802.1X / dot1x supplicant support on AOS-CX switches

Presenters

Yash

Technical Marketing Engineer

Note:
Detailed instructions on how to replace sample pictures like the one shown here can be found in the speaker notes of this slide.

Tip!
Remember to remove this text box.
Agenda

1. Overview
2. Details and Caveats
3. Configuration
4. Best Practices
5. Troubleshooting
6. Demo
7. Additional Resources
AOS-CX 10.09: dot1x supplicant

- dot1x authentication involves three entities:
  - a supplicant (PC/AP/Clients/ Access Switches)
  - an authenticator, (Aruba AOS-CX Switches)
  - an authentication server (Aruba ClearPass)

- **dot1x authenticator** feature is supported from AOS-CX 10.04 release.

- To secure network infrastructure, **dot1x supplicant** feature is supported from AOS-CX 10.09 release.
Details and Caveats
# dot1x supplicant support on AOS-CX Switches

<table>
<thead>
<tr>
<th>dot1x Features</th>
<th>10.09 Support</th>
<th>Not Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>IEEE 802.1X - 2010</td>
<td></td>
</tr>
<tr>
<td>EAP Methods</td>
<td>EAP-TLS</td>
<td>EAP-TLS based MACsec (client MACsec)</td>
</tr>
<tr>
<td></td>
<td>EAP-MD5</td>
<td></td>
</tr>
<tr>
<td>Certificate</td>
<td>User Defined</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EST enrollment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IDevID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ZTP workflow</td>
<td></td>
</tr>
<tr>
<td>Interface Type</td>
<td>Only L2 Physical Interface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>L2/L3 LAG, RoP</td>
<td></td>
</tr>
<tr>
<td>MIB</td>
<td>NA</td>
<td>dot1x 2010 PAE MIB</td>
</tr>
<tr>
<td>AOS-CX platforms</td>
<td>4100i, 6000, 6100 6200, 6300, 6400, 8360</td>
<td>8320, 8325, 8400, 10000</td>
</tr>
<tr>
<td>Mutual Exclusion Feature</td>
<td>Same interface support dot1x</td>
<td>Infrastructure MACsec and dot1x supplicant on same interface not</td>
</tr>
<tr>
<td></td>
<td>supplicant and dot1x authenicator</td>
<td>supported</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
AOS-CX dot1x supplicant sub-features

- eap-method (Default: eap-tls)
- canned-eap-success (Default: disabled)
- eapol-force-multicast (Default: disabled)
- fail-mode (Default: fail-open)
- start-mode (Default: start-open)
- eapol-protocol-version (Default: 3)
dot1x Supplicant- eapol-force-multicast

With force-multicast

Without force-multicast
Note: Canned EAP success configuration required on both dot1x supplicant and authenticator
dot1x Supplicant EAP-Method: EAP-TLS EST enrollment certificate
dot1x Supplicant EAP-Method: EAP-TLS - User defined certificate

show crypto pki certificate client | in Issuer
dot1x Supplicant EAP-Method: EAP-MD5
## dot1x Supplicant support on AOS-CX CX_SWes

<table>
<thead>
<tr>
<th>AOS-CX_SW dot1x supplicant</th>
<th>AOS-CX dot1x supplicant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implements the dot1x 2004 standard.</td>
<td>Implements the dot1x 2010 standard.</td>
</tr>
<tr>
<td>Only support EAP-MD5 for authentication.</td>
<td>Supports EAP-TLS and EAP-MD5 for authentication.</td>
</tr>
<tr>
<td>Designed to use only CX_SW base mac address</td>
<td>Designed to use only interface MAC address</td>
</tr>
<tr>
<td>eapol-protocol-version 2</td>
<td>eapol-protocol-version 2 &amp; 3 (default)</td>
</tr>
</tbody>
</table>
**AOS-CX dot1x supplicant certificate enrollment**

- Associates a leaf certificate with a feature (application) on the switch. By default, all features are associated with the default, self-signed certificate local-cert. This certificate is created by the switch the first time it starts.

---

<table>
<thead>
<tr>
<th>Associated Applications</th>
<th>Certificate Name</th>
<th>Cert Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>captive-portal</td>
<td>not configured, using local-cert</td>
<td></td>
</tr>
<tr>
<td>dot1x-supplicant</td>
<td>est_certificate1</td>
<td>valid</td>
</tr>
<tr>
<td>est-client</td>
<td>not configured, using local-cert</td>
<td></td>
</tr>
<tr>
<td>https-server</td>
<td>not configured, using local-cert</td>
<td></td>
</tr>
<tr>
<td>radsec-client</td>
<td>not configured, using local-cert</td>
<td></td>
</tr>
<tr>
<td>syslog-client</td>
<td>not configured, using local-cert</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Cert Status</th>
<th>EST Status</th>
<th>Associated Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>CX_SUP</td>
<td>installed</td>
<td>n/a</td>
<td>none</td>
</tr>
<tr>
<td>client</td>
<td>installed</td>
<td>n/a</td>
<td>none</td>
</tr>
<tr>
<td>local-cert</td>
<td>installed</td>
<td>n/a</td>
<td>captive-portal, est-client, https-server, radsec-client, syslog-client</td>
</tr>
<tr>
<td>est_certificate1</td>
<td>installed enroll success</td>
<td></td>
<td>dot1x-supplicant</td>
</tr>
<tr>
<td>device-identity</td>
<td>installed</td>
<td>n/a</td>
<td>none</td>
</tr>
</tbody>
</table>

---

Access-CXSW(config)# crypto pki application

<table>
<thead>
<tr>
<th>captive-portal</th>
<th>Captive Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x-supplicant</td>
<td>802.1X supplicant</td>
</tr>
<tr>
<td>est-client</td>
<td>EST Client</td>
</tr>
<tr>
<td>https-server</td>
<td>HTTPS Server</td>
</tr>
<tr>
<td>radsec-client</td>
<td>RadSec Client</td>
</tr>
<tr>
<td>syslog-client</td>
<td>Syslog Client</td>
</tr>
</tbody>
</table>

Access-CXSW(config)# show crypto pki certificate

---

Access-CXSW(config)# show crypto pki certificate

---

Access-CXSW(config)# crypto pki certificate

---

Access-CXSW(config)#
AOS-CX dot1x supplicant

- Enable dot1x supplicant on the system. **By default, dot1x supplicant is disabled on the system.**

- Create a **dot1x supplicant policy**

  - eapol-protocol-version:
    - Configure the EAPoL protocol version to use in EAPoL frames

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)#
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# enable

CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_dot1x_supplicant_uplink
CX_SW(config-dot1x-supp-policy)#

CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)#   enable
CX_SW(config-dot1x-supp)# policy cx_dot1x_supplicant
CX_SW(config-dot1x-supp-policy)# eapol-protocol-version
<2-3> Specify the protocol version. (Default: 3)
```
dot1x supplicant- Sub features

- **canned EAP success**: Configure the CX_SW to accept an EAP success from the authenticator without going through the complete authentication cycle.

Note: Canned EAP success configuration required on both dot1x supplicant and authenticator

**CX_SW(config)# aaa authentication port-access dot1x supplicant**

**CX_SW(config-dot1x-supp)# policy CX_dot1x_supplicant_uplink**

**CX_SW(config-dot1x-supp-policy)# canned-eap-success**

**no canned-eap-success (default)**

**With canned EAP success**

**Without canned EAP success**
**dot1x Supplicant- EAPoL force multicast**

**EAPoL force multicast:** Configure the dot1x supplicant to send only multicast EAPoL packets irrespective of receiving unicast EAPoL packets from the authenticator.

```
CX_Sw(config)# aaa authentication port-access dot1x supplicant
CX_Sw(config-dot1x-supp)# policy CX_Policy
CX_Sw(config-dot1x-supp-policy)# eapol-force-multicast
no eapol-force-multicast (default)
```
dot1x Supplicant- Sub features

- **max-retries**: Configure the maximum number of authentication attempts before authentication fails.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_supplicant_Policy
CX_SW(config-dot1x-supp-policy)# max-retries 5
max-retries 2 (default)
```

- **eapol-timeout**: Configure the time period (in seconds) to wait for a response from an authenticator before reattempting authentication.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_supplicant_Policy
CX_SW(config-dot1x-supp-policy)# eapol-timeout 10
eapol-timeout 30 (default)
```

- **EAP method**: Configure the EAP method to use for authentication.

```
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_supplicant_Policy
CX_SW(config-dot1x-supp-policy)# eap-method eap-md5
eap-method eap-tls (default)
```
dot1x Supplicant- Sub features

- EAP identity: Configure the EAP identity to use for authentication. The information includes an identity string and an optional password.

- discovery-timeout: Configure the time period (in seconds) to wait for a potential dot1x authenticator on the other end before considering the link to be non dot1x capable and opening the interface on the data-plane. On a timeout, the switch will not use the authentication result to determine the forwarding behavior of the interface until a link flap. If not set, the switch will wait for the dot1x authentication cycle to complete before determining the forwarding state of the interface.

```bash
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_Policy
CX_SW(config-dot1x-supp-policy)# eap-identity identity yash
CX_SW(config-dot1x-supp-policy)# eap-identity password plaintext CXTME
```

```bash
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_Policy
CX_SW(config-dot1x-supp-policy)# discovery-timeout 15
no discovery-timeout (default)
```
dot1x Supplicant - Sub features

- **Held-period**: Configure the time period (in seconds) to wait after a failed authentication attempt before another attempt is permitted.

- **Start mode**: Configure the forwarding behavior of the interface on the data-plane when the authentication is in-progress during the first run of the supplicant.

- **Fail mode**: Configure the forwarding behavior of the interface when the dot1x authentication fails.

- **dot1x supplicant restart**: Configure the EAPoL protocol version to use in EAPoL frames.

```bash
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_supplicant_Policy
CX_SW(config-dot1x-supp-policy)# held-period 30

held-period 60 (default)
```

```bash
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_policy
CX_SW(config-dot1x-supp-policy)# start-mode start-closed

start-mode start-open (default)
```

```bash
CX_SW(config)# aaa authentication port-access dot1x supplicant
CX_SW(config-dot1x-supp)# policy CX_policy
CX_SW(config-dot1x-supp-policy)# fail-mode fail-closed

fail-mode fail-open (default)
```

```bash
CX_SW # port-access dot1x supplicant restart
interface  Restart the 802.1X supplicant for specified interfaces
<cr>
```
dot1x supplicant show commands

CX_SW# show aaa authentication port-access dot1x supplicant status

802.1X Supplicant Status

<table>
<thead>
<tr>
<th>Interface</th>
<th>Policy</th>
<th>PAE State</th>
<th>Authenticator</th>
<th>EAP Method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>CX_Policy_01</td>
<td>Authenticated</td>
<td>38:21:c7:59:ad:27</td>
<td>EAP-TLS</td>
<td>Secured</td>
</tr>
<tr>
<td>1/1/2</td>
<td>CX_Policy_02</td>
<td>Authenticating</td>
<td>38:21:c7:59:ad:28</td>
<td>EAP-MD5</td>
<td>Blocked</td>
</tr>
<tr>
<td>1/1/3</td>
<td>CX_Policy_01</td>
<td>Unauthenticated</td>
<td>38:21:c7:59:ad:29</td>
<td>EAP-TLS</td>
<td>Fail-Open</td>
</tr>
<tr>
<td>1/1/4</td>
<td>CX_Policy_03</td>
<td>Unauthenticated</td>
<td>--</td>
<td>--</td>
<td>Open</td>
</tr>
</tbody>
</table>

1. show aaa authentication port-access dot1x supplicant policy
2. show aaa authentication port-access dot1x supplicant status
   1. show aaa authentication port-access dot1x supplicant status interface 1/1/1 802.1X Supplicant Status
3. show aaa authentication port-access dot1x supplicant statistics
4. diag-dump dot1x-supplicant basic
5. port-access dot1x supplicant restart
6. show tech dot1x-supplicant [local-file]
Best Practices
AOS-CX dot1x supplicant configuration

**Recommended dot1x supplicant configuration**

aaa authentication port-access dot1x supplicant

  enable

  policy `cx_dot1x_supplicant_uplink_1`

    eap-identity identity `cxtme`

    eap-identity password plaintext `setpasswd` `###(EAP-MD5)`

    discovery-timeout 60

    start-mode start-closed

    fail-mode fail-closed

interface 1/1/48

  aaa authentication port-access dot1x supplicant

  associate policy `cx_dot1x_supplicant_uplink_1`

  enable

**New Show commands**

```
show aaa authentication port-access dot1x supplicant status

CXdot1xsupplicant# sh aaa authentication port-access dot1x supplicant status

802.1X supplicant Status

<table>
<thead>
<tr>
<th>Interface</th>
<th>Policy</th>
<th>PAF State</th>
<th>Authenticator</th>
<th>EAP Method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/48</td>
<td>cx_dot1x_supp...</td>
<td>Authentic</td>
<td>EAP-TLS</td>
<td>Setpasswd</td>
<td>Secured</td>
</tr>
</tbody>
</table>

CXdot1xsupplicant#
```
Troubleshooting
Recommended troubleshooting flow

1. Check dot1x supplicant policy configuration
2. Check dot1x supplicant policy is associated to right uplink interface
3. Check dot1x authenticator switch interface eapol is reaching and authenticator has required configuration
4. Check radius server configuration
5. Check required certificate are installed and attached to right application

- Have a topology diagram ready
- Ensure IPs, interface details are included
- Check physical cabling and generate “show tech” when opening a TAC case
- Check network: show LLDP neighbor, ensure underlay network works using ping and traceroute between loopbacks and interfaces, fix any issues found
Recommended dot1x supplicant configuration

aaa authentication port-access dot1x supplicant
   enable
   policy `cx_dot1x_supplicant_uplink_1`
       eap-identity identity `cxtme`
       eap-identity password plaintext `setpasswd ***(EAP-MD5)`
   discovery-timeout 60
   start-mode start-closed
   fail-mode fail-closed
interface 1/1/48
   aaa authentication port-access dot1x supplicant
   associate policy `cx_dot1x_supplicant_uplink_1`
   enable

New Show commands

show aaa authentication port-access dot1x supplicant status
CXdot1xsupplicant# sh aaa authentication port-access dot1x supplicant status

802.1X supplicant Status

<table>
<thead>
<tr>
<th>Interface</th>
<th>Policy</th>
<th>PAE State</th>
<th>Authenticator</th>
<th>EAP Method</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/48</td>
<td>cx_dot1x_supp....</td>
<td>Authenticated</td>
<td>64:e8:81:b8:e3:fb</td>
<td>EAP-TLS</td>
<td>Secured</td>
</tr>
</tbody>
</table>

CXdot1xsupplicant#
AOS-CX dot1x authenticator configuration

Recommended dot1x supplicant configuration

```
interface 1/1/5
aaa authentication port-access client-limit 5
    aaa authentication port-access dot1x authenticator enable
    aaa authentication port-access mac-auth enable
radius-server tracking interval 60
radius-server tracking retries 2
radius-server host 50.1.1.2 key ciphertext AQBapdAz4irjSK61Zg/CFArsNWyKbn1L0bqDD/v9SH1eMQ6ABQAAASY2611
u tracking enable tracking-mode dead-only
```

New Show commands

```
Agg-Core-CXSW# show port-access clients
Port Access Clients
Status Codes: d device-mode, c client-mode, m multi-domain

<table>
<thead>
<tr>
<th>Port</th>
<th>MAC-Address</th>
<th>Onboarding</th>
<th>Status</th>
<th>Role</th>
<th>Device Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>c 1/1/5</td>
<td>8c:85:61:46:e7:d2 dot1x</td>
<td>Success</td>
<td>RADIUS_652982728</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c 1/1/5</td>
<td>8c:85:61:46:e7:c0 mac-auth</td>
<td>Success</td>
<td>RADIUS_652982728</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Agg-Core-CXSW#
```
Troubleshooting - Mirror

```plaintext
Mirror session 1
Source interface 1/1/1 both
Destination CPU
enable
diag utilities tshark file
copy tshark-pcap tftp://10.80.2.187/supplicant.pcap vrf mgmt
```
dot1x supplicant Troubleshooting

**New Show & Tech Command**
- show crypto pki certificate
- show aaa authentication port-access dot1x supplicant policy
- show aaa authentication port-access dot1x supplicant status
- show aaa authentication port-access dot1x supplicant statistics
- show running-config aaa authentication port-access dot1x supplicant
- port-access dot1x supplicant restart
- diag-dump dot1x-suppliant basic
- show tech dot1x-suplicant [local-file]

**New Event Logs**

<table>
<thead>
<tr>
<th>Daemon</th>
<th>Event ID</th>
<th>Severity</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x-suppd</td>
<td>12301</td>
<td>INFO</td>
<td>dot1x supplicant has blocked the interface {iface}.</td>
<td>The dot1x supplicant is blocking the interface on the data-plane.</td>
</tr>
<tr>
<td>dot1x-suppd</td>
<td>12302</td>
<td>INFO</td>
<td>dot1x supplicant has unblocked the interface {iface}.</td>
<td>The dot1x supplicant is opening the interface on the data-plane.</td>
</tr>
<tr>
<td>dot1x-suppd</td>
<td>12303</td>
<td>INFO</td>
<td>dot1x supplicant PAE restarted on interface {iface} due to change in policy {policy}.</td>
<td>The dot1x supplicant PAE is restarted due to a change in the policy used on the interface.</td>
</tr>
<tr>
<td>dot1x-suppd</td>
<td>12304</td>
<td>ERR</td>
<td>dot1x supplicant is not supported on the port {port}.</td>
<td>The dot1x supplicant is enabled on a port that is not supported (Ex: LAG, ROP).</td>
</tr>
</tbody>
</table>

**New Debug Logs**

<table>
<thead>
<tr>
<th>Daemon</th>
<th>Severity</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x-suppd</td>
<td>INFO</td>
<td>dot1x supplicant FSM for PAE with MAC {mac} transitioned from {old-state} to {new-state}.</td>
<td>The dot1x supplicant PAE’s state machine has changed state.</td>
</tr>
<tr>
<td>dot1x-suppd</td>
<td>INFO</td>
<td>dot1x supplicant status on interface {iface} changed from {old-status} to {new-status}.</td>
<td>The dot1x supplicant status changed on the interface.</td>
</tr>
</tbody>
</table>
Demo: dot1x supplicant

- EAP-Method
  - EAP-TLS
    - User-defined Certificate
    - EST enrollment
  - EAP-MD5
- start-mode & fail-mode
- canned eap success
- eapol-force-multicast
dot1x Supplicant: EAP-TLS User defined Certificate

crypto pki application dot1x-supplicant certificate client

aaa authentication port-access dot1x supplicant
    enable
    policy cx_dot1x_supplicant
        eap-identity identity cxtme
interface 1/1/48
    aaa authentication port-access dot1x supplicant
    associate policy cx_dot1x_supplicant
    enable
dot1x Supplicant: EAP-TLS User defined Certificate

Access-CXSW(config)# crypto pki application dot1x-supplicant certificate client
Access-CXSW(config)# end

Access-CXSW# sh crypto pki certificate

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Cert Status</th>
<th>EST Status</th>
<th>Associated Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>installed</td>
<td>n/a</td>
<td>dot1x-supplicant</td>
</tr>
<tr>
<td>local-cert</td>
<td>installed</td>
<td>n/a</td>
<td>captive-portal, est-client, https-server, radsec-client, syslog-client</td>
</tr>
<tr>
<td>est_certificat1</td>
<td>installed</td>
<td>enroll success</td>
<td>none</td>
</tr>
<tr>
<td>device-identity</td>
<td>installed</td>
<td>n/a</td>
<td>none</td>
</tr>
</tbody>
</table>

Access-CXSW# show crypto pki certificate client pem

Certificate Name: client
Associated Applications:
- dot1x-supplicant

Certificate Status: installed
EST Status: n/a
Certificate Type: regular
Intermediates:
- none
**dot1x Supplicant: EAP-TLS EST Enrolled Certificate**

```plaintext
crypto pki application dot1x-supplicant certificate est_certificate1

aaa authentication port-access dot1x supplicant
    enable
    policy cx_dot1x_supplicant
        eap-identity identity cxtme

interface 1/1/48
    aaa authentication port-access dot1x supplicant
    associate policy cx_dot1x_supplicant
    enable
```
dot1x Supplicant: EAP-TLS User defined Certificate

Access-CXSW(config)# crypto pki application dot1x-supplicant certificate est_certificate1

Access-CXSW(config)# end

Access-CXSW# sh crypto pki certificate

<table>
<thead>
<tr>
<th>Certificate Name</th>
<th>Cert Status</th>
<th>EST Status</th>
<th>Associated Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>client</td>
<td>installed</td>
<td>n/a</td>
<td>none</td>
</tr>
<tr>
<td>local-cert</td>
<td>installed</td>
<td>n/a</td>
<td>captive-portal, est-client, https-server,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>radsec-client, est-client, syslog-client</td>
</tr>
<tr>
<td>est_certificate1</td>
<td>installed</td>
<td>enroll success</td>
<td>dot1x-supplicant</td>
</tr>
<tr>
<td>device-identity</td>
<td>installed</td>
<td>n/a</td>
<td>none</td>
</tr>
</tbody>
</table>

Access-CXSW# sh crypto pki certificate est_certificate1.pem

Certificate Name: **est_certificate1**
Associated Applications: dot1x-supplicant
Certificate Status: installed

**EST Status: enroll success**
Certificate Type: regular
aaa authentication port-access dot1x supplicant
   enable
   policy cx_dot1x_supplicant
     eap-method eap-md5
     eap-identity identity cxtme
     eap-identity password ciphertext AQBapfhltTYjsSH9N05UJseS5cOG2Fv6QRKD8AIL2BgTQ2jdCAAAAAAC7hfPijBaqs
interface 1/1/48
   aaa authentication port-access dot1x supplicant
      associate policy cx_dot1x_supplicant
      enable
dot1x Supplicant: start-mode and fail-mode

```
aaa authentication port-access dot1x supplicant
   enable
   policy cx_dot1x_supplicant
      eap-method eap-md5
      eap-identity identity cxtme
      eap-identity password ciphertext AQBapfhltTYjsSH9NO5UJeS5cOG2Fv6QRKDB8AIL2BqTQ2jdCAAAAAC7hfP1jBaq
   start-mode start-closed
   fail-mode fail-closed
interface 1/1/48
   aaa authentication port-access dot1x supplicant
   associate policy cx_dot1x_supplicant
   enable
```
dot1x Supplicant: Canned EAP Success

```
aaa authentication port-access dot1x supplicant
    enable
    policy cx_dot1x_supplicant
        eap-method eap-md5
        eap-identity identity cxtme
        eap-identity password ciphertext
            AQBaPFhLTYj5SH9NO5UJseS5cOG2FV6QRKKD8AIL2BgTQ2jdCAAAAC7hfPi jBaqs
    canned-eap-success
interface 1/1/48
    aaa authentication port-access dot1x supplicant
        associate policy cx_dot1x_supplicant
        enable
```
dot1x Supplicant: force-multicast

```bash
dot1x Supplicant: force-multicast

aaa authentication port-access dot1x supplicant
  enable
  policy cx_dot1x_supplicant
    eap-method eap-md5
    eap-identity identity cxtme
    eap-identity password ciphertext AQBapfhltTYjsSH9NO5UJseS5cOG2Pv6QRKD8AIL2BgTQ2jdCAAAAC7hfPi jBaqs
  eapol-force-multicast
    eapol-protocol-version 2
    canned-eap-success
discovery-timeout 60
start-mode start-closed
fail-mode fail-closed
interface 1/1/48
  aaa authentication port-access dot1x supplicant
  associate policy cx_dot1x_supplicant
  enable
```
Additional information (internal)

- Functionality guide dot1x supplicant
- Design guide dot1x supplicant
- IEEE dot1x
Thank you

yashavantha.n.n@hpe.com