

Aruba 控制器如何安装第三方 SSL 证书

ARUBA 控制器如何安装第三方 SSL 证书	1
1. 前言	3
2. 查看控制器默认证书	4
3. 导入证书	5
3.1. 导入 PFX 格式证书	6
3.2. 导入 PEM 格式证书	7
3.3. 导入 Cert 格式证书	9
4. 证书调用	10
5. 改造 PORTAL 服务器 FORM 表单	10
5.1. ClearPass	10
5.2. 第三方 portal	11
6. 测试:	12

修订历史记录

下表列出了这个文档的修订历史记录

版本	日期	变更说明
V1.0	2021/07/15	最初发布

1. 前言

Aruba 控制器默认的 SSL 证书是自签名证书。Common Name(CN)是 securelogin.arubanetworks.com。默认情况下，控制器会使用 SSL 证书里的 CN 作为域名，也就意味着在集中转发模式下，任何无线客户端连接一个 Aruba 控制器释放出来的 portal 认证的 SSID 时候。终端在解析 securelogin.arubanetworks.com 域名时，默认情况下，控制器都会返回 controller-ip。

然而当 portal 认证的 ssid 启用 https 认证时。由于浏览器默认不信任自签名 SSL 证书，就会弹出不安全告警，如下图。



您的连接不是私密连接

攻击者可能会试图从 securelogin.arubanetworks.com 窃取您的信息（例如：密码、通讯内容或信用卡信息）。[了解详情](#)

NET::ERR_CERT_AUTHORITY_INVALID



如果您想获得 Chrome 最高级别的安全保护，请[开启增强型保护](#)

高级

返回安全连接

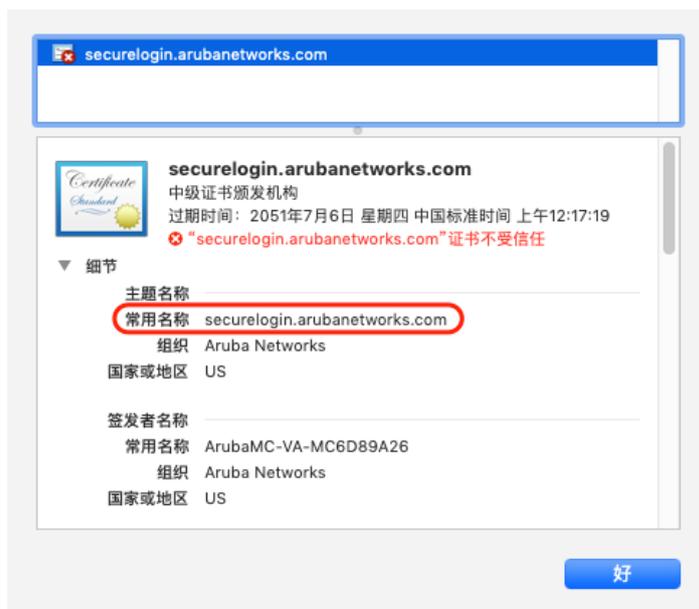
这在部署基于 https porta 认证时候，给客户带来了非常不好的体验。这时，我们就需要在 aruba 控制器上部署浏览器信任的 public ca 签发的 ssl 证书。

如果上传的是单域名证书（例如:上传的证书的域名是 md.example.com），那么控制器在上传了证书以后的域名将会变成 md.example.com。控制器将会对 md.example.com 域名解析成控制器的 controller-ip

如果上传的是通配符证书（例如:上传的通配符证书的域名是*.example.com），那么控制器在上传了证书以后的域名将会用 captiveportal-login 代替*号，域名将变成 captiveportal-login.example.com。同样，控制器将会对 captiveportal-login.example.com 域名解析成控制器的 controller-ip

2. 查看控制器默认证书

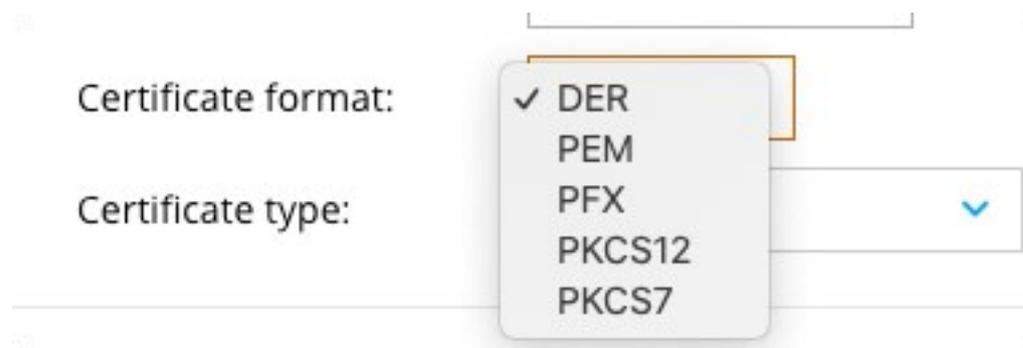
以 chrome 浏览器为例，我们可以点击不安全按钮，证书，来查看控制器 /MM 的默认 SSL 证书，我们可以看到默认 SSL 证书的 CN 是 securelogin.arubanetworks.com



3. 导入证书

Aruba 控制器支持导入的证书格式有 DER、PEM、PFX、PKCS12、PKCS7。通常我们去 Public CA 申请了 SSL 证书，会给 crt、pfx、pem 格式

的证书。如果是 pfx 格式的证书即可直接导入，如果是 pem 格式的证书需要将 pem 证书和 key 文件做合并操作后导入。如果是 crt 格式的证书需要使用工具将 crt 格式证书转换成 pem 或者 pfx 格式证书。本文档介绍 pfx 和 pem 证书的安装。



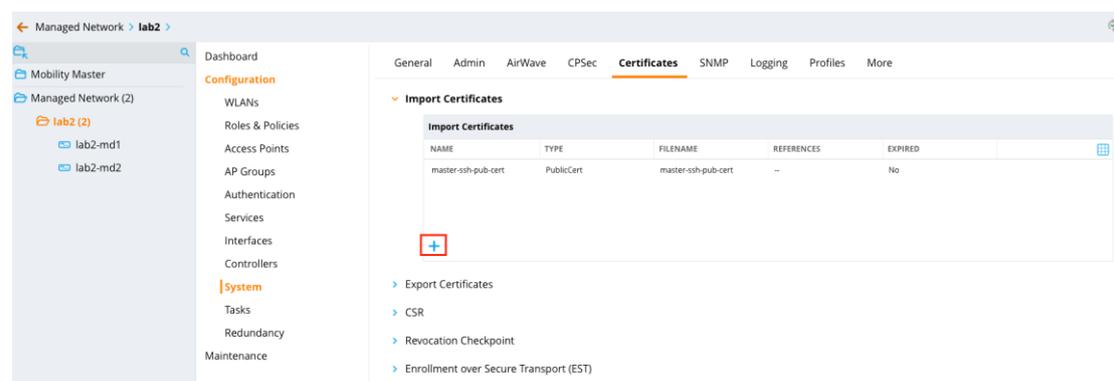
3.1. 导入 PFX 格式证书

第 1 步：准备工作：

通常 pfx 格式的证书会提供 pfx 证书，和 pfx-password 两个文件。



第 2 步：按照截图，找到 Configuration -> System -> Certificates，在 Import Certificates 选项卡中点击 “+” 导入证书



在弹出的对话框中，填写以下参数

- Certificate name: test-pfx-cert # <配置名称>
- Certificate filename: # 选择 pfx 证书
- Optional passphrase: # 填写 pfx 对应的密码
- Retype passphrase: # 确认 pfx 对应的密码
- Certificate format: PFX # 选择证书格式为 PFX
- Certificate type: ServerCert # 选择证书类型为 ServerCert

General Admin AirWave CPsec **Certificates** SNMP Logging Profiles More

Import Certificates

NAME	TYPE	FILENAME	REFERENCES	EXPIRED
master-ssh-pub-cert	PublicCert	master-ssh-pub-cert	--	No

+

New Certificate

Certificate name: test-pfx-cert

Certificate filename: 4697665_... Browse

Optional passphrase:

Retype passphrase:

Certificate format: PFX

Certificate type: ServerCert

> Export Certificates

Cancel Submit

3.2. 导入 PEM 格式证书

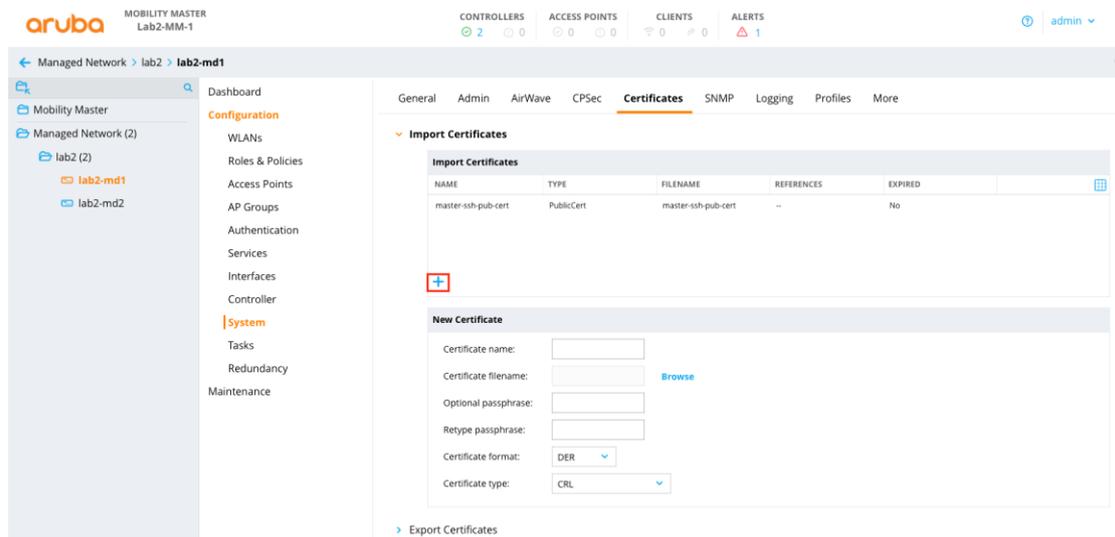
第 1 步：准备工作：pem 格式证书，key 文件



第 2 步：合并 key 文件和 pem 证书

有文本编辑器打开 pem 证书和 key 文件，复制 key 文件的所有内容，添加到 pem 证书的最后，另存为 xxx.pem

第 3 步：按照截图，找到 Configuration -> System -> Certificates，在 Import Certificates 选项卡中点击 “+” 导入证书



在弹出的对话框中，填写以下参数

- Certificate name: test-pem-cert # <配置名称>
- Certificate filename: # 选择 PEM 证书
- Optional passphrase: # 空
- Retype passphrase: # 空
- Certificate format: PEM # 选择证书格式为 PEM
- Certificate type: ServerCert # 选择证书类型为 ServerCert

General Admin AirWave CPsec **Certificates** SNMP Logging Profiles More

▼ Import Certificates

NAME	TYPE	FILENAME	REFERENCES	EXPIRED
master-ssh-pub-cert	PublicCert	master-ssh-pub-cert	--	No
test_pfx_cert	ServerCert	4697665_njmu.edu.cn.pfx	--	No

+

New Certificate

Certificate name:

Certificate filename: [Browse](#)

Optional passphrase:

Retype passphrase:

Certificate format:

Certificate type:

> Export Certificates

[Cancel](#) [Submit](#)

General Admin AirWave CPsec **Certificates** SNMP Logging Profiles More

▼ Import Certificates

NAME	TYPE	FILENAME	REFERENCES	EXPIRED
master-ssh-pub-cert	PublicCert	master-ssh-pub-cert	--	No
test_pfx_cert	ServerCert	n.pfx	--	No

+

New Certificate

Certificate name:

Certificate filename: [Browse](#)

Optional passphrase:

Retype passphrase:

Certificate format:

Certificate type:

> Export Certificates

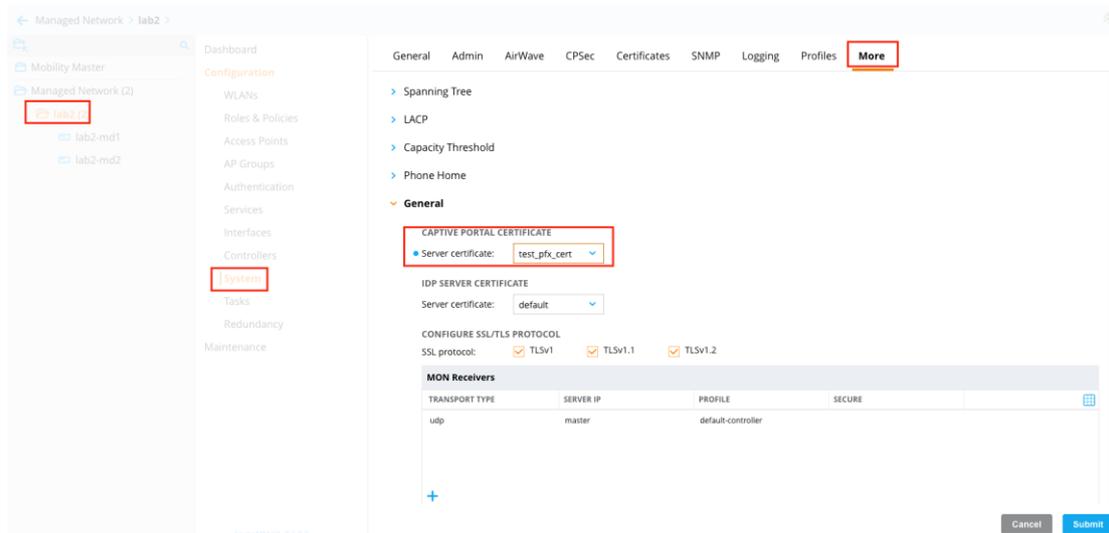
[Cancel](#) [Submit](#)

3.3. 导入 Cert 格式证书

需要将 cert 格式证书转换成 pem 或者 pfx 格式证书

4. 证书调用

按照截图，找到 Configuration -> System -> More，在 General 选项卡中点击 Server Certificate 下拉选项，选择导入的证书配置文件。



5. 改造 portal 服务器 form 表单

这里要分上传到证书是通配符证书还是单域名证书。

- 如果是通配符证书（例如:上传的通配符证书的域名是*.example.com），那么控制器在上传了证书以后的域名将会变成 captiveportal-login.example.com。
- 如果上传的是单域名证书（例如:上传的证书的域名是 md.example.com），那么控制器在上传了证书以后的域名将会变成 md.example.com。

5.1. ClearPass

这里默认是 securelogin.arubanetworks.com，需要更改成 captiveportal-login.example.com

主页 » 配置 » 页面 » Web 登录

Web Login (new)

使用此表单来创建一个新的RADIUS网络登录。

Web Login Editor	
* 名字:	<input type="text" value="login"/> 键入网页登陆页面名称
页面名称:	<input type="text" value="login"/> 输入此Web登录页的名称。 该网站的登录将可从 "page_name.php"
描述:	<input type="text"/> 关于网页登陆的注释和描述。
* 供应商设置:	Aruba Networks 选择一个预定义组设置符合标准网络配置。
Login Method:	Controller-initiated — Guest browser performs HTTP form submit Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.
* 地址:	<input type="text" value="captiveportal-login.example.com"/> 在此输入供应商产品的IP地址或者主机名。
安全登录:	使用供应商默认值 为该网站登录过程选择一个安全选项为该网站登录过程。
Dynamic Address:	<input type="checkbox"/> The controller will send the IP to submit credentials In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.

5.2. 第三方 portal

默认情况下，第三方 portal 服务器通过 http/https post 方式和 Aruba 控制器对接时。Form 表单的格式如下：

```
<form method="post" action="securelogin.arubanetworks.com/cgi-bin/login">  
  
    Username:<input type="text" name="user">  
  
    Password:<input type="password" name="password">  
  
    <input type="submit" value="login">  
  
</form>
```

在证书上传完成以后，需要将 form 表单 http/https post action 改成 **captiveportal-login.example.com/ cgi-bin/login**

```
<form method="post" action="captiveportal-login.example.com/cgi-bin/login">

    Username:<input type="text" name="user">

    Password:<input type="password" name="password">

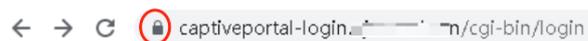
    <input type="submit" value="login">

</form>
```

6. 测试:

连接 portal 认证 ssid, 输入用户密码点击登录。认证成功可以看到如下截图。

表示 SSL 证书上传成功。



Authentication successful

In 10 seconds you will be automatically redirected to http://www.gstatic.com/generate_204.

Click [here](#) to go there directly.

Press control-d to bookmark this page.

[logout](#)