

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 http://www.pulsesecure.net/support/eula/. 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.

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

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 Ce	ertificates Certifica	ites Validity Check						
Port Selection f Internal Po Note: Port Selection Save	or OCSP and CRL Traffic rt <u>Externa</u> settings are node-specific. Please	I Port	Management Port ally for different nodes	in cluster						
Users can be required Auto-import option	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 • r	ecords per page								Search:	
Trusted Cli	ent CA		Trusted for clie authentication?	nt ?	Valid dates			Status checking		
D PF	Contract 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

Aut Er	Authentication Servers Enable Auth Traffic Control					
New	New: (Select server type)					
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 > R	ole Mapping Rule	
Role Mapping Rule		
* Name: Access Rule		
❤ Rule:If username		
is v	If more that	n one username should match, enter one username per line. You can use * wildcards.
	11	
❤ then assign these roles		
Available Roles:	Selected Roles:	
ENGG	FullAccessRole	<u>^</u>
Guest Remove	LimitedAccessRole	
Guest Admin		
Guest Wired Restricted		*
Stop processing rules when this rule	matches	
To manage roles, see the Roles configuration p	age.	
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
i igai e o	5181111 61169

Signing In > Sign-in Po	licies > */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 🔻		
olginin page.	To create or manage pages, see Sign-In p	ages.	
 Authentication real Specify what realms 	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 gro 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:		
		1	
	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.



huork Access >	Padiue Attributes > DADILIS	C Daturn Attributes >	FULL ACCESS						
ILL ACCES	S	5 Return Attributes -	TULLAUULUU						
0									
General									
ſ	FULL 400500								
scription:	FULL ACCESS								
comparent.									
		4							
L									
Location Gro	oup								
ocation Gro	oups					Selected Rad	lius Clients		
Specify the Loca	ation Group for which this polic	cy applies. Selected Location	on Groups:			Below list is pop	ulated dynamica	ally based on the selec	ted Location Gro
Default	Add ->	Cert Auth	≜ since			Vendor (Mar	nufacturer)	Client Details	*
Guest	Remove					Cisco Syster	ms	Cisco 2960X	
Guest Wired	1								
	*		*						
Access Control elect below opti Provide ful Control the Access can b Control	ton Policy Settings tion to control the access level III Access (Open Port) e Access be controlled using the VLAN I of using VLAN Id:	for the device/user cor Id, ACLs and Radius R (1 - 4094)	nnecting to the netwo eturn Attribute setting	rk js below		Note: Selecting this Note: Selecting this Note: This option is	s option will resu s option enables s used for assign	It in opening the port v control of the device i ning devices to corresp	without any restric or user access
Access Contro Provide ful Control the Access can b Control Control Control	tion to control the access level ill Access (Open Port) e Access be controlled using the VLAN I of using VLAN Id: ol access using Access Co ol access using Radius Ref te	for the device/user con id, ACLs and Radius R (1 - 4004) ontrol List (ACL) set turn Attributes	necting to the netwo eturn Attribute setting tings (Supported o	rk js below only for Cisco, Junip	er, HP)	Note: Selecting this Note: Selecting this Note: This option is Note: These attribu	s option will resu s option enables used for assign tes are sent to s	It in opening the port of control of the device i sing devices to corresp witch for controlling th	without any restriction or user access bonding VLAN on re access
Access Contro elect below opti Control the Access can t Contro Contro Contro	tion to control the access level all Access (Open Port) e Access be controlled using the VLAN I of using VLAN Id: of access using Access Co of access using Radius Ref te • • • Return Attribute	for the device/user cor id, ACLs and Radius R (1 - 4004) ontrol List (ACL) set turn Attributes	eturn Attribute setting ttings (Supported (Radius Auth Set	rk js below only for Cisco, Junip rver Attribute Value	er, HP) Auth Server Ca	Note: Selecting this Note: Selecting this Note: This option is Note: These attribu	coption will resu soption enables used for assign tes are sent to s Value	It in opening the port v control of the device r sing devices to corresp	without any restrict or user access bonding VLAN on re access
Access Contro Provide ful Control the Access can b Control Contro Contro Dete	ton to control the access level III Access (Open Port) e Access be controled using the VLAN I of using VLAN Id: of access using Access Co of access using Radius Ref tet Return Attribute Filter-Id	for the device/user con id, ACLs and Radius R (1 - 4094) ontrol List (ACL) set turn Attributes	eturn Attribute setting tings (Supported of Radius Auth Ser -none-	rk js below only for Cisco, Junip rver Attribute Value	er, HP) Auth Server Ca -none-	Note: Selecting this Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	: option will resu s option enables used for assign tes are sent to s Value	It in opening the port v control of the device in ning devices to corresp witch for controlling th	without any restrict or user access conding VLAN on re access
Access Contro Select below opti Provide fuil Control the Access can t Control Contro Contro Deter Contro	ton to control the access level ill Access (Open Port) e Access be controlled using the VLAN I of using VLAN Id: of access using Access Co of access using Radius Ref ter Return Attribute Filter-Id Filter-Id	for the device/user cor id, ACLs and Radius R (1 - 4004) ontrol List (ACL) set turn Attributes	eturn Attribute setting ttings (Supported of Radius Auth Set -none-	rk js below only for Cisco, Junip rver Attribute Value	er, HP) Auth Server Ci -none- -none-	Note: Selecting this Note: Selecting this Note: This option is Note: These attribu	s option will resu s option enables used for assign tes are sent to s Value FULL-ACCE	It in opening the port of control of the device it aing devices to corresp witch for controlling th	without any restriction of user access aconding VLAN on the access acces
Access Control Provide full Control the Access can t Control Control Control Deleter Control	ton to control the access level III Access (Open Port) e Access be controled using the VLAN I of using VLAN Id: of access using Access Co of access using Radius Ref etce Return Attribute Filter-Id Filter-Id	for the device/user con id, ACLs and Radius R (1 - 4004) ontrol List (ACL) set turn Attributes	eturn Attribute setting tings (Supported of Radius Auth Set -none-	rk js below only for Cisco, Junip rver Attribute Value	er, HP) Auth Server Ca -none- -none-	Note: Selecting this Note: Selecting this Note: This option is Note: These attribut stalog Attribute Value	s option will resu s option enables used for assign tes are sent to s Value FULL-ACCE	It in opening the port v control of the device of ing devices to corresp witch for controlling th	without any restri or user access bonding VLAN on the access
Access Contr Select below opti Provide ful Control the Access can t Control Con	ton to control the access level all Access (Open Port) e Access be controlled using the VLAN I of using VLAN Id: in access using Access Co of access using Radius Ref iter (Inter-In	for the device/user cor Id, ACLs and Radius R (1 - 4004) Introl List (ACL) set turn Attributes for the device upon exp F	eturn Attribute setting eturn Attribute setting ttings (Supported of Radius Auth Ser -none- -none- piration of session tim Re-authenticate the	rk is below only for Cisco, Junip rver Attribute Value ver Attribute Value ession	er, HP) Auth Server Ca -none- -none-	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	s option will result s option enables used for assign tes are sent to s Value FULL-ACCE	It in opening the port v control of the device r ing devices to corresp awitch for controlling th ESS-ACL ut attribute equal to se	without any restri or user access bonding VLAN on the access Add
Access Contr Select below opti Provide ful Control the Access can t Control Co	ton to control the access level III Access (Open Port) e Access be controlled using the VLAN I of using VLAN Id: Control access using Access Co of access using Radius Ref Return Attribute Filter-Id Filter-Id Ession-Timeout attribute the action that needs to taken 1 minate the session	for the device/user cor Id, ACLs and Radius R (1 - 4004) ontrol List (ACL) set turn Attributes for the device upon exp F	eturn Attribute setting eturn Attribute setting ttings (Supported of -none- -none- -none-	rk is below only for Cisco, Junip rver Attribute Value reout on the switch e session	er, HP) Auth Server C: -none- -none-	Note: Selecting this Note: Selecting this Note: This option is Note: These attribu atalog Attribute Value	s option will result s option enables used for assign tes are sent to s Value FULL-ACCE d session timeor	It in opening the port v control of the device r ing devices to corresp awitch for controlling th ESS-ACL	without any restri or user access bonding VLAN on the access
Access Control Provide full Control the Access can t Control	ton to control the access level III Access (Open Port) e Access be controled using the VLAN I of using VLAN Id: of access using Access Co of access using Radius Ref tet Return Attribute Filter-Id Filter-Id Filter-Id session-Timeout attribute the action that needs to taken f minate the session ples to which this policy is	for the device/user cor Id, ACLs and Radius R (1 - 4094) ontrol List (ACL) set turn Attributes for the device upon exp o F applicable	eturn Attribute setting ttings (Supported of -none- -none- piration of session tim Re-authenticate the	rk Is below only for Cisco, Junip rver Attribute Value	er, HP) Auth Server C: -none- -none-	Note: Selecting this Note: Selecting this Note: This option is Note: These attribut atalog Attribute Value	s option will resu s option enables used for assign tes are sent to s Value FULL-ACCR d session timeor	It in opening the port v control of the device of ing devices to corresp switch for controlling th ESS-ACL ut attribute equal to se	without any restri or user access conding VLAN or re access Add
Access Contro Provide fui Control the Access can t Contro	rol Policy Settings tion to control the access level II Access (Open Port) e Access be controled using the VLAN I of using VLAN Id: of access using Radius Ref tel Return Attribute Filter-Id Filter-Id Filter-Id Ession-Timeout attribute the action that needs to taken the minate the session bles to which this policy is is e	for the device/user cor Id, ACLs and Radius R (1 - 4004) ontrol List (ACL) set turn Attributes for the device upon exp o F applicable Selected belo	eturn Attribute setting eturn Attribute setting ttings (Supported of Radius Auth Ser -none- -none- piration of session tim Re-authenticate the	rk ps below only for Cisco, Junip rver Attribute Value reout on the switch e session O Other than sele	er, HP) Auth Server Ci -nonenone-	Note: Selecting this Note: Selecting this Note: This option is Note: These attribu atalog Attribute Value	s option will resu s option enables used for assign tes are sent to s Value FULL-ACCE	It in opening the port v control of the device it ang devices to corresp witch for controlling th ESS-ACL	without any restri or user access conding VLAN on re access Add
Access Contro Provide ful Control the Control the Control Contro	ton to control the access level all Access (Open Port) e Access be controlled using the VLAN I of using VLAN Id: in access using Access Co of access using Radius Ref iter in the section Refute Return Attribute Filter-Id Filter-Id Filter-Id be action that needs to taken the minate the session	for the device/user cor Id, ACLs and Radius R (1 - 4004) Introl List (ACL) set turn Attributes for the device upon exp o F applicable Selected belo	eturn Attribute setting eturn Attribute setting ttings (Supported of Radius Auth Ser -none- -none- piration of session tim Re-authenticate the	rk ps below only for Cisco, Junip nver Attribute Value reout on the switch e session Other than sele Calacted relact	er, HP) Auth Server Cr -nonenone- ected below	Note: Selecting this Note: This option is Note: These attribu stalog Attribute Value	s option will result s option enables used for assign tes are sent to s Value FULL-ACCS d session timeor	It in opening the port v control of the device r aing devices to corresp awitch for controlling th ESS-ACL ut attribute equal to se	without any restriction of user access and any restriction of the access
Access Contre elect below opti- Provide ful Control the Control the Control Co	ton to control the access level III Access (Open Port) e Access be controlled using the VLAN I of using VLAN Id: control access using Access Co of access using Radius Ref the extern Attribute Filter-Id Filter-Id Filter-Id Easion-Timeout attribute the action that needs to taken to minate the session cless to which this policy is e e	for the device/user cor Id, ACLs and Radius R (1 - 4004) ontrol List (ACL) set turn Attributes for the device upon exp for the device upon exp F applicable Selected belo	eturn Attribute setting eturn Attribute setting ttings (Supported of Radius Auth Ser -none- -none- piration of session tim Re-authenticate the	rk ps below only for Cisco, Junip rver Attribute Value reout on the switch e session Other than sele Selected roles: FullAccessRole	er, HP) Auth Server Cr -nonenone- ected below	Note: Selecting this Note: This option is Note: These attribu stalog Attribute Value	s option will result s option enables used for assign tes are sent to s Value FULL-ACCE	It in opening the port v control of the device r ing devices to corresp awitch for controlling th ESS-ACL	without any restrict or user access bonding VLAN on the access
Access Control Provide ful Control the Access can t Control C	rol Policy Settings tion to control the access level III Access (Open Port) e Access be controled using the VLAN I of using VLAN Id: of access using Radius Rel tete Return Attribute Filter-Id Filter-Id Filter-Id Settion that needs to taken the minate the session cless to which this policy is e	for the device/user cor d, ACLs and Radius R (1 - 4094) ontrol List (ACL) set turn Attributes for the device upon exp for the device upon exp plicable Selected belo	eturn Attribute setting eturn Attribute setting tings (Supported of -none- -none- piration of session tim Re-authenticate the	rk is below only for Cisco, Junip rver Attribute Value rver Attribute Value o Other than sele Selected roles: FullAccessRole	er, HP) Auth Server Ca -nonenone- ected below	Note: Selecting this Note: Selecting this Note: This option is Note: These attribut atalog Attribute Value	s option will resu s option enables used for assign tes are sent to s Value FULL-ACCE	It in opening the port of control of the device of sing devices to corresp switch for controlling th ESS-ACL	without any restriction user access aconding VLAN on the access
Access Contro Provide ful Control the Access can to Control C	rol Policy Settings tion to control the access level II Access (Open Port) e Access be controled using the VLAN I of using VLAN Id: of access using Radius Ref tel Return Attribute Filter-Id	for the device/user cor Id, ACLs and Radius R (1 - 4004) ontrol List (ACL) set turn Attributes for the device upon exp for the device upon exp plicable Selected belo Add -> Remove	eturn Attribute setting ttings (Supported of Radius Auth Ser -none- -none- piration of session tim Re-authenticate the	rk ps below poly for Cisco, Junip rver Attribute Value rver Attribute Value o O Conter than sele Selected roles: FullAccessRole	er, HP) Auth Server C: -nonenone- ected below	Note: Selecting this Note: This option is Note: These attribu atalog Attribute Value	s option will resu s option enables used for assign tes are sent to s Value FULL-ACCI d session timeor	It in opening the port v control of the device it and devices to corresp awitch for controlling th ESS-ACL ut attribute equal to se	without any restriction of user access acces
Access Contro Provide ful Control the Access can t Control Co	rol Policy Settings tion to control the access level all Access (Open Port) e Access be controlled using the VLAN I of using VLAN Id: Control of access using Access Co of access using Radius Ref Return Attribute Filter-Id Filter-Id Filter-Id Dession-Timeout attribute the action that needs to taken the minate the session control of access to which this policy is e control of access to which this policy is e	for the device/user cor Id, ACLs and Radius R (1 - 4004) Introl List (ACL) set turn Attributes for the device upon exp for the device upon exp applicable Selected belor Add -> Remove	eturn Attribute setting eturn Attribute setting ttings (Supported of -none- -none- piration of session tim Re-authenticate the	rk ps below only for Cisco, Junip rver Attribute Value • • • • • • • • • • • • •	er, HP) Auth Server Ci -nonenone- ected below	Note: Selecting this Note: This option is Note: These attribu talog Attribute Value	s option will result s option enables used for assign tes are sent to s Value FULL-ACCI d session timeor	It in opening the port v control of the device r ang devices to corresp awitch for controlling th ESS-ACL ut attribute equal to se	without any restrict or user access anonding VLAN on the access Add

Figure 12 RADIUS Return Attributes Certificate Authentication

Netwo	Network Access > Radius Athibutes > RADIUS Return Attributes												
RAD	RADIUS Return Attributes												
F	ADIUS	lictionary	RADIUS Vendor	Location Group	RADIUS Client	RADIUS Attributes	Network Infrastructure Device	SNMP Enforcement Policies					
Ret	Return Attributes Request Attributes Attribute Logging												
Chou	nation	that apply to	All colors	- Undate									
Show	policies	that apply to	All roles	• Optime									
ARA	A RADIUS return attributes policy specifies the return list attributes to send to an 802.1X network access device, such as which VLAN endpoints must use to access the network. If no policy applies, Open Port is the default action.												
Ne	New Policy Duplicate Delete												
		Dellalas				101.0-10-0	44-2-4	Location Course	Interface	tenting to only			
		Policies				ACL Settings	Attributes	Location Group	Internace	Applies to role			
-	1.	FULL AC	CESS			N/A	Filter-Id=FULL-ACCESS- ACL	Cert Auth	N/A	FullAccessRole			
	2.	LIMITED	ACCESS			N/A	Filter-Id=LIMITED-ACCESS- ACL	Cert Auth	N/A	LimitedAccessRole			
	_												

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
1
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"
```