



Pulse Policy Secure: Session Bridging using Certificate Authentication

Cook Book

Published **June 2020**

Document Version **1.0**

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

© 2020 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse Policy Secure: Session Bridging using Certificate Authentication

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.pulsesecure.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

INTRODUCTION	3
CONFIGURING PPS FOR SESSION BRIDGING	3
CONFIGURING MAC OS X NATIVE SUPPLICANT FOR PPS 802.1X AUTHENTICATION..	3
CONFIGURING PULSE POLICY SECURE	6
CONFIGURING CISCO SWITCH.....	11
TROUBLESHOOTING.....	12

Introduction

On Mac OS X, Windows and Linux endpoint using native supplicant, PPS Host checking can be enforced only for Layer 3 connection. Once the endpoint gets authenticated using native supplicant and gains network access, you can launch and install Pulse Secure client using web browser deployment or SCCM advertisement to establish a Layer 3 session.

This evaluates the health status of the endpoints and thereby ensuring legitimate resource access behind PPS Enforcer. There will be only one session for Layer 2 and Layer 3 connections on PPS which will consume single license.

For agentless host checking, native supplicant is used to perform 802.1x authentication. The compliance check is performed using browser based agentless L3 session. The L2 and agentless L3 session are bridged on PPS to provide compliance based layer 2 access control. For access control, RADIUS return attribute Filter-ID with Radius COA is used.

Session Bridging Support Matrix

Table 1 Supported Session Bridging Matrix

Clients	Session	Operating System	Authentication Mechanism
Pulse Client/Browser Sessions (Agentless)	Layer 3	Windows/Mac OS X	User Name, Password/Certificate
Native Supplicant	Layer 2	Windows/Mac OS X	802.1X, SNMP, RADIUS, Mac Authentication

Configuring PPS for Session Bridging

- [“Configuring Mac OS X Native Supplicant for PPS 802.1X Authentication” on page 3](#)
- [“Configuring Pulse Policy Secure” on page 6](#)
- [Configuring Cisco Switch 11](#)
- [“Troubleshooting” on page 12](#)

Configuring Mac OS X Native Supplicant for PPS 802.1X Authentication

This section details the procedure for configuring native Mac OS X supplicant for PPS 802.1X authentication.

Requirements:

- Apple Mac OS X endpoint
- iPhone Configuration utility
- Client certificate must be installed on Mac OS X endpoint.

Configuring MAC OS X Native Supplicant

Authentication to a PPS 802.1X server in MAC OS X endpoints is achieved using Apple Configurator. This tool allows you to easily create, maintain, and install configuration profiles, track and install provisioning profiles, and capture device information including console logs.

Note: The latest MAC OS X endpoints can be configured using Apple Configurator 2 tool.

This section covers the following configuration:

- ["Configuring 802.1x profile" on page 4](#)
- ["Configuring PEAP Authentication Profile" on page 4](#)

Configuring 802.1x profile

You can create various profiles (TTLS/PAP, TTLS/MS-CHAP-V2, and PEAP/MS-CHAP-V2) required for PPS 802.1x authentication using Apple Configurator. The generated configuration profiles can be exported to a Mac OS X endpoint. To create profiles, install the profiles (by double clicking on the exported files) on their OS X endpoints and that will provision Layer 2 access when connected to 802.1x enabled switch port.

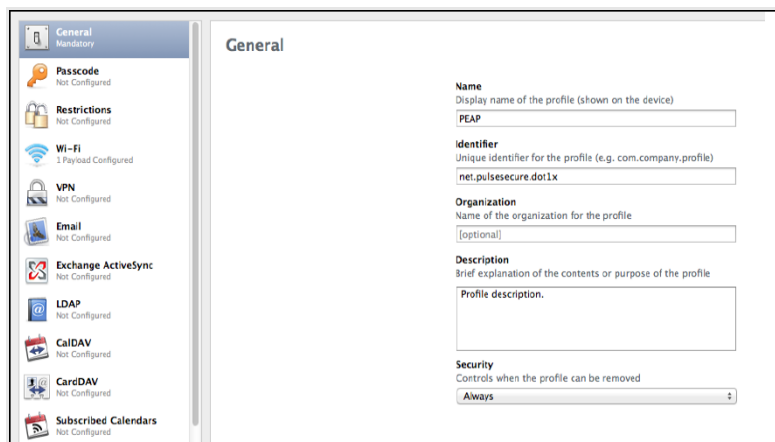
Configuring 802.1x profiles -PEAP applies only for General and Wi-Fi settings. If the authentication server is Certificate Auth Server, use **EAP-PEAP/EAP-TLS**.

Configuring PEAP Authentication Profile

To configure PEAP, perform the following:

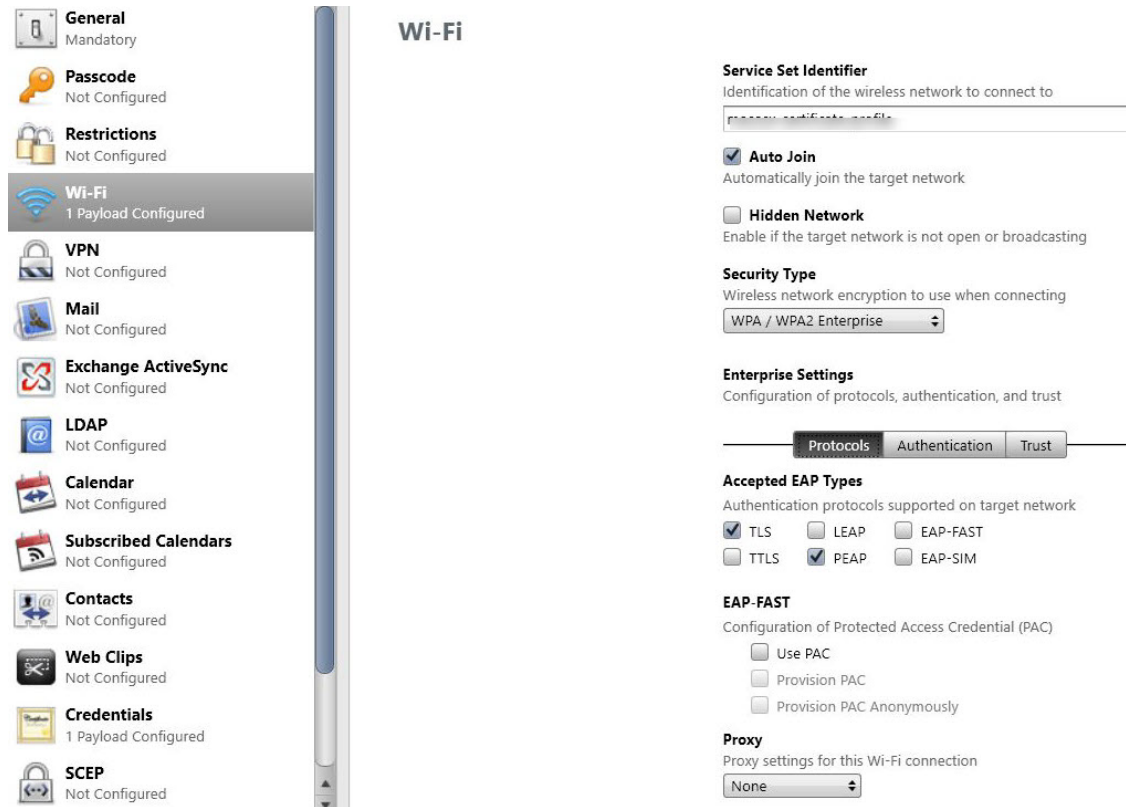
1. On the iPhone configuration utility (IPCU) navigate to **Configuration Profiles** tab.
2. On configuration Profiles page, select **General** and enter the required values.

Figure 1 PEAP: TLS General



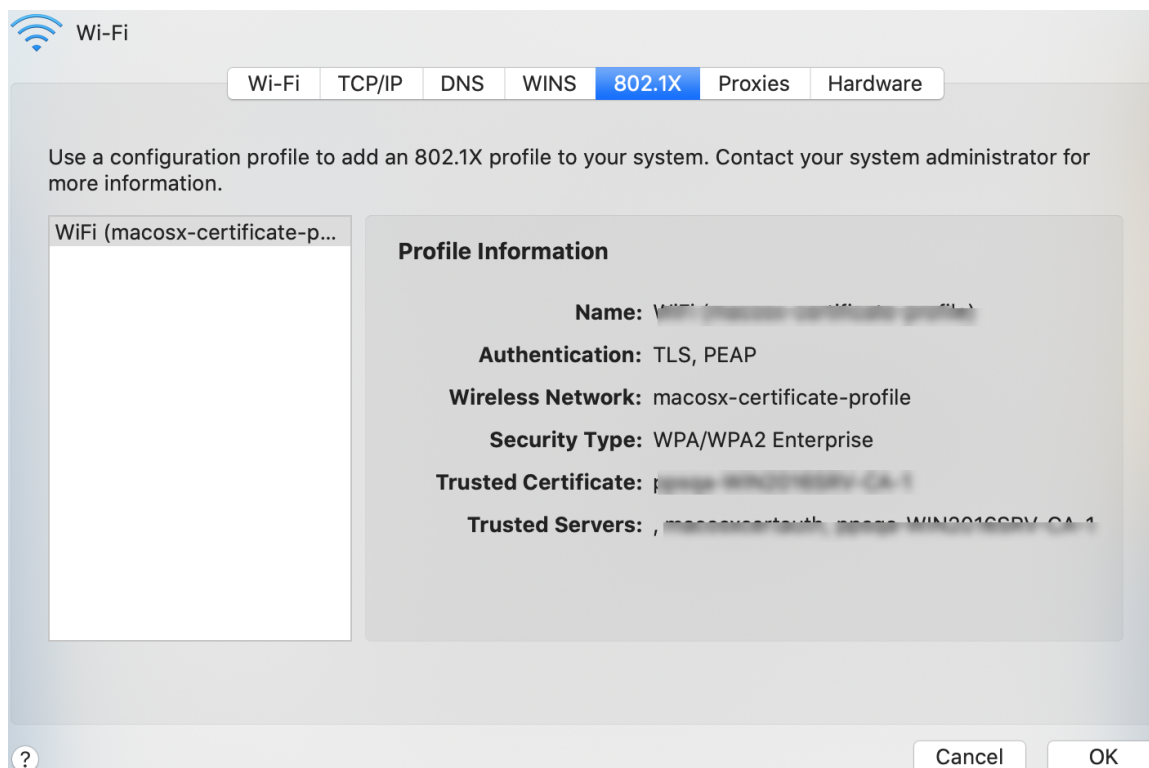
3. Select **Wi-Fi** and enter the required values. Ensure TLS/PEAP are selected under Accepted EAP types.

Figure 2 PEAP: TLS Wi-Fi



Once the profile is successfully imported, you see the below screen shot.

Figure 3 WiFi Profile

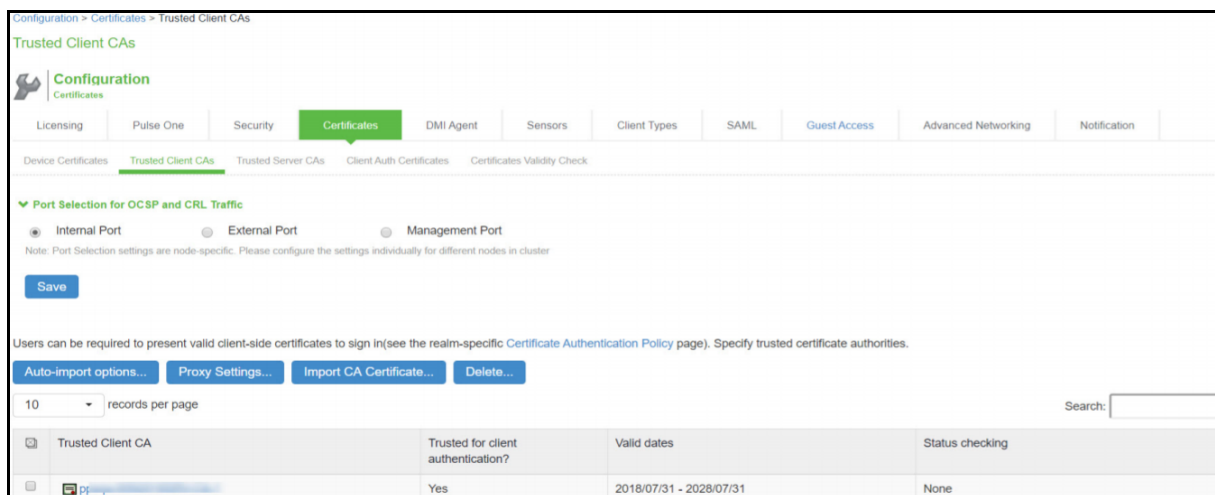


Configuring Pulse Policy Secure

To configure PPS for guest wireless authentication:

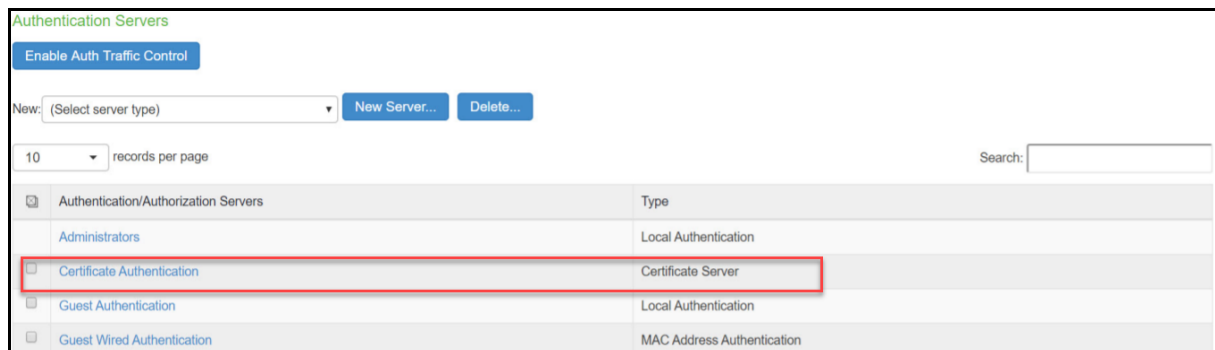
1. Select **System > Configuration > Certificates > Trusted Client CAs**. Install the certificate from the CA that Pulse Policy Secure is using for trusted Client CAs.

Figure 4 Client CA



2. Select **Authentication > Auth.Servers**. The Authentication Servers screen appears. Use the Default Certificate Authentication Server.

Figure 5 Certificate Authentication Server



3. Select **Users > User Realms**, Click **Cert Auth** realm available by default to view the settings. Under Servers, Select the Certificate Authentication server.

Figure 6 Cert Auth Realm Settings

General

Name: Cert Auth

Description: System created authentication realm for Certificate

☒ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Certificate Authentication

User Directory/Attribute: None

Accounting: None

Device Attributes: None

Additional Authentication Server

☐ Enable additional authentication server

4. Create Role Mapping rules to associate with the roles.

Figure 7 Role Mapping Rules

User Realms > Cert Auth > Role Mapping > Role Mapping Rule

Role Mapping Rule

Name: Access Rule

Rule: if username...

is *

If more than one username should match, enter one username per line. You can use * wildcards.

then assign these roles

Available Roles:

- ENGG
- Guest
- Guest Admin
- Guest Sponsor
- Guest Wired Restricted

Selected Roles:

- FullAccessRole
- LimitedAccessRole

☐ Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

Save Changes **Save as Copy**

5. Selecting **Authentication > Signing In > Sign-In Policies**. Associate the default Cert Auth authentication protocol set with the realm.

Figure 8 Sign-In Policy

Signing In > Sign-In Policies > */certauth/

***/certauth/**

User type: ☒ Users ☐ Administrators

Sign-In URL: Format: <host>/<path>/ Use * as wildcard in the beginning of the host name.

Description:

Sign-in page: To create or manage pages, see [Sign-In pages](#).

▼ Authentication realm

Specify what realms will be available when signing in.

	Available realms	Authentication protocol set	
	<input type="text" value="Cert Auth"/>	<input type="text" value="- Not applicable -"/>	<input type="button" value="Add"/>
<input checked="" type="checkbox"/>	Cert Auth	Cert Auth	

If more than one realm appears above, the Policy Secure sign-in page will ask the user to choose. Other endpoints cannot choose a realm, the Policy Secure will assign the first suitable realm from the list. If no realms appear above, sign-in will fail.

6. Select **Endpoint Policy > Network Access > Location Group**. Select the default ***/certauth/** sign-in policy.

Figure 9 Location Group

Network Access > Location Group > Cert Auth

Cert Auth

▼ Location Group

* Name: Label to reference this Location Group.

Description:

* Sign-in Policy: To manage policies, see the [Sign-In Policies](#)

MAC Authentication Realm: To manage realm, see the [MAC Address Realms](#)

* indicates required field

7. Configure the RADIUS client. Ensure that the default **Cert Auth** location group and Support Disconnect Messages and Support CoA Messages options are enabled.

Figure 10 RADIUS Client

Network Access > RADIUS Client > Cisco 2960X

Cisco 2960X

▼ RADIUS Client

* Name: Cisco 2960X Label to reference this RADIUS Client.

Description:

* IP Address: 1 IP Address of this RADIUS Client.

* IP Address Range: 1 Number of IP Addresses for this RADIUS Client

* Shared Secret: RADIUS shared secret

* Make/Model: Cisco Systems To manage make/model, see the [RADIUS Vendor](#)

Key Wrap ☐ Key Wrap (Support for RFC 6218)

* Location Group: Cert Auth To manage groups, see the [Location Group](#)

▼ Dynamic Authorization Support

Support Disconnect Messages ☒ Disconnect Message Support

Support CoA Messages ☒ Change of Authorization Message Support

*Dynamic Authorization Port: 3799 Dynamic Authorization Extensions Port

[Save Changes](#)

8. Configure the RADIUS return attributes for Guest Wired policy. Select **Endpoint Policy > Network Access > RADIUS Return Attribute Policies**. Click **New Policy**. Under RADIUS Attributes tab, select the check box for **Return Attribute**. The RADIUS return attributes are required for MAB authentication initially when the user connects to the SSID (where the redirection happens) and then the session is bridged after the user authenticates.

Figure 11 RADIUS Return Attributes

Network Access > Radius Attributes > RADIUS Return Attributes > FULL ACCESS

FULL ACCESS

General

* Name:

Description:

Location Group

Specify the Location Group for which this policy applies.

Available Location Groups:
Guest
Guest Wired

Add -> Remove

Selected Location Groups:

Selected Radius Clients
Below list is populated dynamically based on the selected Location Groups

Vendor (Manufacturer)	Client Details
Cisco Systems	Cisco 2960X

Access Control Policy Settings

Select below option to control the access level for the device/user connecting to the network

☐ Provide full Access (Open Port)

☒ Control the Access

Access can be controlled using the VLAN Id, ACLs and Radius Return Attribute settings below

☐ Control using VLAN Id:
(1 - 4094)

☐ Control access using Access Control List (ACL) settings (Supported only for Cisco, Juniper, HP)

☒ Control access using Radius Return Attributes

Note: Selecting this option will result in opening the port without any restrictions

Note: Selecting this option enables control of the device or user access

Note: This option is used for assigning devices to corresponding VLAN on the switch

Note: These attributes are sent to switch for controlling the access

Delete

Return Attribute	Radius Auth Server Attribute Value	Auth Server Catalog Attribute Value	Value	
<input type="text" value="Filter-Id"/>	-none-	-none-	<input type="text"/>	<input type="button" value="Add"/>
<input checked="" type="checkbox"/> Filter-Id	-none-	-none-	FULL-ACCESS-ACL	

☐ Add Session-Timeout attribute

Specify the action that needs to be taken for the device upon expiration of session timeout on the switch

☒ Terminate the session ☐ Re-authenticate the session

Note: This will send session timeout attribute equal to session lifetime

Roles

Select the roles to which this policy is applicable

☐ Any Role ☒ Selected below ☐ Other than selected below

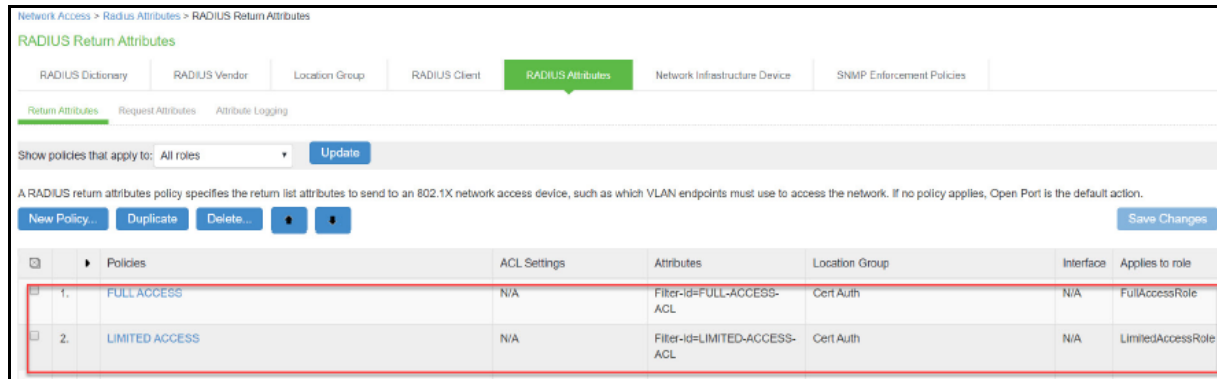
Available roles:
Guest
Guest Admin
Guest Sponsor
Guest Wired Restricted
Limited Access Role

Add -> Remove

Selected roles:

NOTE: Any changes to this page results in termination of existing L2 connections and triggers reconnections.

Figure 12 RADIUS Return Attributes Certificate Authentication



Configuring Cisco Switch

CLI command to configure session bridging on Cisco switch. The switch configuration varies for each switch type.

Run the show run command on your switch to ensure that your access interface connections are set up.

```

aaa accounting network default start-stop group PPS-QA

aaa accounting Identity default start-stop broadcast group PPS-QA
aaa accounting send stop-record authentication failure
aaa accounting update periodic 3
!
aaa server radius dynamic-author
client PPS-SERVER server-key 7 000E06080D4B0E14
server-key 7 051B150A22595C0C
port 3799
ignore session-key
ignore server-key
!
radius server PPS-SERVER
address ipv4 <PPS-SERVER-IP> auth-port 1812 acct-port 1813
key 7 1315021E1809557878

radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 55 include-in-acct-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 2 tries 5
radius-server retransmit 3
!
aaa group server radius PPS-QA
server name PPS-SERVER
!
!
aaa local authentication PPS-QA authorization PPS-QA
aaa new-model
aaa session-id common

```

```
Extended IP access list FULL-ACCESS-ACL
 10 permit ip any any
```

```
Extended IP access list LIMITED-ACCESS-ACL
 10 permit ip any host <PPS IP>
 20 permit ip any host <PATCH-MGMT-SERVER>
 30 permit udp any any eq domain
 40 permit tcp any any eq domain
 50 permit udp any eq bootps any
 60 permit udp any any eq bootpc
 70 permit udp any eq bootpc any
 80 deny ip any any
```

Troubleshooting

For troubleshooting you can verify the user access logs.

Figure 13 User Access Logs

```
"Agent session bridged for macuser/Cert_Realm from 10.20.30.40 with Junos-Pulse9.1.2.xxxx
(Macintosh) Pulse/9.1.2.xxxxx"
```