a Hewlett Packard Enterprise company

# Aruba RadSec 配置手册

V1.0

杨正鑫

# 目录

# 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 |
| --- | --- | --- |
| 1.0 | 2022/02/20 | 最初发布 |

# 1 ARUBA RADSEC GUIDE

## 1.1 用户需求

传统RADIUS：如果你在讨论传统的RADIUS协议时，比如它是如何工作的，比如传统的RADIUS协议有什么缺陷?那你们都知道RADIUS数据通常是明文的，采用普通的RADIUS协议，比如用户名、IP地址和登录时间等等。如果网络中捕获了这些RADIUS数据包，无需解密，您就可以直接看到所有这些信息——例如，用户名是什么，哪个用户正在进行身份验证，以及这个用户的IP地址是什么，这些信息在RADIUS协议里都是暴露的。

因此，用户认证密码是采用共享的安全key来加密的，但是它使用了相当弱的加密算法——这通常是一个安全问题的挑战，即RADIUS报文传输在互联网上(即公共网络上)，那该如何实现RADIUS协议的安全性呢?

场景A—使用Cloud Auth， 需要将RADIUS认证请求在Internet上传输，为了保证认证数据在互联网上传输的安全性。

场景B—客户需要在内网使用增强的RADIUS认证报文的安全性（控制器和RADIUS Server之间通讯的安全性，即需要对RADIUS报文进行安全加密），防止用户认证账号信息被窃取，导致安全风险。

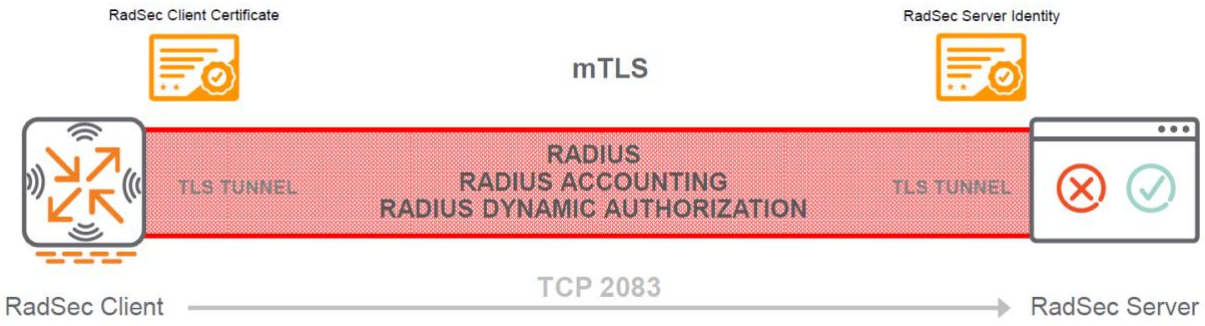
那从基础架构角度来看，有一种做法是建立额外的IPSec VPN隧道，在隧道内部再跑RADIUS报文，实现安全传输，但是这个毕竟需要部署额外的IPSec VPN产品，那最简单最直接的一种做法就是NAS和RADIUS都实现支持RadSec，直接在设备之间建立TLS隧道。RadSec可以用于任何类型的认证，比如MAC、Dot1x或Captive Portal，来解决RADIUS协议在互联网或者本地网络上传输安全性问题。

## 1.2 实现思路

Radsec就是基于TLS隧道上的RADIUS （即RADIUS报文封装在TLS流中）。那么，RadSec是如何克服传统RADIUS协议存在的问题的呢?

这个Radsec是在RADIUS服务器和NAS（在我们的例子中泛指是Aruba控制器等)之间提供一个安全通道。所以基本上是在发送RADIUS请求报文到RADIUS Server之前，来建立一个安全的TLS隧道。因此，可以在Internet等不安全的网络上，可以安全地可靠地发送RADIUS认证和计费数据。RadSec被正式定义为一个官方协议，它是在RFC 6614中有定义。而且，该TLS协议将整个RADIUS数据包载荷全都封装到TLS流中。所以,这里没有UDP报文。

Radsec采用RADIUS报头，并将该报头封装到TLS里面作为TLS的载荷。RADIUS over TLS的缺省目的端口是TCP 2083。身份验证、计费或授权变更不在使用各自独立的端口，因为通常传统上我们使用UDP 1812端口做身份验证和授权，UDP 1813端口做计费。但是在RadSec的例子中，我们为所有这些服务(就像所有AAA服务)使用单一端口，即TCP 2083。缺省情况下对于AOS，该功能处于禁用状态。因此，如果需要，在向RADIUS服务器发送RADIUS报文之前，你需要启用该特性才能建立TLS隧道。

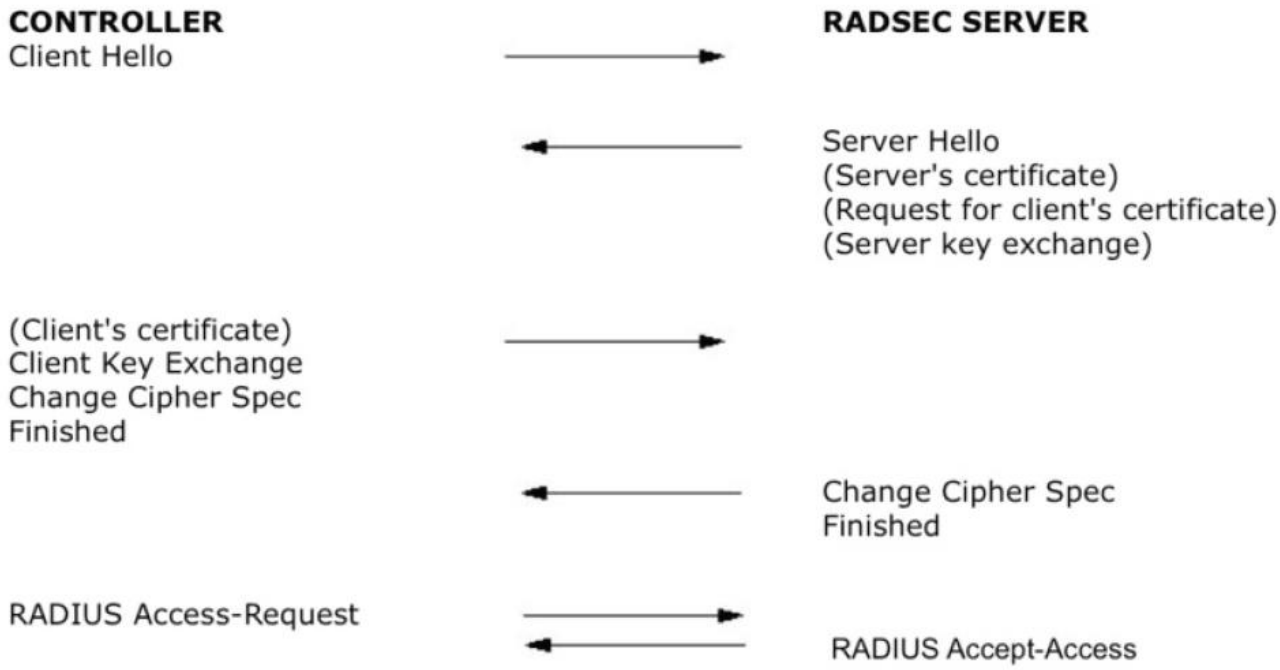



Aruba支持的平台：

1） 所有的Aruba无线控制器都支持这个特性，支持6.4.3.0及更高版本。

2） 所有的Aruba ClearPass策略管理器支持这个特性，支持 v6.8.x及更高版本。

我们看下RADIUS over TLS的隧道建立过程：




Controller 就是 RadSec Client ， 也叫作 TLS Client
ClearPass 就是 RadSec Server， 也叫作 TLS Server

1) Client--------→ Server ( Client Hello)
2) Client←------- Server (Server Hello ----包括 Server certificate， request for a client certificate， server key exchanges information)
3) Client--------→ Server (发送 Client certificate and key exchanges， some cipher specification)
4) Cleint←-------→ Server (一旦前面的 the cipher certifications have been finished, TLS tunnel 就会被建立)
5) 在 TLS Tunnel 里面交互 Access –Request 和 Access-Accept/Reject 等 （所以 RADIUS 报文是被加密在 TLS Tunnel 隧道里面的）

我们来看看拓扑结构，从RadSec Server的角度来看，有两种可能的部署，这意味着服务器可以采用两种方式部署。

支持的拓扑1：

RadSec服务器可像扮演RADIUS服务器角色一样，既可以是TLS服务器，也可以是RADIUS服务器——这意味着，RADIUS数据包将终结在同一服务器上，同样RadSec TLS隧道也终结在相同的服务器上。意味着，既有TLS报文也有RADIUS报文都终结在同一个服务器上。

支持的拓扑2：

这里我们部署两台服务器，因此，这意味着TLS隧道将在代理服务器上终结，接着代理服务器将这些RADIUS报文转发给后面实际的RADIUS服务器上。这是客户可以部署的另外一种部署类型，这个更现实些，因为如果你有客户已经有了RADIUS服务器，而它不支持TLS隧道终结，所以可以在它前面放置一个新的代理服务器CPPM，在代理服务器和控制器之间建立TLS隧道，并且代理服务器可以将RADIUS请求报文转发给后面实际的RADIUS服务器，而不影响客户原有的RADIUS基础设施。

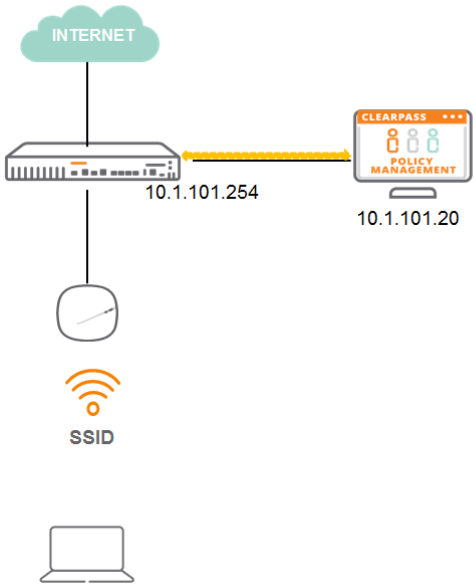
## 1.3 配置步骤

### 1.3.1 网络拓扑参考

# 拓扑图

**Controller ip ： 172.16.0.254**
**VLAN 1： 172.16.0.254**
**VLAN 101： 10.1.101.254 （和CPPM互联地址）**

```
(Aruba7010_9A_D5_D7) [mynode] #show ip radius nas-ip
Wed Jan 26 11:34:12.837 2022
RADIUS client NAS IP address = 172.16.0.254
RADIUS client NAS IPv6 address = ::1

(Aruba7010_9A_D5_D7) [mynode] #show ip radius source-interface
Wed Jan 26 11:34:17.054 2022
Global radius client source IP address = 0.0.0.0, vlan 0
Global radius client source IPv6 address = ::, vlan 0
Per-server client source IPv4/6 addresses:
```




相关系统版本：

CearPass*1 v6.9.8 （ClearPass 从 v6.8.x 开始正式支持 RadSec）

AOS*1 v8.6.0.15 （Standalone 模式）

这里手册仅仅介绍的是 ClearPass 即做 TLS Server 也做 RADIUS Server

### 1.3.2 ClearPass 侧配置

首先，我们需要配置好相关的TLS Client 证书和TLS Server 证书，关于证书的配置，我们需要了解下面的知识点：

虽然我们硬件控制器作为TLS Client,如果在RADIUS Profile中不调用RadSec Client Cert的话，系统默认会使用设备内置的Device Certificate（即 TPM证书）来和TLS Server通讯，但是软件VMC没有TPM，所以必须要签发TLS Client 证书，同时我们测试CLEARPASS V6.9.8时，发现该

版本的CLEARPASS无法使用内置的 CN=Aruba Networks Trusted Computing Root CA 1.0 来验证控制器的TPM(TLS Client) 证书，所以我们本次配置统一使用Onboard CA来给硬件控制器和CLEARPASS签发TLS Client证书并导入到 CLEARPASS（作为RadSec Server证书）和控制器（作为 ServerCert）。

控制器的角色就是TLS Client，CLEARPASS的角色就是TLS Server，为了建立TLS Tunnel，TLS Client 和TLS Server之间必须相互采用证书认证。

我们建议全部采用ClearPass Onboard CA来统一签发 HTTPs类型的证书，然后该签发好的证书导入到TLS Server （由CLEARPASS创建CSR，由ClearPass Onboard CA来签发HTTPs类型证书，作为 RadSec服务器证书）和TLS Client（可以先从ClearPass上导出RadSec服务器证书，格式为 PKCS12，含Private Key；或者由控制器直接创建CSR，再由ClearPass Onboard CA来签发HTTPs类型证书。作为 ServerCert）

在TLS Server上添加Onboard Root CA到Trust List中（默认就有，但需勾选usage=RadSec）

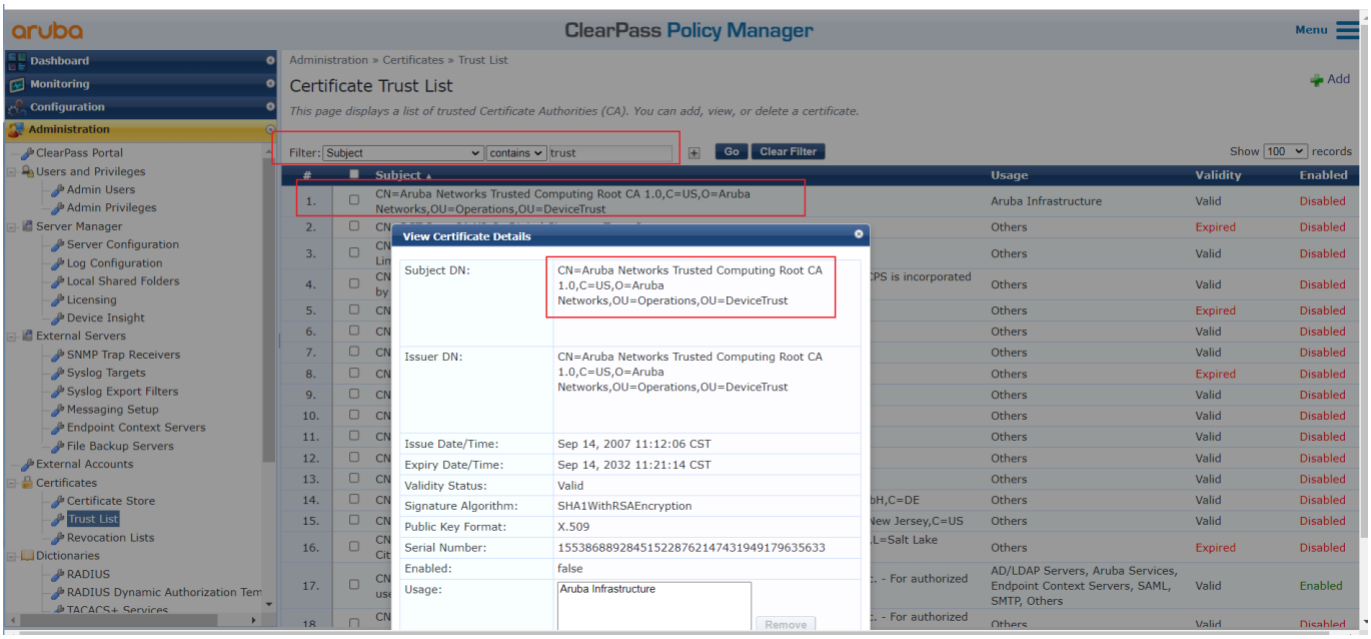
接着在TLS Client上需要上传ClearPass Onboard Root CA作为TrustedCA（如果 TLS Server是自签证书，那就需要将该自签证书上传到控制器上，作为PublicCert），上传前面的HTTPs类型证书作为ServeCert ，然后在配置RADIUS server profile时，需要Radsec Trusted CA Name调用TrustedCA类型证书，RadSec Client Cert调用ServerCert类型证书。

TLS Client需要验证TLS Server证书（即RadSec Server Cert服务器证书），该TLS Server证书是ClearPass Onboard Root CA签发的HTTPs类型证书，且ClearPass Onboard Root CA已经在控制器的TrustedCA中，所以信任。

TLS Server需要验证 TLS Client 证书 （该TLS Client证书是由同一个ClearPass Onboard Root CA签发的HTTPs类型证书，且ClearPass Onboard Root CA已经在ClearPass的Trusted List中，所以也是信任的）

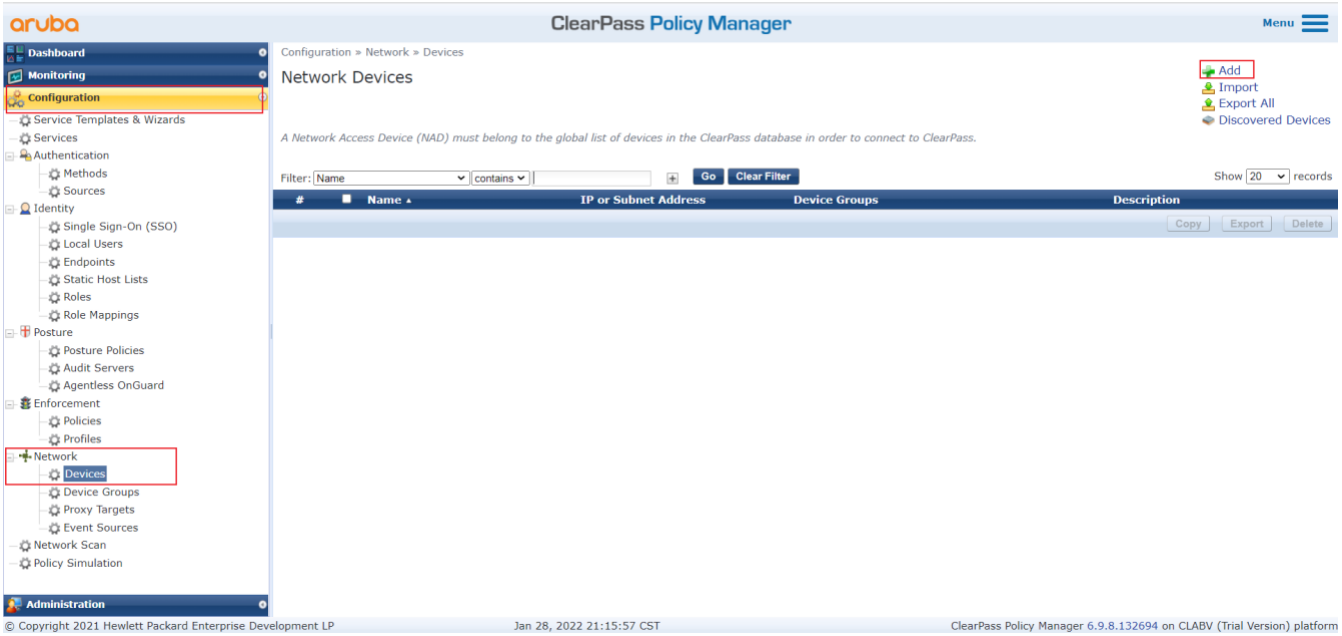
Note：硬件控制器，在配置RADIUS server profile时，RadSec Client Cert如果没有调用任何证书。那硬件控制器会采用内置TPM证书作为 TLS Client证书， CLEARPASS会采用内置的证书

CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust 来验证（需要提前设置Usage=RadSec，并且启用它）。




第1步:　　在 ClearPass 上添加 Device（即添加 NAS 设备）

登录到 ClearPass Policy Manager 管理界面，导航到 Configuration » Network » Devices 页面，点击右上角的 Add 按钮



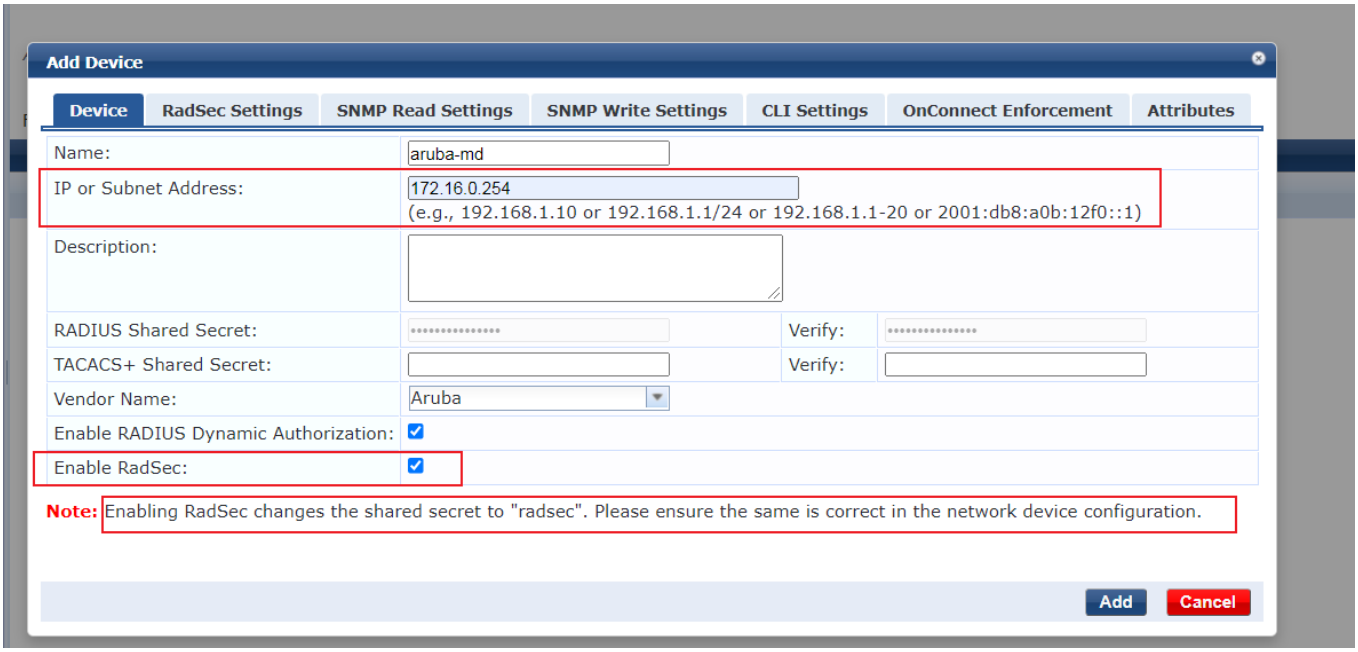

在配置之前，我们先要了解下 Aruba 控制器的 RADIUS 报文的 NAS-IP 和 Source-IP 是不同的，Standalone 模式下，默认 NAS-IP=Controller-IP

MM+MD 模式下，默认 NAS-IP=MM-IP，如果同时启用了 Cluster 并且配置了 Cluster VRRP-IP，那么 NAS-IP=Cluster VRRP-IP

而控制器的默认 RADIUS 报文源 IP 地址是 默认路由出接口的 IP 或者直连 ClearPass 的接口 IP，除非你配置了指定的 Source Interface VLAN。

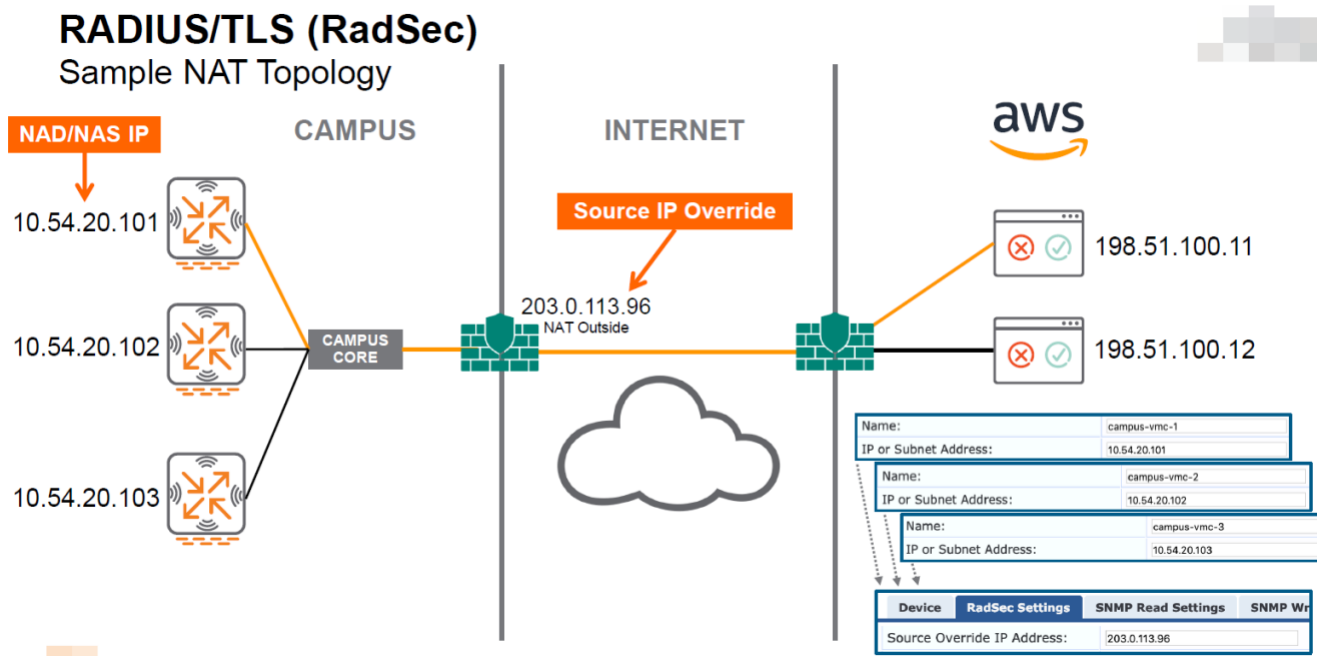
在 Device 选项卡中，

- Name： 输入自己定义的名称
- IP or Subnet Address: 输入控制器的 NAS-IP（注意: 这里不能是 RADIUS 报文的源 IP 地址，该配置项是区别于不启用 RadSec 的 RADIUS 设置的。）
- RADIUS Shared Secret: 输入 radsec （都是小写字母）
- Enable RadSec : 勾选

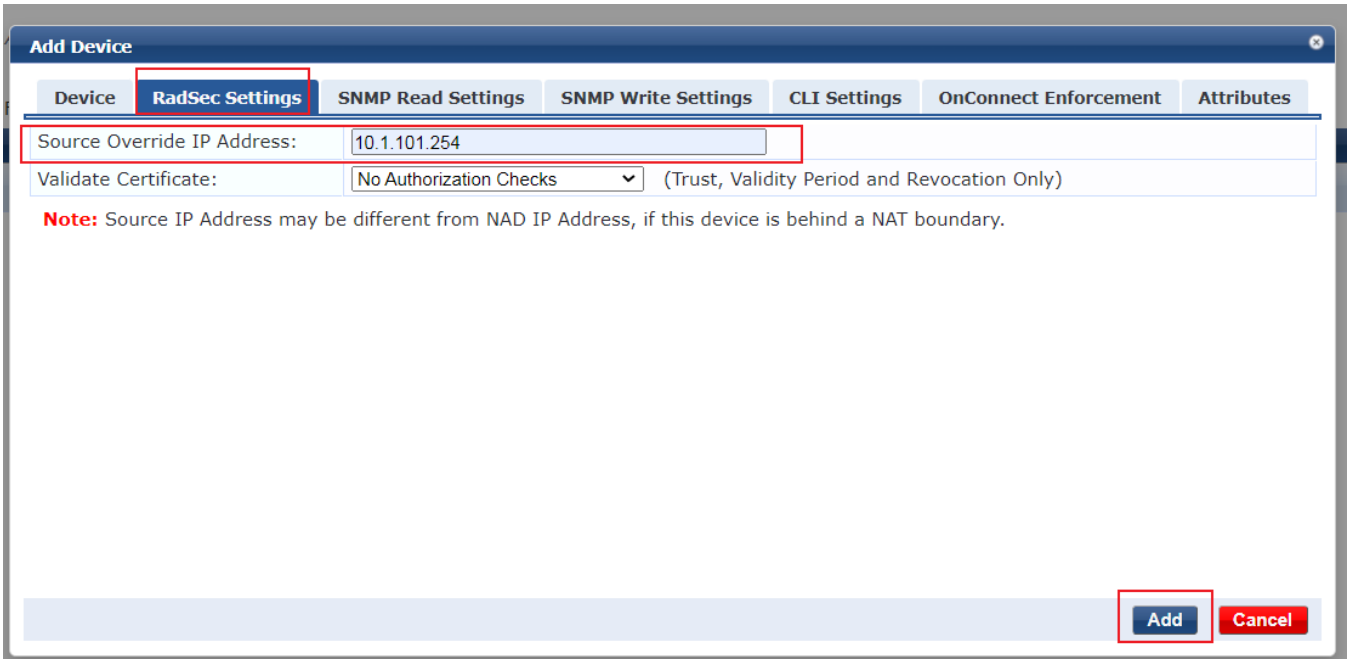


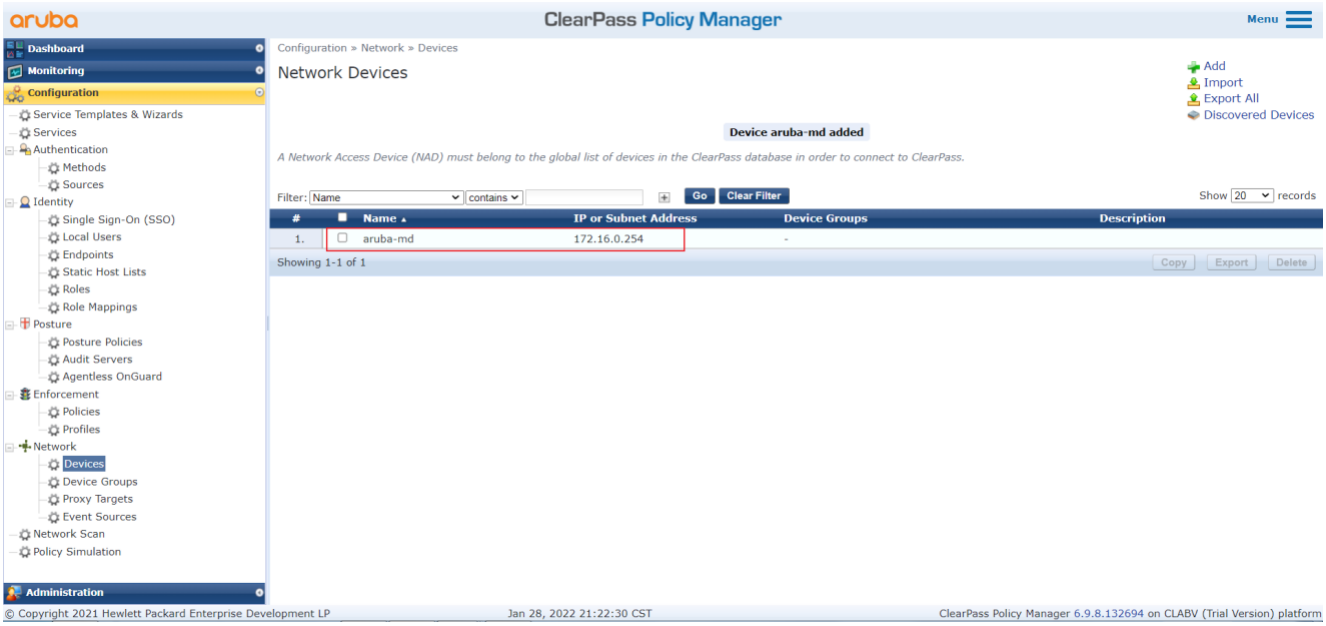

在 RadSec Settings 选项卡中，

- Source Override IP Address 输入控制器的 RADIUS 报文的源 IP 地址（注意：不能是 NAS-IP 地址，如果控制器和 ClearPass 之间没有 Firewall NAT Outside，那这个 IP 地址就是控制器上的 RADIUS 报文的源 IP。如果控制器和 ClearPass 之间有 Firewall NAT Outside，那么该地址就是 Firewall NAT 后的 IP 地址）


RADIUS/TLS (RadSec)
Sample NAT Topology
NAD/NAS IP
CAMPUS
INTERNET
aws
10.54.20.101
10.54.20.102
10.54.20.103
CAMPUS CORE
Source IP Override
203.0.113.96
NAT Outside
198.51.100.11
198.51.100.12
Name:
campus-vmc-1
IP or Subnet Address:
10.54.20.101
Name:
campus-vmc-2
IP or Subnet Address:
10.54.20.102
Name:
campus-vmc-3
IP or Subnet Address:
10.54.20.103
Device
RadSec Settings
SNMP Read Settings
Source Override IP Address:
203.0.113.96

最后点击 Add 按钮


Add Device
Device
RadSec Settings
SNMP Read Settings
SNMP Write Settings
CLI Settings
OnConnect Enforcement
Attributes
Source Override IP Address:
10.1.101.254
Validate Certificate:
No Authorization Checks
(Trust, Validity Period and Revocation Only)
Note: Source IP Address may be different from NAD IP Address, if this device is behind a NAT boundary.
Add
Cancel

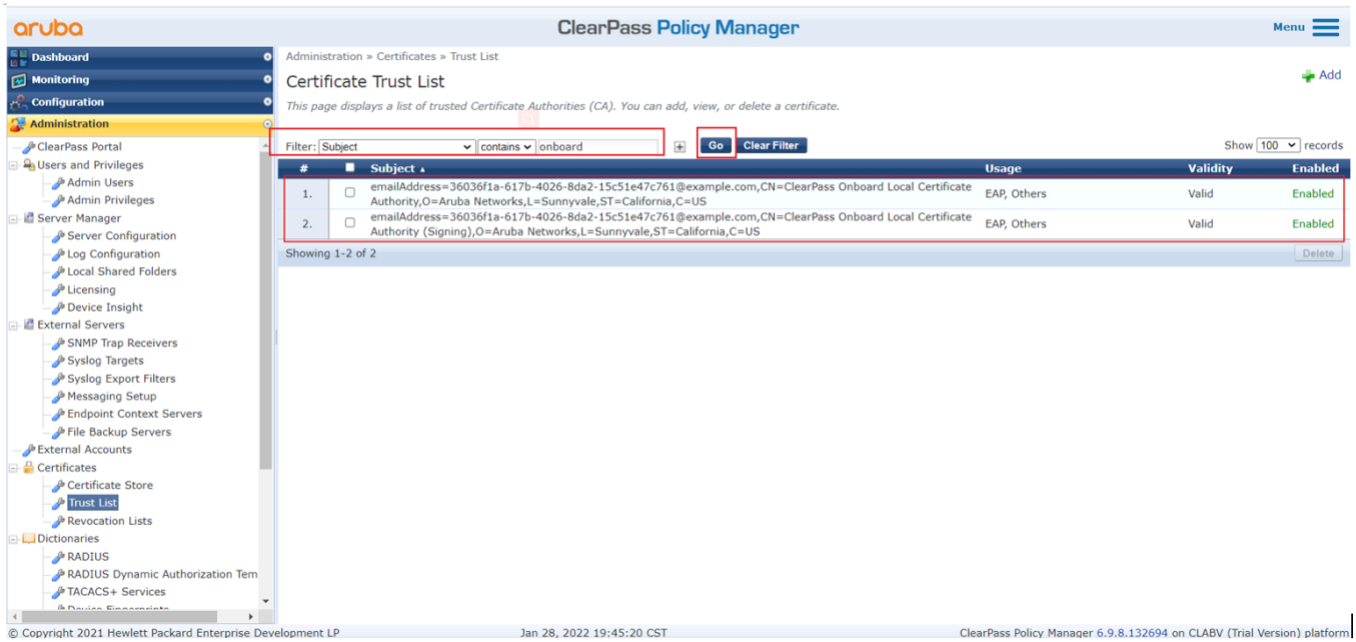



第2步： 更新 Onboard CA 设置 Usage 包含 RadSec

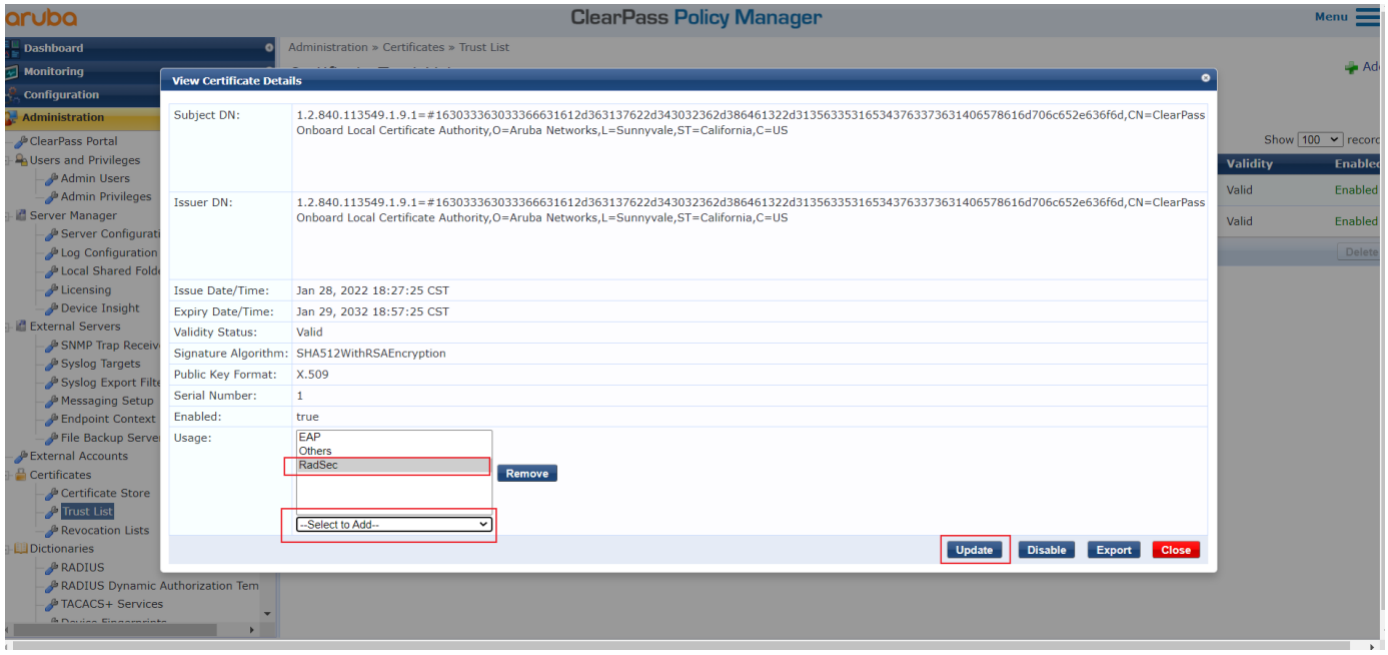
登录到 ClearPass Policy Manager 管理界面，导航到 Administration » Certificates » Trust List 页面，在 Filter：Subject，contains 后输入 onboard，点击 Go 按钮，过滤 Onboard 证书，得到两张 ClearPass Onboard CA:

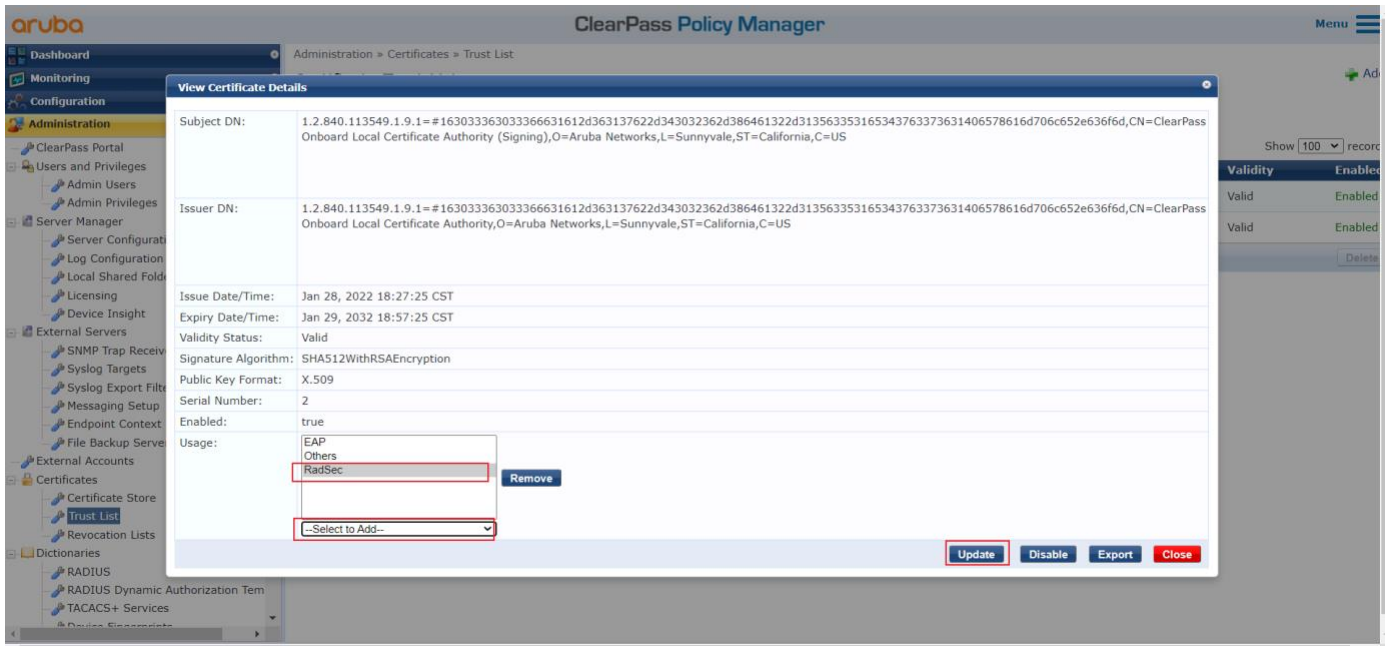
CN=ClearPass Onboard Local Certificate Authority

CN=ClearPass Onboard Local Certificate Authority (Signing)

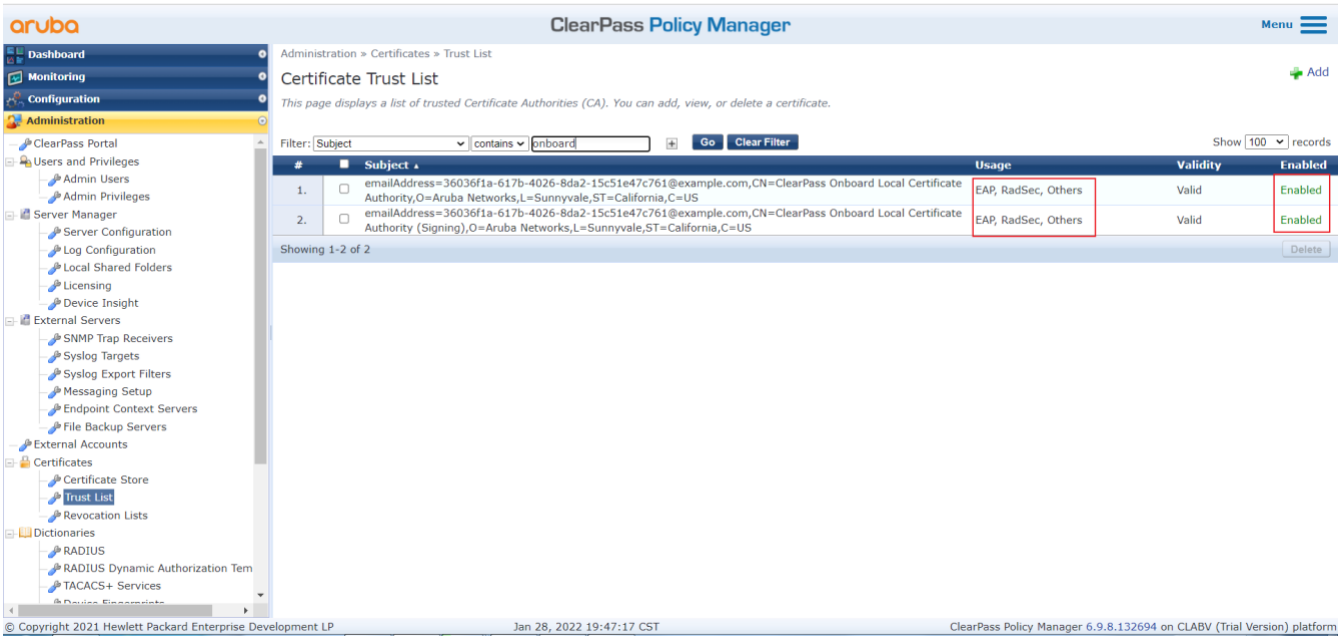


分别点击每张证书，进入到详细配置页，在 Usage 下面的 Select to Add，选择增加 RadSec，最后点击 Update 按钮



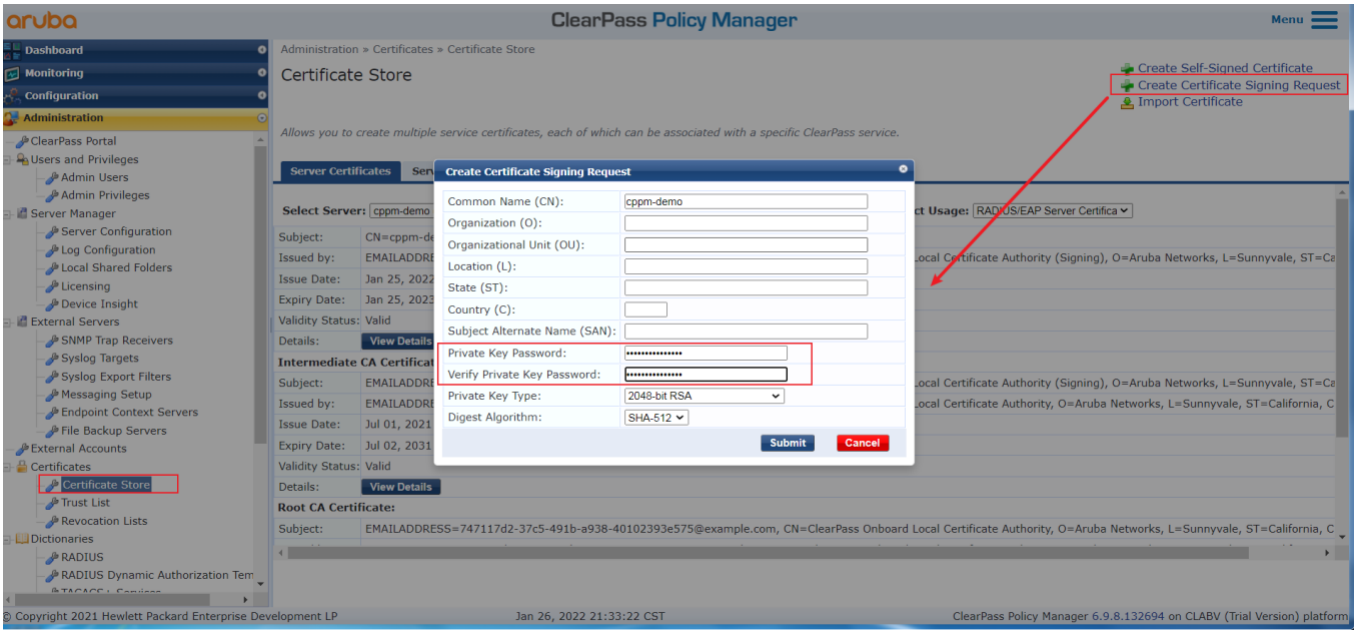




最后确认，这两张 Root CA 的 Usage 中都具备了 RadSec，且状态是 Enabled

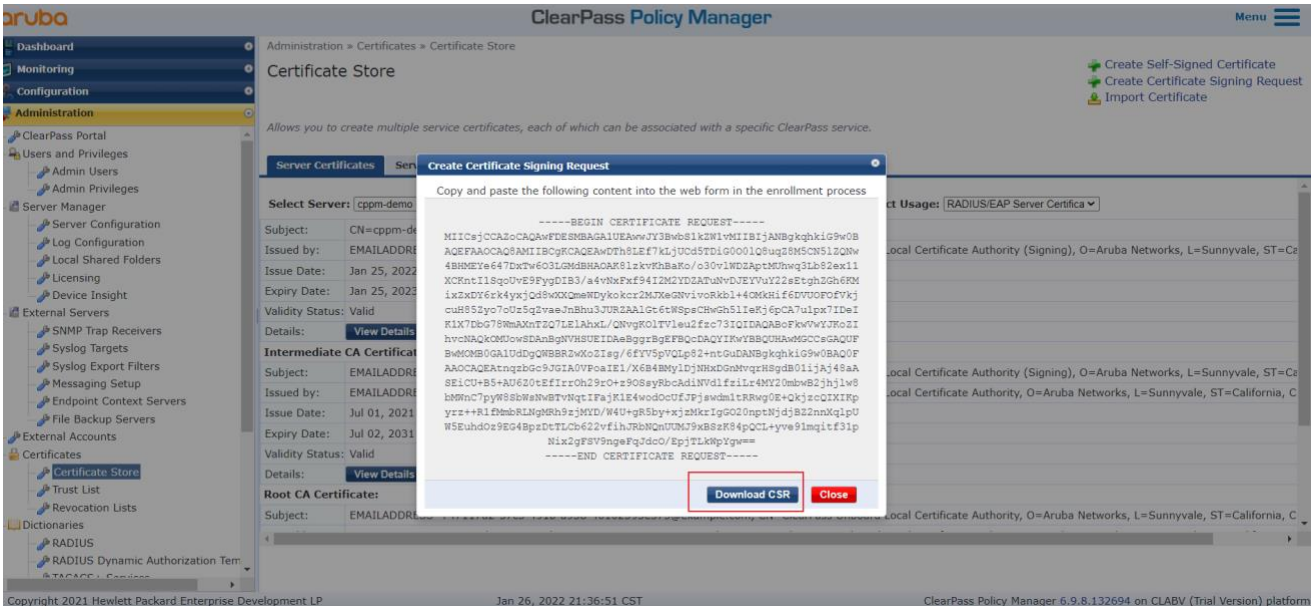



第3步： 在 ClearPass Policy Manager 上创建 CSR，然后由 Onboard Root CA 来签发一张 HTTPs 证书，最后再导入到 ClearPass 上，完成 ClearPass Radsec Server 证书的签发

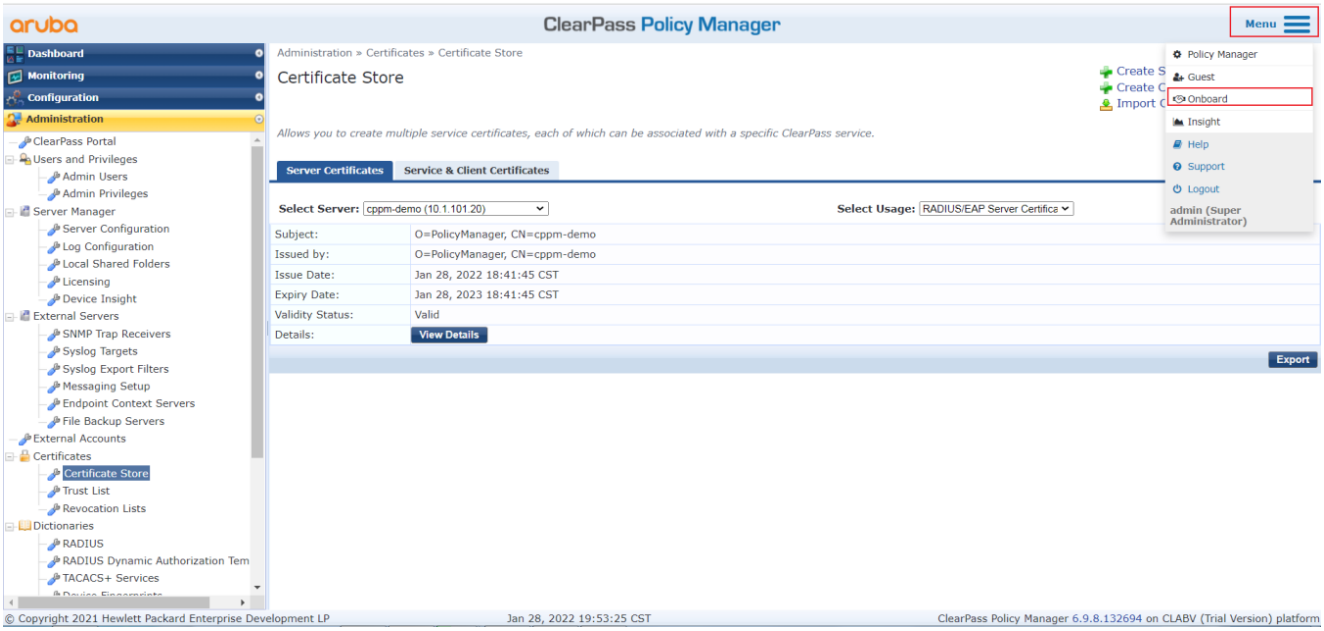
导航到 Administration » Certificates » Certificate Store ，点击右上角的 Create Certificate Signing Request，仅仅输入 Private key Password 即可，最后点击 Submit 按钮



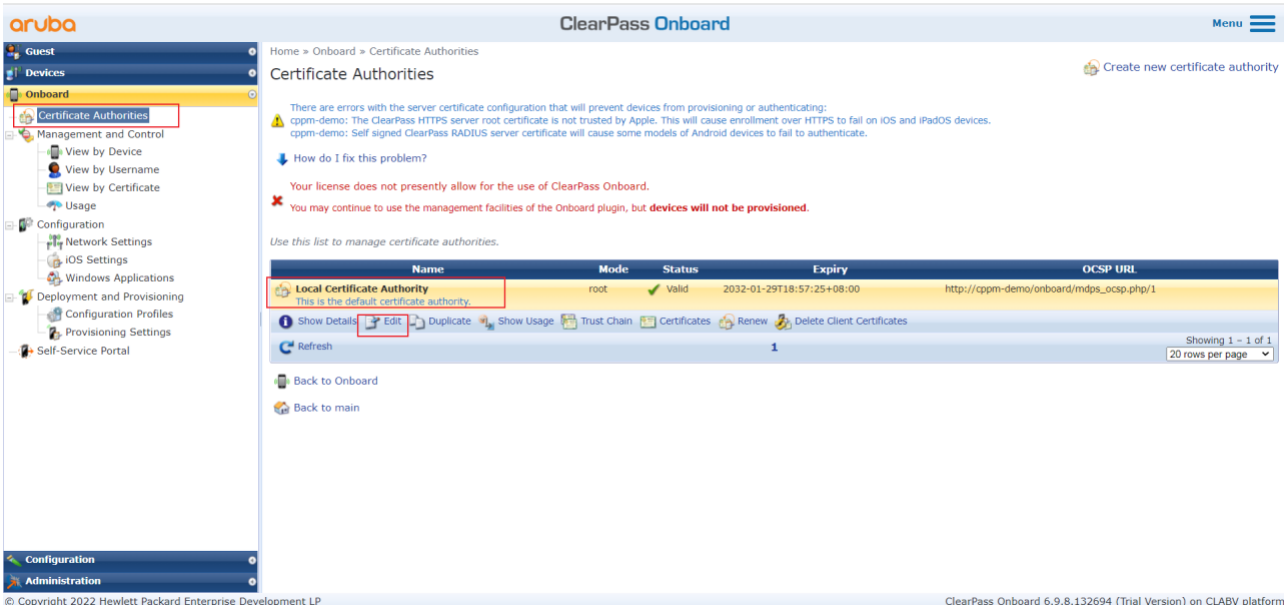
得到 CSR 证书签名请求文件，点击 Download CSR，将文件下载到电脑本地（记住保存的路径，默认文件名称是 CertSignRequest.csr）



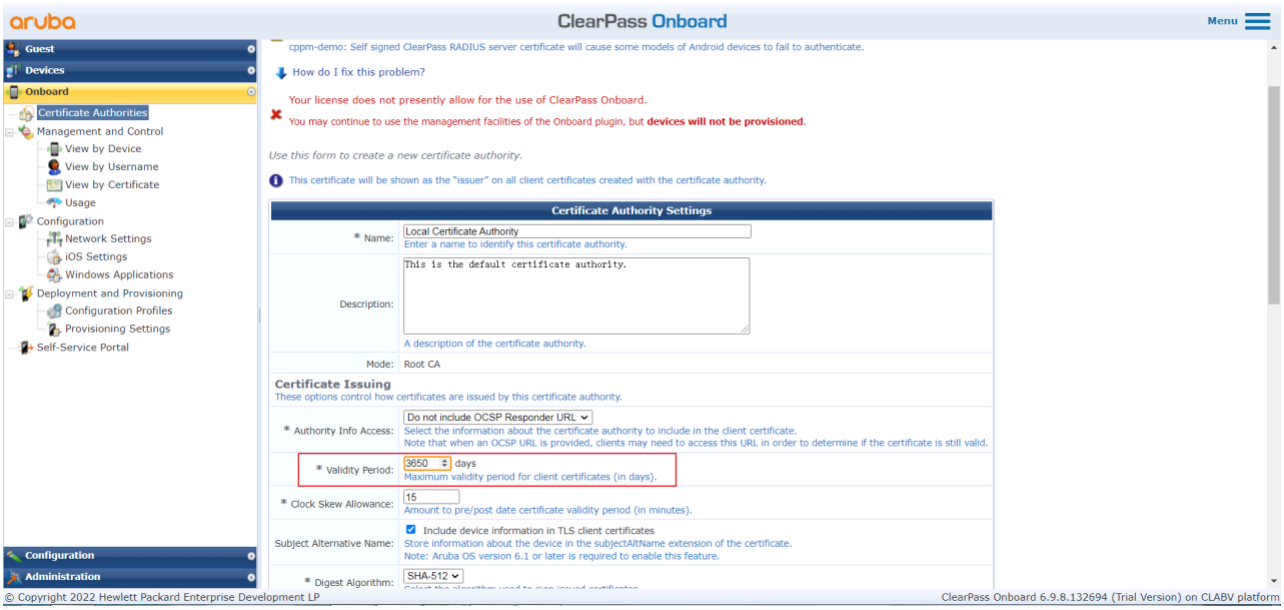

鼠标点击右上角 Menu 按钮，弹出菜单中，选择 Onboard，进入到 Onboard 管理页面。

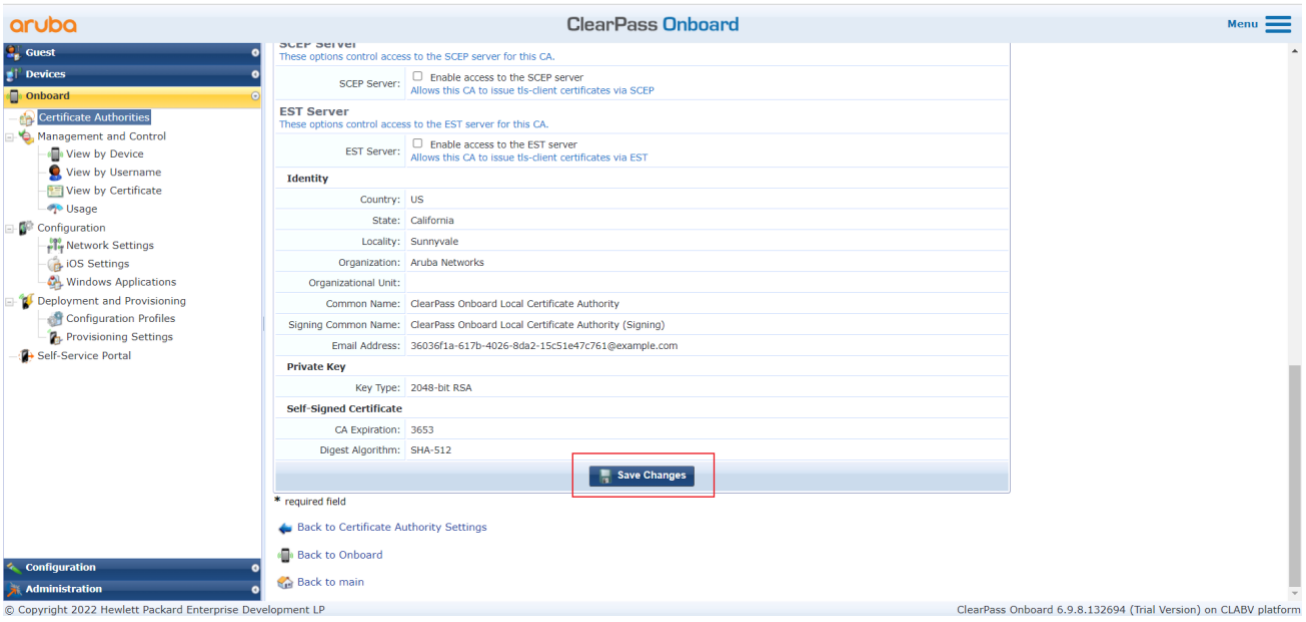



导航到 Onboard » Certificate Authorities 页面，选择 Local Certificate Authority，然后弹出下面的隐藏菜单，点击 Edit 按钮，进入到编辑界面。

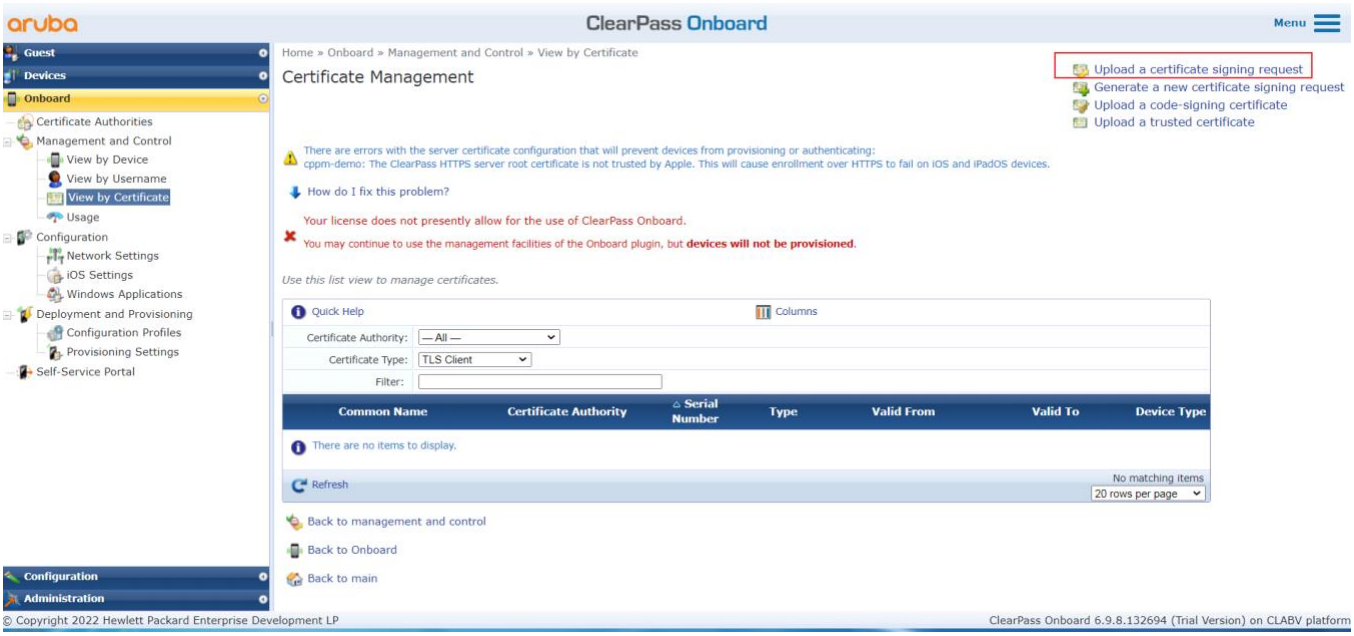

aruba
ClearPass Onboard
Menu
Guest
Devices
Onboard
Certificate Authorities
Management and Control
View by Device
View by Username
View by Certificate
Usage
Configuration
Network Settings
iOS Settings
Windows Applications
Deployment and Provisioning
Configuration Profiles
Provisioning Settings
Self-Service Portal
Configuration
Administration
Home » Onboard » Certificate Authorities
Certificate Authorities
Create new certificate authority
There are errors with the server certificate configuration that will prevent devices from provisioning or authenticating:
cppm-demo: The ClearPass HTTPS server root certificate is not trusted by Apple. This will cause enrollment over HTTPS to fail on iOS and iPadOS devices.
cppm-demo: Self signed ClearPass RADIUS server certificate will cause some models of Android devices to fail to authenticate.
How do I fix this problem?
Your license does not presently allow for the use of ClearPass Onboard.
You may continue to use the management facilities of the Onboard plugin, but devices will not be provisioned.
Use this list to manage certificate authorities.
Name
Mode
Status
Expiry
OCSP URL
Local Certificate Authority
This is the default certificate authority.
root
Valid
2032-01-29T18:57:25+08:00
http://cppm-demo/onboard/mdps_ocsp.php/1
Show Details
Edit
Duplicate
Show Usage
Trust Chain
Certificates
Renew
Delete Client Certificates
Refresh
1
Showing 1 – 1 of 1
20 rows per page
Back to Onboard
Back to main
© Copyright 2022 Hewlett Packard Enterprise Development LP
ClearPass Onboard 6.9.8.132694 (Trial Version) on CLABV platform

设置 Validity Period:3650 天（10 年），最后点击最下面的 Save Changes 按钮



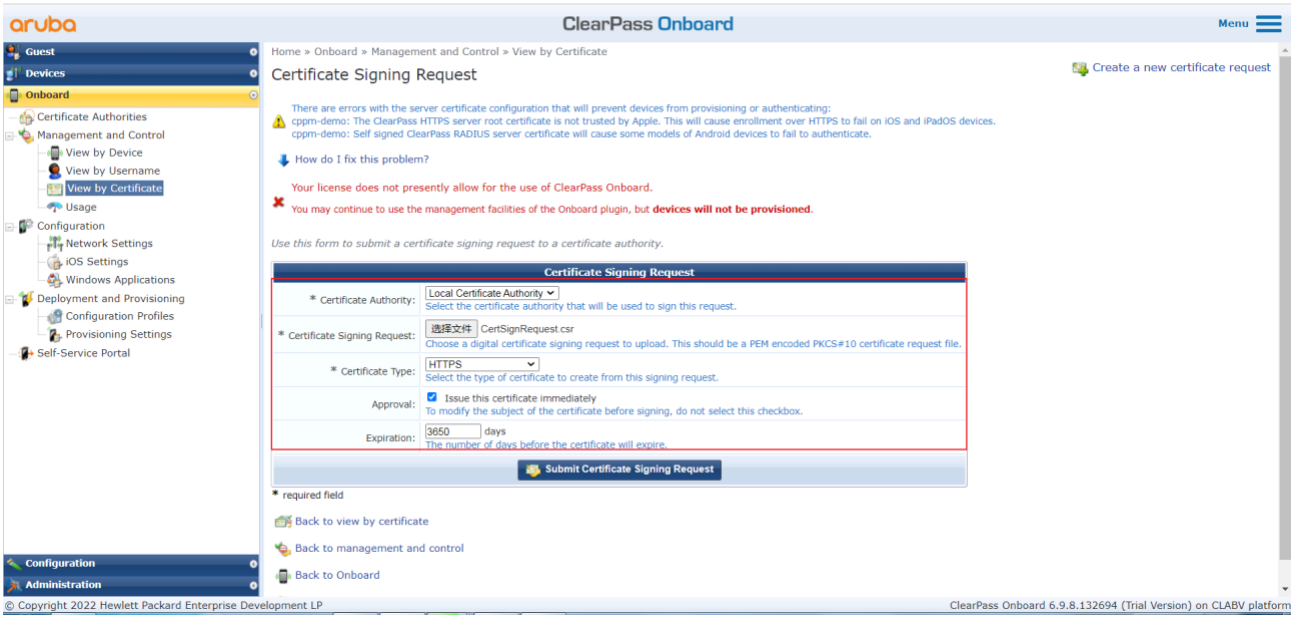



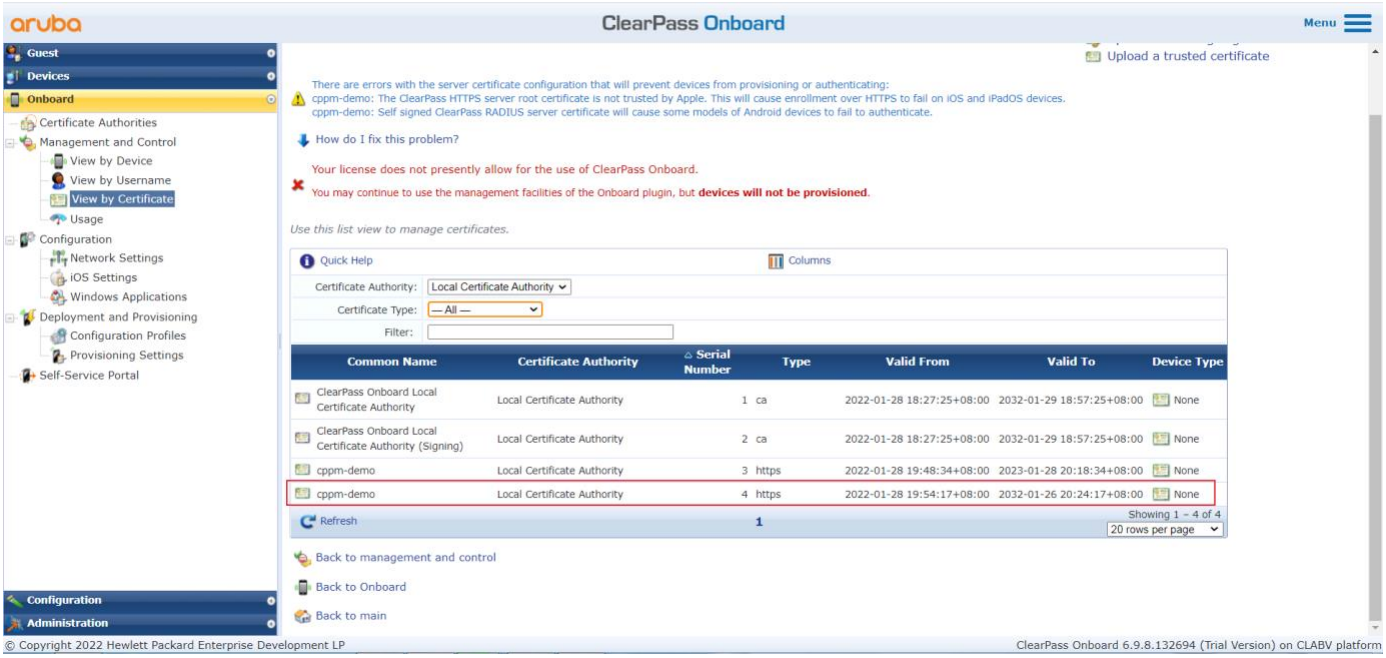

导航到 Onboard » Management and Control » View by Certificate 页面，点击右上角的 Upload a certificate signing request 按钮。




- Certificate Authority　选择 Local Certificate Authority，
- Certificate Signing Request　选择之前保存到电脑本地的 CSR 文件（CertSignRequest.csr）
- Certificate Type　选择 HTTPS （注意这里是 HTTPS 类型证书）
- Approval　（Issue this certificate immediately）　勾选
- Expiration 设置 3650 days

最后点击 Submit Certificate Signing Request 按钮，得到 HTTPS 证书

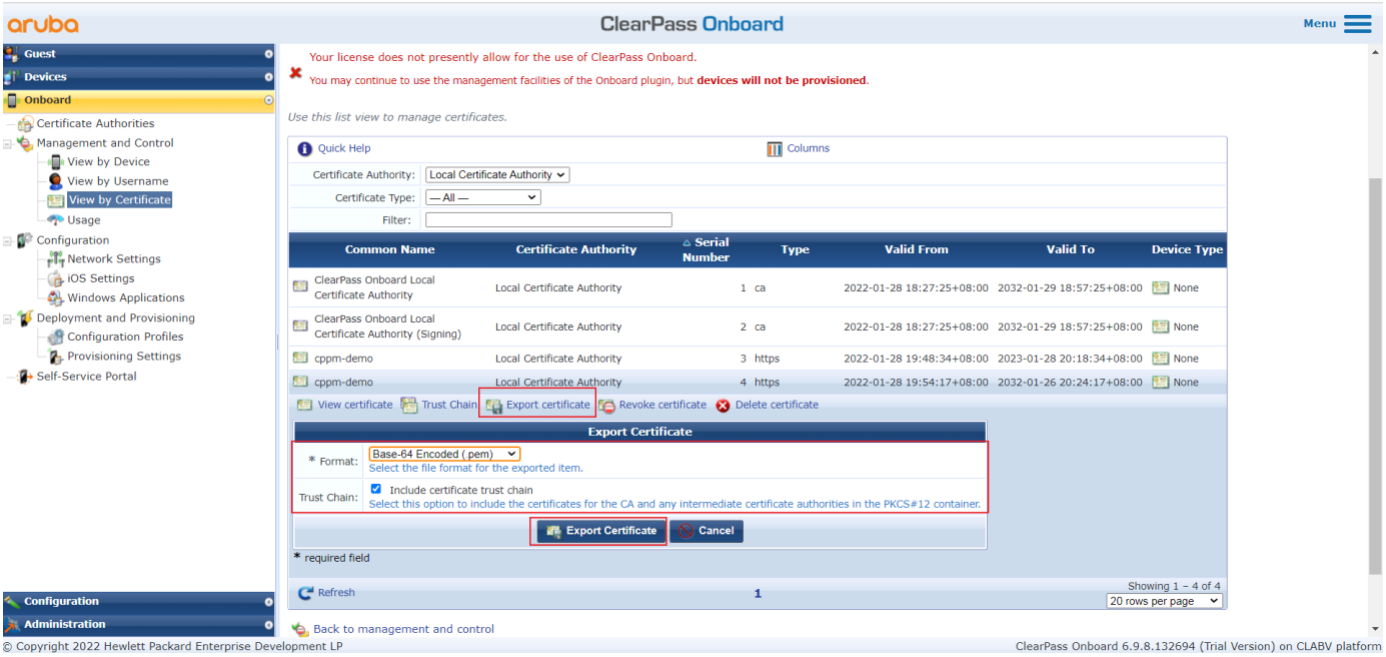




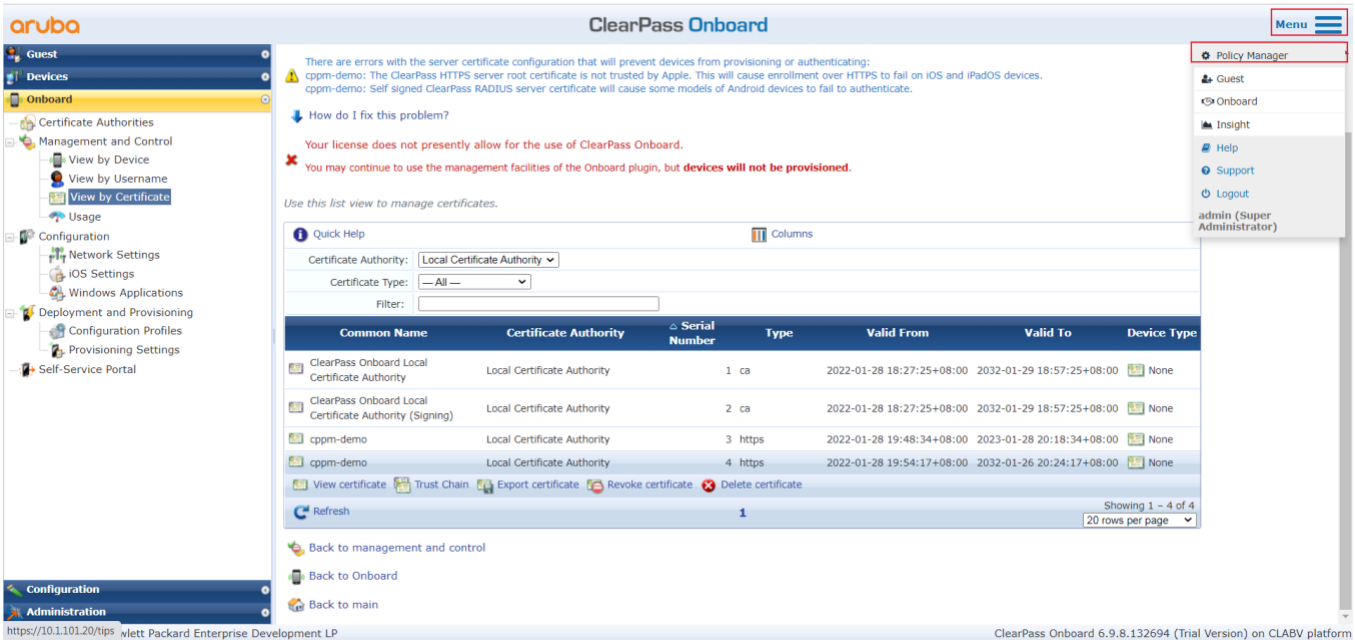

选中签发好的 HTTPS 证书，弹出隐藏菜单，点击 Export certificate 按钮，弹出导出设置，

- Format 选择 Base-64 Encoded (.pem)
- Trust Chain (Include certificate trust chain) 勾选

最后点击 Export Certificate 按钮，导出到电脑本地（记住保存路径, 本次演示中的文件名是 cppm-demo.pem）




鼠标点击右上角 Menu 按钮，弹出菜单中，选择 Policy Manager，进入到策略管理页面。

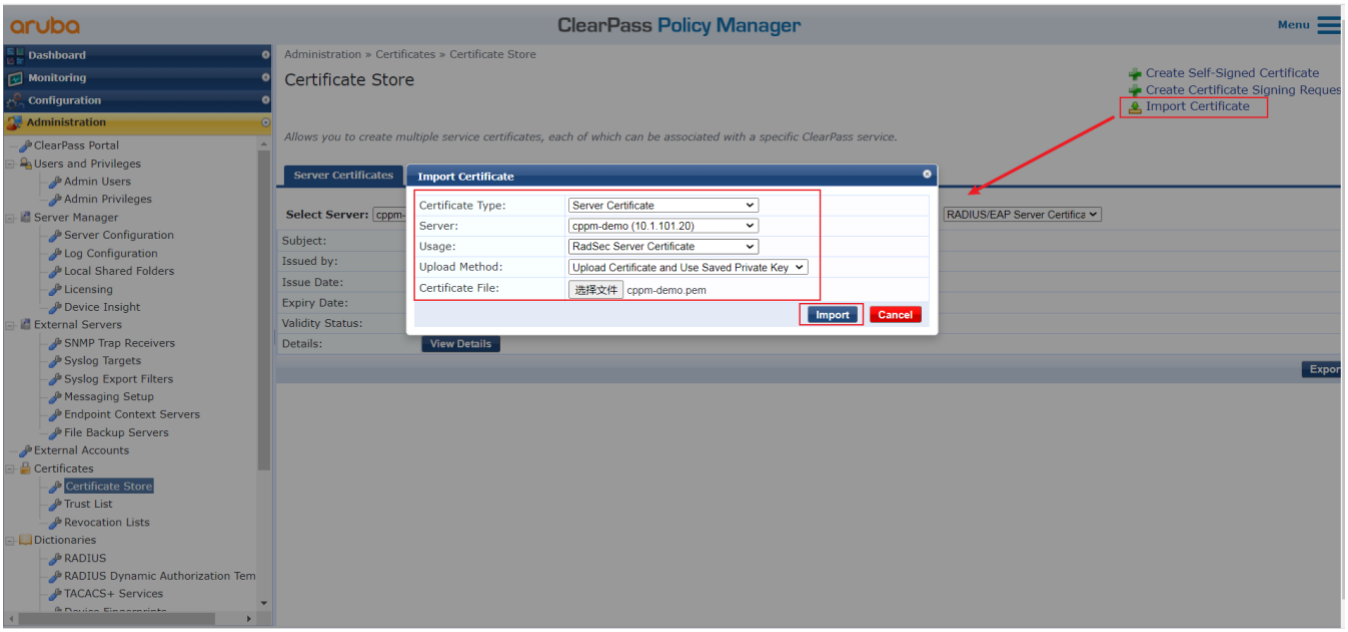



导航到 Administration » Certificates » Certificate Store 页面，点击右上角的 Import Certificate 按钮，

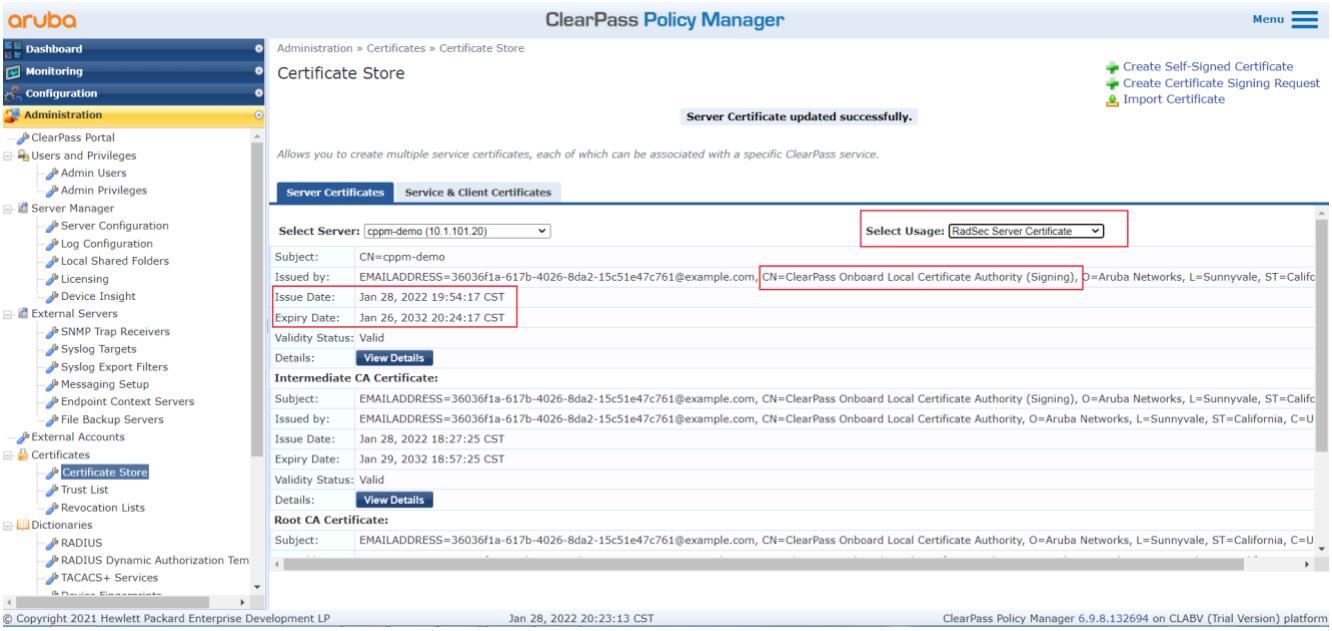
- Certificate Type 选择 Server Certificate
- Server 选择 你环境中需要的 ClearPass node
- Usage 选择 RadSec Server Certificate

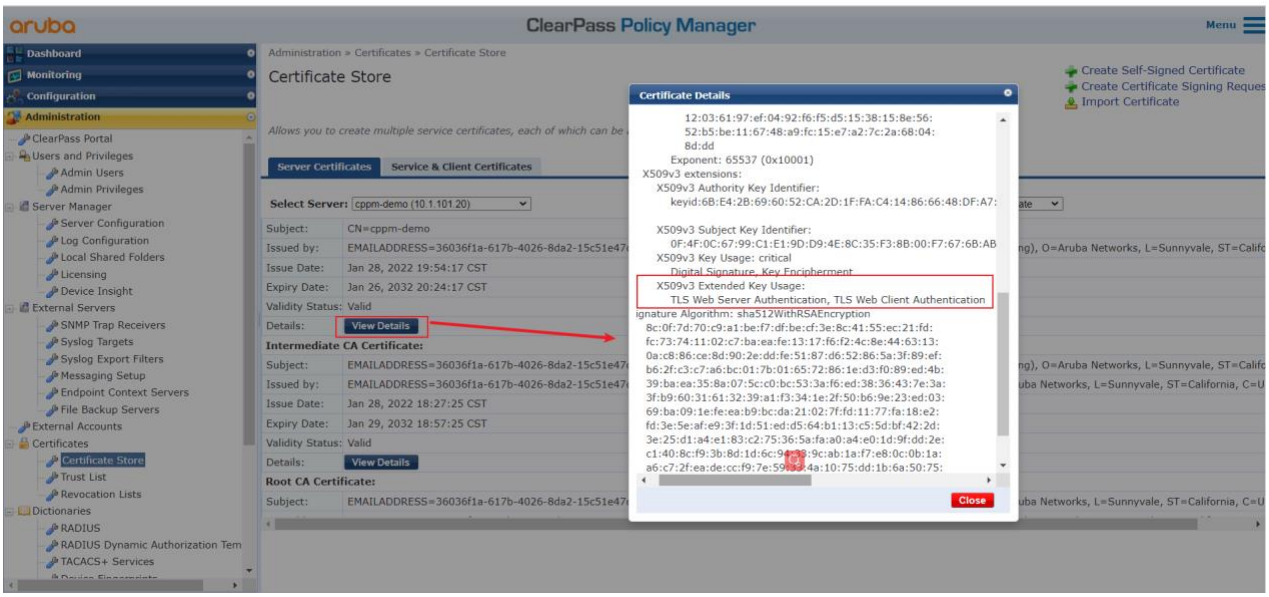
- Upload Method 选择 Upload Certificate and Use Saved Private Key
- Certificate File 选择前面步骤中签发好的 HTTPs 证书，格式为.pem（本次演示中的文件名是 cppm-demo.pem）

最后点击 Import 按钮



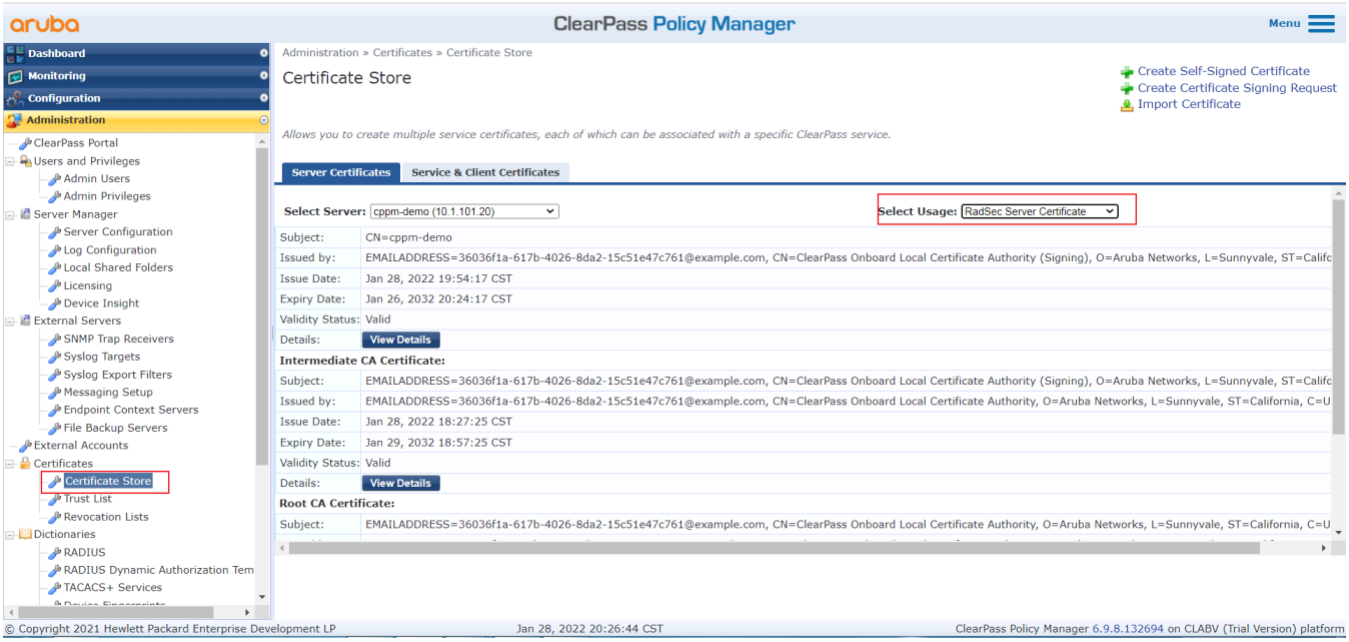

页面提示 Server Certificate uploaded successful 后，Select Usage 选择 RadSec Server Certificate，查看签发好的 HTTPS 证书信息是否证正确。

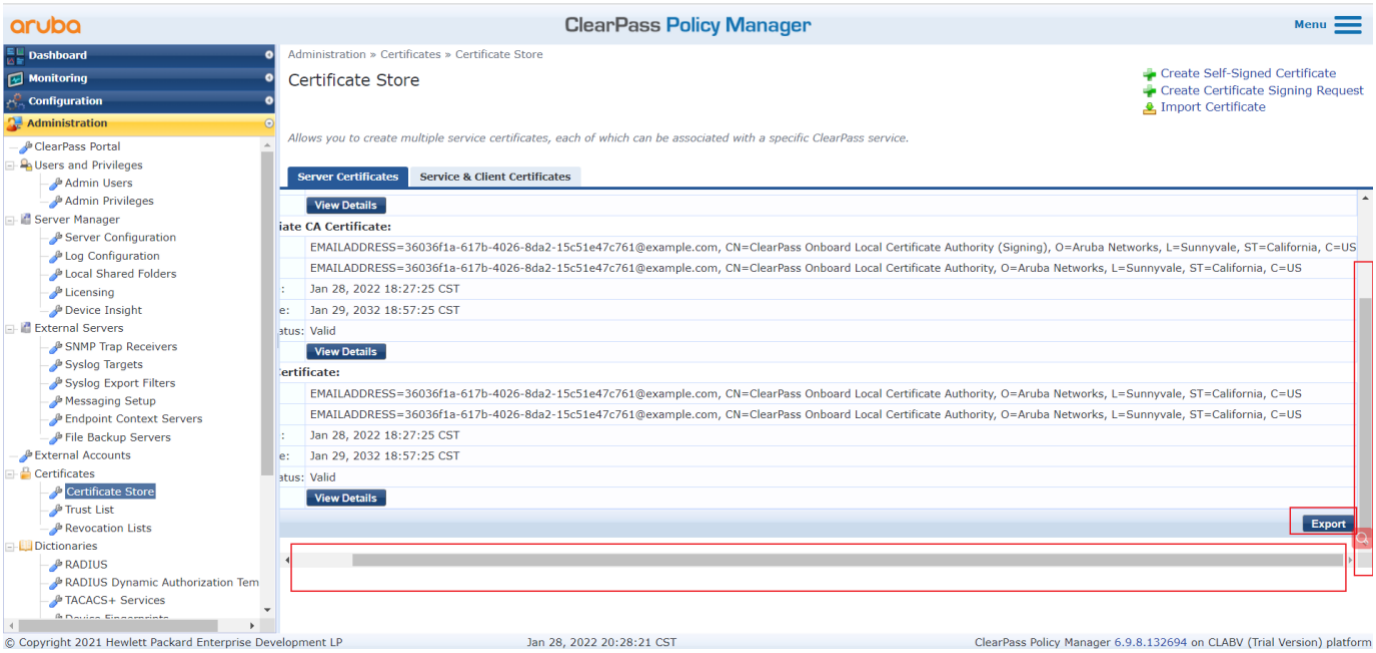




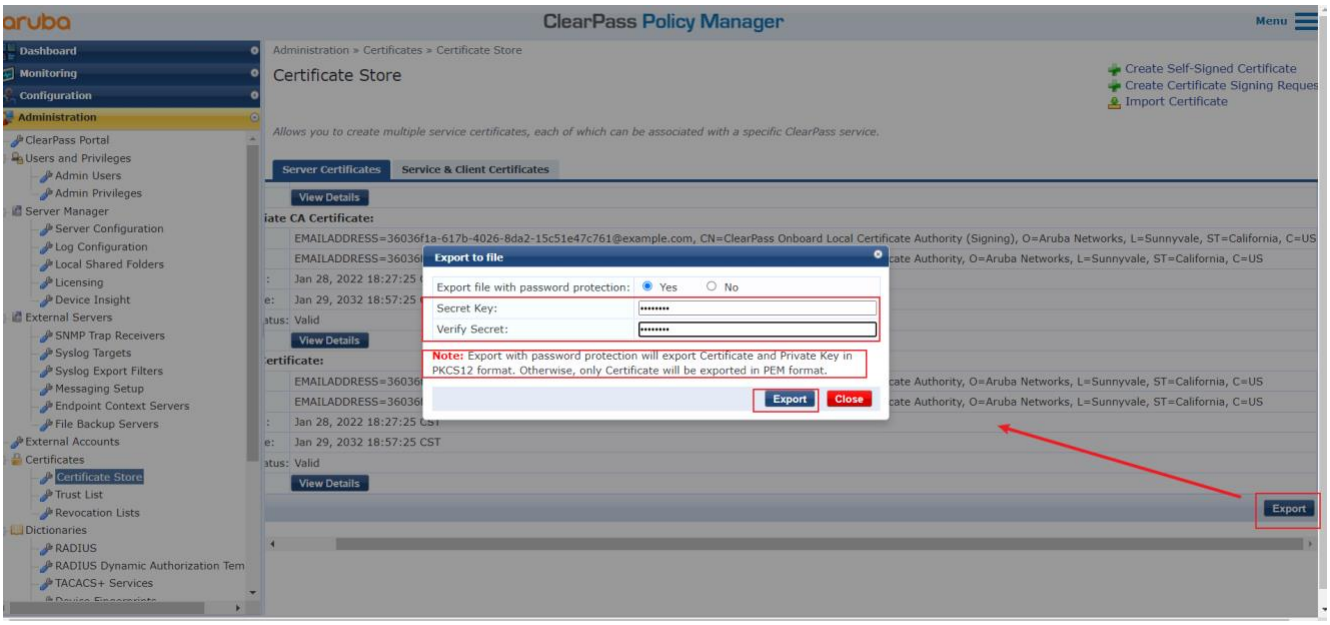

第4步： 在 CLEARPASS 上将前面已经导入成功的 radsec server certificate 服务器证书（HTTPs 类型的），再次导出为 PKCS12 格式（含 Private Key），必须要设置 secret key。

导航到 Administration » Certificates » Certificate Store 页面， Select Usage 选择 RadSec Server Certificate， 右边竖条拉到最低，底部横条拉到右边，点击 Export 按钮



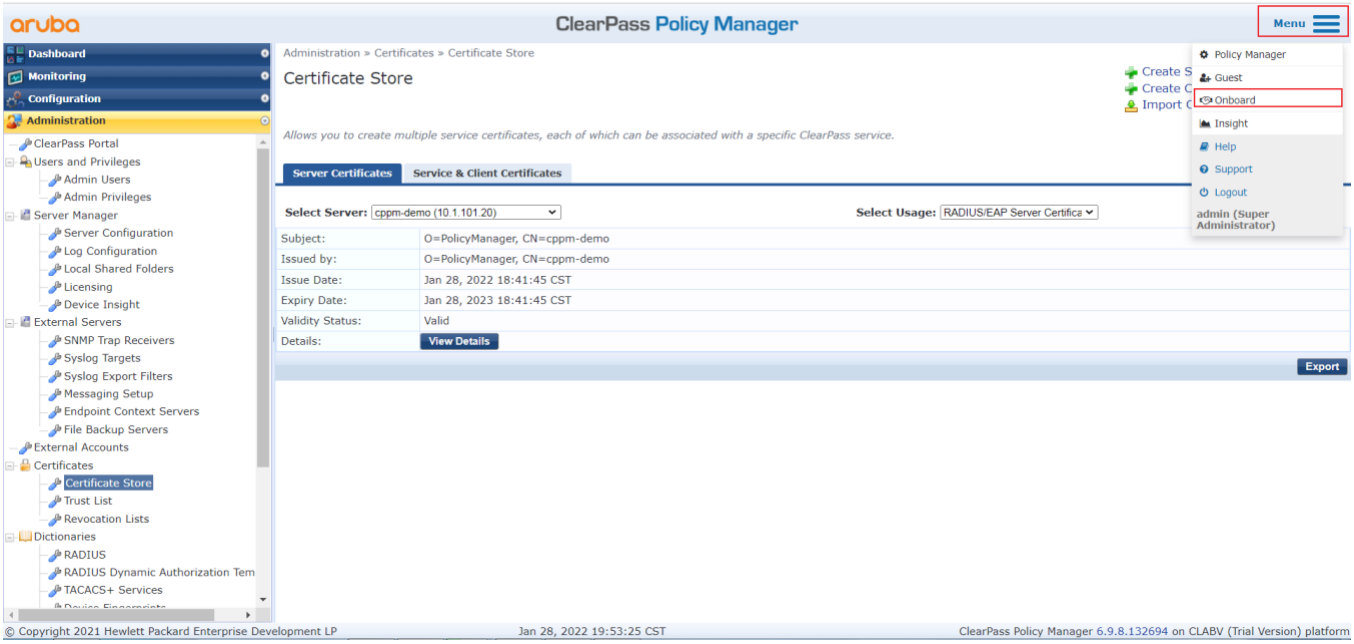



必须输入 Secret Key（才会导出含 Private key 的 PKCS12 格式证书），然后点击 Export 按钮，保存到电脑本地（记住保存路径，默认文件名是 RadSecServerCertificate.p12）




第5步：　　将 onboard root ca 或者 Onboard root CA( signing) 导出到电脑本地（格式为 .pem）

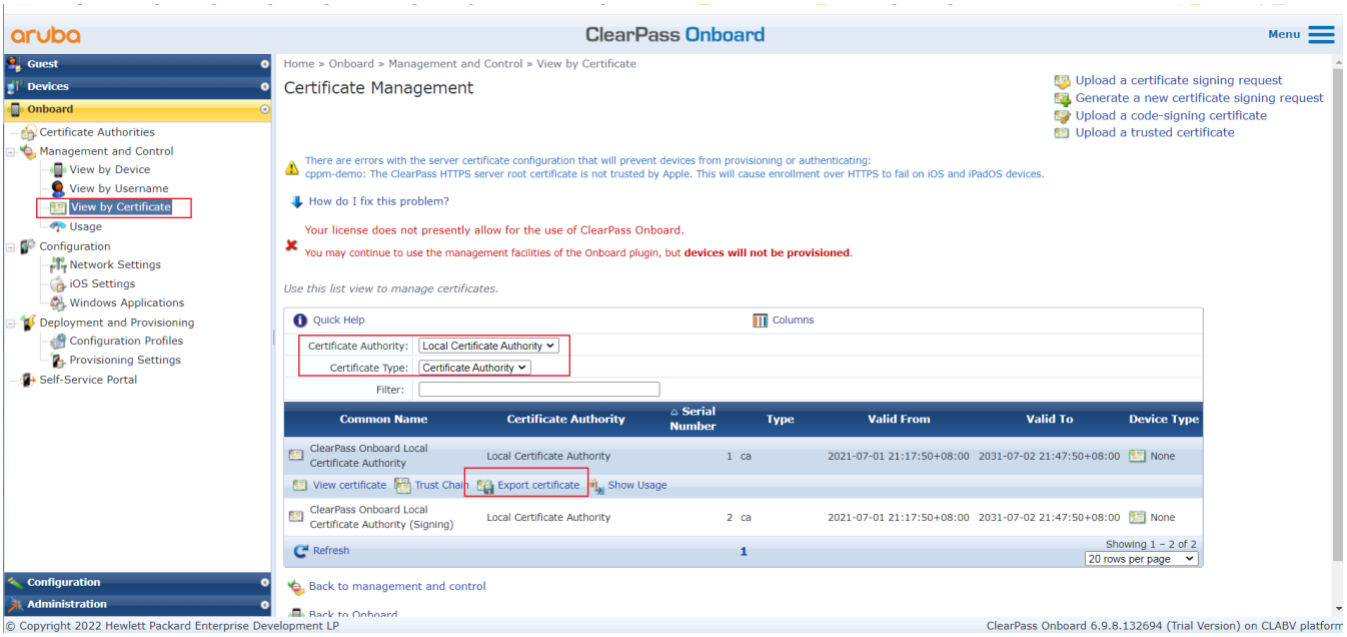
鼠标点击右上角 Menu 按钮，弹出菜单中，选择 Onboard，进入到 Onboard 管理页面。




导航到 Onboard » Management and Control » View by Certificate 页面，

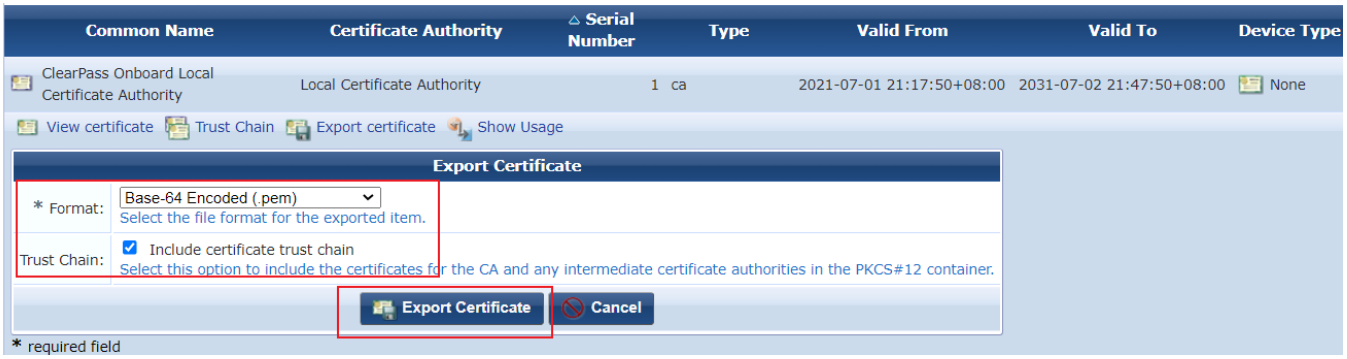
- Certificate Authority 选择 Local Certificate Authority （当然如果你创建了其他的 Root CA，选择相应的证书名称即可）
- Certificate Type 选择 Certificate Authority

选择 ClearPass Onboard Local Certificate Authority 证书，弹出隐藏菜单，点击 Export certificate 按钮，

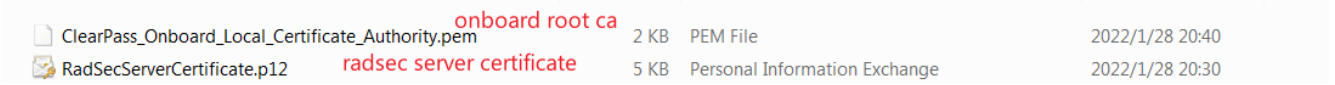


- Format 选择 Base-64 Encoded（.pem）
- Trust Chain (Include certificate trust chain) 勾选

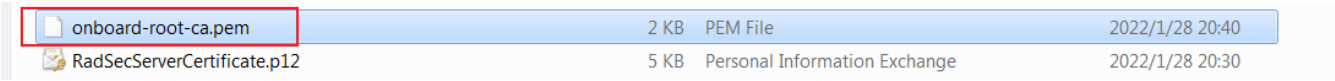
点击 Export Certificate 按钮，导出到电脑本地（记住保存路径，默认文件名是 ClearPass_Onboard_Local_Certifixate_Authority.pem）




到此，你的电脑上应该有两张证书：



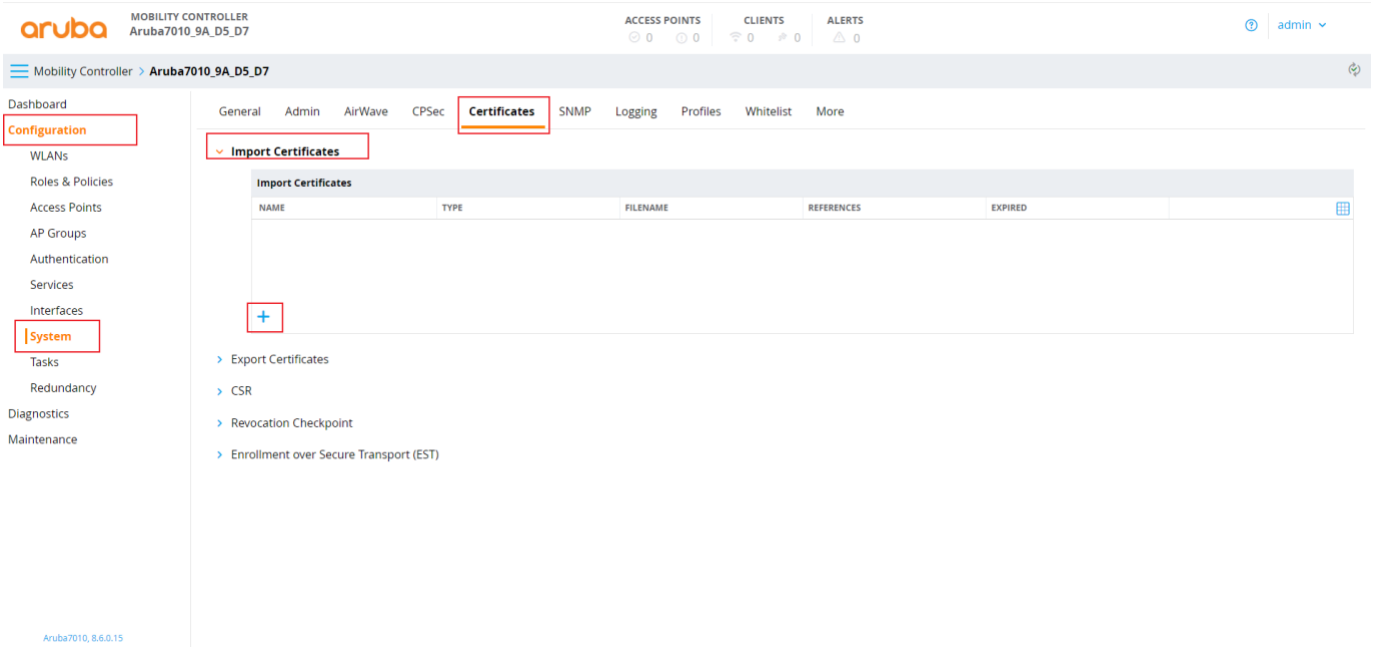

由于系统导出的文件名称太长，我们可以更改下名称，便于后面控制器上的导入操作。




### 1.3.3 控制器侧配置

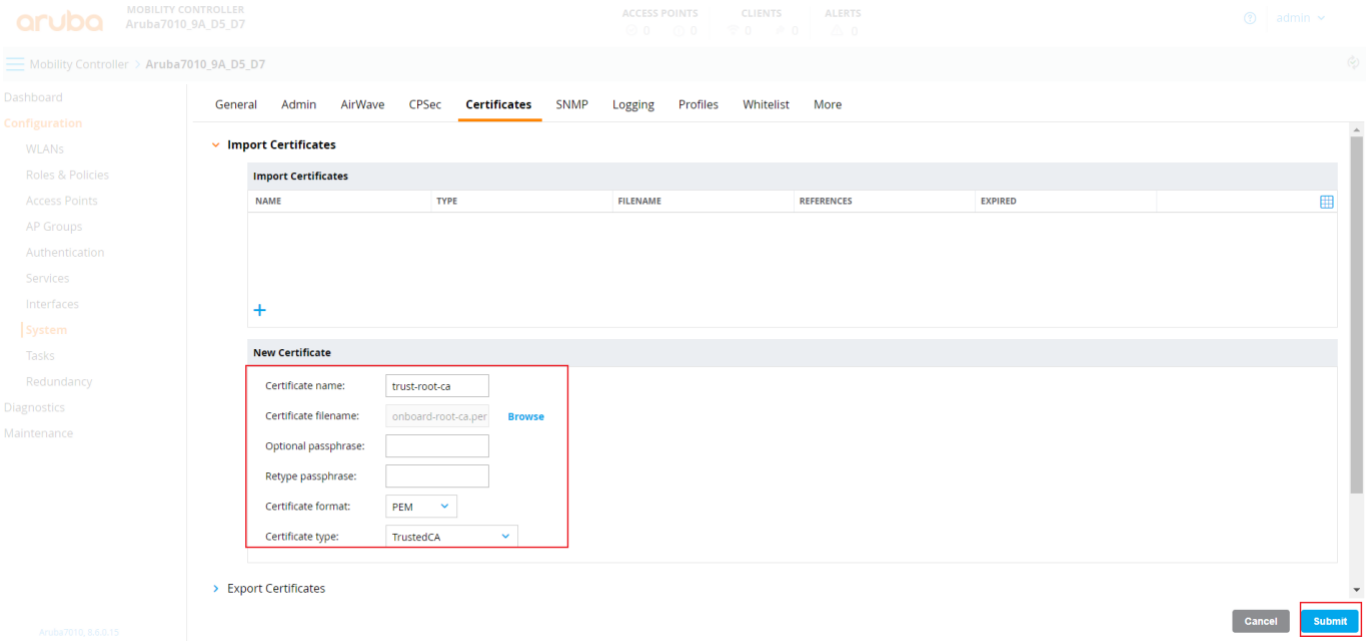
第1步：　　将前面的 Onboard root ca　（.pem 格式） 和 clearpass radsec server certificate（PKCS12 格式）　都导入到控制器中

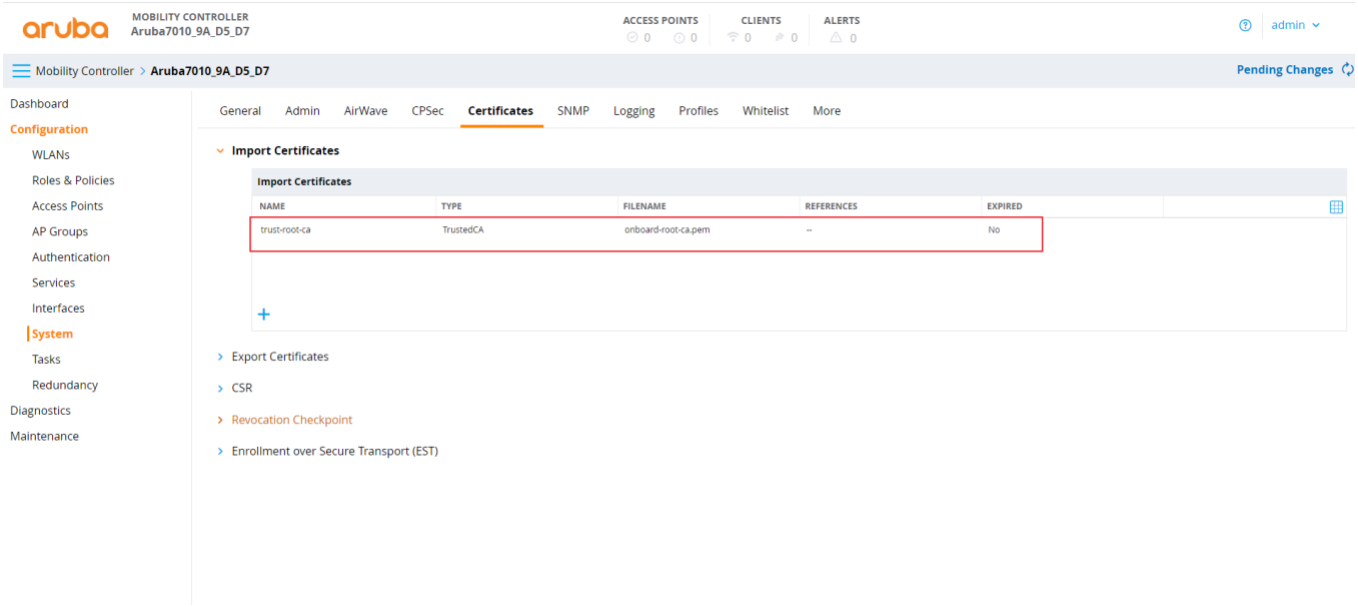
导航到 Configuration» System » Certificates » Import Certificates，　点击下面的+ 按钮，新增一个证书




- Certificate name 设置自己定义的名称，这里演示为 trust-root-ca
- Certificate filename 选择 onboard-root-ca.pem
- Certificate format 选择 PEM
- Certificate type 选择 TrustedCA

最后点击 Submit 按钮提交配置

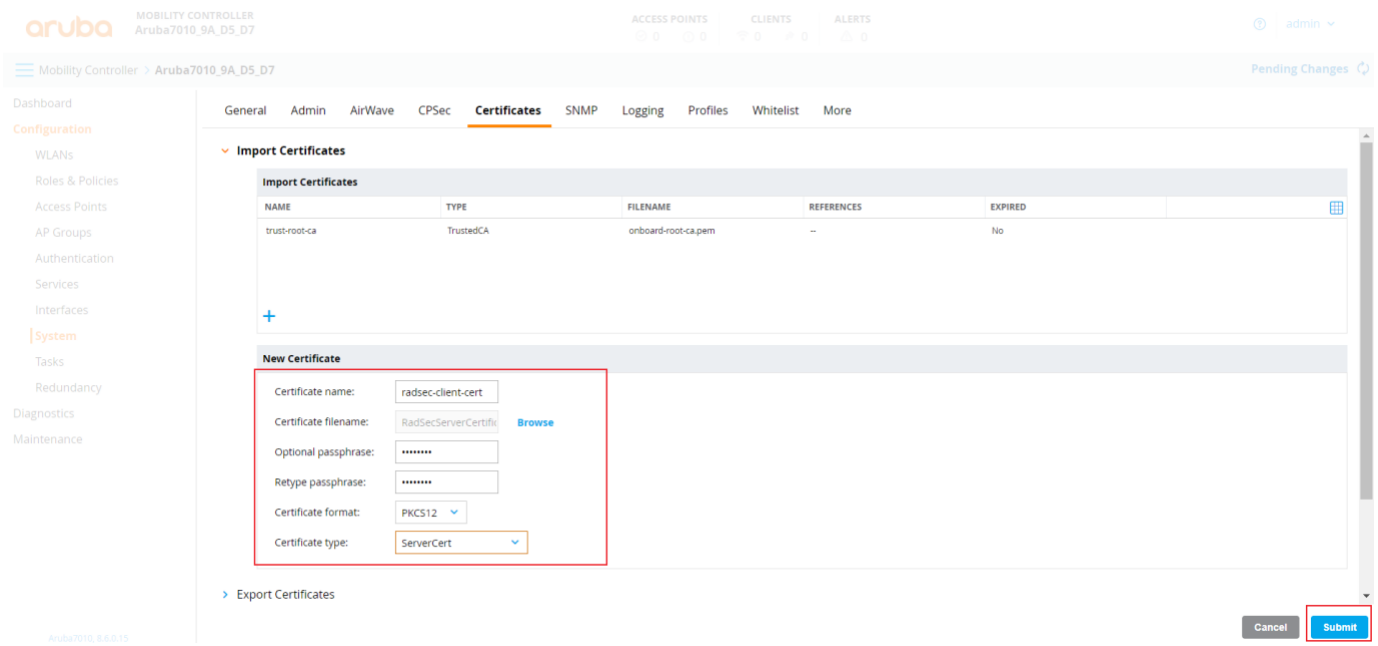




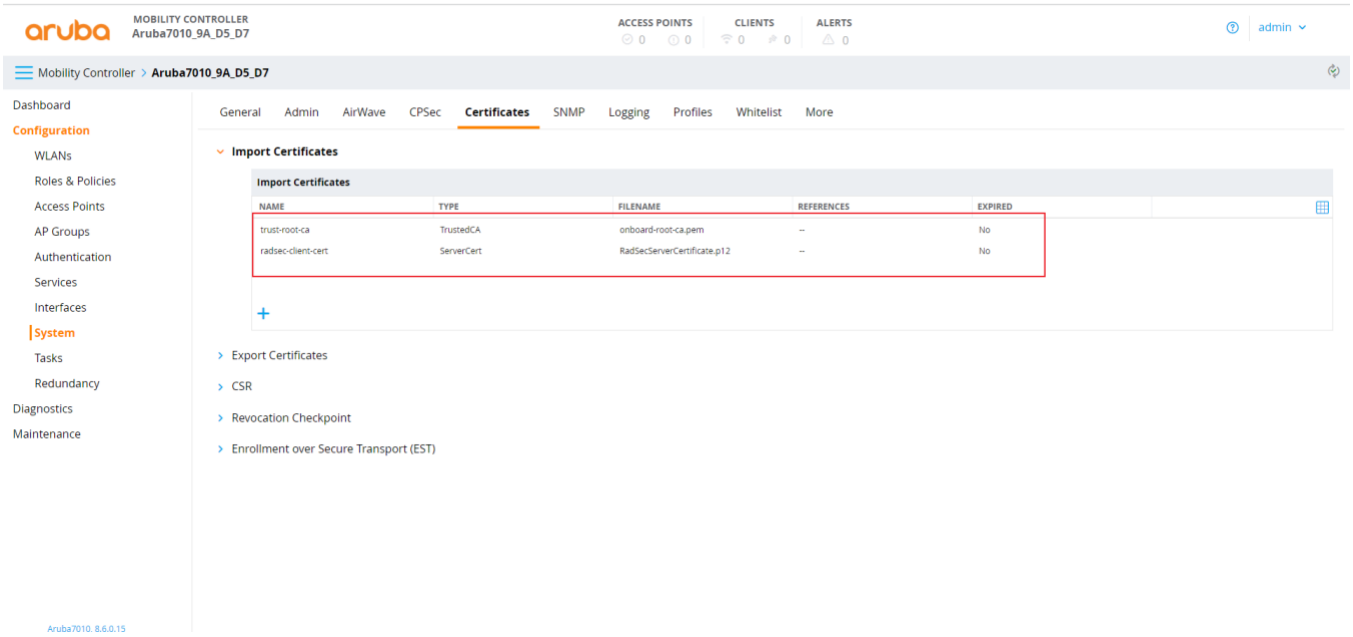

继续点击+ 按钮，添加另外一张证书。

- Certificate name 设置自己定义的名称，这里演示为 radsec-client-cert
- Certificate filename 选择 RadSecServerCertificate.p12
- Optional passphrase 输入之前导出 radsec server certificate 证书时的 Secret Key
- Certificate format 选择 PKCS12
- Certificate type 选择 ServerCert

最后点击 Submit 按钮提交配置

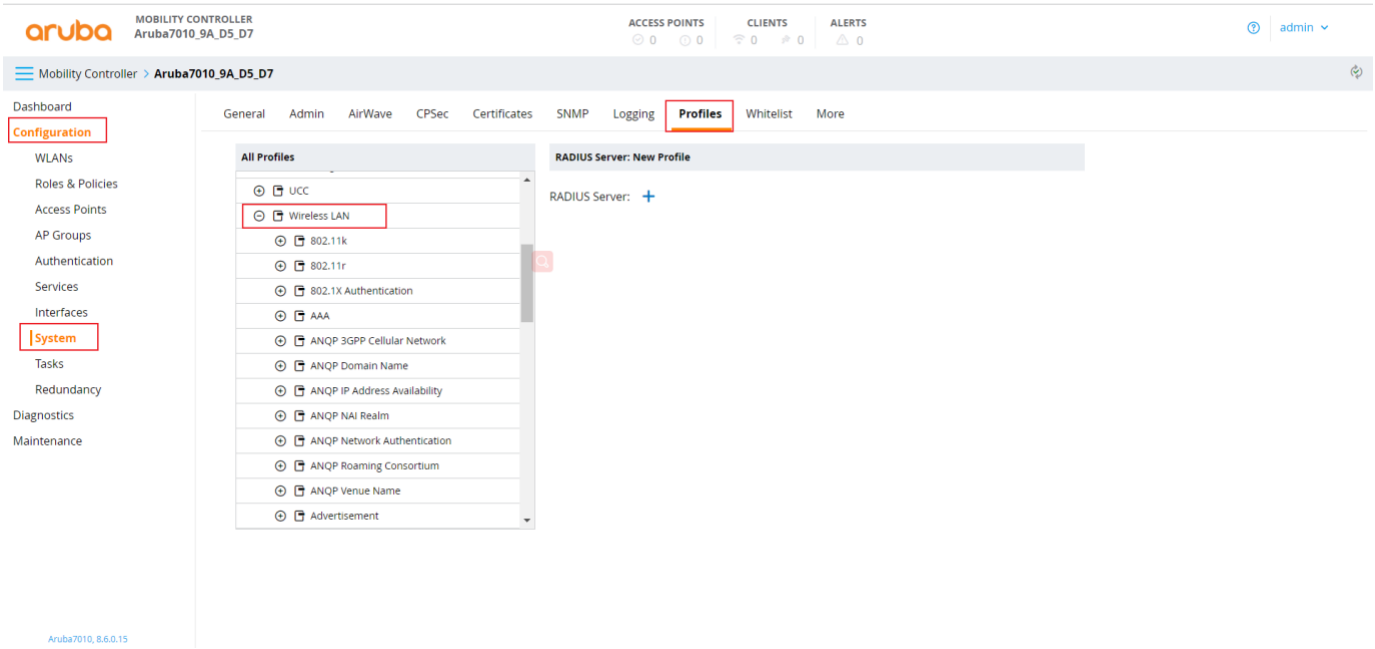



最后两张证书上传成功，如果右上角有 Pending Changes， 请点击保存部署。

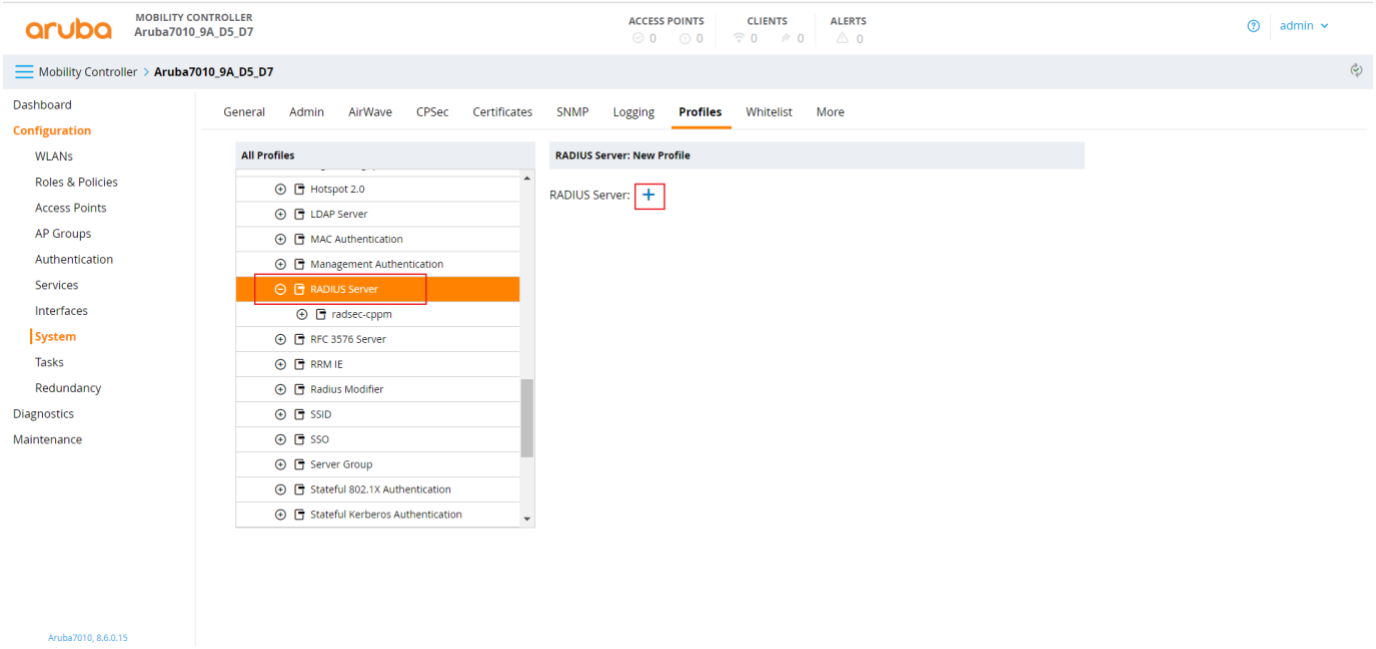



第2步：　　在控制器上创建 Radius Server Profile

导航到 Configuration» System » Profiles，展开 Wireless LAN

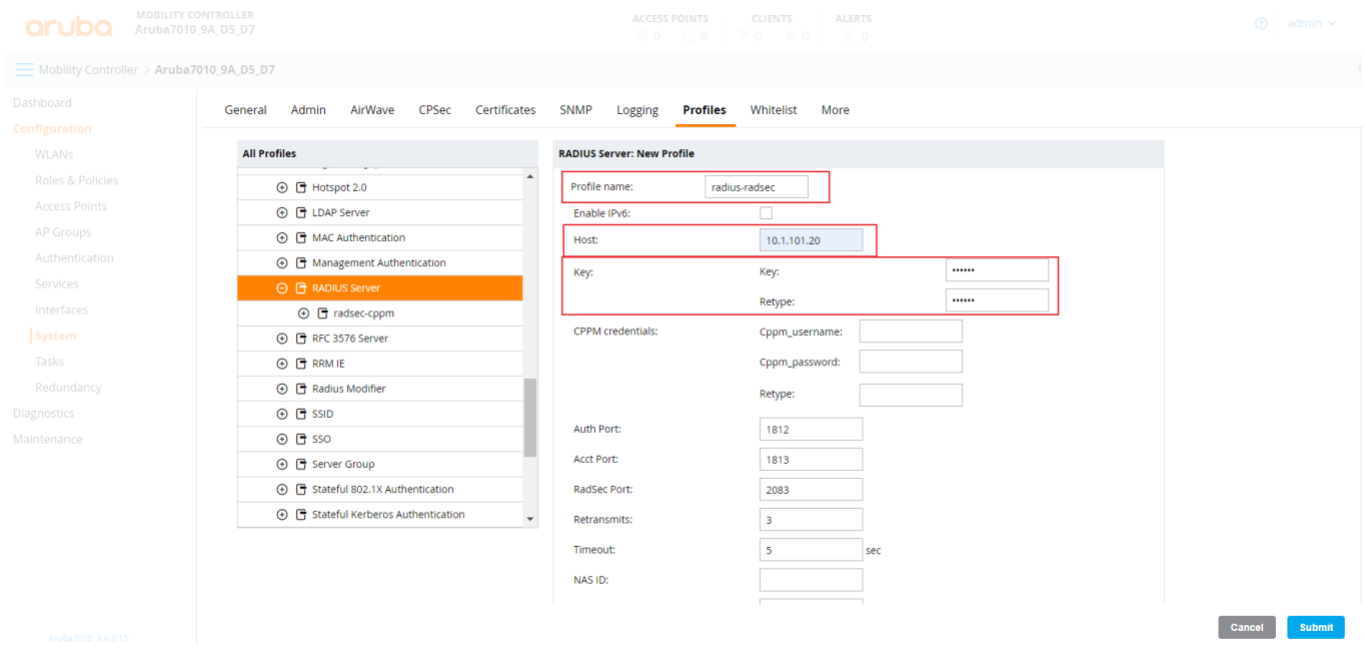


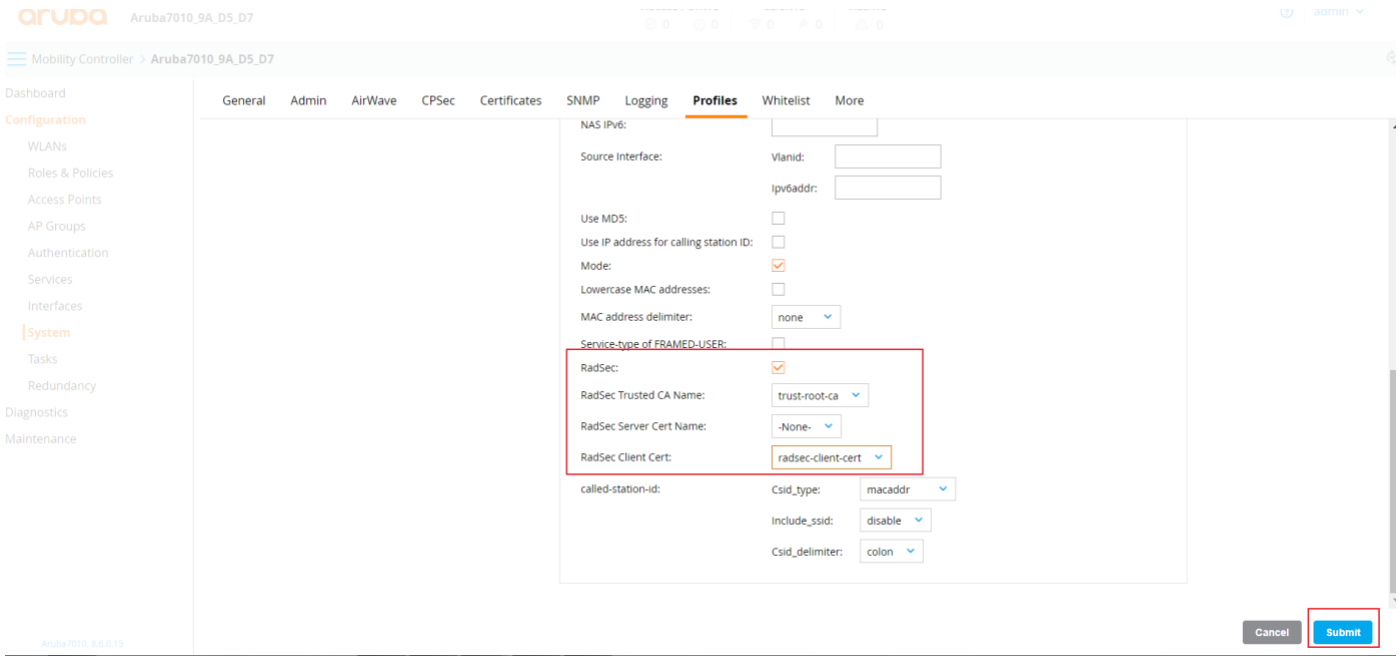
找到并鼠标点击 RADIUS Server，在右边窗口中，点击+ 按钮，新增一个 RADIUS Server



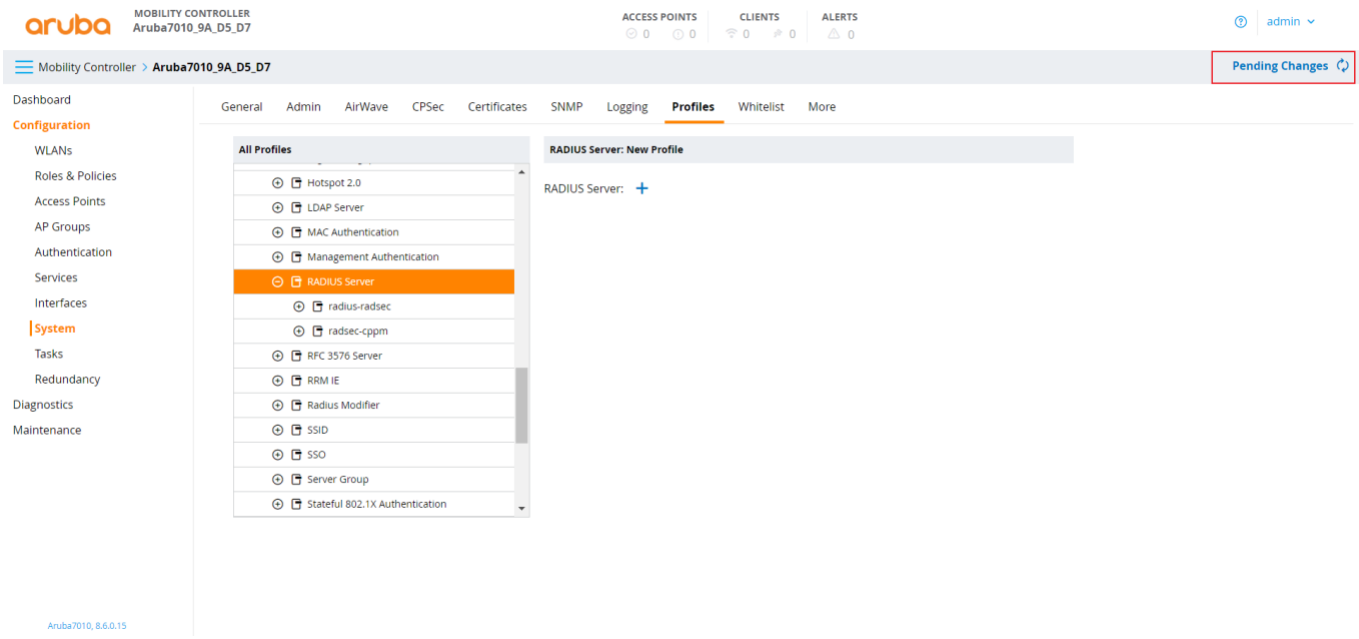

- Profile name 输入自己定义的名称，这里演示为 radius-radsec
- Host 输入 你的环境中真实的 ClearPass 的 IP 地址
- Key 输入 radsec （必须是 radsec，RFC 统一要求的，不能是其他的 key）
- Radsec 勾选
- RadSec Trusted CA Name 选择 trust-root-ca
- RadSec Client Cert 选择 radsec-client-cert

最后点击 Submit 按钮提交



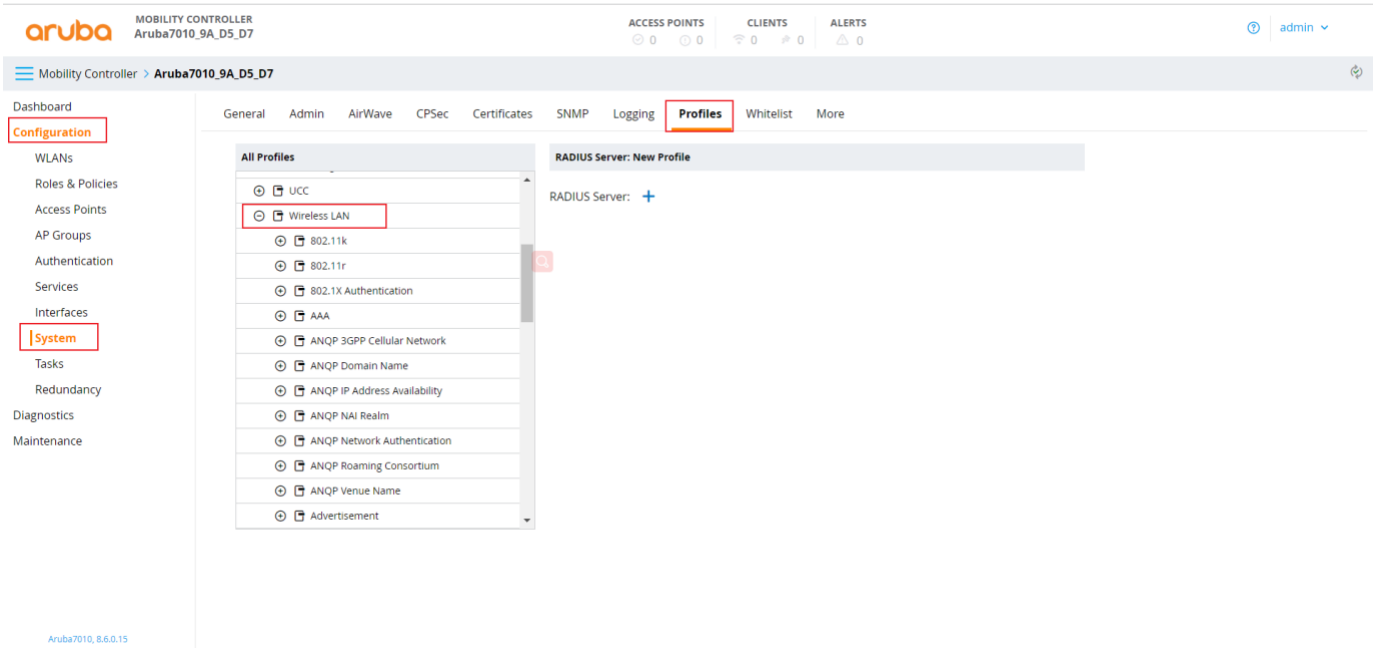




点击右上角的 Pending Changes 按钮，保存配置

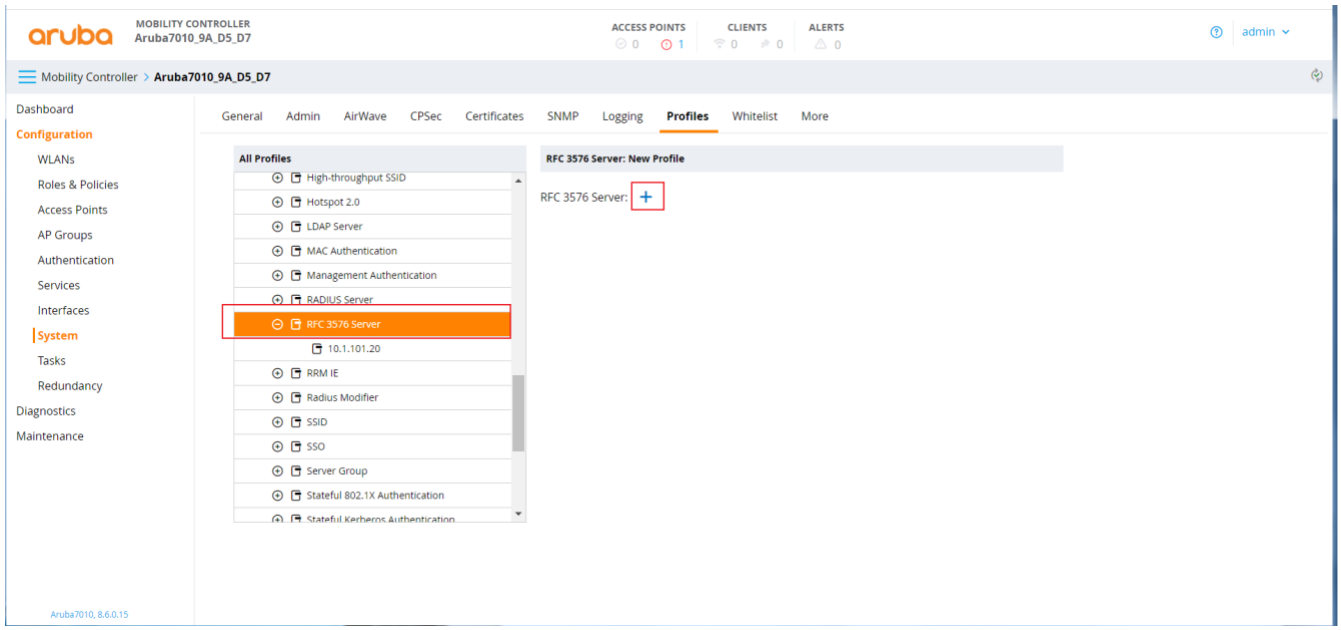



第3步： 在控制器上创建 RFC3576 Server

导航到 Configuration» System » Profiles，展开 Wireless LAN



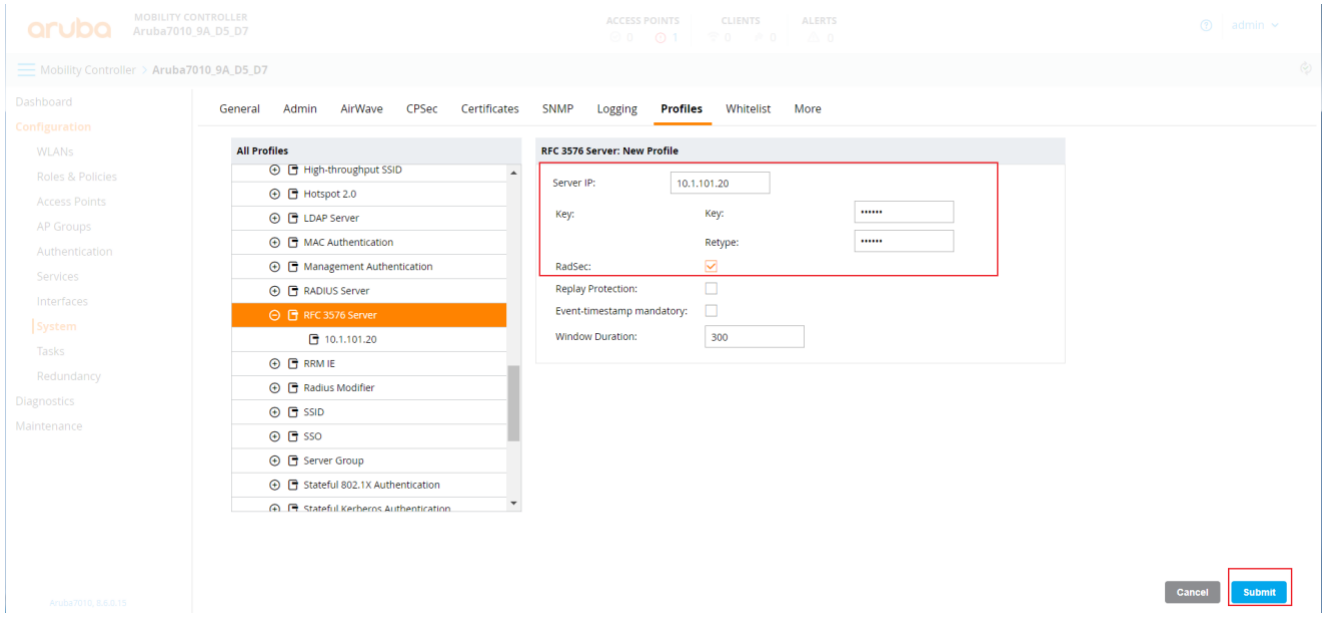

找到并鼠标点击 RFC 3576 Server，在右边窗口中，点击+ 按钮，新增一个 RFC 3576 Server



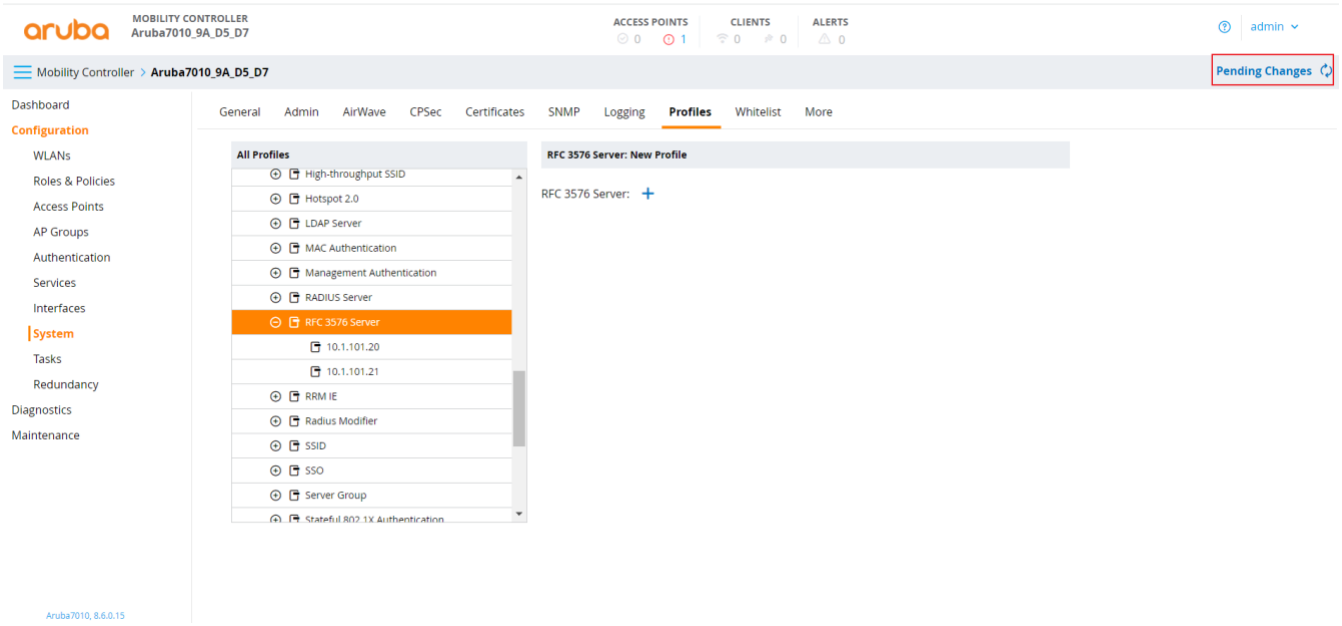

在 RFC 3576 Server 编辑页面

- Server IP 输入你环境中的实际 ClearPass 的 IP
- Key 输入 radsec （必须是 radsec，RFC 统一要求的，不能是其他的字符）
- Radsec 勾选

最后点击 Submit 按钮



最后点击右上角的 Pending Changes 按钮，保存配置




### 1.3.4 验证 TLS Tunnel 是否建立成功

将前面步骤创建的 Radius Server 和 RFC 3576 Server 调用到你需要的相关 Server Group 和 AAA profile 配置中（这里省略）

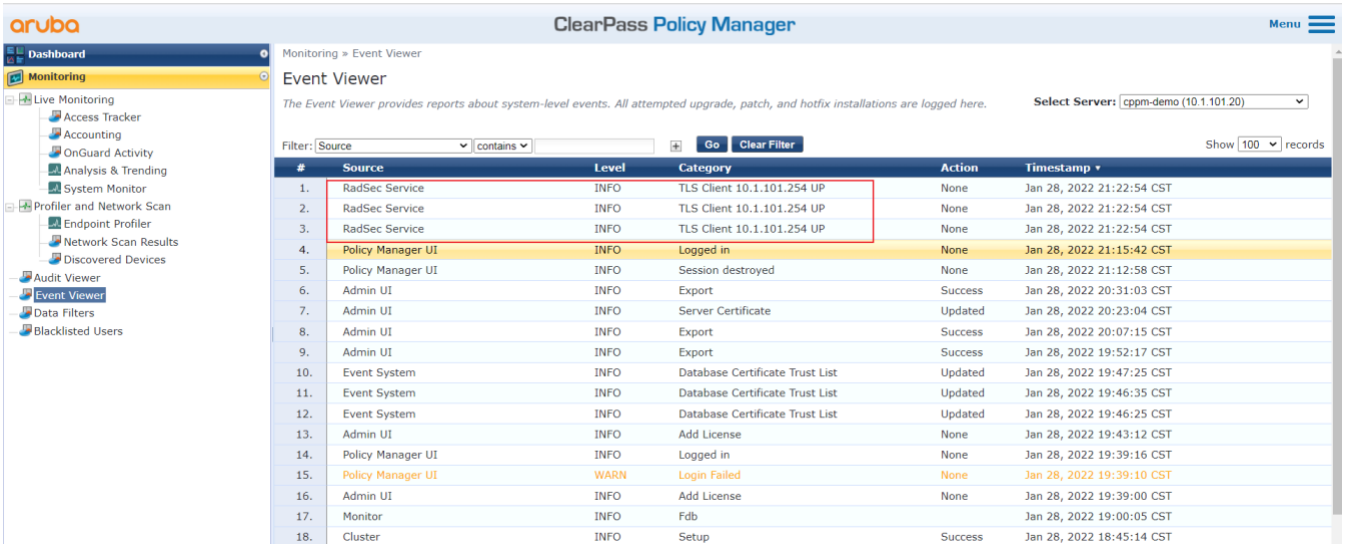
在控制器上，输入下面的 CLI 来查看 RadSec 状态， In Service 需要是 Yes 的

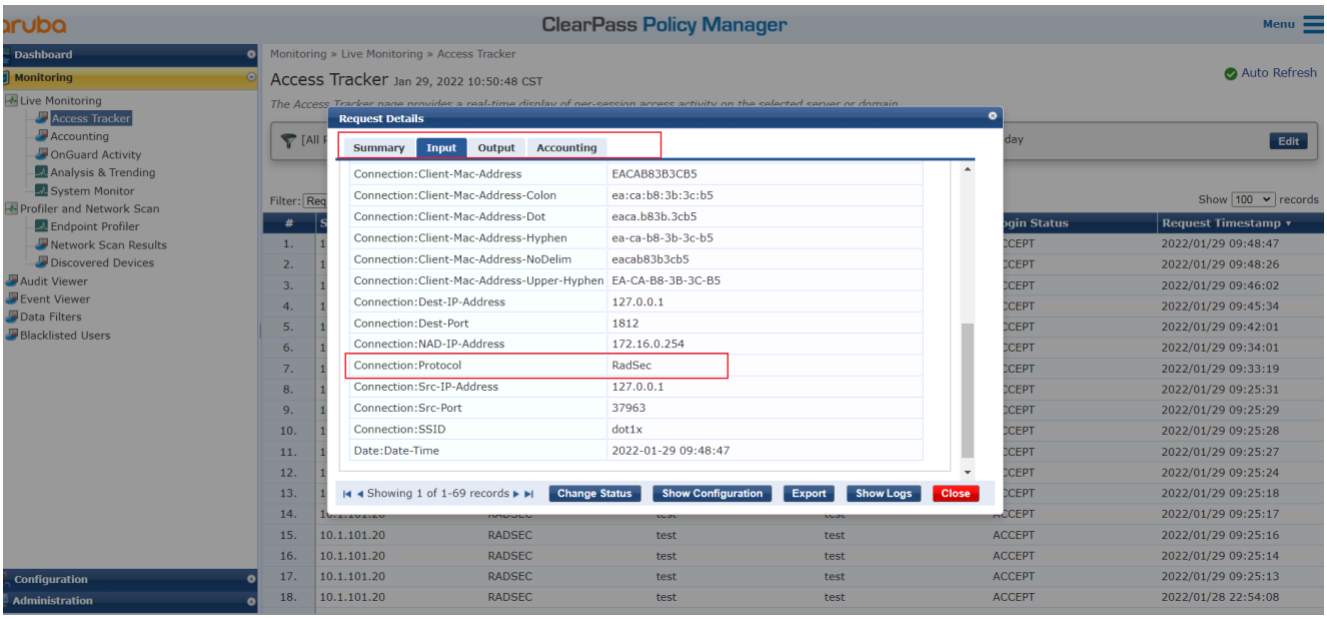
```
(Aruba7010_9A_D5_D7) [mynode] #show aaa authentication-server radius radius-radsec radsec status

RADIUS Server "radius-radsec" RadSec Status
-------------------------------------------
RadSec Server Attribute  Value
-----------------------  -----
In Service               Yes
Connected Sockets        1
```

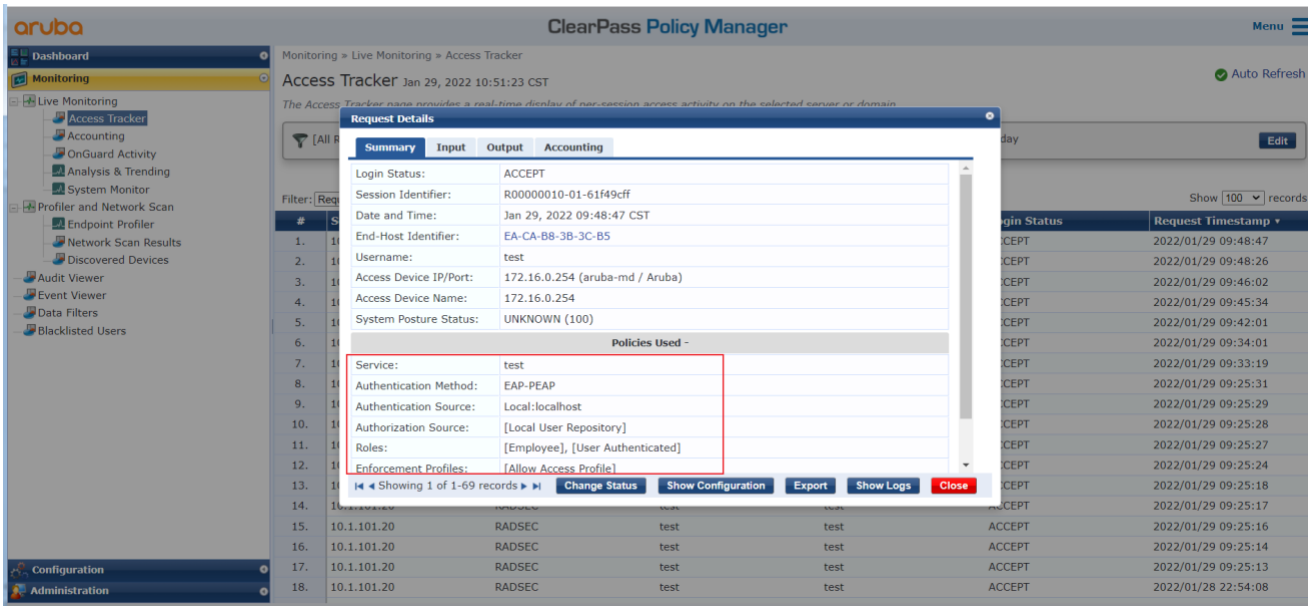
控制器上，输入下面的 CLI 来进行 AAA test

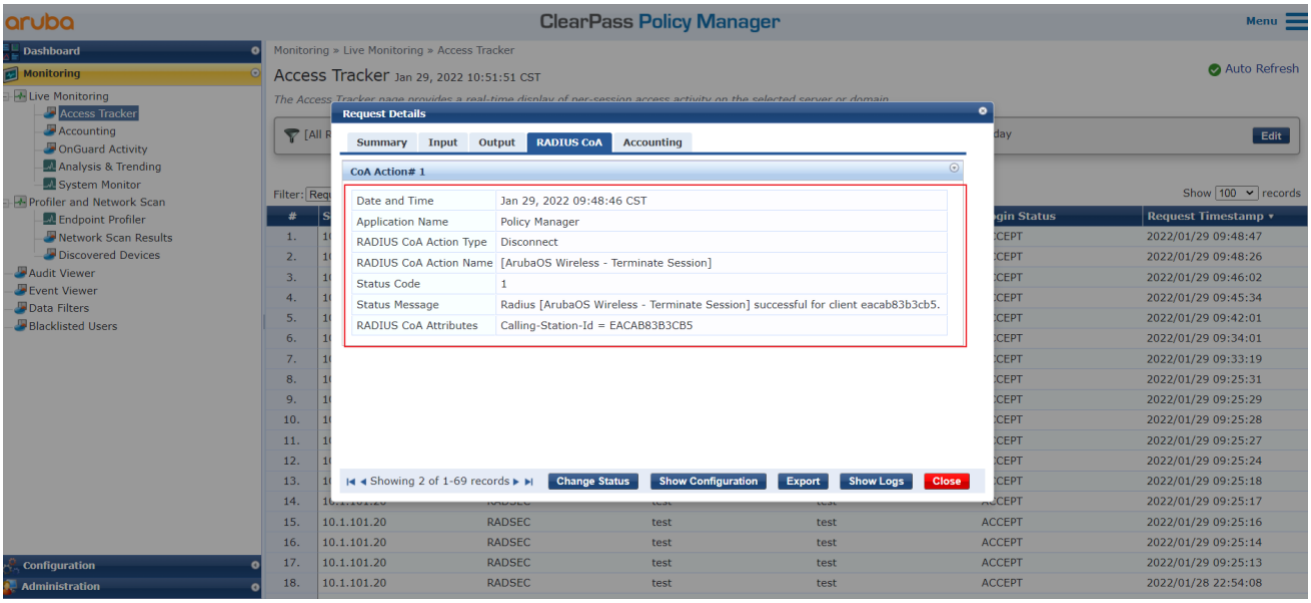
```
(Aruba7010_9A_D5_D7) [mynode] #aaa test-server pap radius-radsec test 1234567890
Authentication Successful
```

在 CLEARPASS 的 Event Viewer 上看到 RadSec Service 提示 TLS Client 10.1.101.254 UP




ClearPass Policy Manager
Menu
Dashboard
Monitoring
Live Monitoring
Access Tracker
Accounting
OnGuard Activity
Analysis & Trending
System Monitor
Profiler and Network Scan
Endpoint Profiler
Network Scan Results
Discovered Devices
Audit Viewer
Event Viewer
Data Filters
Blacklisted Users
Configuration
Administration
Monitoring » Live Monitoring » Access Tracker
Access Tracker Jan 29, 2022 10:51:23 CST
Auto Refresh
Edit
Request Details
Summary
Input
Output
Accounting
Login Status: ACCEPT
Session Identifier: R00000010-01-61f49cff
Date and Time: Jan 29, 2022 09:48:47 CST
End-Host Identifier: EA-CA-B8-3B-3C-B5
Username: test
Access Device IP/Port: 172.16.0.254 (aruba-md / Aruba)
Access Device Name: 172.16.0.254
System Posture Status: UNKNOWN (100)
Policies Used -
Service: test
Authentication Method: EAP-PEAP
Authentication Source: Local:localhost
Authorization Source: [Local User Repository]
Roles: [Employee], [User Authenticated]
Enforcement Profiles: [Allow Access Profile]
Showing 1 of 1-69 records
Change Status
Show Configuration
Export
Show Logs
Close
Request Timestamp
2022/01/29 09:48:47
2022/01/29 09:48:26
2022/01/29 09:46:02
2022/01/29 09:45:34
2022/01/29 09:42:01
2022/01/29 09:34:01
2022/01/29 09:33:19
2022/01/29 09:25:31
2022/01/29 09:25:29
2022/01/29 09:25:28
2022/01/29 09:25:27
2022/01/29 09:25:24
2022/01/29 09:25:18
2022/01/29 09:25:17
2022/01/29 09:25:16
2022/01/29 09:25:14
2022/01/29 09:25:13
2022/01/28 22:54:08


ClearPass Policy Manager
Menu
Monitoring » Live Monitoring » Access Tracker
Access Tracker Jan 29, 2022 10:51:51 CST
Auto Refresh
Edit
Request Details
Summary
Input
Output
RADIUS CoA
Accounting
CoA Action# 1
Date and Time Jan 29, 2022 09:48:46 CST
Application Name Policy Manager
RADIUS CoA Action Type Disconnect
RADIUS CoA Action Name [ArubaOS Wireless - Terminate Session]
Status Code 1
Status Message Radius [ArubaOS Wireless - Terminate Session] successful for client eacab83b3cb5.
RADIUS CoA Attributes Calling-Station-Id = EACAB83B3CB5
Showing 2 of 1-69 records
Change Status
Show Configuration
Export
Show Logs
Close