Contents

1 RadSec for IAPs and ClearPass

RadSec is used to secure/encrypt the authentication session between Instant APs (IAP), Switches and ClearPass. The main use case is when you have your authentication sever AKA ClearPass installed in AWS or Azure and you need to use Internet as a medium to transport the RADIUS authentication.

Common facts about RadSec

- RadSec establishes a TLS tunnel (TCP/2083) between the RADIUS client commonly referred to as network access device (NAD) and RADIUS server.
- Enabling RadSec on the NAD or on CPPM, the RADIUS secret is automatically will be set to "radsec"
- During the TLS tunnel establishment, the NAD and RADIUS server authenticate each other with certificates.
- After the TLS tunnel comes up, the NAD and RADIUS server exchange all RADIUS messages over the tunnel, including authentication and accounting.
- When CPPM and the NAD are using RadSec, CPPM sends the CoA messages in the RadSec tunnel.
- The source address of the NAD is used for the TLS session. The NAS-IP is used for sub-RADIUS processes.
- NAD can also detect Radius server connectivity loses much faster.

This is the first part of this 3x parts technote and in this part we'll cover RadSec configuration for IAPs and ClearPass.

1.1 Before you start

NADs must be configured by admins to trust the root Certificate Authority (CA) associated with this certificate. Often a private CA works well for issuing the RadSec certificate. The organisation has control over its own devices and can ensure they trust the CA.

Devices that participate in RadSec session need

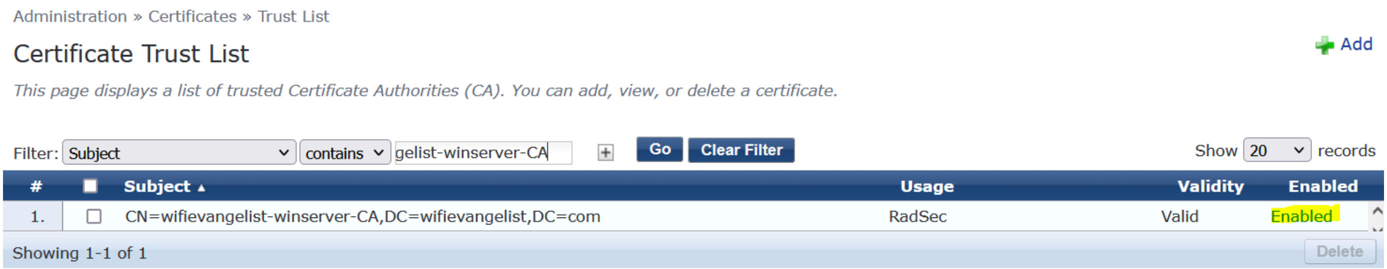
- A device certificate to authenticate themselves.
- To trust the root CA certificate of the issuer of the other end of the RadSec tunnel.

Here we'll use the TPM Cert for the IAP to authenticate against ClearPass. RadSec is mutual, you will need to load the RadSec CA cert that generates the RadSec Server cert that is in ClearPass on the IAP through Central. You will also need to enable trust for the Aruba Device CAs in ClearPass.

Once that is in place the IAP will present its TPM cert to ClearPass, ClearPass will validate the cert against the Aruba Device CA it has in its store, and conversely the IAP will validate the ClearPass RadSec Server cert against the corresponding RadSec CA cert you imported into Central.

1.2 ClearPass Configuration

We have a RadSec Server certificate that is signed by "wifievangelist-winserver-CA" that we upload and trust.



Administration » Certificates » Trust List

Certificate Trust List

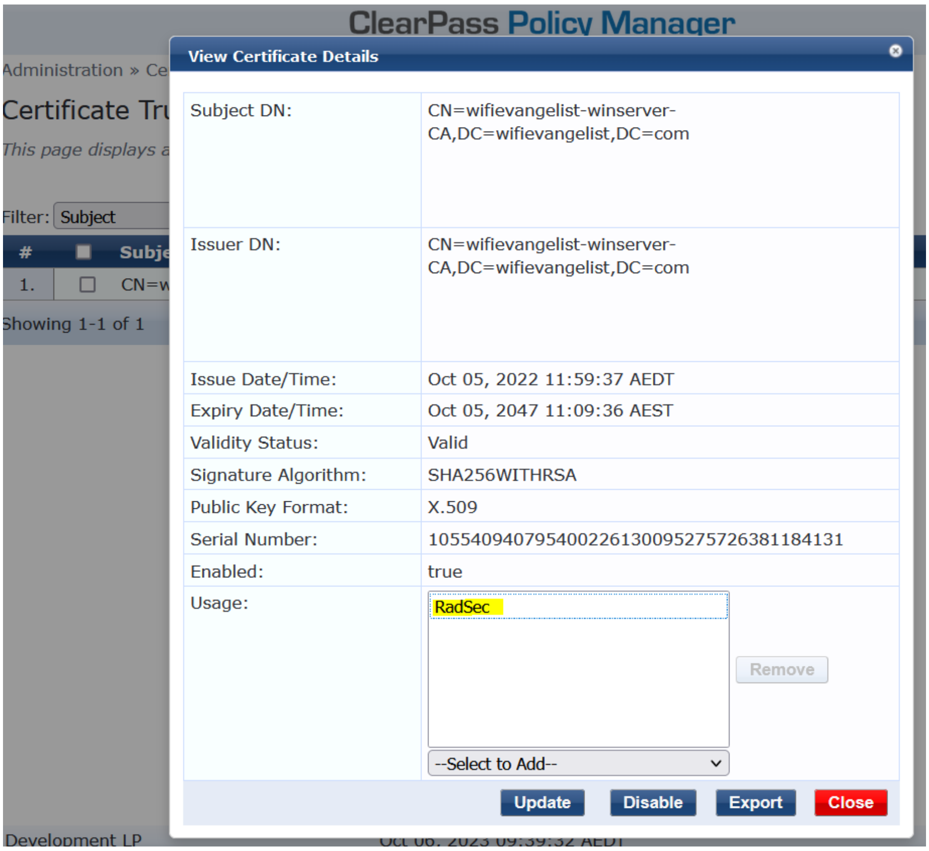
This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains gelist-winserver-CA

#	□	Subject ▲	Usage	Validity	Enabled
1.	□	CN=wifievangelist-winserver-CA,DC=wifievangelist,DC=com	RadSec	Valid	Enabled

Showing 1-1 of 1

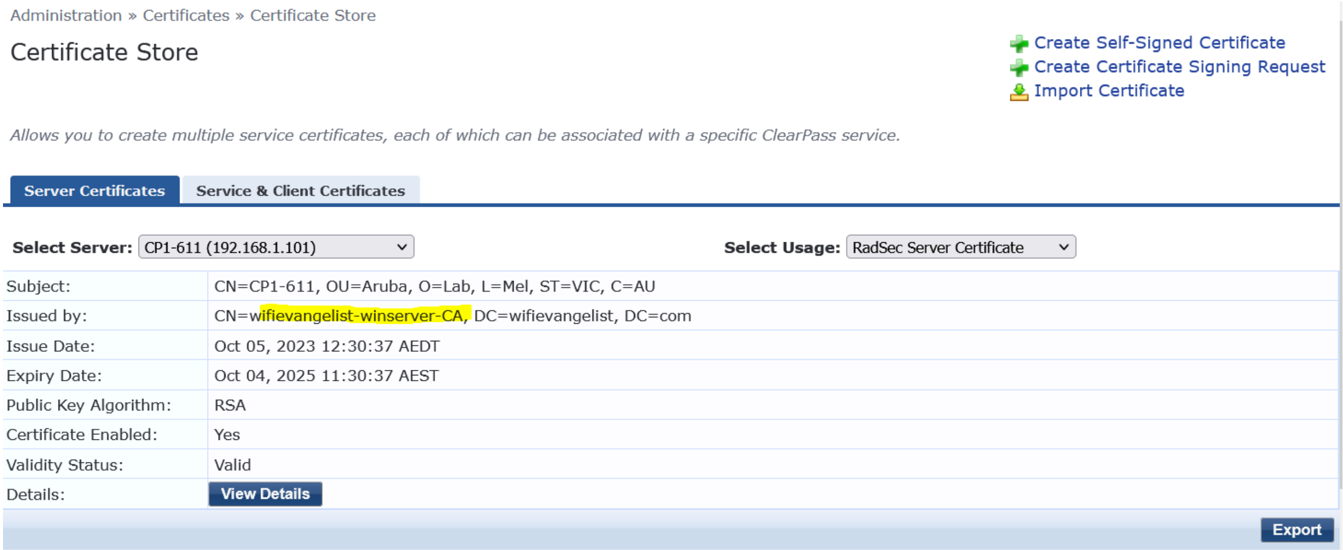
Remember to add the RadSec usage.



View Certificate Details

Subject DN:	CN=wifievangelist-winserver-CA,DC=wifievangelist,DC=com
Issuer DN:	CN=wifievangelist-winserver-CA,DC=wifievangelist,DC=com
Issue Date/Time:	Oct 05, 2022 11:59:37 AEDT
Expiry Date/Time:	Oct 05, 2047 11:09:36 AEST
Validity Status:	Valid
Signature Algorithm:	SHA256WITHRSA
Public Key Format:	X.509
Serial Number:	105540940795400226130095275726381184131
Enabled:	true
Usage:	RadSec --Select to Add--

Then upload the server cert for it.



Administration » Certificates » Certificate Store

Certificate Store

Create Self-Signed Certificate
Create Certificate Signing Request
Import Certificate

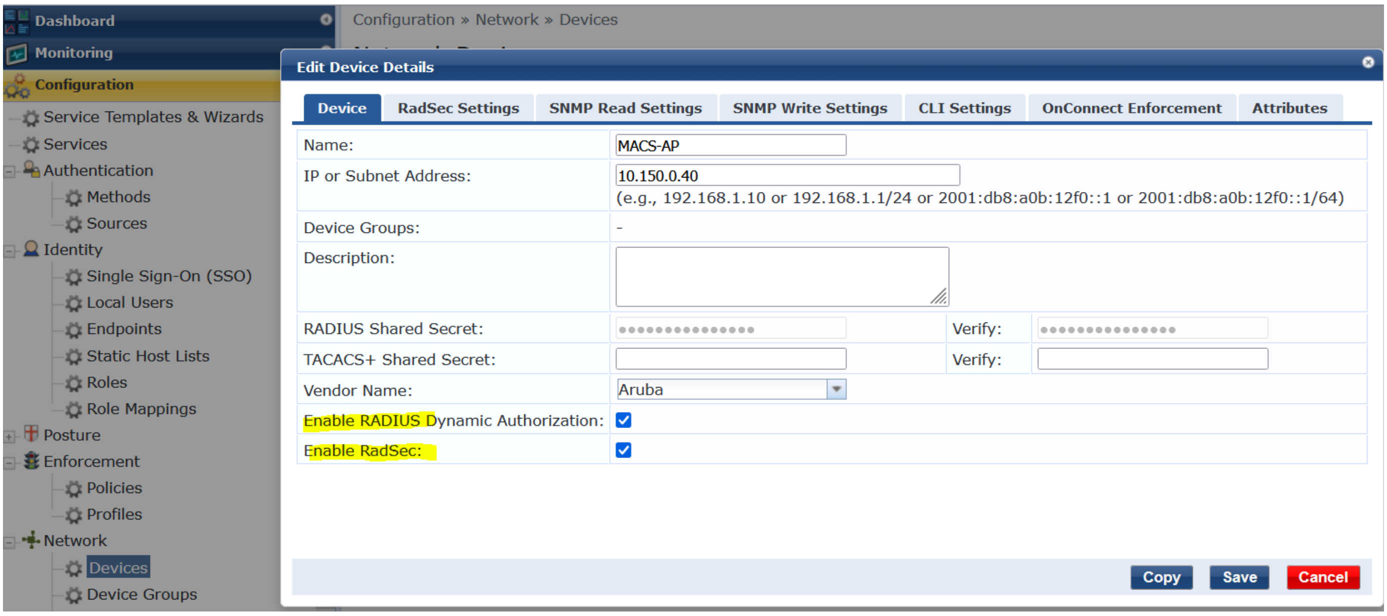
Allows you to create multiple service certificates, each of which can be associated with a specific ClearPass service.

Server Certificates
Service & Client Certificates

Select Server: CP1-611 (192.168.1.101) **Select Usage:** RadSec Server Certificate

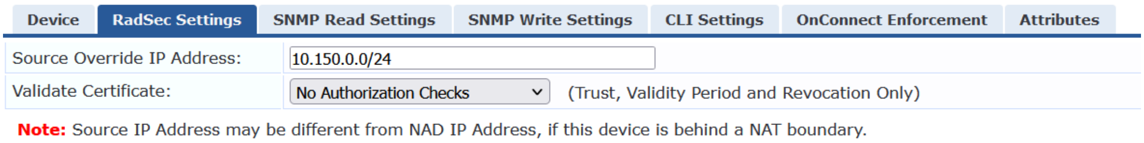
Subject:	CN=CP1-611, OU=Aruba, O=Lab, L=Mel, ST=VIC, C=AU
Issued by:	CN=wifievangelist-winserver-CA, DC=wifievangelist, DC=com
Issue Date:	Oct 05, 2023 12:30:37 AEDT
Expiry Date:	Oct 04, 2025 11:30:37 AEST
Public Key Algorithm:	RSA
Certificate Enabled:	Yes
Validity Status:	Valid
Details:	View Details

Now add the NAD, note that Dynamic RADIUS Proxy (DRP) can’t be used with RadSec as individual APs will establish the TLS tunnel for RadSec.



Edit Device Details

Name:	MACS-AP		
IP or Subnet Address:	10.150.0.40 (e.g., 192.168.1.10 or 192.168.1.1/24 or 2001:db8:a0b:12f0::1 or 2001:db8:a0b:12f0::1/64)		
Device Groups:	-		
Description:			
RADIUS Shared Secret:	•••••••••••••••	Verify:	•••••••••••••••
TACACS+ Shared Secret:		Verify:	
Vendor Name:	Aruba		
Enable RADIUS Dynamic Authorization:	☑		
Enable RadSec:	☑		



Source Override IP Address:	10.150.0.0/24
Validate Certificate:	No Authorization Checks (Trust, Validity Period and Revocation Only)

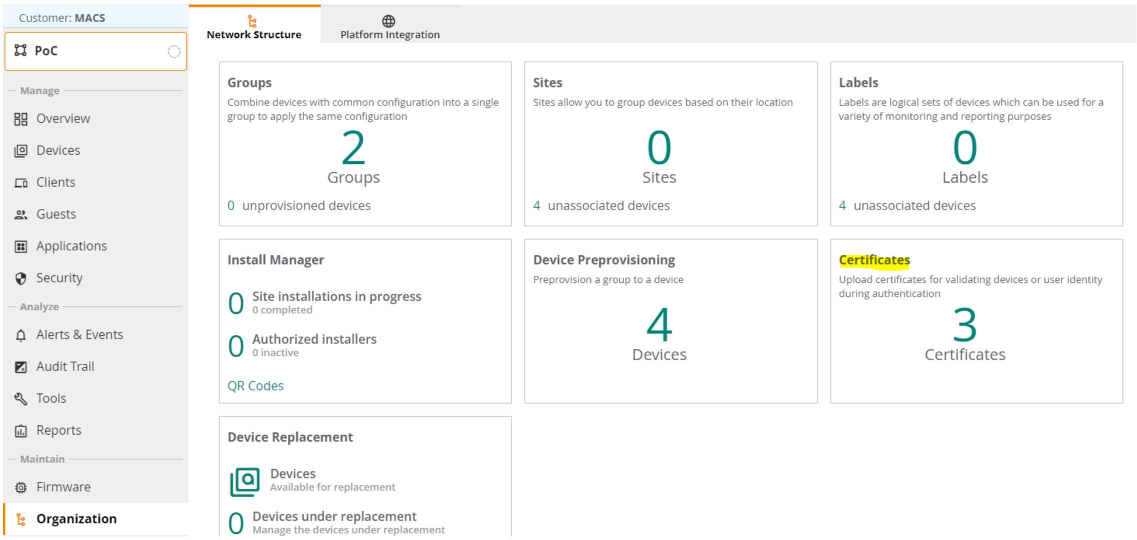
Note: Source IP Address may be different from NAD IP Address, if this device is behind a NAT boundary.

Note that :

- TPM Cert for the IAP is issued by Root CA “Aruba Networks Trusted Computing Root CA”.
- The CoA of a public NATed connection is expected to be possible with CPPM. The "Source Override IP Address" field shown above is for this use case and should be set to the public IP.
- Since DRP can’t be used with RADSEC, the device IP address that you add in ClearPass should be the NAS-IP for the IAP/AOS controller (RADIUS client NAS IP address) , not the RADIUS client source IP address. If not done this way, you’ll see the RADSEC tunnels doing up and down in event viewer.

1.3 Aruba Central Configuration

Here since IAPs are managed by Aruba Central, we’ll upload the root CA that issued ClearPass’s RadSec certificate, so the IAPs can trust.



Groups
Combine devices with common configuration into a single group to apply the same configuration
2 Groups
0 unprovisioned devices

Sites
Sites allow you to group devices based on their location
0 Sites
4 unassociated devices

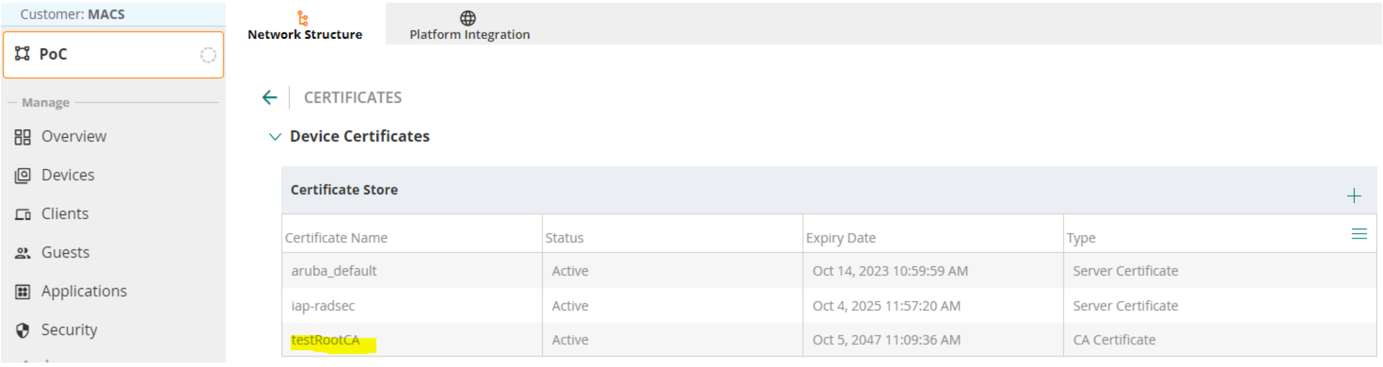
Labels
Labels are logical sets of devices which can be used for a variety of monitoring and reporting purposes
0 Labels
4 unassociated devices

Install Manager
0 Site installations in progress
0 completed
0 Authorized installers
0 inactive
QR Codes

Device Preprovisioning
Preprovision a group to a device
4 Devices

Certificates
Upload certificates for validating devices or user identity during authentication
3 Certificates

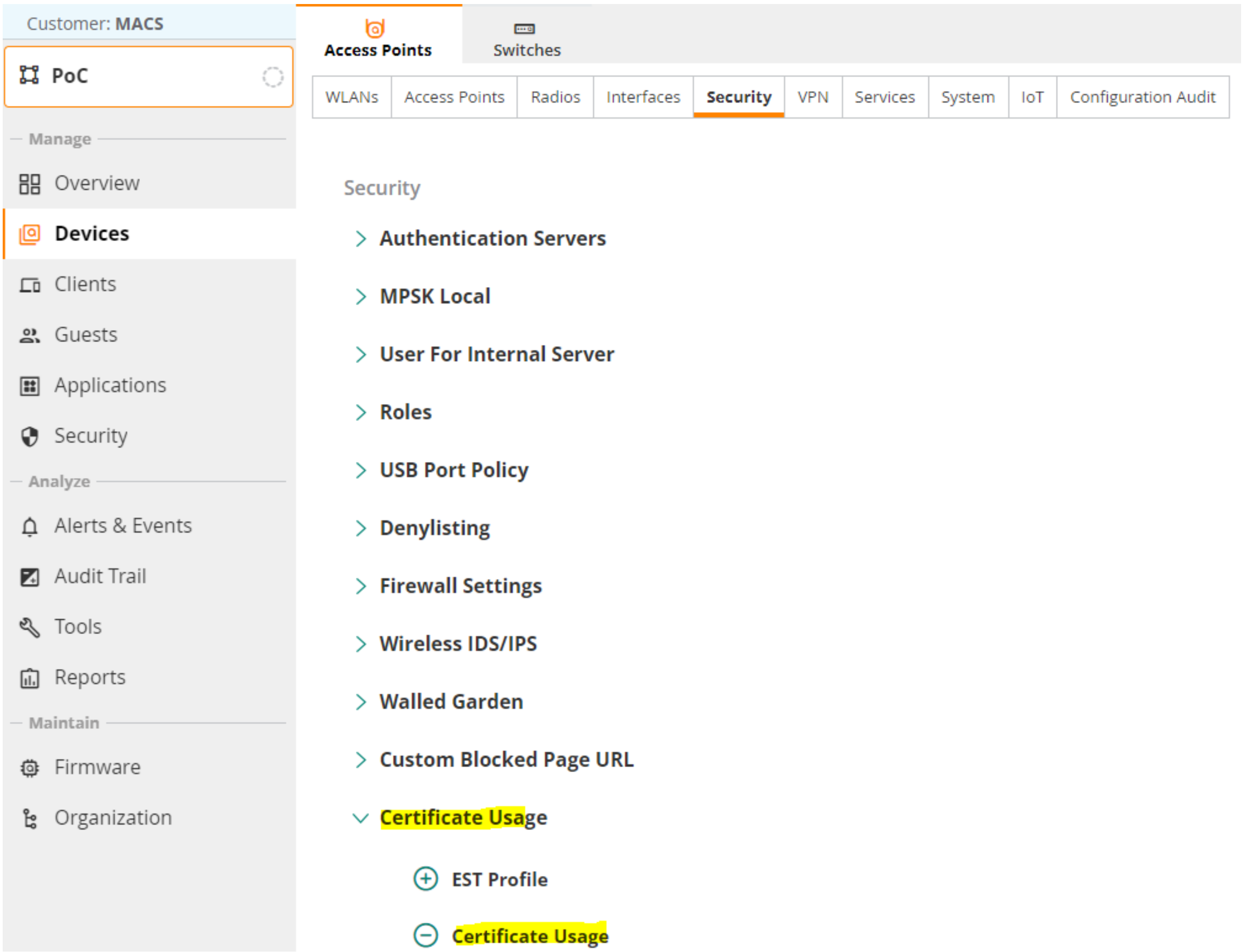
Device Replacement
Devices
Available for replacement
0 Devices under replacement
Manage the devices under replacement

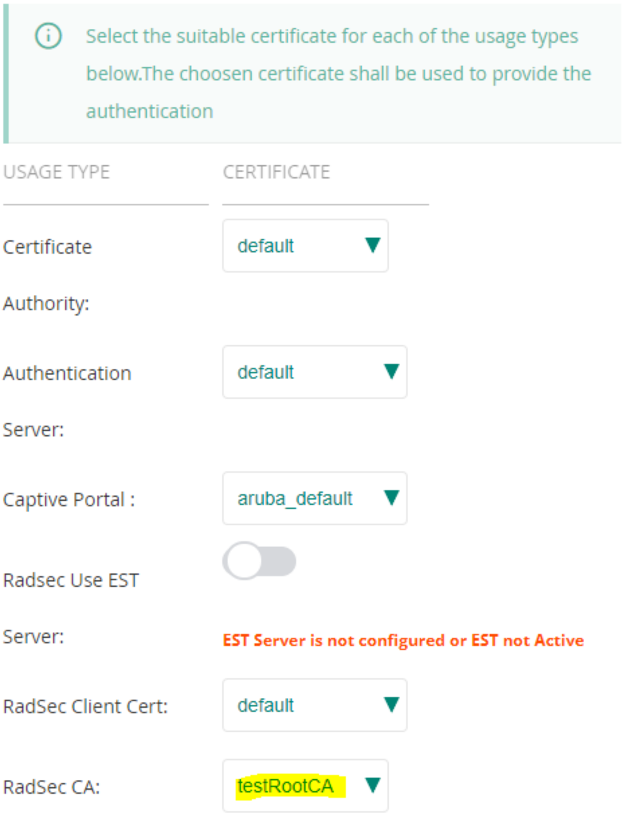


Device Certificates

Certificate Store

Certificate Name	Status	Expiry Date	Type
aruba_default	Active	Oct 14, 2023 10:59:59 AM	Server Certificate
iap-radsec	Active	Oct 4, 2025 11:57:20 AM	Server Certificate
testRootCA	Active	Oct 5, 2047 11:09:36 AM	CA Certificate

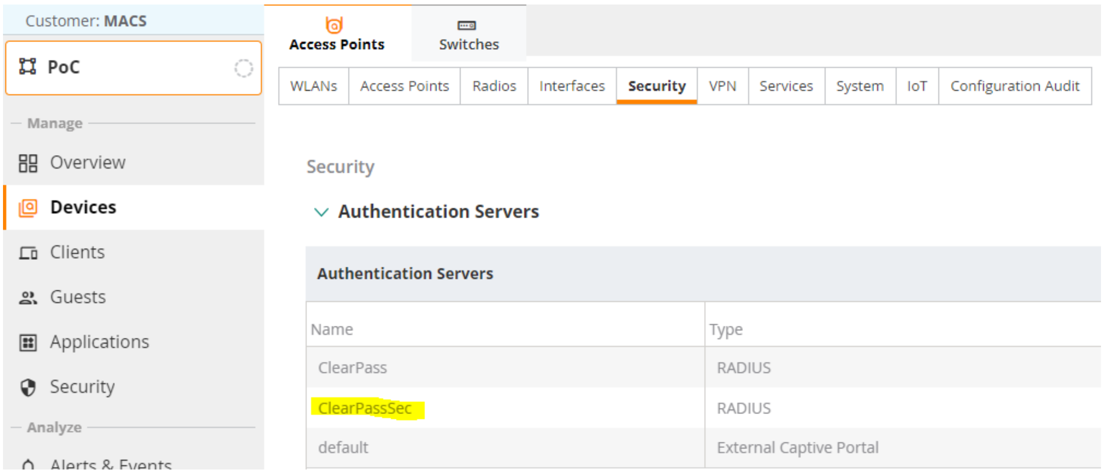




Select the suitable certificate for each of the usage types below.The choosen certificate shall be used to provide the authentication

USAGE TYPE	CERTIFICATE
Certificate Authority:	default
Authentication Server:	default
Captive Portal :	aruba_default
Radsec Use EST Server:	EST Server is not configured or EST not Active
RadSec Client Cert:	default
RadSec CA:	testRootCA

Next we 'll configure the authentication server.

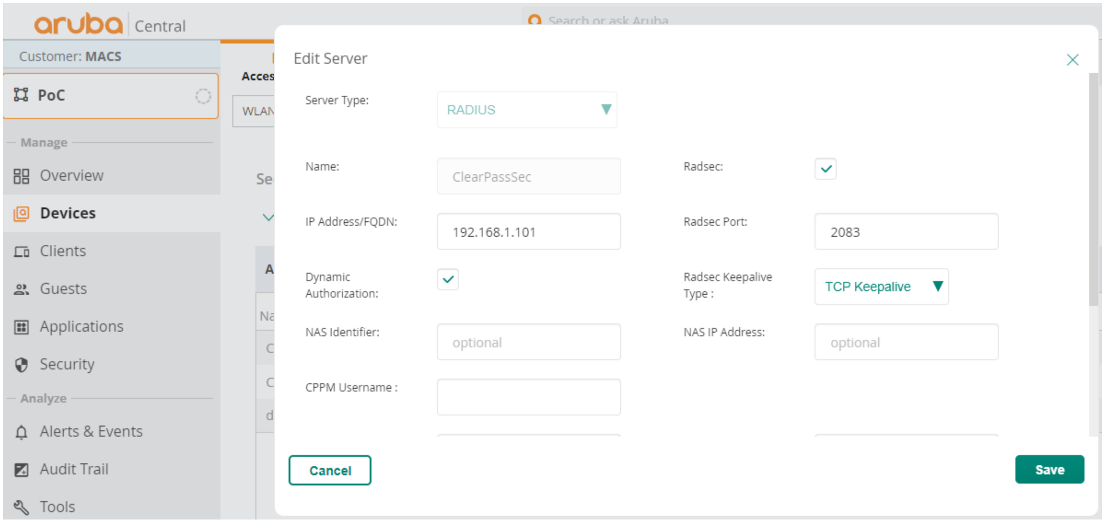


Security

Authentication Servers

Authentication Servers

Name	Type
ClearPass	RADIUS
ClearPassSec	RADIUS
default	External Captive Portal



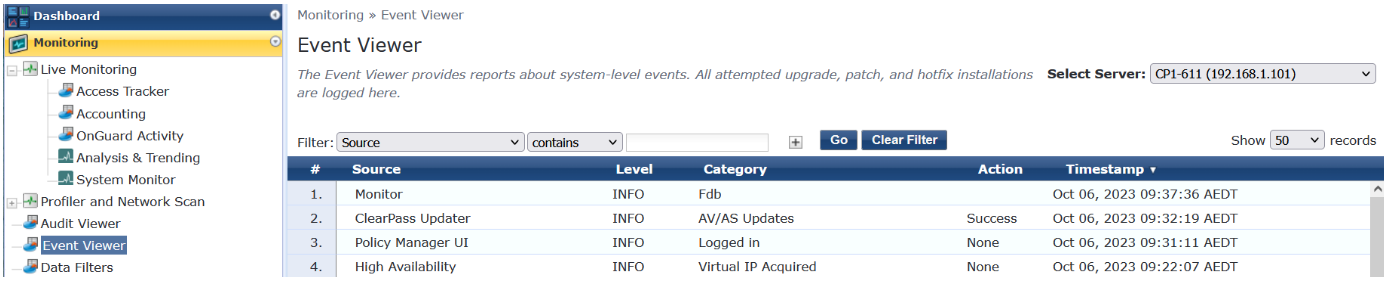
Edit Server

Server Type:	RADIUS		
Name:	ClearPassSec	Radsec:	✓
IP Address/FQDN:	192.168.1.101	Radsec Port:	2083
Dynamic Authorization:	✓	Radsec Keepalive Type :	TCP Keepalive
NAS Identifier:	optional	NAS IP Address:	optional
CPPM Username :			

We are all set, remember you don't need to initiate an authentication request to be able to see if the RadSec tunnel gets established. The RadSec Tunnel should be established before any user authentication. So without any dot1x authentication SSID, you should be able to test if RadSec is working or not.

1.4 Testing

ClearPass Event viewer should indicate if the RadSec tunnels are established.

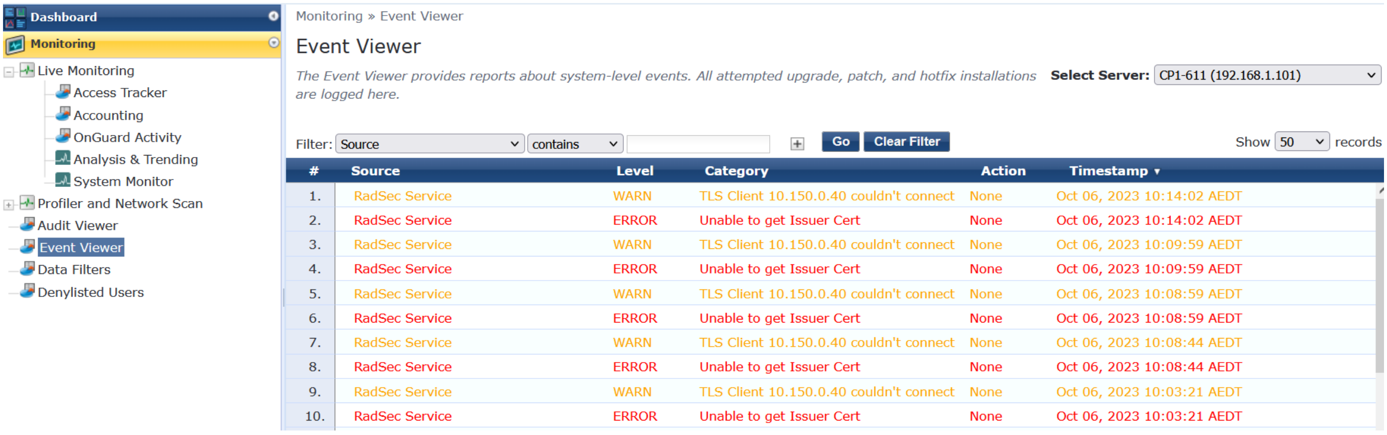


Event Viewer

The Event Viewer provides reports about system-level events. All attempted upgrade, patch, and hotfix installations are logged here.

Select Server: CP1-611 (192.168.1.101)

#	Source	Level	Category	Action	Timestamp ▾
1.	Monitor	INFO	Fdb		Oct 06, 2023 09:37:36 AEDT
2.	ClearPass Updater	INFO	AV/AS Updates	Success	Oct 06, 2023 09:32:19 AEDT
3.	Policy Manager UI	INFO	Logged in	None	Oct 06, 2023 09:31:11 AEDT
4.	High Availability	INFO	Virtual IP Acquired	None	Oct 06, 2023 09:22:07 AEDT



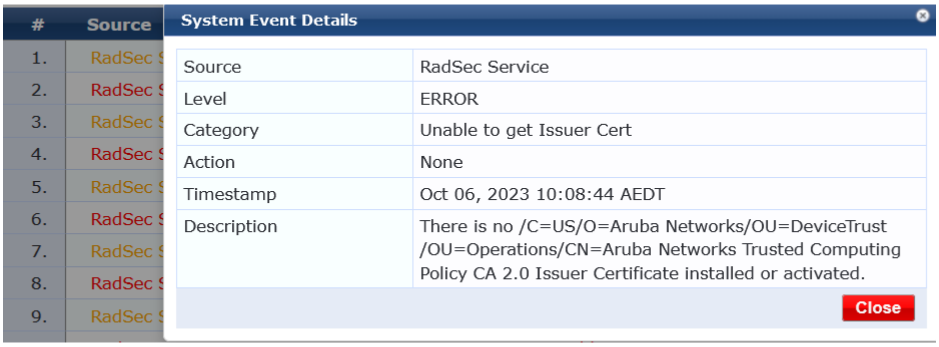
Event Viewer

The Event Viewer provides reports about system-level events. All attempted upgrade, patch, and hotfix installations are logged here.

Select Server: CP1-611 (192.168.1.101)

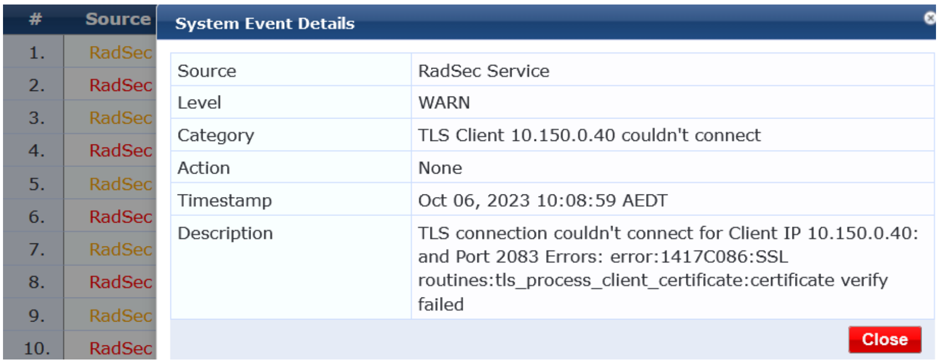
#	Source	Level	Category	Action	Timestamp ▾
1.	RadSec Service	WARN	TLS Client 10.150.0.40 couldn't connect	None	Oct 06, 2023 10:14:02 AEDT
2.	RadSec Service	ERROR	Unable to get Issuer Cert	None	Oct 06, 2023 10:14:02 AEDT
3.	RadSec Service	WARN	TLS Client 10.150.0.40 couldn't connect	None	Oct 06, 2023 10:09:59 AEDT
4.	RadSec Service	ERROR	Unable to get Issuer Cert	None	Oct 06, 2023 10:09:59 AEDT
5.	RadSec Service	WARN	TLS Client 10.150.0.40 couldn't connect	None	Oct 06, 2023 10:08:59 AEDT
6.	RadSec Service	ERROR	Unable to get Issuer Cert	None	Oct 06, 2023 10:08:59 AEDT
7.	RadSec Service	WARN	TLS Client 10.150.0.40 couldn't connect	None	Oct 06, 2023 10:08:44 AEDT
8.	RadSec Service	ERROR	Unable to get Issuer Cert	None	Oct 06, 2023 10:08:44 AEDT
9.	RadSec Service	WARN	TLS Client 10.150.0.40 couldn't connect	None	Oct 06, 2023 10:03:21 AEDT
10.	RadSec Service	ERROR	Unable to get Issuer Cert	None	Oct 06, 2023 10:03:21 AEDT

These are the warning and error messages in event viewer.



System Event Details

Source	RadSec Service
Level	ERROR
Category	Unable to get Issuer Cert
Action	None
Timestamp	Oct 06, 2023 10:08:44 AEDT
Description	There is no /C=US/O=Aruba Networks/OU=DeviceTrust /OU=Operations/CN=Aruba Networks Trusted Computing Policy CA 2.0 Issuer Certificate installed or activated.

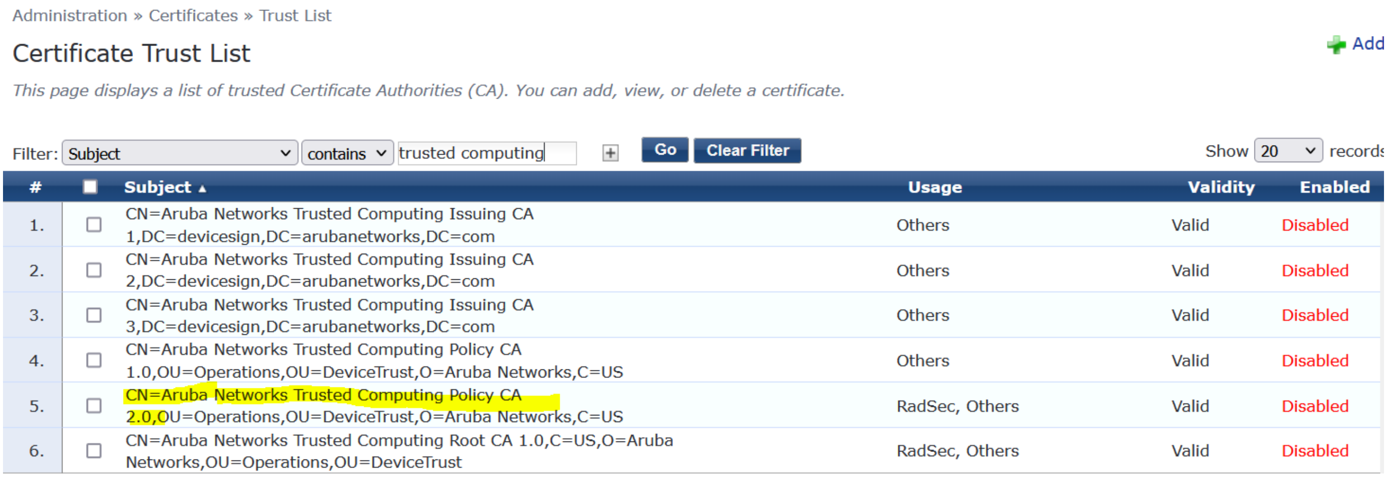


System Event Details

Source	RadSec Service
Level	WARN
Category	TLS Client 10.150.0.40 couldn't connect
Action	None
Timestamp	Oct 06, 2023 10:08:59 AEDT
Description	TLS connection couldn't connect for Client IP 10.150.0.40: and Port 2083 Errors: error:1417C086:SSL routines:tls_process_client_certificate:certificate verify failed

```
CN=Aruba Networks Trusted Computing Policy CA 2.0 Issuer Certificate installed or
activated.
```

We need to find the CA that signed the device certificate of the IAP and enable and trust it. As you can see they are already part of ClearPass CA certificates by default.



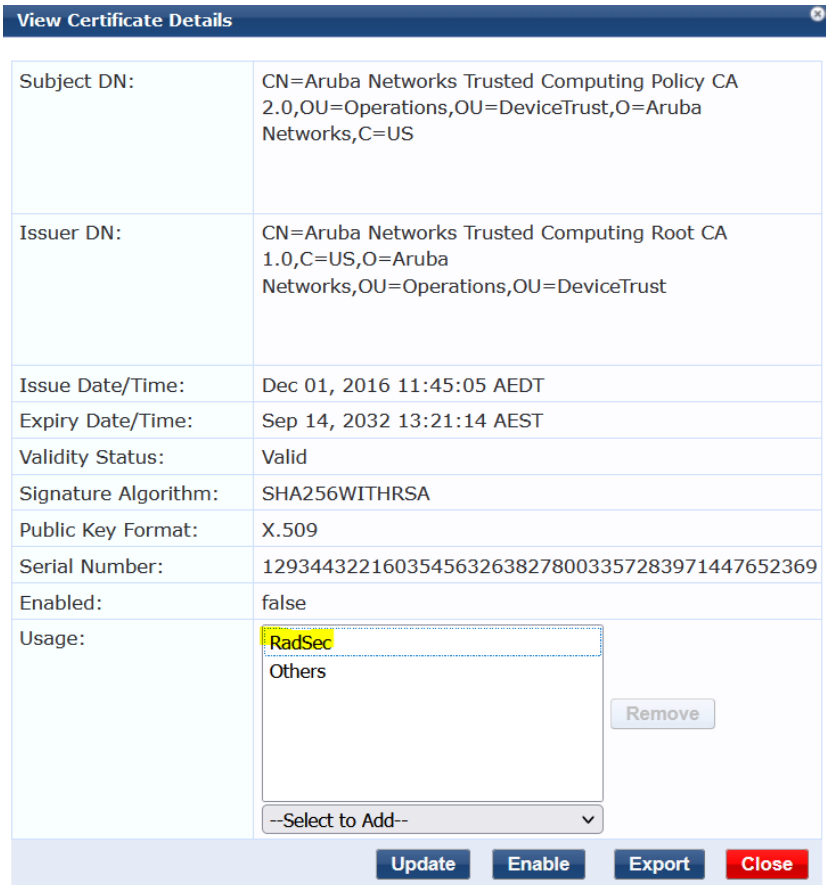
Administration » Certificates » Trust List

Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

Filter: Subject contains trusted computing

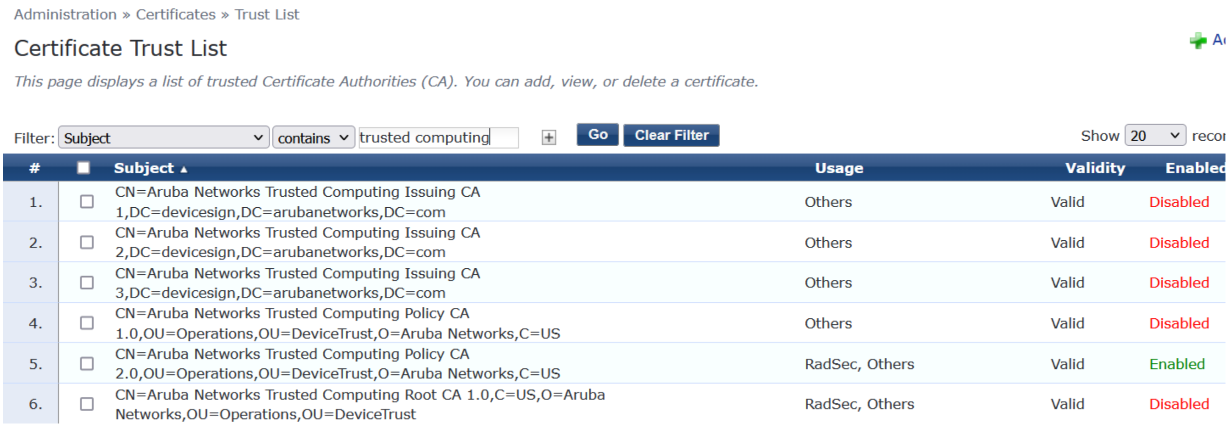
#	□	Subject ▲	Usage	Validity	Enabled
1.	□	CN=Aruba Networks Trusted Computing Issuing CA 1,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
2.	□	CN=Aruba Networks Trusted Computing Issuing CA 2,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
3.	□	CN=Aruba Networks Trusted Computing Issuing CA 3,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
4.	□	CN=Aruba Networks Trusted Computing Policy CA 1.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US	Others	Valid	Disabled
5.	□	CN=Aruba Networks Trusted Computing Policy CA 2.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US	RadSec, Others	Valid	Disabled
6.	□	CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust	RadSec, Others	Valid	Disabled



View Certificate Details

Subject DN:	CN=Aruba Networks Trusted Computing Policy CA 2.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US
Issuer DN:	CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust
Issue Date/Time:	Dec 01, 2016 11:45:05 AEDT
Expiry Date/Time:	Sep 14, 2032 13:21:14 AEST
Validity Status:	Valid
Signature Algorithm:	SHA256WITHRSA
Public Key Format:	X.509
Serial Number:	1293443221603545632638278003357283971447652369
Enabled:	false
Usage:	RadSec Others --Select to Add--

Note that we also need to trust the issuer of this certificate.

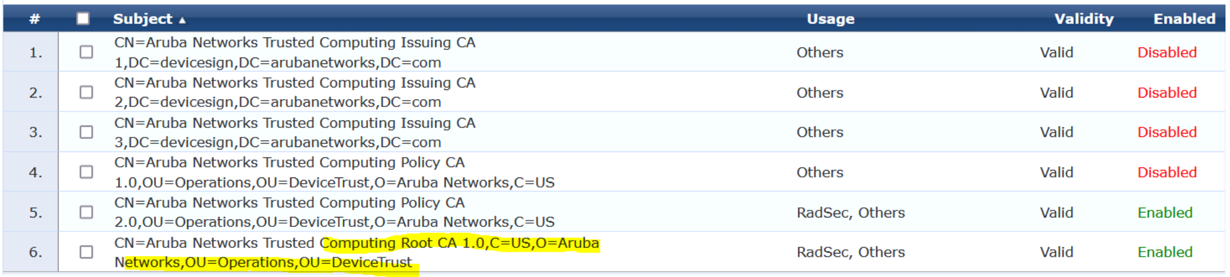


Certificate Trust List

This page displays a list of trusted Certificate Authorities (CA). You can add, view, or delete a certificate.

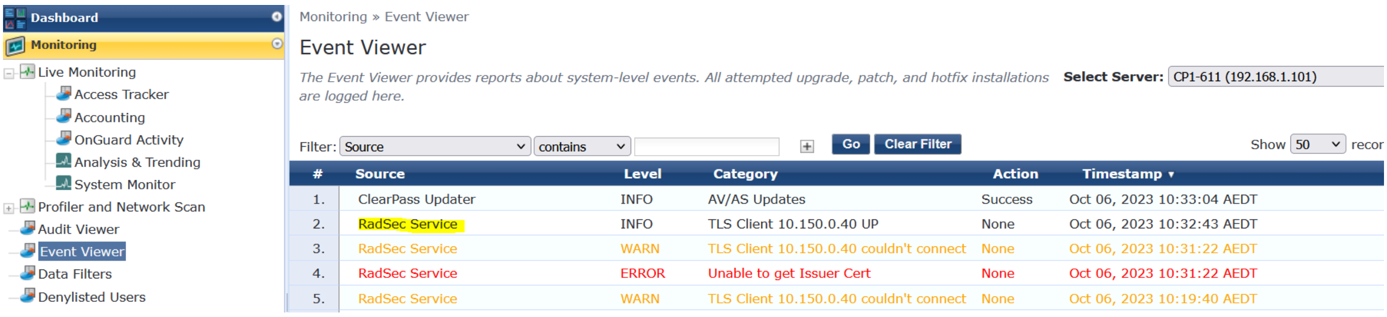
Filter: Subject contains trusted computing

#	□	Subject ▴	Usage	Validity	Enabled
1.	□	CN=Aruba Networks Trusted Computing Issuing CA 1,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
2.	□	CN=Aruba Networks Trusted Computing Issuing CA 2,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
3.	□	CN=Aruba Networks Trusted Computing Issuing CA 3,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
4.	□	CN=Aruba Networks Trusted Computing Policy CA 1.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US	Others	Valid	Disabled
5.	□	CN=Aruba Networks Trusted Computing Policy CA 2.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US	RadSec, Others	Valid	Enabled
6.	□	CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust	RadSec, Others	Valid	Disabled



#	□	Subject ▴	Usage	Validity	Enabled
1.	□	CN=Aruba Networks Trusted Computing Issuing CA 1,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
2.	□	CN=Aruba Networks Trusted Computing Issuing CA 2,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
3.	□	CN=Aruba Networks Trusted Computing Issuing CA 3,DC=devicesign,DC=arubanetworks,DC=com	Others	Valid	Disabled
4.	□	CN=Aruba Networks Trusted Computing Policy CA 1.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US	Others	Valid	Disabled
5.	□	CN=Aruba Networks Trusted Computing Policy CA 2.0,OU=Operations,OU=DeviceTrust,O=Aruba Networks,C=US	RadSec, Others	Valid	Enabled
6.	□	CN=Aruba Networks Trusted Computing Root CA 1.0,C=US,O=Aruba Networks,OU=Operations,OU=DeviceTrust	RadSec, Others	Valid	Enabled

Once we do that, we get the successful event viewer entry.



Event Viewer

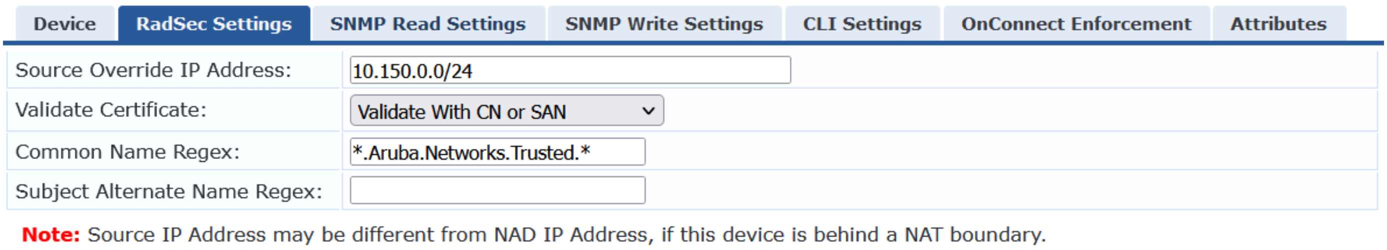
The Event Viewer provides reports about system-level events. All attempted upgrade, patch, and hotfix installations are logged here.

Select Server: CP1-611 (192.168.1.101)

Filter: Source contains

#	Source	Level	Category	Action	Timestamp ▾
1.	ClearPass Updater	INFO	AV/AS Updates	Success	Oct 06, 2023 10:33:04 AEDT
2.	RadSec Service	INFO	TLS Client 10.150.0.40 UP	None	Oct 06, 2023 10:32:43 AEDT
3.	RadSec Service	WARN	TLS Client 10.150.0.40 couldn't connect	None	Oct 06, 2023 10:31:22 AEDT
4.	RadSec Service	ERROR	Unable to get Issuer Cert	None	Oct 06, 2023 10:31:22 AEDT
5.	RadSec Service	WARN	TLS Client 10.150.0.40 couldn't connect	None	Oct 06, 2023 10:19:40 AEDT

Now we can add extra validation using regex.



Source Override IP Address:	10.150.0.0/24
Validate Certificate:	Validate With CN or SAN
Common Name Regex:	*.Aruba.Networks.Trusted.*
Subject Alternate Name Regex:	

Note: Source IP Address may be different from NAD IP Address, if this device is behind a NAT boundary.

1.5 Source Override IP Address

As shown the above screenshot, ClearPass also provide Source Override IP Address that generally it is the NAT public IP address of the client which in my case is the NAT public address of my IAP.

Since in most cases you'll have a number of IAPs and switches in a single site, all using the same NAT Public IP address , you can use a single NAT public IP address for all or if you have multiple sites you can use network range like /23, etc. Then you can use the same IP range on your AWS/Azure firewalls to allow incoming Radsec sessions.

Here I am using a Lab setup and I don't require Source Override IP Address.

1.6 IAP Monitoring Commands

```
48:b4:c3:c1:04:fc# sh cert all

Default Server Certificate:
Version       :2
Serial Number :3D
Issuer        :/CN=Aruba615-CNPVKZD1K9/ST=California/O=Aruba Networks/OU=Instant/C=US
Subject       :/CN=securelogin.arubanetworks.com/L=Sunnyvale/ST=California/O=Aruba
Networks/OU=Instant/C=US
Issued On     :Sep  7 05:02:57 2023 GMT
Expires On    :Sep  4 05:02:59 2033 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Current CP Server Certificate:
Version       :2
Serial Number :05687CCAE59BF7AD069F3C3A3A8FA4E0
Issuer        :/C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
Subject       :/C=US/ST=California/L=Palo Alto/O=Hewlett Packard Enterprise
Company/CN=securelogin.hpe.com
Issued On     :Oct 13 00:00:00 2022 GMT
Expires On    :Oct 13 23:59:59 2023 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Version       :2
Serial Number :085F94C02D857BE8CC14FF53EDA23E2A
Issuer        :/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
Subject       :/C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
Issued On     :Sep 24 00:00:00 2020 GMT
Expires On    :Sep 23 23:59:59 2030 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Version       :2
Serial Number :033AF1E6A711A9A0BB2864B11D09FAE5
Issuer        :/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
Subject       :/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
Issued On     :Aug  1 12:00:00 2013 GMT
Expires On    :Jan 15 12:00:00 2038 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Current RadSec CA Certificate:
Version       :2
Serial Number :4F6672217FF1FCA74052FBE944B2F483
Issuer        :/DC=com/DC=wifievangelist/CN=wifievangelist-winserver-CA
Subject       :/DC=com/DC=wifievangelist/CN=wifievangelist-winserver-CA
Issued On     :Oct  5 00:59:37 2022 GMT
Expires On    :Oct  5 01:09:36 2047 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Current Web UI Server Certificate:
Version       :2
Serial Number :05687CCAE59BF7AD069F3C3A3A8FA4E0
Issuer        :/C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
Subject       :/C=US/ST=California/L=Palo Alto/O=Hewlett Packard Enterprise
Company/CN=securelogin.hpe.com
Issued On     :Oct 13 00:00:00 2022 GMT
Expires On    :Oct 13 23:59:59 2023 GMT
```

```
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Version       :2
Serial Number :085F94C02D857BE8CC14FF53EDA23E2A
Issuer        :/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
Subject       :/C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
Issued On     :Sep 24 00:00:00 2020 GMT
Expires On    :Sep 23 23:59:59 2030 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Version       :2
Serial Number :033AF1E6A711A9A0BB2864B11D09FAE5
Issuer        :/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
Subject       :/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
Issued On     :Aug  1 12:00:00 2013 GMT
Expires On    :Jan 15 12:00:00 2038 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

IoT Operations CA Certificate:
Version       :2
Serial Number :9B1F072626878672
Issuer        :/C=US/ST=CA/L=Sunnyvale/O=HPE Aruba
Networks/CN=*.test.pdt1.arubathena.com/emailAddress=''
Subject       :/C=US/ST=CA/L=Sunnyvale/O=HPE Aruba
Networks/CN=*.test.pdt1.arubathena.com/emailAddress=''
Issued On     :Nov  1 16:54:34 2016 GMT
Expires On    :Mar 19 16:54:34 2044 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA1

Version       :2
Serial Number :7FCA90A09238929F485E8F5154C67AA2
Issuer        :/C=US/O=Aruba Networks/OU=DeviceTrust/OU=Operations/CN=Aruba Networks
Platform Root CA 1.0
Subject       :/C=US/O=Aruba Networks/OU=DeviceTrust/OU=Operations/CN=Aruba Networks
Platform Root CA 1.0
Issued On     :Apr  6 22:59:05 2017 GMT
Expires On    :Apr  6 23:05:11 2032 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Version       :2
Serial Number :3800000009AF9A9FE60ECF990B000000000009
Issuer        :/C=US/O=Aruba Networks/OU=DeviceTrust/OU=Operations/CN=Aruba Networks
Platform Root CA 1.0
Subject       :/C=US/O=Aruba Networks/OU=DeviceTrust/OU=Operations/CN=Aruba Networks
Central Policy CA 1.1
Issued On     :May 10 19:30:49 2017 GMT
Expires On    :Apr  6 23:05:11 2032 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Version       :2
Serial Number :6100000006A4FF835CFF438D09000000000006
Issuer        :/C=US/O=Aruba Networks/OU=DeviceTrust/OU=Operations/CN=Aruba Networks
Central Policy CA 1.1
Subject       :/C=US/O=Aruba Networks/OU=DeviceTrust/OU=Operations/CN=Aruba Networks
Central Issuing CA dev
Issued On     :May 12 20:01:06 2017 GMT
Expires On    :Apr  6 23:05:11 2032 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256
```

```
Version        :2
Serial Number :61000000077633EE5299404FC0000000000007
Issuer        :/C=US/O=Aruba Networks/OU=DeviceTrust/OU=Operations/CN=Aruba Networks
Central Policy CA 1.1
Subject       :/C=US/O=Aruba Networks/OU=DeviceTrust/OU=Operations/CN=Aruba Networks
Central Issuing CA 1.1
Issued On     :May 24 21:18:43 2017 GMT
Expires On    :Apr  6 23:05:11 2032 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Version        :2
Serial Number :61000000084D5A5C46363A311D000000000008
Issuer        :/C=US/O=Aruba Networks/OU=DeviceTrust/OU=Operations/CN=Aruba Networks
Central Policy CA 1.1
Subject       :/C=US/O=Aruba Networks/OU=DeviceTrust/OU=Operations/CN=Aruba Networks
Central Issuing CA 1.2
Issued On     :May 24 21:57:07 2017 GMT
Expires On    :Apr  6 23:05:11 2032 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

Device Certificate:
Version        :2
Serial Number :47BA2C78000200335B86
Issuer        :/DC=com/DC=arubanetworks/DC=devicesign/CN=Aruba Networks Trusted
Computing Issuing CA 1
Subject       :/CN=CNPVKZD1K9::48:b4:c3:c1:04:fc
Issued On     :Jan 27 06:05:08 2023 GMT
Expires On    :Sep 14 03:21:14 2032 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256

48:b4:c3:c1:04:fc#
```

Note that the root CA cert was uploaded through Aruba Central.

```
48:b4:c3:c1:04:fc# sh RadSeccert

Current RadSec CA Certificate:
Version        :2
Serial Number :4F6672217FF1FCA74052FBE944B2F483
Issuer        :/DC=com/DC=wifievangelist/CN=wifievangelist-winserver-CA
Subject       :/DC=com/DC=wifievangelist/CN=wifievangelist-winserver-CA
Issued On     :Oct  5 00:59:37 2022 GMT
Expires On    :Oct  5 01:09:36 2047 GMT
RSA Key size  :2048 bits
Signed Using  :RSA-SHA256


RadSec will use default Client cert  and custom CA cert

48:b4:c3:c1:04:fc#
```