ArubaOS Certificate Enrollment with ClearPass Onboard
Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-01</td>
<td>10/24/17</td>
<td>Tim Cappalli</td>
<td>Initial Release</td>
</tr>
</tbody>
</table>

Copyright

© Copyright 2017 Hewlett Packard Enterprise Development LP.

Contents

Overview and Requirements.................................................................3
Requirements .........................................................................................3
ClearPass Onboard Configuration .........................................................4
Overview...............................................................................................4
Certificate Authority Configuration .....................................................4
Controller Configuration ........................................................................10
CA Upload ...........................................................................................11
EST Profile .........................................................................................13
Enabling EST .......................................................................................14
Verification and Troubleshooting .........................................................15
ClearPass Policy Configuration for EAP-TLS ......................................17
AP Provisioning ...................................................................................18
Overview and Requirements

ArubaOS 8.2 introduced a new certificate enrollment feature that leverages the Enrollment over Secure Transport (EST) standard to allow access points and controllers to automatically request a device certificate via ClearPass Onboard.

This certificate is then used to build trust between controllers and APs. The certificate can also be used to authenticate the AP to the upstream switching infrastructure via EAP-TLS which is the subject of this configuration guide.

**NOTE:** Every Aruba access point also contains a factory certificate burned in the TPM that can be used for EAP-TLS. In most environments, that is the preferred path for authenticating access points to the upstream switch. This document covers a unique use case where a custom certificate is desired.

Requirements

- Mobility controller running ArubaOS 8.2 or greater
  - For additional ArubaOS-specific requirements and caveats, see the ArubaOS 8.2 User Guide
- ClearPass 6.6 or greater (latest release is recommended)
- Time synchronization should be enabled between all devices involved in EST enrollment
- ClearPass should have a public CA-signed or internal CA-signed HTTPS certificate. Self-signed certificates are highly discouraged
- Access points and controllers must be able to resolve the FQDN of ClearPass and reach it on TCP port 443 (HTTPS)
ClearPass Onboard Configuration

Overview

This section will cover creating a new Onboard certificate authority in ClearPass for use with infrastructure devices enrolling via EST.

Certificate Authority Configuration

CA Creation

Navigate to ClearPass Onboard (Guest > Onboard) and select Certificate Authorities from the left menu.

At the top right, click Create new certificate authority.

Give the certificate authority a friendly name.

For example: Aruba Boston Secure Infrastructure CA – G1.

It is a general best practice to append a version or generation indication to a CA common name. In this example "G1" is used to indicate generation 1. This will be helpful in the event the CA needs to be replaced or retired.
In the Identity section, enter the appropriate information for **Country, State, Locality, Organization** and optionally **Organizational Unit**.

For **Common Name**, use the same name as defined in the first step, this time adding **Root** before **CA** (ex: Aruba Boston Secure Infrastructure **Root CA – G1**).

For **Signing Common Name**, take the Common Name and replace **Root** with **Signing** (ex: Aruba Boston Secure Infrastructure **Signing CA – G1**).

**Email address** should be set to the appropriate address for the environment.

<table>
<thead>
<tr>
<th>Identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>These details are used to create a Distinguished Name for the certificate authority.</td>
</tr>
<tr>
<td><strong>Country:</strong> US Enter the 2-letter ISO country code of your country.</td>
</tr>
<tr>
<td><strong>State:</strong> Massachusetts Enter the full name of your state or province.</td>
</tr>
<tr>
<td><strong>Locality:</strong> Boston Enter the name of your locality (town or city).</td>
</tr>
<tr>
<td><strong>Organization:</strong> Aruba Boston Enter the name of your organization or company.</td>
</tr>
<tr>
<td><strong>Organizational Unit:</strong> Infrastructure Enter the name of your organizational unit (e.g., section or division of the company).</td>
</tr>
<tr>
<td><strong>Common Name:</strong> Aruba Boston Secure Infrastructure Root CA – G1 Enter a name for the certificate authority. This is the ‘common name’ of the digital certificate.</td>
</tr>
<tr>
<td><strong>Signing Common Name:</strong> Aruba Boston Secure Infrastructure Signing CA – G1 Enter a name for the signing certificate. This is the ‘common name’ of the digital certificate.</td>
</tr>
<tr>
<td><strong>Email Address:</strong> <a href="mailto:certs@arubaboston.com">certs@arubaboston.com</a> Enter an email address.</td>
</tr>
</tbody>
</table>
Under **Private Key**, select **4096-bit RSA** for **Key Type**.

Under **Self-Signed Certificate**, set the **CA Expiration** for the root CA. The default is 10 years and this example uses 20 years (7,300 days).

For **Digest Algorithm**, choose **SHA-384**.

![Certificate Authority Configuration](image)

**NOTE:** A digest algorithm of SHA-384 or lower is required for ArubaOS EST enrollment. SHA-384 is recommend.

Click **Create Certificate Authority** to finish.
OCSP and EST Configuration

Next select the newly created CA in the list and click *Edit*.

In the **Certificate Issuing** section, select **Specify an OCSP Responder URL** under **Authority Info Access**.

For **OCSP URL**, replace the predefined hostname with the appropriate value, ensuring that the trailing path is left intact ( /guest/mdps_ocsp.php/X ):

- In a single cluster environment, replace with *localhost*.
- In a multi cluster environment, replace the predefined hostname with the fully qualified domain name of the cluster (usually the publisher/standby publisher virtual IP’s FQDN).
  
  *Example: clearpass.arubaboston.com*

**Validity Period** is the maximum lifetime (in days) for a client certificate. It’s recommended to set this to at least one year (365). In this example, two years is used (730).

Set the **Digest Algorithm** to **SHA-256**.

In the **Retention Policy** section, modify the **Maximum Period** value as necessary. In this example, 1 week is used as this CA is for infrastructure devices.
Next move down to the **SCEP & EST Server** section and check **Enable access to the SCEP and EST servers**.

Make note of the **EST URL** as it will be required during the controller configuration.

For the **SCEP & EST Secret** fields, enter a strong, randomly generated string and then securely store it.

![SCEP & EST Server Table]

Scroll down to the bottom and click **Edit Certificate Authority** to finish.
Trust Chain Download

Back in the list, select the CA and this time click **Trust Chain**.

Click **Download Bundle** and then select **Base-64 Encoded (.pem)** in the **Format** dropdown list. Ensure that **Include certificate trust chain** is selected.

When the download completes, open the file in a text editor.

The file will contain two certificates. Delete the first certificate (from the first instance of **-----BEGIN CERTIFICATE-----** to the first instance of **-----END CERTIFICATE-----**) and save the file. This will be required during the controller configuration.
Controller Configuration

Log in to the mobility master (or directly into the controller if running in standalone mode) and navigate to the appropriate configuration node where this EST configuration will apply. The certificate trust and EST configuration should be applied at the highest applicable configuration node:

- In a standalone controller environment, this will be at the device node
- In a smaller mobility master environment, this may be at highest node under Managed Devices (ex: /md/Production)
- In a large global mobility master deployment, certificates may be issued from different ClearPass clusters by region. For example, a ClearPass cluster in EMEA will have a different Onboard CA than Americas. The mobility master configuration node should follow the ClearPass topology (ex: /md/Production/EMEA, /md/Production/AMER, /md/Production/APAC)

For smooth deployment in a mobility master environment, EST activation should be done first on the MM and then on the MDs.

The EST server configuration should be common across all the controllers deployed in the enterprise.
CA Upload

Once the appropriate configuration node has been selected, navigate to **Configuration > System > Certificates > Import Certificates** and click **+**.

The first certificate to upload will be the Onboard root CA that was downloaded and modified in the previous section.

<table>
<thead>
<tr>
<th>Certificate name</th>
<th>give the certificate a friendly name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate filename</td>
<td>browse and find the modified CA cert from the previous section</td>
</tr>
<tr>
<td>Optional passphrase</td>
<td>skip</td>
</tr>
<tr>
<td>Certificate format</td>
<td>PEM</td>
</tr>
<tr>
<td>Certificate type</td>
<td>TrustedCA</td>
</tr>
</tbody>
</table>

Click **Submit** to upload the certificate.
Click + again. This time, the root CA for the ClearPass HTTPS certificate needs to be uploaded.

<table>
<thead>
<tr>
<th><strong>Certificate name</strong></th>
<th>give the certificate a friendly name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Certificate filename</strong></td>
<td>browse and find the root CA certificate</td>
</tr>
<tr>
<td><strong>Optional passphrase</strong></td>
<td>skip</td>
</tr>
<tr>
<td><strong>Retype passphrase</strong></td>
<td>skip</td>
</tr>
<tr>
<td><strong>Certificate format</strong></td>
<td>PEM</td>
</tr>
<tr>
<td><strong>Certificate type</strong></td>
<td>TrustedCA</td>
</tr>
</tbody>
</table>

Click **Submit** to upload the CA certificate.
**EST Profile**

Navigate to Configuration > System > Profiles > EST Profile > EST and click next to EST Profile.

Give the profile a name.

For **Server host**, enter the fully-qualified domain name for the ClearPass cluster.

**Server port** will be 443.

The **Challenge Password** is the secret that was set in the ClearPass certificate authority EST configuration.

The **Arbitrary label** will be the end of the EST URL presented in the CA configuration in ClearPass (ex: http://CLEARPASS-1/.well-known/est/\texttt{/ca:8}).

For **Server’s CA cert name**, enter the friendly name defined during the upload of the ClearPass HTTPS certificate root CA.

![EST Profile: New Profile](image)

Click **Submit** to finish.
Enabling EST

Next, navigate to **Configuration > System > Certificates > Enrollment over Secure Transport (EST)**. Toggle **Enable certificate provisioning using EST protocol**.

For **EST server**, select the EST profile created in the previous step.

Click **Submit** to finish. Commit the configuration.
Verification and Troubleshooting

This section covers basic troubleshooting and verification. Additional information is available in the "Certificate Enrollment Using EST" section of Chapter 37 in the ArubaOS 8.2 User Guide.

After enabling EST, controllers at the configuration node (and below) and APs provisioned to those controllers will begin requesting certificates from ClearPass via EST.

NOTE: APs will reboot after requesting their certificate via EST in order to reestablish the CPsec tunnel using the new certificate. Controllers will not reboot.

Verification

To verify that a controller has successfully enrolled and has been issued a certificate, the following commands can be used. Any errors will be shown for Enrollment Error.

```
(AP-EST) *[mynode] (config) #show est status

EST STATUS
-----------
Profile Name : CLEARPASS
Server Host  : clearpass.arubaboston.com
Server Port  : 443
Arbitrary label : /ca:8
Enrollment status : Enrolled
Enrollment error   : Failed to resolve EST server host
Expiry status      : NOT EXPIRED
Valid from         : 2017-10-11 19:21:38
Re-enrollment due  : 2018-07-12 13:44:08
```

```
(AP-EST) *[mynode] (config) #show est status all

EST Status for All Switches
---------------------------
IP Address   Name    Type        Version   Profile    Status    Expiry time      Expiry status
----------   ----    -----        -------   --------    ------      -----------      ------------
100.81.9.11  AP-EST standalone 8.2.0.0 CLEARPASS ENROLLED 2018-10-11 19:51:38 NOT EXPIRED
```
Access points that have successfully enrolled with a custom EST certificate will have the e flag in the AP database.

```
(AP-EST) *[mynode] (config) # show ap database
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Group</th>
<th>AP Type</th>
<th>IP Address</th>
<th>Status</th>
<th>Flags</th>
<th>Switch IP</th>
<th>Standby IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap--bos-225-1</td>
<td>default</td>
<td>225</td>
<td>100.81.20.10</td>
<td>Up 3m:33s</td>
<td>21e</td>
<td>100.81.9.11</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

**Logging and Debugging**

Enabling debug logging for EST:

```
(AP-EST) *[mynode] (config) # logging security subcat est level debugging
```

Displaying EST debug logs:

```
(AP-EST) *[mynode] # show log security all | include est
```

Sample EST log entry. The controller could not resolve the FQDN of ClearPass:

```
Oct 11 20:31:29 certmgr[3296]: <118014> <25746> <DBUG> |certmgr| |est| est_thread_handler: EST retry timer started with 5 min interval for enrollment
Oct 11 20:31:29 certmgr[3296]: <118014> <25746> <DBUG> |certmgr| |est| mypub_est_status: Publishing est status. Status 0 profile-name CLEARPASS enroll-status 3
Oct 11 20:31:29 certmgr[3296]: <118015> <25746> <ERRS> |certmgr| |est| est_obtain_cacerts: /cacerts operation failed, ret 6 error: Couldn't resolve host name
Oct 11 20:31:29 certmgr[3296]: <118015> <25746> <ERRS> |certmgr| |est| est_thread_handler: EST enrollment failed
```

AP log message after successful EST enrollment:

```
Oct 11 20:43:10 nanny[2393]: <303022> <WARN> |AP ap--bos-225-1@100.81.20.10 nanny| Reboot Reason: AP rebooted Wed Oct 11 20:40:08 EDT 2017; SAPD: Rebooting after EST enrollment. Need to open a secure channel(IPSEC) with EST certificate
```

**NOTE:** For additional controller debugging and troubleshooting information, please see the "Certificate Enrollment Using EST" section of Chapter 37 in the [ArubaOS 8.2 User Guide](#).
ClearPass Policy Configuration for EAP-TLS

An Aruba AP using a client certificate with 802.1X will authenticate to the network in the same manner as any other device.

The signing CA of the client certificate can be used as a part of role mapping and/or policy. In this example, it is used in combination with profiling data to tag the request with "DEVICE_ACCESS-POINT".

This tag/TIPS role can then be used in the enforcement to assign an enforcement action. An Aruba user role is being returned in this case with an Aruba switch.
AP Provisioning

To enable 802.1X via EAP-TLS on the access point's supplicant, APs must be re-provisioned with this new configuration.

**NOTE:** In 8.2, EAP-TLS supplicant configuration can only be enabled via CLI AP provisioning.

A new configuration option is available in the provision-ap context: `apdot1x-tls`. Adding this option to a provisioning set will instruct the AP to use the certificate enrolled via EST for 802.1X to authenticate to the upstream network.

For additional information about provisioning access points, please see the AP Provisioning section of Chapter 25 in the *ArubaOS 8.2 User Guide*. 