

# Pulse Policy Secure: Session Bridging using Certificate Authentication Cook Book

PublishedJune 2020Document Version1.0

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 <a href="http://www.pulsesecure.net/support/eula/">http://www.pulsesecure.net/support/eula/</a>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

NTRODUCTION	. 3
ONFIGURING 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 3connection. 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 1Supported 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**

Figure 1 PEAP: TLS General

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.

Ceneral Mandatory	General
Passcode Not Configured	Name Display name of the profile (shown on the device)
Restrictions Not Configured	PEAP
VI-Fi 1 Payload Configured	<b>Identifier</b> Unique identifier for the profile (e.g. com.company.profile)
O VPN	net.pulsesecure.dot1x
Not Configured	Organization Name of the organization for the profile
Email Not Configured	[optional]
Exchange ActiveSync Not Configured	Description Brief explanation of the contents or purpose of the profile
DAP Not Configured	Profile description.
CaIDAV Not Configured	Security
CardDAV Not Configured	Controls when the profile can be removed Always
Subscribed Calendars Not Configured	*

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

#### Figure 2 PEAP: TLS Wi-Fi General 8 Wi-Fi Mandatory Service Set Identifier Passcode Identification of the wireless network to connect to Not Configured Restrictions Not Configured 🖌 Auto Join Automatically join the target network Wi-Fi 1 Payload Configured Hidden Network Enable if the target network is not open or broadcasting VPN 11 Not Configured Security Type Wireless network encryption to use when connecting Mail WPA / WPA2 Enterprise 🗘 Not Configured Exchange ActiveSync **Enterprise Settings** Not Configured Configuration of protocols, authentication, and trust LDAP Not Configured Protocols Authentication Trust **Accepted EAP Types** Calendar 47 Not Configured Authentication protocols supported on target network TLS 🔲 LEAP 📄 EAP-FAST **Subscribed Calendars** 3 TTLS PEAP EAP-SIM Not Configured Contacts EAP-FAST Not Configured Configuration of Protected Access Credential (PAC) Web Clips Use PAC Not Configured Provision PAC Provision PAC Anonymously Credentials 1 Payload Configured Proxy Proxy settings for this Wi-Fi connection SCEP Not Configured None \$

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	L.								
Configuration > Certi	ficates > Trusted Client CAs									
Trusted Client C	CAs									
Configur Certificates	ation									
Licensing	Pulse One Securit	y Certificates	DMI Agent	Sensors	Client Types	SAML	Guest Access	Advanced Networking	Notification	
Device Certificates	Trusted Client CAs Trustee	d Server CAs Client Auth Co	ertificates Certifica	tes Validity Check						
Internal Po	or OCSP and CRL Traffic rt  © Externa settings are node-specific. Please		Management Port ally for different nodes	in cluster						
	Users can be required to present valid client-side certificates to sign in(see the realm-specific Certificate Authentication Policy page). Specify trusted certificate authorities. Auto-import options Proxy Settings Import CA Certificate Delete									
10 • records per page Search:										
Trusted Cl	ent CA		Trusted for clie authentication?		Valid dates			Status checking		
🔲 🖬 pr	Contract of Contract of Contract		Yes		2018/07/31 - 20	28/07/31		None		

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

Figure 5 Certificate Authentication Server

_	Authentication Servers Enable Auth Traffic Control					
New	(Select server type)   New Server  Delete					
10	✓ records per page	Search:				
	Authentication/Authorization Servers	Туре				
	Administrators	Local Authentication				
	Certificate Authentication	Certificate Server				
	Guest Authentication	Local Authentication				
	Guest Wired Authentication	MAC Address Authentication				

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		
General Authentication Policy	Role Mapping	
* Name:	Cert Auth	Label to reference this realm
Description:	System created authentication realm for Certificate	
	When editing, start on the Role Mapping page     ■	
✓ Servers		
Specify the servers to use for authentication and author	orization. To create or manage servers, see the Servers page.	
Authentication:	Certificate Authentication 💌	Specify the server to use for authenticating users.
User Directory/Attribute:	None	Specify the server to use for authorization.
Accounting:	None •	Specify the server to use for Radius accounting.
Device Attributes:	None •	Specify the server to use for device authorization.
✤ 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 that	n one username should match, enter one username per line. You can use * wildcards.
	10	
❤ then assign these roles		
Available Roles:	Selected Roles:	
ENGG	FullAccessRole	
Guest Remo	LimitedAccessRole	
Guest Sponsor		
Guest Wired Restricted		*
Stop processing rules when this rules	le 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
0	- 0)

Signing In > Sign-in Po	blicies > */certauth/		
/certauth/			
User type:	Users Administrators		
Sign-in URL:	*/certauth/	Format: <host>/<path>/; Use * as wildcard in the beginning of the host name.</path></host>	
Description:	System created Certificate Authentication Sign In		
Sign-in page:	Default Sign-In Page 🔻		
oign in page.	To create or manage pages, see Sign-In p	ages.	
<ul> <li>Authentication re</li> <li>Specify what realm</li> </ul>	alm s will be available when signing in.		
Delete 🔹	•		
	Available realms	Authentication protocol set	
	Cert Auth	- Not applicable -	Add
	Cert Auth	Cert Auth	

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:	Cert Auth		Label to reference this Location Group.
Description:	System created location grou Certificate Authentication	up for	
* Sign-in Policy:	*/certauth/	]	To manage policies, see the Sign-In Policies
MAC Authentication Realm:	(none) 🔻	-	To manage realm, see the MAC Address Realms
Save Changes * 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

Networ	k Access > RADIUS Client > Cisco 2960X		
Cisco	2960X		
¥ RA	DIUS 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
❤ Dy	namic Authorization Support		
Sup	port Disconnect Messages 🕝	Disconnect Message Support	
Sup	port CoA Messages 🛛 🖉	Change of Authorization Message Support	
*Dyn	amic Authorization Port 3799	Dynamic Authorization Extensions Port	
Sav	e 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.



work Access	Radius Attributes > RADIUS	S Deturn Attributes >	FULL ACCESS						
JLL ACCES		5 Return Attributes >	FULLAGGESS						
General									
ſ									
scription:	FULL ACCESS								
scription.									
L		//)							
Location Gro	oup								
ocation Gro	oups					Selected Rad	ius Clients		
Specify the Loca	cation Group for which this polic					Below list is pop	ulated dynamica	ally based on the selec	ted Location Gro
Available Loc Default	cation Groups:	Selected Locatio	on Groups:			Vendor (Mar	oufacturor)	Client Details	
Guest	Remove	Cert Autri							
Guest Wired	t i i i i i i i i i i i i i i i i i i i					Cisco Syster	115	Cisco 2960X	
	-		~						
elect below opti Provide ful Control the								It in opening the port we control of the device of	
<ul> <li>Provide ful</li> <li>Control the Access can b</li> <li>Control</li> <li>Control</li> <li>Control</li> </ul>	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id:	d, ACLs and Radius R (1 - 4094) ontrol List (ACL) set	leturn Attribute setting	s below	er, HP)	Note: Selecting this Note: This option is	option enables used for assign		or user access onding VLAN on
Provide ful Control the Access can b Control	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id:	d, ACLs and Radius R (1 - 4094) ontrol List (ACL) set	tetum Attribute setting	s below		Note: Selecting this Note: This option is	option enables used for assign	control of the device of the device of the devices to correspond the devices to correspond to the device of the	or user access onding VLAN on
elect below opti Provide ful Control the Access can b Control Control Dele	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id: ol access using Access Co ol access using Radius Ref ster	d, ACLs and Radius R (1 - 4094) ontrol List (ACL) set	tetum Attribute setting	s below Inly for Cisco, Junip		Note: Selecting this Note: This option is Note: These attribu	option enables used for assign tes are sent to s	control of the device of the device of the devices to correspond the devices to correspond to the device of the	or user access onding VLAN on
Select below opt Provide ful Control the Access can b Control Control Dele	III Access (Open Port) e Access be controlled using the VLAN 1 ol using VLAN Id: ol access using Access Co ol access using Radius Ref etc.	d, ACLs and Radius R (1 - 4004) httrol List (ACL) set turn Attributes	tetum Attribute setting ttings (Supported c Radius Auth Ser	s below Inly for Cisco, Junip ver Attribute Value	Auth Server Ca	Note: Selecting this Note: This option is Note: These attribu	option enables used for assign tes are sent to s	control of the device i ing devices to corresp witch for controlling th	or user access
Select below opt Provide ful Control the Access can b Control Control Dele	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id: ol access using Access Co ol access using Radius Rel etce • • • Return Attribute Filter-Id	d, ACLs and Radius R (1 - 4004) httrol List (ACL) set turn Attributes	tings (Supported c Radius Auth Ser -none-	s below Inly for Cisco, Junip ver Attribute Value	Auth Server Ca	Note: Selecting this Note: This option is Note: These attribu	s option enables used for assign tes are sent to s Value	control of the device i ing devices to corresp witch for controlling th	or user access
<ul> <li>Provide full</li> <li>Control the Access can te</li> <li>Control</li> <li>Control</li></ul>	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id: ol access using Access Co ol access using Radius Rel etce • • • Return Attribute Filter-Id	d, ACLs and Radius R (1 - 4094) ontrol List (ACL) sel turn Attributes	tetum Attribute setting ttings (Supported of Radius Auth Ser -none- -none-	s below nly for Cisco, Junip wer Attribute Value	Auth Server Ca	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	voption enables used for assign tes are sent to s Value FULL-ACCE	control of the device i ing devices to corresp witch for controlling th	or user access onding VLAN on e access Add
Select below opti Provide full Control the Access can t Control Contro	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id: ol access using Access Co ol access using Radius Re access to access using Radius Re access to access using Radius Re access to access to acc	d, ACLs and Radius R (1 - 4004) untrol List (ACL) sel turn Attributes	teturn Attribute setting ttings (Supported c Radius Auth Ser -nonenone- piration of session tim	s below nly for Cisco, Junip wer Attribute Value	Auth Server Ca	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	voption enables used for assign tes are sent to s Value FULL-ACCE	control of the device i ing devices to corresp witch for controlling th ESS-ACL	or user access onding VLAN on e access
Select below opti Provide fully Control the Access can t Control Contr	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id: ol access using Access Co ol access using Radius Re access access access access access access access response access access access access access access access response access access access access access access access response access acce	d, ACLs and Radius R (1 - 4004) untrol List (ACL) sel turn Attributes	teturn Attribute setting Radius Auth Ser -none- -none- piration of session tim Re-authenticate the	s below nly for Cisco, Junip wer Attribute Value	Auth Server Ca -none- -none-	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	voption enables used for assign tes are sent to s Value FULL-ACCE	control of the device i ing devices to corresp witch for controlling th ESS-ACL	or user access onding VLAN on e access
Belett below opti Provide fully Control the Access can t Control Contr	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id: ol access using Access Co ol access using Radius Re access access access access access access access response access access access access access access access response access access access access access access access response access acce	d, ACLs and Radius R (1 - 4004) untrol List (ACL) sel turn Attributes	teturn Attribute setting Radius Auth Ser -none- -none- piration of session tim Re-authenticate the	s below nly for Cisco, Junip ver Attribute Value	Auth Server Ca -none- -none-	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	voption enables used for assign tes are sent to s Value FULL-ACCE	control of the device i ing devices to corresp witch for controlling th ESS-ACL	or user access onding VLAN on e access
elect below opti Provide fully Control the Access can t Control Contro	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id: ol access using Access Co ol access using Radius Re access to the this policy is access to which this policy is access to the	d, ACLs and Radius R (1 - 4004) untrol List (ACL) sel turn Attributes	teturn Attribute setting tings (Supported o Radius Auth Ser -nonenone- piration of session tim Re-authenticate the w	s below nly for Cisco, Junip ver Attribute Value	Auth Server Ca -none- -none-	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	voption enables used for assign tes are sent to s Value FULL-ACCE	control of the device i ing devices to corresp witch for controlling th ESS-ACL	or user access onding VLAN on e access Add
Belet below opti Provide fully Control the Access can t Control Contro	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id: ol access using Access Co ol access using Radius Re access to the this policy is access to which this policy is access to the	d, ACLs and Radius R (1 - 4004) Introl List (ACL) sel turn Attributes	Radius Auth Ser -none- piration of session tim Re-authenticate the	s below nly for Cisco, Junip ver Attribute Value ver Attribute Value eout on the switch s session Other than sele	Auth Server Ca -none- -none-	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	voption enables used for assign tes are sent to s Value FULL-ACCE	control of the device i ing devices to corresp witch for controlling th ESS-ACL	or user access onding VLAN on e access Add
Belett below opti Provide full Control the Access can t Control Contro	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id: ol access using Access Co ol access using Radius Re access to the this policy is access to which this policy is access to the	d, ACLs and Radius R (1 - 4004) untrol List (ACL) sel turn Attributes	Radius Auth Ser -none- piration of session tim Re-authenticate the	s below nly for Cisco, Junip ver Attribute Value ver attribute value	Auth Server Ca -none- -none-	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	voption enables used for assign tes are sent to s Value FULL-ACCE	control of the device i ing devices to corresp witch for controlling th ESS-ACL	or user access onding VLAN on e access Add
Select below opti Provide full Control the Access can t Control Contro	III Access (Open Port) e Access be controlled using the VLAN I ol using VLAN Id: col access using Access Co ol access using Radius Re Return Attribute Filter-Id Filter-Id Filter-Id ession-Timeout attribute the action that needs to taken to minate the session cless to which this policy is e	d, ACLs and Radius R (1 - 4004) Introl List (ACL) sel turn Attributes	Radius Auth Ser -none- piration of session tim Re-authenticate the	s below nly for Cisco, Junip ver Attribute Value ver attribute value	Auth Server Ca -none- -none-	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	voption enables used for assign tes are sent to s Value FULL-ACCE	control of the device i ing devices to corresp witch for controlling th ESS-ACL	or user access onding VLAN on e access Add
Select below opti Provide full Control the Access can t Control Contro	III Access (Open Port) e Access be controlled using the VLAN J ol using VLAN Id: col access using Access Co ol access using Radius Re the filter-Id Filter-Id Filter-Id Filter-Id col access using Radius Re the action that needs to taken triminate the session coles to which this policy is e	d, ACLs and Radius R (1 - 4004) Introl List (ACL) sel turn Attributes	Radius Auth Ser -none- piration of session tim Re-authenticate the	s below nly for Cisco, Junip ver Attribute Value ver attribute value	Auth Server Ca -none- -none-	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	voption enables used for assign tes are sent to s Value FULL-ACCE	control of the device i ing devices to corresp witch for controlling th ESS-ACL	or user access onding VLAN on e access Add

Figure 12 RADIUS Return Attributes Certificate Authentication

RADIUS Diction	RADIUS Vendor	Location Group	RADIUS Client	RADIUS Attributes	Network Infrastructure Device	SNMP Enforcement Policies		
Return Attributes	Request Attributes Attribute Log	gging						
iow policies that	apply to: All roles	• Update						
RADIUS return a	ttributes policy specifies the retu	um list attributes to send	to an 802.1X network	access device, such as whic	h VLAN endpoints must use to ac	cess the network. If no policy applies,	Open Port is the default :	action.
	ttributes policy specifies the retu Duplicate Delete	um list attributes to send	l to an 802.1X network	access device, such as whic	h VLAN endpoints must use to ac	cess the network. If no policy applies,	Open Port is the default :	action. Save Change
New Policy		um list attributes to send	l to an 802.1X network	access device, such as whic ACL Settings	h VLAN endpoints must use to ac	cess the network. If no policy applies,		
New Policy	Duplicate Delete	Im list attributes to send	l to an 802.1X network					Save Chang

## **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
I.
aaa server radius dynamic-author
client PPS-SERVER server-key 7 000E06080D4B0E14
server-key 7 051B150A22595C0C
port 3799
ignore session-key
ignore server-key
1
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
1
L
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 eq bootps any
  60 permit udp 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"
```