# SafeNet Authentication Service Push OTP Integration Guide

Using RADIUS Protocol for Pulse Connect Secure



All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2015 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013338-001, Rev. C Release Date: November 2015

## Contents

Third-Party Software Acknowledgement	4
Description	4
Applicability	5
Environment	5
Audience	5
RADIUS-based Authentication using SAS Cloud	5
RADIUS Authentication Flow using SAS	6
RADIUS Prerequisites	7
Push OTP Prerequisites	7
Configuring SafeNet Authentication Service	7
Creating Users Stores in SAS	7
Assigning an Authenticator in SAS	8
Adding Pulse Connect Secure as an Authentication Node in SAS	9
Checking the SAS RADIUS Server's IP Address	.11
Enabling the Software Token Push OTP Setting	.12
Enabling the Allowed Targets Policy	.13
Configuring Pulse Connect Secure	.15
Creating a RADIUS Authentication Server	.15
Configuring an Authentication Realm	.18
Configuring Push OTP Hybrid Mode	.22
Running the Solution	.26
Connecting to the Pulse Connect Secure Portal using Simple Mode	.26
Connecting to the Pulse Connect Secure Portal using Hybrid Mode	.28
Support Contacts	.30

## **Third-Party Software Acknowledgement**

This document is intended to help users of Gemalto products when working with third-party software, such as Pulse Connect Secure.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

## **Description**

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

The Pulse Connect Secure appliances meet the needs of companies of all sizes. The Junos Pulse Gateway MAG series appliances use SSL—the security protocol found in all standard web browsers. The use of SSL eliminates the need for pre-installed client software, changes to internal servers, and costly ongoing maintenance and desktop support. The SA Series also offers sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups without requiring infrastructure changes, demilitarized zone (DMZ) deployments, or software agents.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Pulse Connect Secure using the SafeNet Push OTP solution managed by SafeNet Authentication Service.
- Configure Pulse Connect Secure to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Pulse Connect Secure environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Pulse Connect Secure can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with the SafeNet Authentication Service Push OTP solution.

The primary objective of the Push OTP solution is to reduce the friction around two-factor authentication, and provide users with an improved two-factor authentication experience.

It's likely that most users already own and always carry a device that can be used as a second factor of authentication. Using the mobile phone as an authenticator replaces the need for a user to carry any additional hardware. So, with Push OTP, a user can:

- Receive authentication requests in real-time via push notifications to his or her smart phone.
- Assess the validity of the request with the information displayed on the screen.
- Respond quickly with a one-tap response to approve or deny the authentication.

## Applicability

The information in this document applies to:

- SafeNet Authentication Service (SAS)—SafeNet's cloud-based authentication service
- MobilePASS+ application

## Environment

The integration environment that was used in this document is based on the following software versions:

- SafeNet Authentication Service (SAS)—Cloud version 3.5
- Pulse Connect Secure Gateway—Version 7.2R2

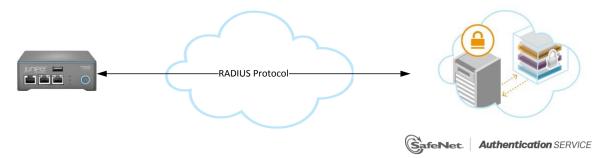
### Audience

This document is targeted to system administrators who are familiar with Pulse Connect Secure, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

## **RADIUS-based Authentication using SAS Cloud**

SAS Cloud provides two RADIUS mode topologies:

• **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.



• Local RADIUS hosted on-premises—A RADIUS agent that is implemented in the existing customer's RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.



This document demonstrates the solution using the SAS cloud hosted RADIUS service.

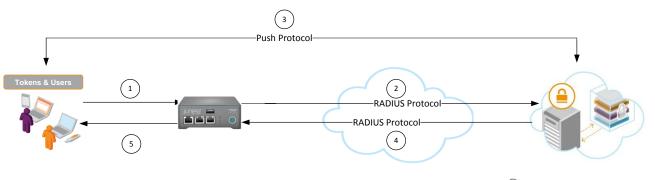
For more information on how to install and configure SAS Agent for IAS/NPS, refer to: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.

## **RADIUS Authentication Flow using SAS**

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Pulse Connect Secure.



SafeNet. Authentication SERVICE

- 1. A user attempts to log on to Pulse Connect Secure using a Push OTP authenticator.
- 2. Pulse Connect Secure sends a RADIUS request with the user's credentials to SafeNet Authentication Service for validation.
- 3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
  - SAS will directly trigger a Push OTP authentication request.
  - The user receives a push notification on the configured mobile device to indicate there is a login request pending.
  - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token's PIN code).
- 4. The SAS authentication reply is sent back to Pulse Connect Secure.
- The user is granted or denied access to Pulse Connect Secure based on the OTP value calculation results from SAS.

## **RADIUS Prerequisites**

To enable SafeNet Authentication Service to receive RADIUS requests from Pulse Connect Secure, ensure the following:

- End users can authenticate from the Pulse Connect Secure environment with a static password before configuring the Pulse Connect Secure to use RADIUS authentication.
- Ports 1812/1813 are open to and from Pulse Connect Secure.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.
- On the client machine, set the RADIUS timeout value at least 60 seconds.

### **Push OTP Prerequisites**

To use Push OTP, you will need:

- SAS configured to enable Push OTP
- MobilePASS which is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x, 5.x
    - iOS 7+

### **Configuring SafeNet Authentication Service**

The deployment of multi-factor authentication using SAS with Pulse Connect Secure using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Pulse Connect Secure as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Server's IP Address, page 11
- Enabling the Software Token Push OTP Setting, page 12
- Enabling the Allowed Targets Policy, page 13

### **Creating Users Stores in SAS**

Before SAS can authenticate any user in your organization, you must create a user store in SAS that reflects the users who would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the Create User shortcut
- Manually, by importing one or more user records via a flat file

 Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to "Creating Users" in the SafeNet Authentication Service Subscriber Account Operator Guide:

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

### Assigning an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Pulse Connect Secure.

The following authenticators are supported:

MobilePASS

Authenticators can be assigned to users in two ways:

- Manual provisioning—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to "Provisioning Rules" in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-SPE-SubscriberAccountOperatorGuide.pdf

### Adding Pulse Connect Secure as an Authentication Node in SAS

Add a RADIUS entry in the SAS **Auth Nodes** module to prepare it to receive RADIUS authentication requests from Pulse Connect Secure. You will need the IP address of Pulse Connect Secure and the shared secret to be used by both SAS and Pulse Connect Secure.

1. Log in to the SAS console with an Operator account.

Shortcuts 4	Manage	: Yarivl							
Create User	SNAPSHOT	ASSIGNMENT	TOKENS	GROUPS REP	ORTS SELF-SERVICE	OPERATORS	POLICY	COMMS	
	Au	Ithenticatio	n Activity						III 🕜 ->=
	Au	Ithenticatio	n Metrics						-Com
	То	ken States							<b>()</b> -04
	SMS SN	IS Credits							<b>()</b> -04
		location							III 🕡 -044
	🚺 Re	eferences							<b>()</b> -544
									SafeNet

2. Click the **COMMS** tab, and then select **Auth Nodes**.

Shortcuts 4	Manage	: Yarivl								
Create User	SNAPSHOT	ASSIGNMENT	TOKENS	GROUPS	REPORTS	SELF-SERVICE	OPERATORS	POLICY	COMMS	
	Co	mmunicatio	ns							() -Q=
	Au	thenticatio	Proces	sing						
	Au	th Nodes								III 🕢 -04
	SA SA	ML Service	Provider	s						- <del>(</del> )
	Cu	stom Brand	ng							-jui
										SafeNet

3. In the Auth Nodes module, click the Auth Nodes link.

Auth Nodes				III 🛈 🕬
Auth Nodes:				
Task	Description			
Auth Nodes	Create and configure Sa	afeNet Authentica <mark>t</mark> ion Service Authenticatio	on Nodes	
and for alternatives to RADIUS	traffic, refer to the recomme	d security of the traffic between the organ endations included in the SafeNet Authentic Cancel		ithentication service. For improved security ide.
Primary RADIUS Server IP:	64.26.164.68:1812	Primary SafeNet Authentication Service Agent DNS:	sastestagent.safenet- inc.com:443	Max. Auth Nodes: 10
Failover RADIUS Server IP:	64.26.164.68:1812	Failover SafeNet Authentication Service Agent DNS:	sastestagent.safenet- inc.com:443	
No Records				

- 4. Under Auth Nodes, click Add.
- 5. In the Add Auth Nodes section, complete the following fields, and then click Save:

Auth Node Name	Enter a host description.
Resource Name	Enter a resource name which will identify in a push notification which authentication node it relates to.
Host Name	Enter the name of the host that will authenticate with SAS.
Low IP Address In Range	Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS.
High IP Address In Range	Enter the highest IP address in a range of IP addresses that will authenticate with SAS.
Configure FreeRADIUS Synchronization	Select this option.
Shared Secret	Enter the shared secret key.
Confirm Shared Secret	Re-enter the shared secret key.

Add Auth Node Save Cancel Auth Nodes	
Auth Node Name:	Exclude from PIN change requests
Resource Name:	🗹 Configure FreeRADIUS Synchronization
Host Name:	Shared Secret:
Low IP Address In Range:	Confirm Shared Secret:
High IP Address In Range:	FreeRADIUS synchronization may take up to 5 minutes to propagate in the system.

#### The authentication node is added to the system.

🛃 Auth N	Auth Nodes III 🛈								
Auth Nodes:	Auth Nodes:								
Task	Descript	on							
Auth Nodes	Create a	nd configure SafeNet Authenti	ication Service Authentication Nodes						
	Using the RADIUS protocol over the Internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security and for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.								
Primary RADIUS	Server IP:		SafeNet Authentication Agent DNS:	Max. Nodes	10				
Failover RADIUS	Server IP:	Failover	SafeNet Authentication Agent DNS:						
Index	Auth Node Name	Host Name	IP Address	FreeRADIUS Synchronization					
1	Pulse Connect Secure		12.28.52.44	True	Edit	Remove			
Displaying:	1 to 3 of 3	44 4 > >>							

### **Checking the SAS RADIUS Server's IP Address**

Before adding SAS as a RADIUS server in Pulse Connect Secure, check its IP address. The IP address will then be added to Pulse Connect Secure as a RADIUS server at a later stage.

1. Log in to the SAS console with an Operator account.

Shortcuts 4	Manage: Yarivl
O Create User	SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS
	Authentication Activity
	Authentication Metrics
	Token States 0 - 🖓
	SMS Credits 0 -94
	Allocation
	References O -
	Powered by

2. Click the **COMMS** tab, and then select **Auth Nodes**.

Shortcuts <	Manage: Yarivl
Create User	SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS
	Communications 0 -0
	Authentication Processing
	Auth Nodes III 🛈 🕫
	SAML Service Providers
	Custom Branding 💿 🕂
	SafeNet

3. In the Auth Nodes module, click the Auth Nodes link. The SAS RADIUS server details are displayed.

Auth Nodes				III 🕦 -)==
Auth Nodes:				
Task	Description			
Auth Nodes	Create and configure Sa	feNet Authentica <mark>t</mark> ion Service Authenticatio	on Nodes	
and for alternatives to RADIUS	traffic, refer to the recomme	d security of the traffic between the organ ndations included in the SafeNet Authentic Cancel	ization's data center and the au ation Service Administrator Gu	thentication service. For improved security iide.
Primary RADIUS Server IP:	64.26.164.68:1812	Primary SafeNet Authentication Service Agent DNS:	sastestagent.safenet- inc.com:443	Max. Auth Nodes: 10
Failover RADIUS Server IP:	64.26.164.68:1812	Failover SafeNet Authentication Service Agent DNS:	sastestagent.safenet- inc.com:443	
No Records				

### **Enabling the Software Token Push OTP Setting**

To use Push OTP authentication, the setting must be enabled in the SAS token policy.

1. Log in to the SAS console with an Operator account.

Shortcuts 《	Manage: Yarivl	
Create User	SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS	
	Authentication Activity	III 🛈 🖓
	Authentication Metrics	0 -
	Token States	<b>0</b> - Ja
	SMS Credits	0-94
	Allocation	III 🛈 🖓
	References	0 🖓
		wered by eNet

2. Click the **POLICY** tab, and then select **Token Policies**.

Shortcuts	4								
Create User	SNAPSHOT ASS		OKENS GROUPS	REPORTS	SELF-SERVICE	OPERATORS	POLICY	соммя	
	User P	olicies							() <del>(</del>
	Token	Policies							<b>()</b> -i
	Role M	anagement	t						III 🛈 🕂
	Autom	ation Polici	es						() H
									Powered b

3. In the Token Policies module, click the Software Token Push OTP Setting link.

Token Policies		🚺 -im
Use these policies to customize the c	operation of tokens and how they interact with the authentication service.	
Task	Description	
Token Templates	Edit the templates used to customize token operation. Templates are applied during token initialization.	
Token Passcode Processing Policy	Set how the server will evaluate passcodes and support offline authentication.	
Server-side PIN Policy	Set or modify the global server-side PIN policy.	
Global or Groups PIN Change	Trigger a "Global or Groups PIN Change on next use"	
Temporary Password Policy	Set or modify the length, complexity, change frequency, randomness, and lifetime of static passwords.	
Synchronization	Set inner and outer window synchronization parameters.	
SMS/OTP	Set the number of OTPs to be sent in a single SMS message, as well as delivery mode and content.	
Software Token Push OTP Setting	Enable Push OTP communication with MobilePass+	
Token File Creation Policy	Set the default location for token file creation.	
Allowed Targets Settings	Set the allowed targets to software tokens.	
MP Token Devices	Set and format download, installation, and removal messages for SafeNet Authentication Service MP token devices.	
Third-Party Authentication Options	Set authentication options for third-party tokens, such as GrIDsure and RADIUS.	
Software Token Push OTP Settin	ancel Change Log	

4. Select Enable Push OTP communication with MobilePass+, and then click Apply.

### **Enabling the Allowed Targets Policy**

For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the selfenrollment of MobilePASS tokens. You can restrict the targets on which MobilePASS+ or MobilePASS 8 tokens are allowed to be activated or enrolled.

1. Log in to the SAS console with an Operator account.

Shortcuts 4	Manage: Yarivl
Create User	SNAPSHOT ASSIGNMENT TOKENS GROUPS REPORTS SELF-SERVICE OPERATORS POLICY COMMS
	Authentication Activity
	Authentication Metrics
	Token States 0 🖓
	SMS Credits
	Allocation III 🛈 🖓
	References     Image: Comparison of the second
	Powered by

2. Click the **POLICY** tab, and then select **Token Policies**.

Shortcuts										
Create User	SNAPSHOT	ASSIGNMENT	TOKENS	GROUPS	REPORTS	SELF-SERVICE	OPERATORS	POLICY	COMMS	
	Us 🔝	er Policies								() -p=
	Tol	ken Policies								
	Ro	le Managem	ent							III 🛈 -24
	Au	tomation Po	olicies							<b>()</b> ->=
										SafeNet

#### 3. In the Token Policies module, click the Allowed Targets Settings link.

Token Policies	
Use these policies to customize the o	peration of tokens and how they interact with the authentication service.
Task	Description
Token Templates	Edit the templates used to customize token operation. Templates are applied during token initialization.
Token Passcode Processing Policy	Set how the server will evaluate passcodes and support offline authentication.
Server-side PIN Policy	Set or modify the global server-side PIN policy.
Global or Groups PIN Change	Trigger a "Global or Groups PIN Change on next use"
Temporary Password Policy	Set or modify the length, complexity, change frequency, randomness, and lifetime of static passwords.
Synchronization	Set inner and outer window synchronization parameters.
SMS/OTP	Set the number of OTPs to be sent in a single SMS message, as well as delivery mode and content.
Software Token Push OTP Setting	Enable Push OTP communication with MobilePass+
Token File Creation Policy	Set the default location for token file creation.
Allowed Targets Settings	Set the allowed targets to software tokens.
MP Token Devices	Set and format download, installation, and removal messages for SafeNet Authentication Service MP token devices.
Third-Party Authentication Options	Set authentication options for third-party tokens, such as GrIDsure and RADIUS.
Allowed Targets Settings	
Apply	ancel
MobilePASS	-1
MobilePASS+	
🗹 Android 🛛 🗹 iOS	
MobilePASS 8	
Android iOS	🖉 Mac OS X 🖉 Windows Phone 🖉 Windows 🖉 Windows RT 🖉 BlackBerry 10 🖉 BlackBerry Java
One MobilePASS application	per OS type may be selected.

4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application for this virtual server, and then click **Apply**.

## **Configuring Pulse Connect Secure**

Configuring the Pulse Connect Secure to use SAS RADIUS authentication requires the following:

- Creating a RADIUS Authentication Server, page 15
- Configuring an Authentication Realm, page 18
- Configuring Push OTP Hybrid Mode, page 22

### **Creating a RADIUS Authentication Server**

1. Open the Pulse Connect Secure admin console.



(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

2. In the left pane, select **Authentication > Auth. Servers**.

ation +	Authentication Servers			
ederation + toring +	New: (Select server type)	Delete		
tication	Authentication/Authorization Servers	Туре	User Record Synchronization	Logical Auth Server Name
n P	Administrators	Local Authentication		
Security +	AD DEV	Active Directory / Windows NT		
rators	CBA	Certificate Server		
alma >	Eanny-LDAP	LDAP Server		
les ×	Fanny.test-domain	Certificate Server		
ns +	LDAP Oren	LDAP Server		
	Local Users	Local Authentication		
Profiles >	🗐 radius1	Radius Server		
Policies >	RADIUS DEV	Radius Server		
ince	RADIUSRUPINDER	Radius Server		
port »	RadiusTestDomain	Radius Server		
9 *	Safenet Certificate server	Certificate Server		
	SAS-RADIUS	Radius Server		
octing +	SAS-SMS	Radius Server		
	Steel	Radius Server		
	Steel Belted Radius server	Radius Server		
	System Local	Local Authentication		
	TestAD	LDAP Server		
	TK SAS LocalUsers	Local Authentication		
	TK SAS Radius	Radius Server		
	C Token	Radius Server		

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

3. In the New menu, select Radius Server, and then click New Server.

Au	thentication Servers	_			
eration 1 No		New Server.	Delete		
140 1	(Select server type) Local Authentication				
-	A NIS Server	ners	Туре	User Record Synchronization	Logical Auth Server Name
+	AL ACE Server		Local Authentication Active Directory / Windows NT		
1 0	Radius Server		Certificate Server		
tars	Active Directory / Windows NT Fa Anonymous Server		LDAP Server		
A COLORADO	SiteMinder Server	-	Certificate Server		
1.0	Eil Certificate Server	-	LDAP Server		
	MDM Server		Local Authentication		
files +	cadius1		Radius Server		
1048 111	RADIUS DEV		Radius Server		
	RADIUSRUPINDER		Radius Server		
0	RadiusTestDomain		Radius Server		
	Safenet Certificate server		Certificate Server		
* 0	SAS-RADIUS		Radius Server		
-	SAS-SMS		Radius Server		
0	Steel		Radius Server		
0	Steel Belted Radius server		Radius Server		
8	System Local		Local Authentication		
0	TestAD		LDAP Server		
0	TK SAS LocalUsers     TK SAS Radius		Local Authentication		
0			Radius Server		
0	Token		Radius Server		

(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)

4. On the **Settings** tab, complete the following, and the click **Save Changes** at the bottom of the page:

Name	Enter the server name.	
NAS-Identifier	Enter the name of the device.	
Radius Server	Enter the IP address of the SAS RADIUS server.	
Authentication Port	Enter the RADIUS authentication port number. The default is 1812.	
Shared Secret	Enter the RADIUS shared secret.	
Timeout	Set the value to <b>60</b> seconds.	

Do not change the other default values.

S Pulse Secure								
Pulse Connect Secure System Status Configuration Network 1	Auth Servers > SAS-RADIUS			Help   Guidance   Sign Out				
Clustering + IF-MAP Federation +	Settings Users							
Log/Monitoring + Reports +	* Name:	SAS-RADIUS	Label to reference this server.					
- Authentication	NAS-Identifier:	Juniper.sfnt.com	Name of the device as known to Radius server					
Signing In + Endpoint Security +	Primary Server							
Auth. Servers	* Radius Server:	109.73.120.148	Name or IP address					
- Administrators	* Authentication Port:	1812						
Admin Realma +	* Shared Secret:							
E Users	* Accounting Port:	1813	Port used for Radius accounting, if applicable					
User Realms +	NAS-IP-Address:		19 address					
User Roles + Resource Profiles +								
Resource Policies +	* Timeout:	60 seconds						
Pulse Secure Client+	* Retries:	0						
System + Import/Export + Push Config + Archiving + Troubleshooting +	Note: If you select this	e using tokens or one-ti to the device will send the user not be used in automatic \$50	er's subjectication method as "token" if you use SAML,					
	Backup Server (required o	only if Backup server exists)	s)					
	Radius Server:		Name or IP address					
	Authentication Port:							
	Shared Secret:							
	Accounting Port:		Port used for Radius accounting, if applicable					
	Load-Balance Auth		imary and Backup Servers					
	Radius accounting							
	User-Name:	<user>(<realm>)[-</realm></user>	[ <role sep=",">] Template for reporting user identity to fladius server</role>					
		The template can contain all variables.	s bestual characters as well as variables for substitution. Variables should be exclosed in angle brackets like this <vari< td=""><td>able&gt;. Click here to view a list of</td></vari<>	able>. Click here to view a list of				
			set's login name ar's sign in realm					

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

### **Configuring an Authentication Realm**

After the RADIUS authentication server is created, assign it to a user authentication realm.

- 1. Open the Pulse Connect Secure admin console.
- 2. In the left pane, select **Users > Users Realms**.

item us →	User Authentication Realms		
figuration → vork →			
tering >			
Monitoring +	View: Overview   for all realms  Update		
orts +	New Duplicate Delete		
ing In →			
point Security +	Authentication Realm	Servers	Dynamic Policy Evaluation
n. Servers ministrators	CBA	Primary: <u>CBA</u>	Disabled
iin Realms 🛛 🕨	RUPIREALM	Primary: RADIUSRUPINDER Directory: RADIUSRUPINDER	Disabled
in Roles +	User-Steel Belted	Primary: <u>SAS-RADIUS</u> Directory:SAS-RADIUS	Disabled
Realms >	Users	Primary: <u>SAS-RADIUS</u> Directory:SAS-RADIUS	Disabled
ource Profiles →	Users-SMS	Primary: LDAP_Oren Directory:LDAP_Oren Secondary: <u>SAS-SMS</u>	Disabled
e Secure Client ⊢ ntenance			
ort/Export	Authentication realms specify what server to use for authentication, how policies a	are assigned to users, and restrictions on who can attempt to sign-in.	
Config +			
iving → bleshooting →			
bleshooting /			
ed to 0271MNZSJ	00700AYS Pulse Secure, LLC. All rights reserved.		
JHE (© 2001-2015	Poise Secure, LLC. All rights reserved.		

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

3. In the Authentication Realm table, click Users.

4. On the **General** tab, select the **Additional authentication server** check box, and then complete the following fields:

Authentication #2	Select the RADIUS authentication server that you created in the previous section (for example, <b>SAS-RADIUS</b> ).
Username is	Select predefined as: <user>.</user>
Password is Select predefined as, and leave the letter p.	

lare .			Help   Ga				
Users-SMS							
General Authentication Policy	General Authentication Policy Role Happing						
* * Name:	Users		Label to reference this realm				
, Description:							
57.8							
*	When editing	g, start on the Role Map	oping page				
Servers							
*							
Specify the servers to use for authentication of	rel authorization. To ireate ar manage	a nerverb. new live Derivate page					
Authentication:	LDAP		Spanify the server to see for authenticating users.				
User Directory/Attribute:	Same as above	1	Epecify the server to use for authorization.				
Accounting:	None	•	Specify the server to see for Radian accounting.				
Device Attributes:	None •		Specify the server to see for device authorization.				
Additional authentication set	wer						
The can specify an additional authentication in specie papel, or they can be pre-thilling bet	eriver for single sign on (350) access two to which case the user will set be	es. The additional predentials of	an be specified by the user on the argo in ange (the false's for these insult are				
Authentication #2:	SAS						
Username is:	specified by user						
	* predefined as: <						
Password is:	o specified by user						
	predefined as: p						
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	End session if au	thentication against this	s server fails				
		Contraction of the second					

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

5. Click the **Role Mapping** tab, and then click **New Rule**.

Chapter Security / Concentrational / Concentrationa / Concentrationa / Concentrationa / Concentrationa	whe Connect Secur			Help   Guidance   Sign O
International Control       Account account of the state	Status Configuration	uar Automatian Index > Users-SMS		
Name         Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.           Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.         Specify how to assign roles to users.           Specify how to assign roles to users meet these conditions         assign these roles         Rule Name 5           Admontifier         When users meet these conditions         assign these roles         Rule Name 5           Admontifier         Mem or than one role is assigned to a user:         Here Rule         Users           When users meet the set of merged roles         User mut select the set of merged roles assigned to a user:         Here Rule         User mut select the assigned roles           Weer mut select the set of merged roles assigned to a user:         Here Second build         User mut select the assigned roles         User mut select the set of merged roles assigned by each rule           Note Weer mut select the set of merged roles assigned to be asserted to down and a role role assigned roles assigned to be asserted to down and a role role assigned roles assigned to be able to select the se		General Asthentication Policy Role Mapping		
Index to the transmit of the series meet these conditions       assign these roles       Rule Name 5         Address for the series meet these conditions       assign these roles       Rule Name 5         Address for the series meet these conditions       assign these roles       Rule Name 5         Address for the series meet these conditions       assign these roles       Rule Name 5         Address for the series meet these conditions       assign these roles       Rule Name 5         Address for the series meet the second the series       the series       Integ         When more than one role is assigned to a user:       • Herge settings for all assigned roles		Specify how to assign roles to users when they sign in. Users that an	e not assigned a role will not be able to sign in.	
Auch Savers     C     ▶ When uses meet these conditions     assign these roles     Rule Name 5       Administration     1     username is "integ", "integ1", "bob" or "captainfr1"     → Userna     integ       Administration     I     username is "integ", "integ1", "bob" or "captainfr1"     → Userna     integ       Administration     When more than one role is assigned to a user: <ul> <li># Herge settings for all assigned roles</li> <li>User must select from among assigned roles</li> <li>User must select the sets of merged roles assigned by each rule</li> <li>When uses that do not ever any of the above noise will not be able to sign into the selen.</li> <li>Prove than 's the Users that do not ever any of the above noise will not be able to sign into the selen.</li> <li>Prove than's 's the Users that do not ever any of the above noise will not be able to sign into the selen.</li> <li>Prove than's 's the Users that do not ever any of the above noise will not be able to sign into the selen.</li> <li>Prove than's 's the Users that do not ever any of the above noise will not be able to sign into the selen.</li> <li>Prove than's 's the Users that do not ever any of the above noise will not be able to sign into the selen.</li> <li>Prove than 's the Users that do not ever any of the above noise will not be able to sign into the selen.</li> <li>Prove than 's 's the Users that do not ever any of the above noise will not be able to sign into the selen.</li> <li>Prove than 's 's the Users that do not ever any of the above noise will not be able to sign into the selen.</li> <li>Prove than 's 's</li></ul>	Authoritication Digning In	and the second se		Save Changes
Anime Relative Advances     Image: State of the State of	Auth- Servers		assign these roles	Rule Name Stop
User Ream         When more than one role is assigned to a user:           Reamong Multis         Herge settings for all assigned roles           Settement Multis         User must select from annog assigned roles           Settement Multis         User must select from annog assigned roles           Settement Multis         User must select from annog assigned roles           Settement         User must select from annog assigned roles           Settement         User must select from annog assigned roles           Readement         User must select from annog assigned roles           Readement         Settement           Settement         Settement	Admin Raalma Admin Rales	1. <u>username is</u> "integ", "integ1", "bob" or "captainfr1"	→ Users	integ
Spritem To Transfer State State and the sprite the sprite the self. Spritem State Sprite State State State Sprite State St	User Realms User Roles Resource Profiles Resource Publies Pulse Secure Chert	Merge settings for all assigned roles     User must select from among assigned roles		
censed to 0275842300/700473 syngeff © 2001-2015 Pulue Secure, LLC. All rights reserved.	Bystern Import/Ruport Publi Coofig Archiving	Totes: Dans that do not meet any of the above rules will not be able to sign into this mains		
upynight © 2001-2015 Pulae Senure, LLC. All nights reserved.	censed to 027249025	30/704/13		
	ipyright © 2001-201	5 Pulse Secure, LLC. All rights reserved.		

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

6. In the **Role Mapping Rule** window, complete the following fields, and then click **Save Changes**:

Rule based onSelect Username.	
NameEnter a name for the rule.	
Rule: If username Select a user or a list of users that need to authenticate	
then assign these roles	Select a role from the <b>Available Roles</b> window, and then click <b>Add</b> to move it to the <b>Selected Roles</b> window. Repeat as needed to add more roles.

S Pulse Secure						
Pulse Connect Secure	e Help   Guidance   S	ign Out				
Status + Configuration + Network +	User Authenticatien Realms > User-SMS > Role Mapping Rule					
Clustering + IF-MAP Federation + Log/Monitoring +	Rule based on: Username Update					
Reports +	* Name:					
Authentication     Signing In	* Rule: If username					
Endpoint Security → Auth. Servers Administrators Admin Roles → Users Users User Realms →	Is •					
User Roles	then assign these roles					
Resource Profiles > Resource Policies > Pulse Secure Client >	Available Roles: Selected Roles:					
Maintenance System Import/Export Push Config	steelbeltedrole Users Remove					
Archiving > Troubleshooting >	Stop processing rules when this rule matches					
	To manage roles, see the <u>Roles</u> configuration page.					
	Save changes?					
	Save Changes Save + New					
	* Indicates required field					
Licensed to 0271MNZ5J Copyright © 2001-2015	U UDV70AYS S Ruise Secure, LLC. All rights reserved.					

(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)

7. Go back to the User Authentication Realm you created and press on Authentication Policy

Pulse Connect Secur	e		He	p   Guidance   Sign O
System				
Status	Vser Authentication Realms >			
Configuration	Users-SMS			
Network	, 03013 5113			
Clustering	General Authentication Policy Role	Mapping		
IF-MAP Federation		name sources We have seen		_
Log/Monitoring	Source IP Browser Certificate Password	Host Checker Limits		
Reports	P			
Authentication	Allow users to sign in from any IP a	ddraes		
Signing In				
Endpoint Security	, O Allow or deny users from the follow	ing iP addresses:		
Auth. Servers				
Administrators	Delete A -			
Admin Realms	, Delete 🕇 🖡			
Admin Realms	•			
Admin Realms ( Admin Roles ( Users	) IPv4/v6 Address	Netmask/Prefix Length	Allow/Deny	
Admin Realms Admin Roles Users User Realms	•	Netmask/Prefix Length		Add
Admin Realms Admin Roles Users User Realms User Roles	•	Netmask/Prefix Length	Allow/Deny	Add
Admin Realms Admin Roles Users User Realms User Roles Resource Profiles	•	Netmask/Prefix Length		Add
Admin Realms Admin Roles Users User Realms User Roles Resource Profiles Resource Policies I	IPv4/v6 Address	Netmask/Prefix Length		Add
Admin Realms Admin Roles Users User Realms User Roles Resource Profiles Resource Policies Pulse Secure Client	IPv4/v6 Address	Netmask/Prefix Length		Add
Admin Realms 4 Admin Roles 4 User Realms 4 User Roles 4 Resource Profiles 4 Resource Policies 4 Pulse Secure Client 1 Maintenance	IPv4/v6 Address	Netmask/Prefix Length		Add
Admin Realms Admin Roles User S User Realms User Realms User Roles Admin Roles Admin Resource Policies Pulse Secure Client Maintenance System Administration and Admi	IPv4/v6 Address	Netmask/Prefix Length	Allow      Deny	Add
Admin Realms Admin Roles User S User Realms User Realms S User Roles Resource Profiles Resource Profiles Pulse Secure Client I Maintenance System Import/Export S	IPv4/v6 Address		Allow      Deny	Add
Admin Realms 4 Admin Roles 4 User Realms 4 User Roles 4 Resource Profiles 4 Resource Policies 4 Pulse Secure Client 1 Maintenance	IPv4/v6 Address		Allow      Deny	Add

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

8. Press on **Password**, and under **Options for primary authentication server**, select **Allow all users** (passwords of any length)

Also under **Options for additional authentication server**, select **Allow all users (password of any length)** 

S Pulse Secure	
Pulse Connect Secure	Help   Guidance   Sign Out
System Status Configuration Network Clustering IF-MAP Federation	User Authentication Realms > Users-SMS General Authentication Policy Role Mapping
Log/Monitoring > Reports >	Source IP   Browser   Certificate   Password   Host Checker   Limits
- Authentication Signing In	Options for primary authentication server
Endpoint Security → Auth. Servers - Administrators Admin Realms → Admin Roles →	Allow all users (passwords of any length)     Only allow users that have passwords of a minimum length:     Minimum Length: 4 characters
User Realms  User Roles  User Roles  Resource Profiles  Resource Policies  Pulse Secure Client  Maintenance System	Enable Password Management     This option enables the device to relay vital password information to users and enables users to change their passwords.     Display warning 14 day(s) before password expires     Note: Administrators may need to enable and configure LDAP authentication on the LDAP server configuration page.
Import/Export	Options for additional authentication server
Push Config   Archiving  Troubleshooting	Allow all users (passwords of any length)     Only allow users that have passwords of a minimum length:
	Minimum Length: 4 characters

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

### **Configuring Push OTP Hybrid Mode**

To configure Pulse Connect Secure to support Push OTP Hybrid mode, you will need to configure Pulse Connect Secure to support an additional authentication field, and then upload the login page package to replace the default login page.

- 1. Open the Pulse Connect Secure admin console.
- 2. In the left pane, select Users > User Realms.

Connect Secure			Help   Guidance   Si
figuration	User Authentication Realms		
work +	8		
MAP Federation + /Monitoring +	View: Overview   for all realms  Up	date	
orts / thentication sing In /	New Duplicate Delete		
point Security +	Authentication Realm	Servers	Dynamic Policy Evaluation
n. Servers ministrators	CBA	Primary: CBA	Disabled
in Realms 🔹	RUPIREALM	Primary: RADIUSRUPINDER Directory: RADIUSRUPINDER	Disabled
in Roles 🔸	User-Steel Belted	Primary: SAS-RADIUS Directory: SAS-RADIUS	Disabled
Realms >	Users	Primary: <u>SAS-RADIUS</u> Directory: <u>SAS-RADIUS</u>	Disabled
urce Profiles +	Users-SMS	Primary: LDAP_Oren Directory:DAP_Oren Secondary: SAS-SMS	Disabled
e Secure Client + Intenance em + ort/Export + Config + iving + bleshoating +	Authentication realms specify what server to use for authentication, how pol	licies are assigned to users, and restrictions on who can attempt to sign-in.	
ed to 0271MNZSJ	10U700AYS Púlse Secure, LLC: All rights reserved.		

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

- 3. In the Authentication Realm table, click the user realm you created in the previous section.
- 4. Under Additional authentication server, where Safenet Authentication Service is configured, under Password is: select the Specified by user on sign-in page radio button.

			Help		
User Authentication Realms > Users-SMS					
USEIS-SM3					
General Authentication Policy	Role Mapping				
* Name:	Users		Label to reference this realm		
Description:					
	When editing, sta				
	when editing, sta	Int on the Role Ma	pping page		
Servers					
Specify the servers to use for authentication	and authorization. To create or manage serv	ers, see the <u>Servers</u> pag	je.		
Authentication:	LDAP.	•	Specify the server to use for authenticating users.		
User Directory/Attribute:	Same as above 🔻		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					
You can specify an additional authentication	server for single sign-on (SSQ) purposes. Th	e additional credentials	can be specified by the user on the sign-in page (the labels for these inputs :		
sign-in page), or they can be pre-defined be	low, in which case the user will not be prom	sted for the credential.			
Authentication #2:	SAS	•			
Username is:	o specified by user on s	sign-in page			
	predefined as: <use< p=""></use<>	Contraction and the second			
Password is:	<ul> <li>specified by user on s</li> </ul>				
1 dostroi d tot	predefined as: p	ign-in page			
	End session if authent	ication against thi	s server fails		

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

5. Next, upload the login page package to replace the default page. In the left pane, select **Authentication > Signing In**, and then click the **Sign-in Pages** tab.

GET2     GET2     Cu     State     GetAult Sign-In Page     State     State     GetAult Sign-In Page     State     GetAult Sign-In Page     State     GetAult Sign-In Page     State     State     State     State     GetAult Sign-In Page     State     S	e tom page tom page tom page ndard page tom page
Sign-in Page         Sign-in Red/Cation         Sign-in Red/Cation           New Page         Uplead Cutom Page         Delete           Sign-in Page         Cutom         Cutom           6 gin: In Page         Cutom         Cutom           6 gin: In Page         Cutom         Cutom           6 gin: In Page         Cutom         Cutom           7 gin: In Page         Cutom         Cutom           8 gin: In Page         Cutom         Cutom           9 gin: In Page         State         State           9 gin: In Page         State         State	tom page tom page tom page ndard page
New Page         Uplead Custom Page         Delete           Sign-In Page         Try           Grg-crists         Cur           Size         Size	tom page tom page tom page indard page
Sign-In Page         Tyr           G Sign-In Page         Cur           G Sign-In Page         Cur           Sign-In Page         Cur           Sign-In Page         State           Scatch         Cur           Scatch         Cur           Scatch         Cur           K0D-ScatD         Cur           To TP 2 state - SAS SMS         State	tom page tom page tom page indard page
Septe / Page         Ty           U Septe / Page         Cu           U Septe / Page         Cu           U Septe / Page         Su           Cu         Scratch         Cu           Scratch         Cu           K02-Scratch         Cu           Scratch         Cu           Scratch         Cu           Scratch         Cu           Scratch         Cu           Scratch         Su           Scratch         Su           Scratch         Su           Scratch         Su           Scratch         Su           Scratch         Su           Su         Su           Su         Su           Su         Su           Su         Su	tom page tom page tom page indard page
Srahb     Srahb     Cu     Sta     Stab	tom page tom page ndard page
alx         Cur           Default Sign-to Page         Sta           Scratch         Cur           KoncalD         Cur           OTP 2 utep - SAS SMS         Sta	itom page ndard page
IN         Cu           Default Sign: In Page         Sta           Statabb         Cu           KCD-GrID         Cu           OTP 2 utep - SAS SHS         Sta	ndard page
Scratch         Cw           KCD-GrID         Cu           OTP 2 step - SAS SMS         Sta	
Image: KCD-G4D         Cu           Image:	tom name
U OTP 2 step - SAS SMS Sta	
	tom page
	ndard page
	ndard Meeting page
0 07G-1 Cu	tom page

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

- 6. Click Upload Custom Pages.
- 7. On the **Upload Custom Sign-In Pages** window, complete the following, and the click **Upload Custom Pages**:

Name	Enter a name for the custom sign-in page.	
Templates File	Click <b>Choose File</b> , and then select the following zip file:	
	Sample.ZIP (can be downloaded from inquira TE2501 - https://kb.safenet- inc.com/resources/sites/SAFENET/content/staging/TECH_NOTES/2 000/TE2501/en_US/2.0/sample_Pulse.zip	
Skip validation checks during upload	Select this check box.	

Public Connect Secure	Help   Guidance   Sig
Parka         Parka         Parka         Marka         Marka	

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

- 8. When the upload has finished, in the left pane, select **Authentication > Signing In**.
- 9. Press on your **Sign-in** policy.

ulse Connect Secur	re			Help   Guidance   Sign (	
System Status Configuration	Signing In				
Network Clustering	Sign-in Policies Sign-in Pages Sign-in	Notifications Sign-in SAML			
IF-MAP Federation	-				
Log/Monitoring Reports Authentication Signing In	Configuration of the second se	hat Administrators can attempt to sign in even if all rules on th rminate all user sessions.	is page are disabled.		
Endpoint Security Auth. Servers Administrators	Enable multiple user sessions Select this check box and enter the maximum number of sessions per user per realm in Users > User Realms > [Realm Name] > Authentication Policy > Limits page. By default, this is 1, or one session per user per realm. If you do not select this check box, you limit the user to one session for all realms of this user.				
Admin Realms	<ul> <li>Ø Display open user session[5] warning notification Check this option to notify users if they have other active session[3] in progress when they attempt to sign-in. The user has to follow the instructions on the warning notification page to proceed or cancel the login.</li> <li>Select when to display a notification page to users Aways         If the maximum session limit per user for the realm has been reached     </li> </ul>				
User Realms User Roles Resource Profiles Resource Policies Pulse Secure Client	Check this option to notify users if they have othe login. Select when to display a notification pag Always If the maximum session limit per user for the re-	r active session[s] in progress when they attempt to sign-in. T le to users	re user has to follow the instructions on the warning notification page	to proceed or cancel the	
Users User Realms User Roles Resource Profiles Resource Policies Pulse Secure Client	Check this option to notify users if they have othe login. Select when to display a notification pag Always If the maximum session limit per user for the re-	r active session[s] in progress when they attempt to sign-in. T le to users	re user has to follow the instructions on the warning notification page		
Users User Realms User Roles Resource Profiles Pulse Secure Client Maintenance System Import/Export	Check this option to notify users if they have other Check the option to notify users if they have other Select when to display a notification pag Always They are the maximum session limit per user for the rest They wanted they are the they are	r active session[s] in progress when they attempt to sign-in. T le to users alm has been reached		Save Change	
Users User Realms User Roles Resource Profiles Resource Policies Pulse Secure Client Maintenance System Import/Export Push Config	Check this option to notify users if they have other option. Select when to display a notification page Aharya If the maximum session limit per user for the res New URL Delete Enable Disable Check the second secon	r active session[s] in progress when they attempt to sign-in. T le to users alm has been reached Sign-In Page	Authentication Realm(s)	Save Change Enable	
Users User Realms User Roles Resource Profiles Resource Policies Pulse Secure Client Maintenance System Import/Export Push Config Archiving	Check this option to notify users if they have other Check the option to notify users if they have other Select when to display a notification pag Always They are the maximum session limit per user for the rest They wanted they are the they are	r active session[s] in progress when they attempt to sign-in. T le to users alm has been reached			
Users User Realms User Roles Resource Profiles Resource Policies Pulse Secure Client Maintenance System Import/Export Push Config Archiving	Check this option to notify users if they have other option. Select when to display a notification page Aharya If the maximum session limit per user for the res New URL Delete Enable Disable Check the second secon	r active session[s] in progress when they attempt to sign-in. T le to users alm has been reached Sign-In Page	Authentication Realm(s)	Save Change Enable	
Users User Realms User Roles Resource Profiles Resource Policies Pulse Secure Client Maintenance System Import/Export Push Config Archiving	Check this option to notify users if they have other Select when to display a notification pag Always If the maximum session limit per user for the res New URL Delete Enable Disable Administrator URLs #/admin/	r active session[s] in progress when they attempt to sign-in. T te to users alm has been reached Sign-In Page Default Sign-In Page	Authentication Realm(s) Admin Users	Save Change Enable	
Users User Realms User Roles Resource Profiles Resource Policies Pulse Secure Client Maintenance System	Check this option to notify users if they have other Check the option to notify users if they have other Select when to display a notification page Always Always New URL Delete Enable Disable New URL Delete Enable Disable New URL User URLs	r active session[s] in progress when they attempt to sign-in. T ie to users alm has been reached Sign-In Page Sign-In Page	Authentication Realm(s) Admin Users Authentication Realm(s)	Save Change Enable	
User Realms User Realms User Roles Resource Profiles Resource Policies Pulse Secure Client Maintenance System Import/Export Push Config Archiving	Check this option to notify users if they have other option. Select when to display a notification pag Alvays If the maximum session limit per user for the real New URL. Delete Enable Disable Administrator URLs "Admin/ User URLs "Admin/	r active session[s] in progress when they attempt to sign-in. T le to users alm has been reached Sign-In Page Default Sign-In Page Sign-In Page Default Sign-In Page	Authentication Realm(s) Admin Users Authentication Realm(s) Users	Save Change Enable Enable	

(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)

10. In the **Sign-in page** menu, select the custom page you created, and then click **Save Changes**.

S Pulse Secure					
Pulse Connect Secure			Help   Guidance   Sign Out		
System Status > Configuration > Network > Clustering > IF-MAP Federation > Log/Monitoring >	Signing In > */Sms/ Save Changes				
Reports >	User type:	Users O Administrators	Authorization Only Access		
Authentication	Sign-in URL: */	/sms/	Format: <host>/<path>/; Use * as wildcard in the beginning of the host name.</path></host>		
Signing In Endpoint Security Auth. Servers	Description: s	MS for OTG			
Administrators		DTG-1			
Admin Roles +		o create or manage pages, see <u>Sign-I</u>	n pages.		
- Users	Meeting URL: *	/meeting/ 🔻			
User Realms > User Roles >					
Resource Profiles >	Authentication realm				
Resource Policies > Pulse Secure Client >	ure Client i opechy now to select an autoentication realm when signing in.				
Maintenance     System     Import/Export     Push Config     Archiving     Troubleshooting	User types the realm name The user must type the name of one of the available authentication realms.     User picks from a list of authentication realms     The user must choose one of the following selected authentication realms, when they sign in. If only one realm is selected, it is automatically used (the sign-in page will not display the list). To create or mmange realms, see the sign-cholenological page of the definitionable Authentication page.				
	Available realms:	Selected realms			
	CBA RUPIREALM User-Steel_Belted Users	Add -> Users-SMS A	Move Up Move Down		
	Configure Sign-in Notifications				
	Pre-Auth Sign-in Notification				
	Post-Auth Sign-in I				
	Save changes?				
	-				
	Save Chang	es			

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

## **Running the Solution**

After Pulse Connect Secure is configured to use RADIUS with SafeNet Authentication Service, users can log in to the Pulse Connect Secure portal.

### **Connecting to the Pulse Connect Secure Portal using Simple Mode**

In the following scenario, the standard Pulse Connect Secure login page and OOB configuration are used.

1. Login to the Pulse Connect Secure console via the web browser.

<b>Secure</b> Secure	ulse Secure				
Welcome Pulse C	to the onnect Secure				
username password	Sign In	Please sign in to begin your secure session.			

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

2. Enter your LDAP credentials, and then click Sign In.

Pulse Secure		
Welcome Pulse C	to the onnect Secure	
username password	Bob ••••••••	Please sign in to begin your secure session.

(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)

3. You will then receive a push notification on your mobile. Tap Approve.



4. On the Token Authentication screen, enter your PIN code, and then tap Continue.

← Mo	bilePAS	S+	
TOKEN AUTHENTICATION Token PIN  CANCEL CONTINUE			
	-1 minute ago Nov 19, 2015 01-18 PM GMT-02:00		
1	1 2 3		
4	5	6	
7	8	9	
	0		

5. After a successful authentication, you will be logged in to the Pulse Connect Secure portal.

S Pulse Secure		Logged-in as: the Logged-in Asc bob Home Neetings Preferences Halp 1
		Browse
	Welcome to the Pulse Connect Secure, bob.	
	Web Bookmarks	:= + *
	OWA Test-domain	0
	OWA 2010	9
	OWA2010-KCD	0
	Files	≔ <sup>+</sup> = <sup>+</sup> × *
	You don't have any files bookmarked.	Mindow Piles   Min Piles
	Terminul Sessions	*
	You don't have any terminal sessions.	
	Client Application Sensions	·
	Pulse Secure	Start
	A Java Secure Application Manager	Start I=
	Vartual Desktops	Q.
	You don't have any virtual desktops.	
Copyright @ 2001-2015 Pulse	e Secure, LLC. All rights reserved.	

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

### Connecting to the Pulse Connect Secure Portal using Hybrid Mode

In the following scenario, the hybrid mode login screen is used, and you will have the option to choose between authentication using the Push OTP notification message, or manually typing a passcode.

1. Login to the Pulse Connect Secure console via the web browser.

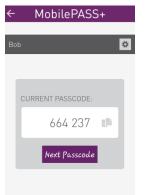
Welcome to the	
Pulse Connect Secure	
username password ® Use my mobile to autosend a passcode	Please sign in to begin your secure session.
Enter a passcode manually	
Enter a passcode manually           Sign In	

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

- 2. Enter your LDAP credentials, and then choose one of the following:
  - Use my mobile to autosend a passcode—If you choose this option, a push notification will be sent to your mobile. Follow the steps as described in the previous scenario.
  - Enter a passcode manually—If you choose this option, you will need to manually enter a passcode.
    - Open the mobile app, and then tap on the token.
    - On the **Token Authentication** screen, enter your PIN code, and then tap **Continue**.

← Mo	bilePAS	SS+	
TOKEN AUTHENTICATION			
Token PIN			
CANCI	CANCEL CONTINUE		
	-1 m	inute ago	
		4:18 PM GMT+02:00	
1	Z	3	
4	5	6	
7	8	9	
	0		

• You will receive a passcode.



3. In the Pulse Connect Secure console, in the **Additional password** field, enter the passcode, and then click **Sign In**.

§ Pulse Secure		
Welcome to t Pulse Con	<sup>the</sup> nnect Secure	
username	Bob	Please sign in to begin your secure session.
password	•••••	
	obile to autosend a passcode sscode manually password Sign In	

(The screen image above is from Pulse Secure<sup>®</sup>. Trademarks are the property of their respective owners.)

4. After a successful authentication, you will be logged in to the Pulse Connect Secure portal.

S Pulse Secure		Logged-in as: 🟠 🧾 🏓 🥸 bob Home Meetings Preferences Halp St
		Browse
	Welcome to the Pulse Connect Secure, bob.	
	Web Bookmarks	i= + <b>*</b>
	OWA Test-domain	9
	OWA 2010	Ø
	@ <u>OWA2010-KCD</u>	Ø
	Files	≍ * <b>*</b> **
	You don't have any files bookmarked.	Windows Eller   Wok. Eller
	Terminal Sessions	*
	You don't have any terminal sessions.	
	Client Application Sessions	*
	Pulse Secure	Start
	🐴 Java Secure Application Manager	Start 1=
	Virtual Desktops	Q -
	You don't have any virtual desktops.	
	se Serum, IJC, All rights reserved.	
Copyright & 2001-2015 Put	an Garma, 2000 ku ulina nanarana	

(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)

## **Support Contacts**

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	