or connecting to the Captive Portal served by a Controller/Switch/Instant AP (if using the default securelogin.arubanetworks.com server certificate) will receive browser warnings such as "There is a problem with this website's security certificate".

   Some browsers might start rejecting the certificate and thus block the Controller/Switch management WebUI and Captive Portals. Users may be able bypass the warning (with varying degrees of difficulty depending on the browser) and continue on to use the system normally.

   WebUI Management for Instant AP uses a self-signed certificate and is therefore not affected.

   Solution: Install a new Server Certificate issued by a public Certificate Authority for management WebUI and Captive Portal Authentication.

   If Captive Portal is offloaded to ClearPass Server please refer to the following KB article for *Weblogin NAS address configuration options in a multi-controller network*

   Workaround: Generate a self-signed certificate and install it as a Server Certificate for Controller/Switch management WebUI. Note that users will still receive browser warnings.

2. For 802.1X authentication, if EAP termination has been enabled on the Controller, Switch or Instant APs, and the default (securelogin.arubanetworks.com) 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.

   Solution: Install a new Server Certificate issued by a Public Certificate Authority (recommended).

   Workaround: Disable EAP termination on the Controller/Switch/IAP 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.

3. Users configured for SSO access to various web-based applications using L2 (802.1x) authentication will not be able to complete authentication if the default securelogin.arubanetworks.com certificate is configured in the Identity Provider IDP Profile. Aruba ClearPass Policy Manager (CPPM) is the only IDP supported and the controller has been optimized to work with CPPM to provide better functionality as an IDP.

   Solution: Install a new Server Certificate issued by a Public Certificate Authority as the IDP Server Certificate. For instructions on configuring the IDP server certificate, please refer to the Application Single Sign-On Using L2 Authentication under 802.1X Authentication chapter in the ArubaOS User Guide.

4. VIA clients may not be able to download profiles from the Controller.

   Solution: Install a new Server Certificate issued by a Public Certificate Authority.

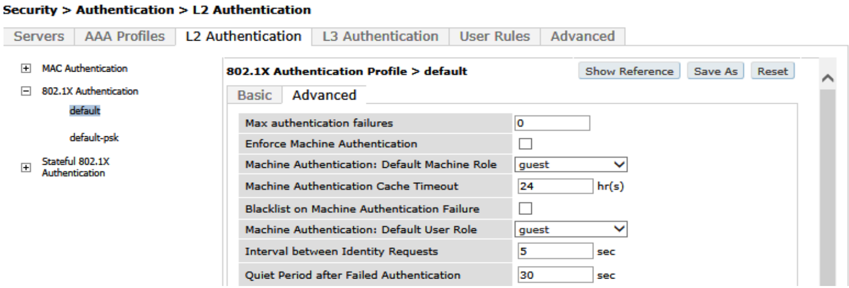
FREQUENTLY ASKED QUESTIONS

Q-1. How to request and install certificate issued by a Public CA (Certificate Authority)?

Ans. Please refer to the ArubaOS User Guide documentation for managing certificates.
http://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/Management_Utilities/Managing_Certificates.htm

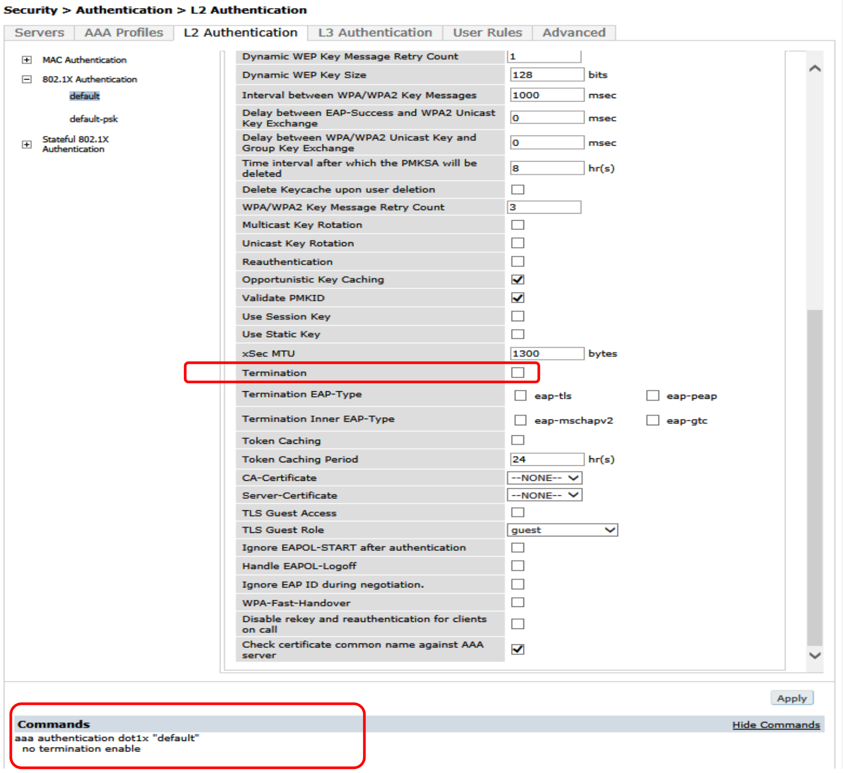
Q-2. How to disable EAP-termination on the Controller?

Ans. From the controller WebUI, navigate to Configuration⇨Security ⇨ Authentication ⇨ L2 Authentication ⇨ 802.1X Authentication Profile ⇨ Advanced and disable the “Termination” option on all active 802.1X authentication profiles that use EAP Termination.



802.1X Authentication Profile > default

Max authentication failures	0	
Enforce Machine Authentication	□	
Machine Authentication: Default Machine Role	guest	
Machine Authentication Cache Timeout	24	hr(s)
Blacklist on Machine Authentication Failure	□	
Machine Authentication: Default User Role	guest	
Interval between Identity Requests	5	sec
Quiet Period after Failed Authentication	30	sec



Dynamic WEP Key Message Retry Count	1		
Dynamic WEP Key Size	128	bits	
Interval between WPA/WPA2 Key Messages	1000	msec	
Delay between EAP-Success and WPA2 Unicast Key Exchange	0	msec	
Delay between WPA/WPA2 Unicast Key and Group Key Exchange	0	msec	
Time interval after which the PMKSA will be deleted	8	hr(s)	
Delete Keycache upon user deletion	□		
WPA/WPA2 Key Message Retry Count	3		
Multicast Key Rotation	□		
Unicast Key Rotation	□		
Reauthentication	□		
Opportunistic Key Caching	☑		
Validate PMKID	☑		
Use Session Key	□		
Use Static Key	□		
xSec MTU	1300	bytes	
Termination	□		
Termination EAP-Type	□ eap-tls		□ eap-peap
Termination Inner EAP-Type	□ eap-mschapv2		□ eap-gtc
Token Caching	□		
Token Caching Period	24	hr(s)	
CA-Certificate	--NONE--		
Server-Certificate	--NONE--		
TLS Guest Access	□		
TLS Guest Role	guest		
Ignore EAPOL-START after authentication	□		
Handle EAPOL-Logoff	□		
Ignore EAP ID during negotiation.	□		
WPA-Fast-Handover	□		
Disable rekey and reauthentication for clients on call	□		
Check certificate common name against AAA server	☑		

Commands

```
aaa authentication dot1x "default"
 no termination enable
```

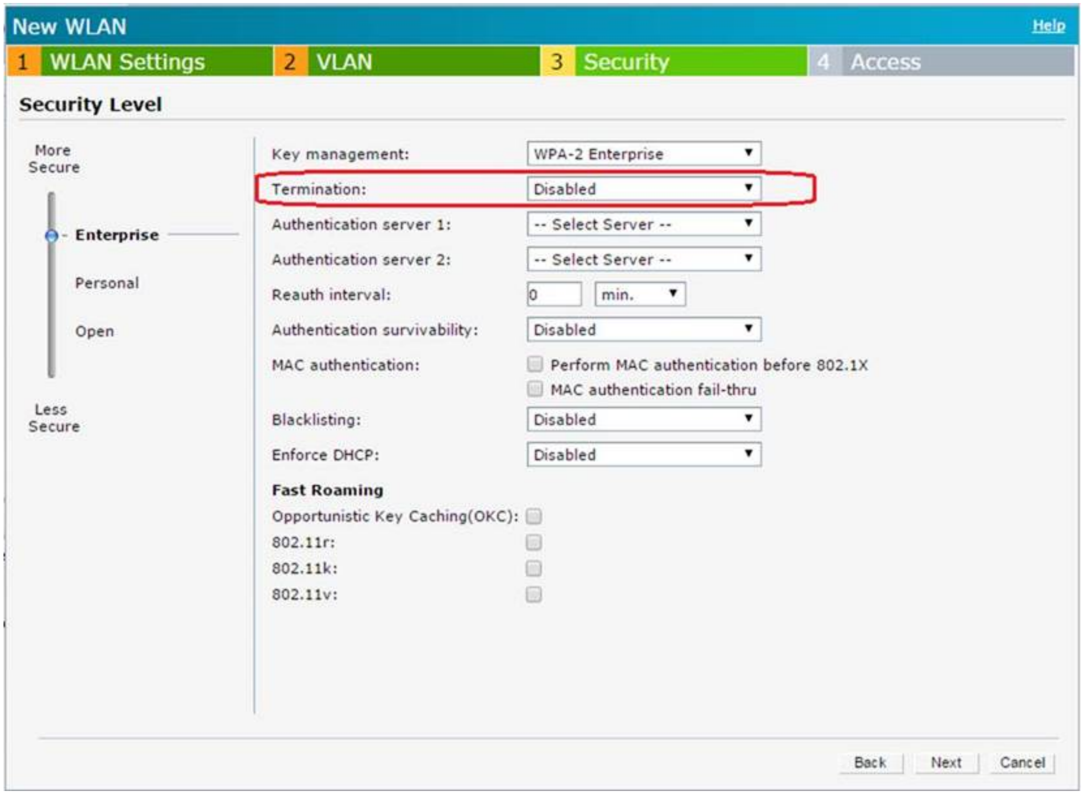
Use the following commands at the CLI to disable dot1x termination from the AAA authentication profile.

```
aaa authentication dot1x "default"
  no termination enable
```

Q-4. How to disable EAP-termination on the Instant AP?

Ans. From the Aruba Instant WebUI, navigate to Network ⇨ Select the SSID ⇨ Edit ⇨ Security and disable the “Termination” option that use EAP Termination.

Instant WebUI configuration screen shot and CLI commands follow.



Security Level

Key management: WPA-2 Enterprise ▾
Termination: Disabled ▾
Authentication server 1: -- Select Server -- ▾
Authentication server 2: -- Select Server -- ▾
Reauth interval: 0 min. ▾
Authentication survivability: Disabled ▾
MAC authentication: □ Perform MAC authentication before 802.1X
□ MAC authentication fail-thru
Blacklisting: Disabled ▾
Enforce DHCP: Disabled ▾

Fast Roaming
Opportunistic Key Caching(OKC): □
802.11r: □
802.11k: □
802.11v: □

Use the following commands at the CLI to disable dot1x termination from the SSID profile.

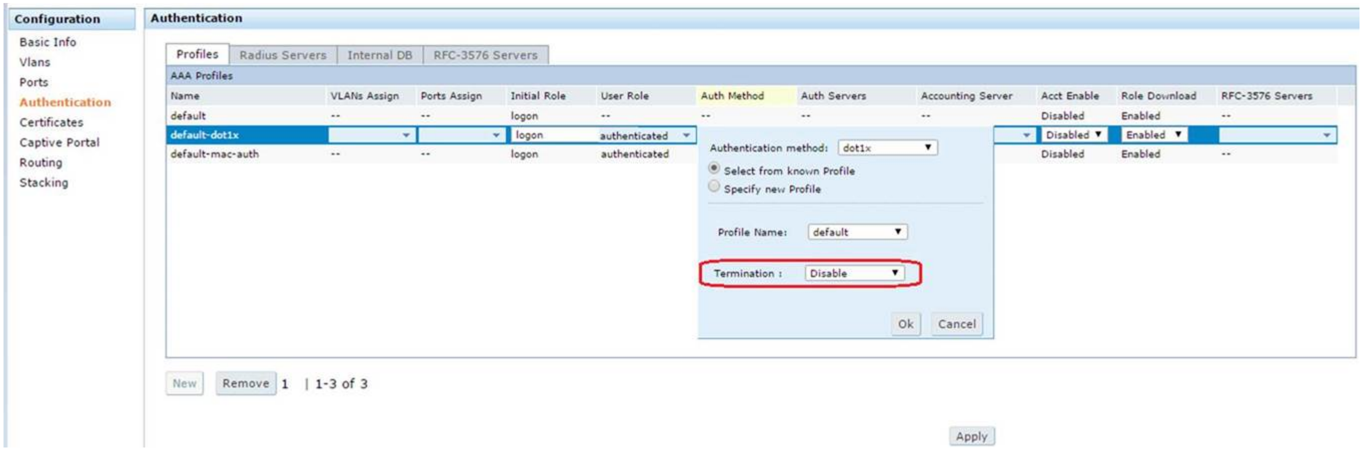
```
wlan ssid-profile Aruba-dot1x
    no termination
```

Q-4. How to generate and install a self-signed certificate for Controller/Switch WebUI management?

Ans. For instructions on generating a self-signed certificate and installing it, please refer to https://community.arubanetworks.com/t5/Controller-Based-WLANs/Generate-self-signed-certificate-with-OpenSSL/ta-p/275357
You can use the same process for Captive Portal certificate as well.

Q-5. How to disable EAP-termination on the Mobility Access Switch?

Ans. From the Mobility Access Switch WebUI, navigate to Configuration ⇨ Authentication ⇨ Profiles ⇨ Choose the AAA Profile ⇨ Authentication method ⇨ dot1x ⇨ Choose Select from known Profile ⇨ Choose the Profile Name ⇨ Termination: select Disable, to disable the “Termination” on all active 802.1X authentication profiles (that are configured for EAP termination)



AAA Profiles

Name	VLANs Assign	Ports Assign	Initial Role	User Role	Auth Method	Auth Servers	Accounting Server	Acct Enable	Role Download	RFC-3576 Servers
default	--	--	logon	--	--	--	--	Disabled	Enabled	--
default-dot1x			logon	authenticated				Disabled	Enabled	
default-mac-auth	--	--	logon	authenticated				Disabled	Enabled	--

Authentication method: dot1x

● Select from known Profile

○ Specify new Profile

Profile Name: default

Termination : Disable

Use the following commands at the CLI to disable dot1x termination from the dot1x authentication profile.

```
aaa authentication dot1x "default"
  no termination enable
```

ADDITIONAL INFORMATION

This Support Advisory will be posted on the Aruba Support Site under the Announcements tab and may be revised as applicable. Kindly refer to the Frequently Asked Questions FAQ for additional details, and check back for further updates.

Aruba is committed to communicating code revision, feature and function recommendations to ensure optimal network operation and high customer satisfaction. Please feel free to contact the Aruba Technical Assistance Center (TAC) if you need further clarifications. The Aruba TAC team can facilitate further product related discussions with the Product Management team for customers that desire to do so.

Thank you,
Aruba Customer Advocacy

Confidential – Distribution Limited to Aruba Customers & Partners only