

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

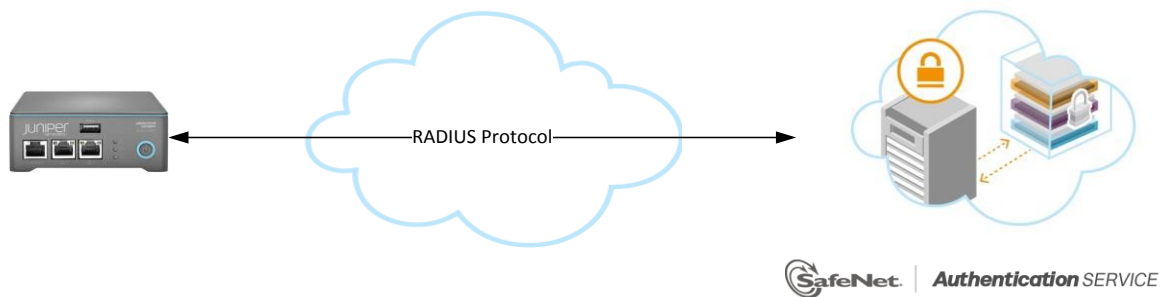
Audience

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.

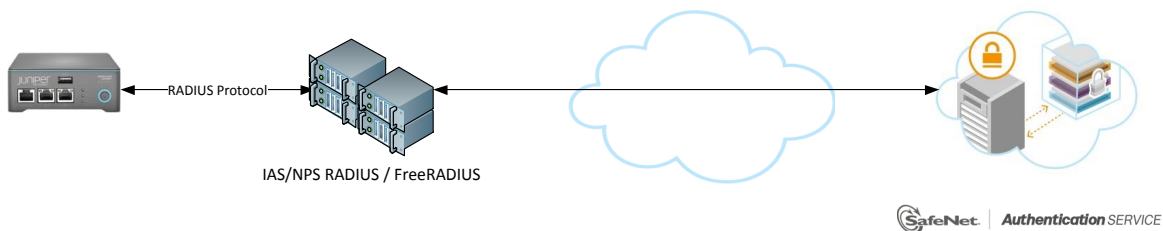
RADIUS-based Authentication using SAS Cloud

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.

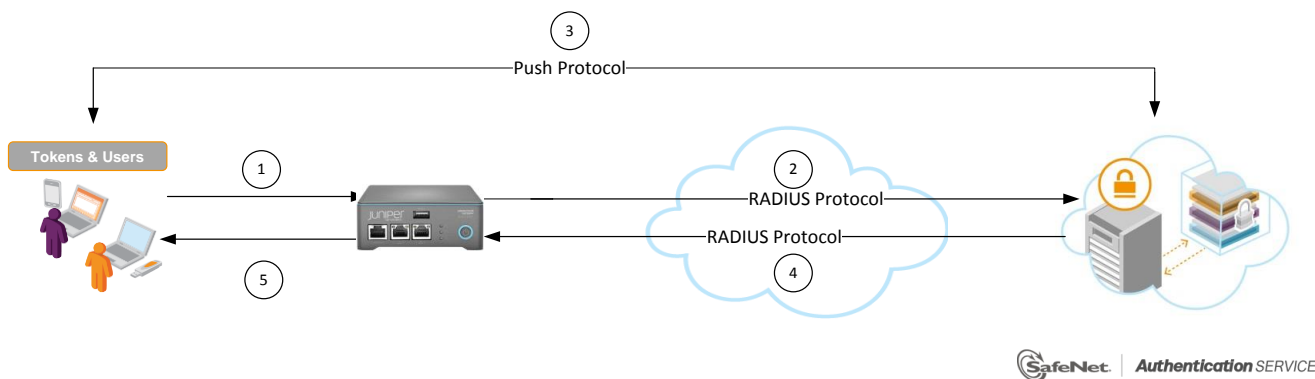
For more information on how to install and configure SAS Agent for IAS/NPS, refer to:
<http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf>

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.



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.
5. 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.

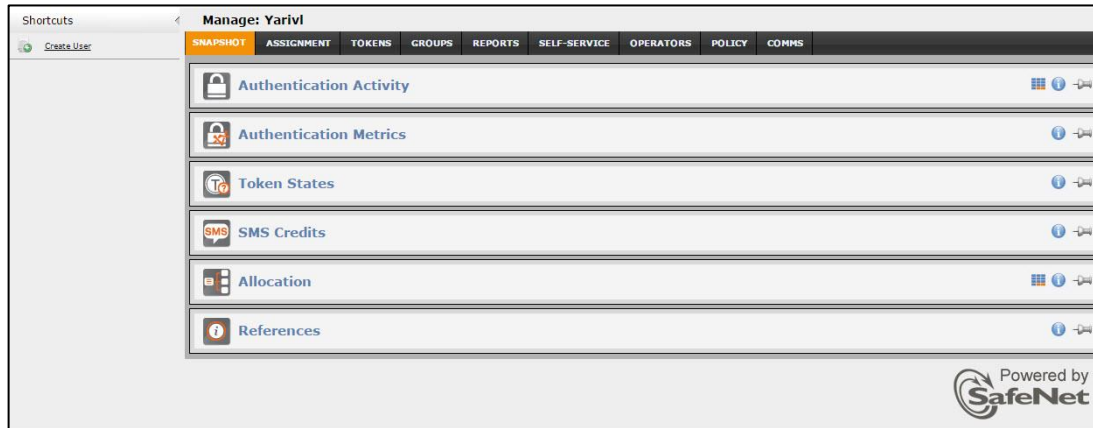
Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

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

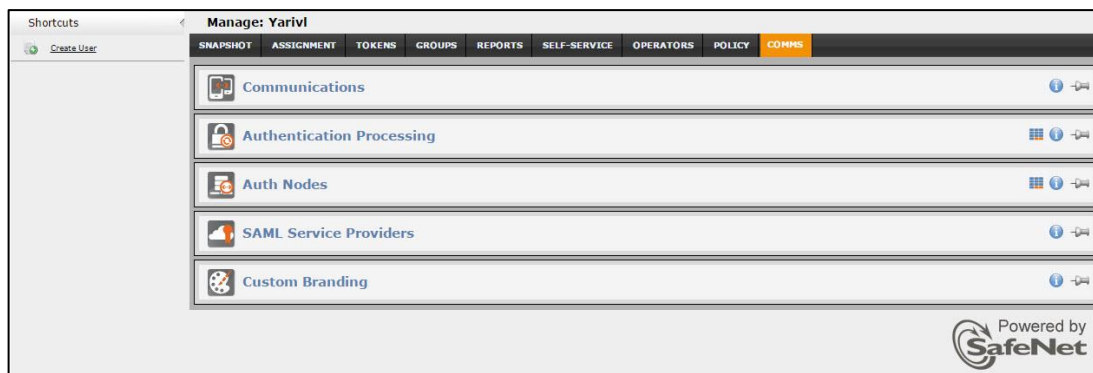
Adding Pulse Connect Secure as an Authentication Node in SAS

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.



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



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



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:
Resource Name:
Host Name:
Low IP Address In Range:
High IP Address In Range:

☐ Exclude from PIN change requests
☒ Configure FreeRADIUS Synchronization
Shared Secret:
Confirm Shared Secret:

Generate

FreeRADIUS synchronization may take up to 5 minutes to propagate in the system.

The authentication node is added to the system.

Auth Nodes

Auth Nodes

Auth Nodes:

Task	Description
Auth Nodes	Create and configure SafeNet Authentication Service Authentication Nodes

Auth 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.

Add
Change Log
Cancel

Primary RADIUS Server IP:

Primary SafeNet Authentication Service Agent DNS:

Max. Auth Nodes: 10

Failover RADIUS Server IP:

Failover SafeNet Authentication Service Agent DNS:

Index	Auth Node Name	Host Name	IP Address	FreeRADIUS Synchronization		
1	Pulse Connect Secure		192.168.10.100	True	Edit	Remove

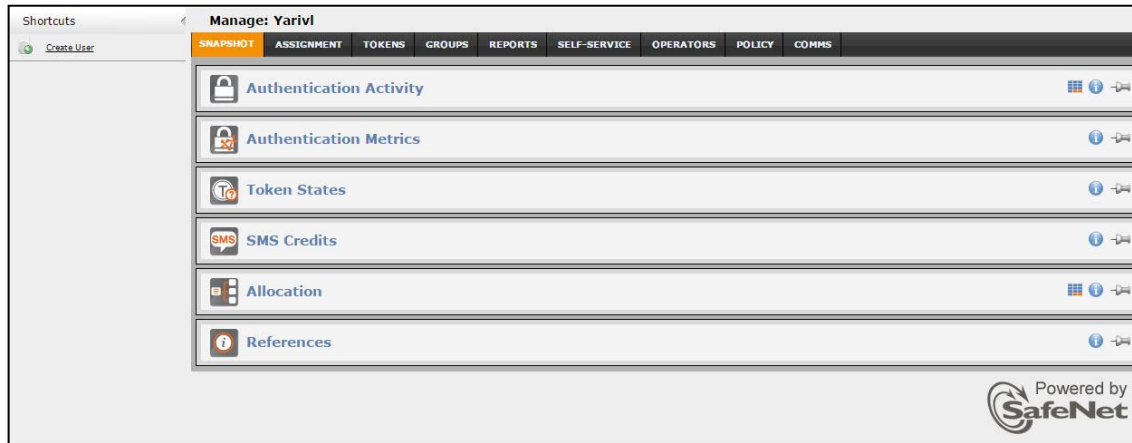
Displaying: 1 to 3 of 3

<<
<
>
>>

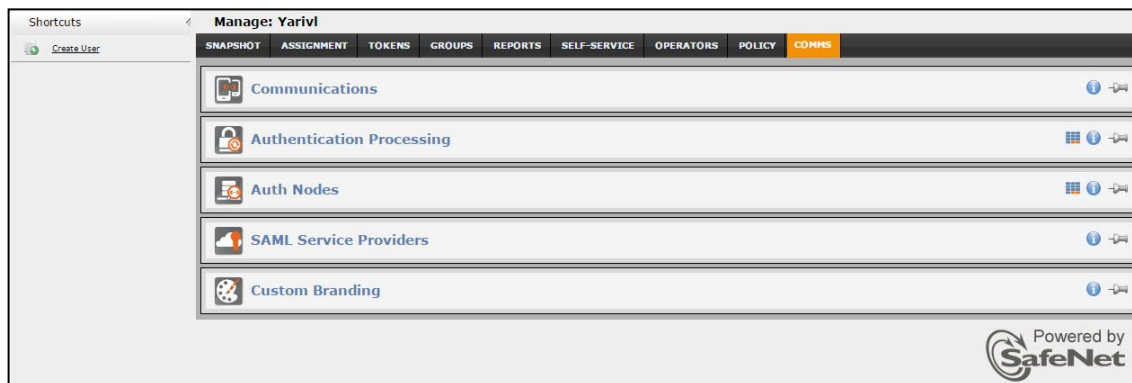
Checking the SAS RADIUS Server's IP Address

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.



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



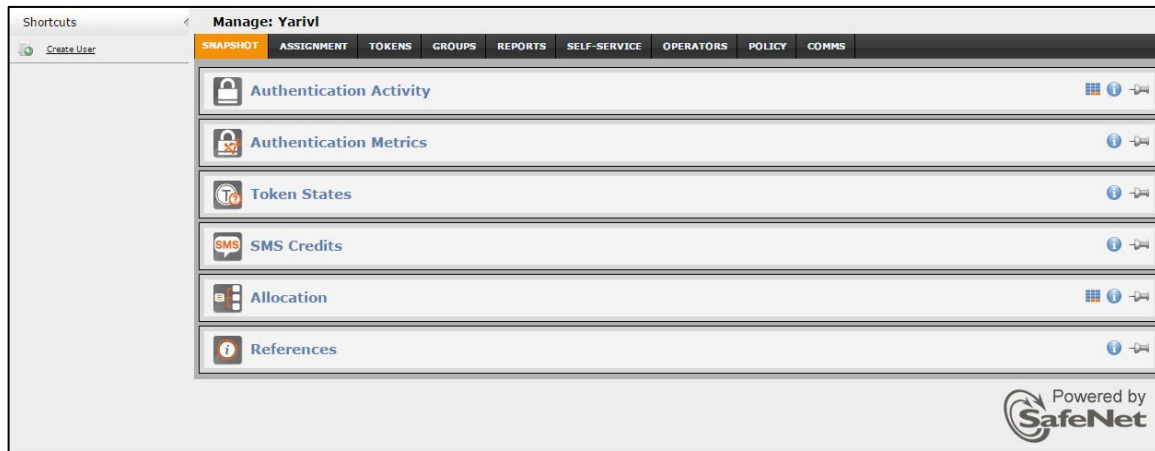
3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.



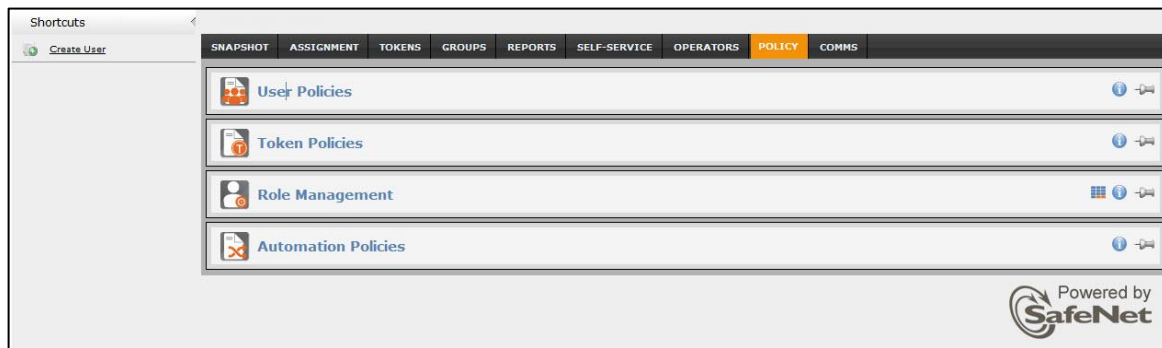
Enabling the Software Token Push OTP Setting

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

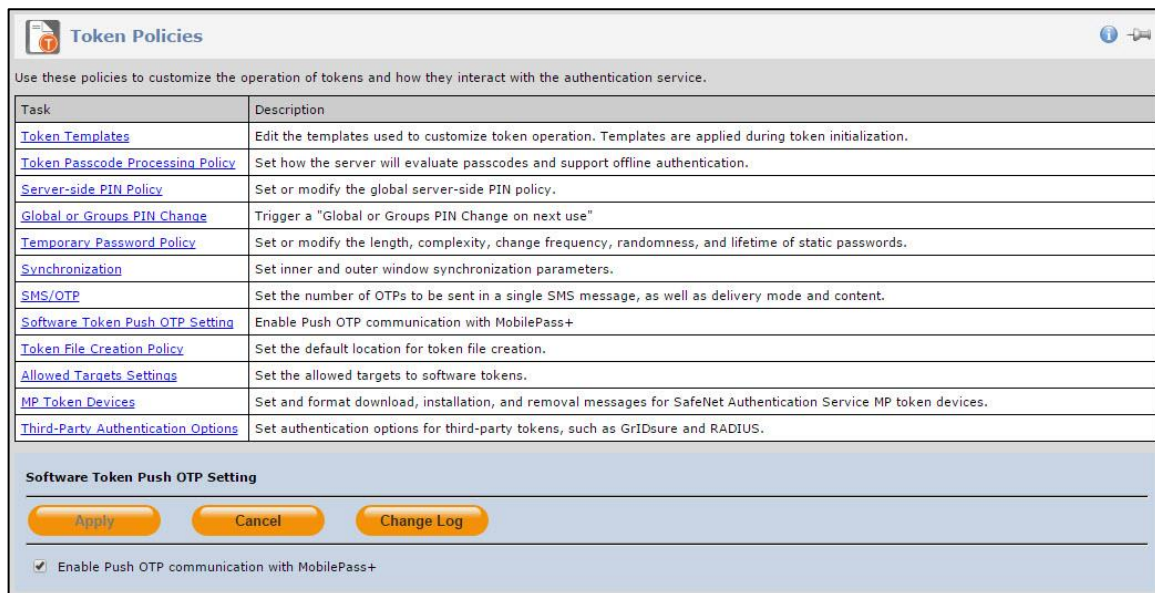
1. Log in to the SAS console with an Operator account.



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



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



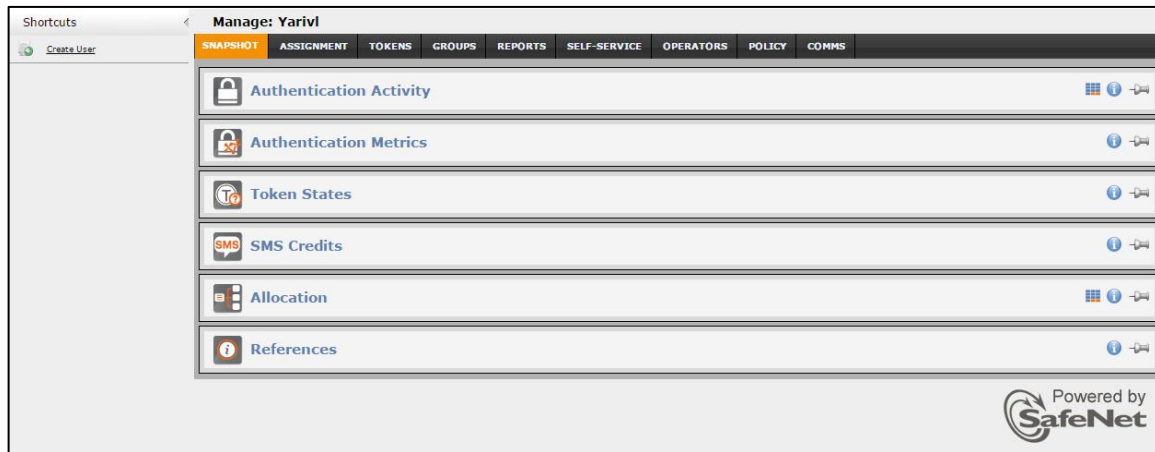
4. Select **Enable Push OTP communication with MobilePass+**, and then click **Apply**.

Enabling the Allowed Targets Policy

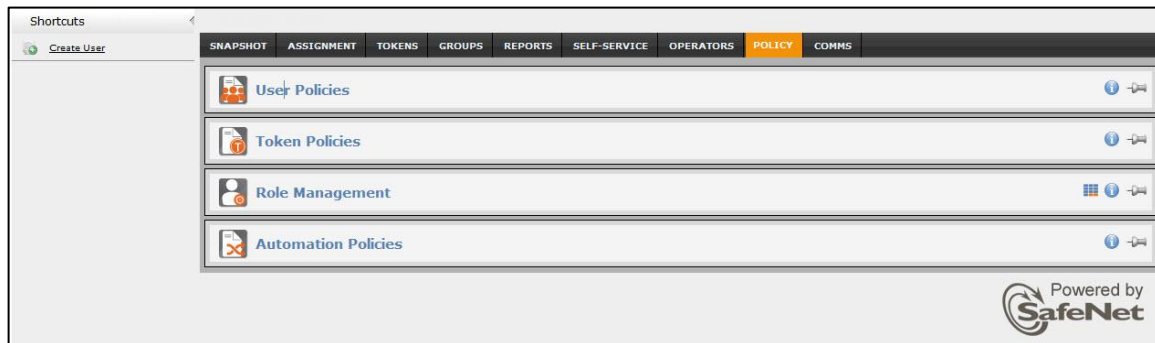
For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the self-enrollment 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.



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



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

The screenshot shows the 'Token Policies' module interface. At the top, there's a header with the 'Token Policies' title and a description: 'Use these policies to customize the operation of tokens and how they interact with the authentication service.' Below this is a table with two columns: 'Task' and 'Description'. The table lists various policies such as 'Token Templates', 'Token Passcode Processing Policy', 'Server-side PIN Policy', 'Global or Groups PIN Change', 'Temporary Password Policy', 'Synchronization', 'SMS/OTP', 'Software Token Push OTP Setting', 'Token File Creation Policy', 'Allowed Targets Settings', 'MP Token Devices', and 'Third-Party Authentication Options'. The 'Allowed Targets Settings' row is highlighted. Below the table, there's a section titled 'Allowed Targets Settings' with 'Apply' and 'Cancel' buttons. Underneath, there are two tabs: 'MobilePASS' and 'MP-1'. The 'MobilePASS' tab is active, showing settings for 'MobilePASS+' and 'MobilePASS 8'. Under 'MobilePASS+', there are checkboxes for 'Android' and 'iOS', both of which are checked. Under 'MobilePASS 8', there are checkboxes for 'Android', 'iOS', 'Mac OS X', 'Windows Phone', 'Windows', 'Windows RT', 'BlackBerry 10', and 'BlackBerry Java'. The 'Mac OS X', 'Windows Phone', 'Windows', 'Windows RT', 'BlackBerry 10', and 'BlackBerry Java' checkboxes are checked, while 'Android' and 'iOS' are unchecked. A note at the bottom states: 'One MobilePASS application per OS type may be selected.'

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 Cancel

MobilePASS MP-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**.

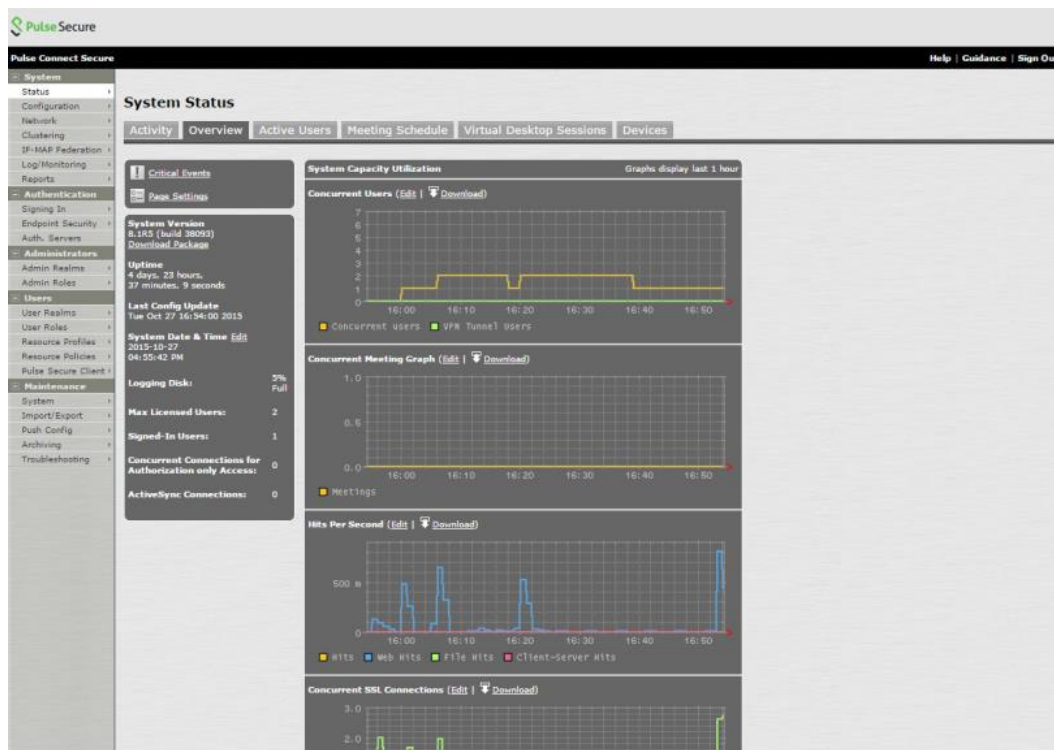
Configuring Pulse Connect Secure

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

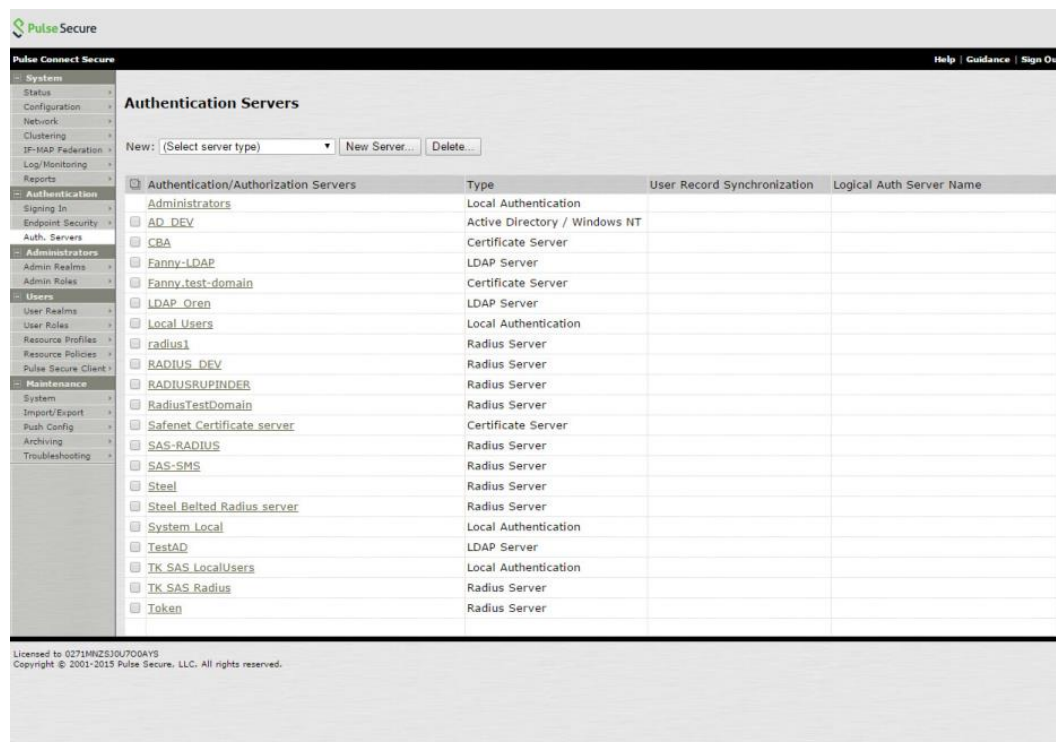
Creating a RADIUS Authentication Server

1. Open the Pulse Connect Secure admin console.



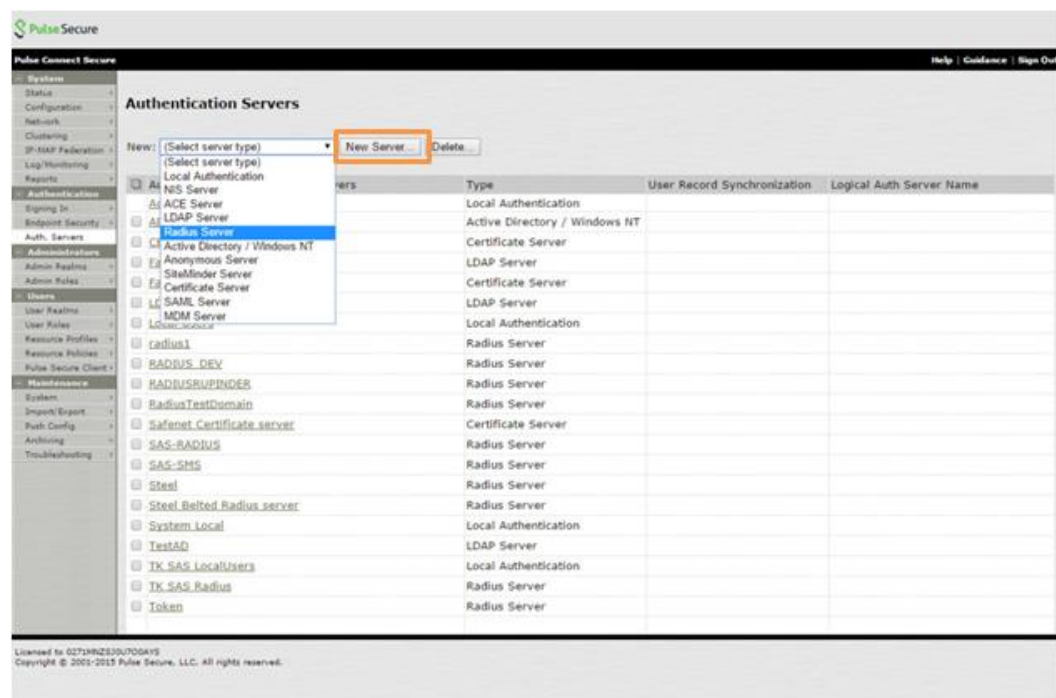
(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)

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



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

- In the **New** menu, select **Radius Server**, and then click **New 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 then 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 60 seconds.

Do not change the other default values.

The screenshot shows the Pulse Connect Secure web interface. The left sidebar contains a navigation menu with categories like System, Authentication, Users, and Maintenance. The main content area is titled 'SAS-RADIUS' and has two tabs: 'Settings' (selected) and 'Users'. The 'Settings' tab contains the following fields and options:

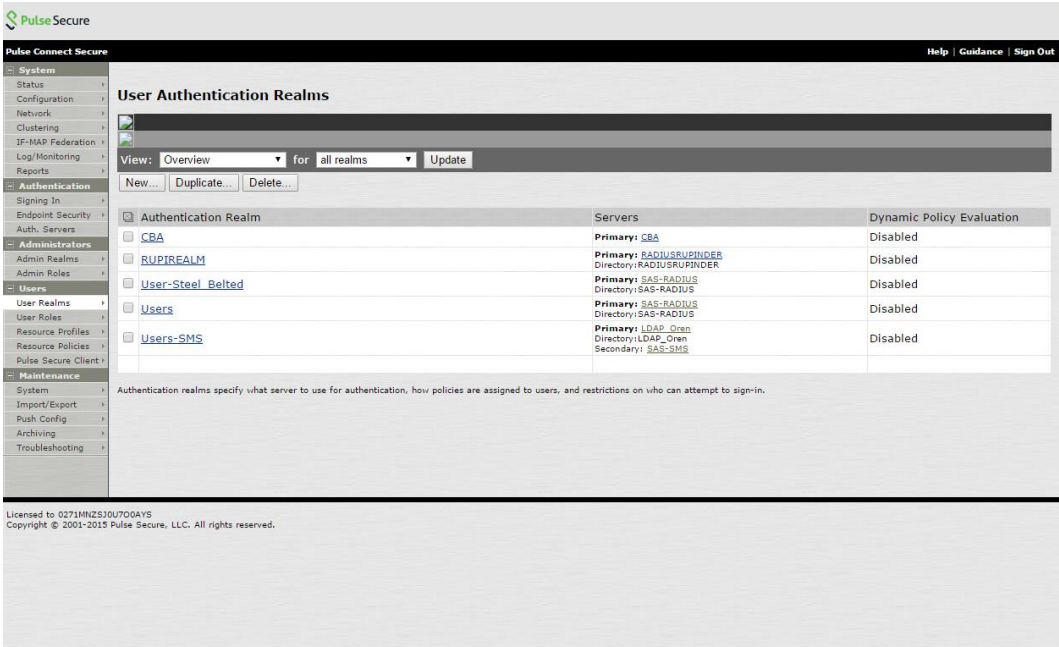
- Name:** SAS-RADIUS (Label to reference this server.)
- NAS-Identifier:** Juniper sfrnt.com (Name of the device as known to Radius server)
- Primary Server:**
 - * Radius Server:** 109.73.120.148 (Name or IP address)
 - * Authentication Port:** 1812
 - * Shared Secret:** ****
 - * Accounting Port:** 1813 (Port used for Radius accounting, if applicable)
 - NAS-IP-Address:** (IP address)
 - * Timeout:** 60 seconds
 - * Retries:** 0
- ☐ **Users authenticate using tokens or one-time passwords**
 Note: If you select this, the device will send the user's authentication method as "token" if you use SAML, and this credential will not be used in automatic SSO to backend applications.
- Backup Server (required only if Backup server exists)**
 - Radius Server:** (Name or IP address)
 - Authentication Port:** (Port used for Radius authentication, if applicable)
 - Shared Secret:** (Port used for Radius accounting, if applicable)
 - Accounting Port:** (Port used for Radius accounting, if applicable)
- ☐ **Load-Balance Auth Requests between Primary and Backup Servers**
 Accounting requests will not be load-balanced.
- Radius accounting**
 - User-Name:** <USER>[<REALM>]<ROLE SEP=","> (Template for reporting user identity to Radius server)
 - The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. Click [here](#) to view a list of all variables.
 - Examples:
 - <USER> The user's login name
 - <REALM> The user's sign-in realm

(The screen image above is from Pulse Secure®. 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**.



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

3. In the **Authentication Realm** table, click **Users**.

- 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, SAS-RADIUS).
Username is	Select predefined as: <USER> .
Password is	Select predefined as , and leave the letter p .

The screenshot shows the Pulse Connect Secure configuration interface. The left sidebar contains a navigation menu with categories like System, Configuration, Network, and Users. The main content area is titled 'Users-SMS' and has tabs for 'General', 'Authentication Policy', and 'Role Mapping'. The 'General' tab is active, showing fields for 'Name' (Users) and 'Description'. Below this is a 'Servers' section with a table for specifying authentication and authorization servers. The 'Additional authentication server' checkbox is checked and highlighted with an orange box. Below this, the 'Authentication #2' is set to 'SAS'. The 'Username is' field is set to 'predefined as: <USER>' and the 'Password is' field is set to 'predefined as: p'. The 'End session if authentication against this server fails' checkbox is also checked.

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

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

The screenshot shows the Pulse Connect Secure configuration interface with the 'Role Mapping' tab selected. The 'New Rule' button is highlighted with an orange box. Below the button, there is a table for defining role mapping rules. The first rule is defined with the condition '1. username is "integ", "integ1", "bob" or "captainfr1"' and is assigned the role 'Users'. The 'Rule Name' is 'Stop' and the 'Role' is 'integ'. Below the table, there are options for 'When more than one role is assigned to a user': 'Merge settings for all assigned roles', 'User must select from among assigned roles', and 'User must select the sets of merged roles assigned by each rule'. The 'Merge settings for all assigned roles' option is selected.

(The screen image above is from Pulse Secure®. 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 on	Select Username .
Name	Enter a name for the rule.
Rule: If username...	Select a user or a list of users that need to authenticate to the realm.
...then assign these roles	Select a role from the Available Roles window, and then click Add to move it to the Selected Roles window. Repeat as needed to add more roles.

Pulse Secure

Pulse Connect Secure

Help | Guidance | Sign Out

System Authentication Realms > Users:SMS > **Role Mapping Rule**

Rule based on: Username Update

* Name:

* Rule: If username...

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

...then assign these roles

Available Roles: RUPINDER-ROLES steelbelledrole Users

Selected Roles: (none)

Add -> Remove

☐ Stop processing rules when this rule matches

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

Save changes?

Save Changes Save + New

* indicates required field

Licensed to 0271M2530U700A1S
Copyright © 2001-2015 Pulse 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**

The screenshot shows the Pulse Connect Secure web interface. The left sidebar contains a navigation menu with categories like System, Authentication, Administrators, Users, and Maintenance. The main content area is titled 'User Authentication Realms > Users-SMS'. Below this, there are tabs for 'General', 'Authentication Policy', and 'Role Mapping'. Under 'Authentication Policy', there are sub-tabs: 'Source IP', 'Browser', 'Certificate', 'Password', 'Host Checker', and 'Limits'. The 'Source IP' sub-tab is selected. It contains two radio buttons: 'Allow users to sign in from any IP address' (selected) and 'Allow or deny users from the following IP addresses:'. Below these is a 'Delete' button and up/down arrow buttons. A table with columns 'IPv4/v6 Address', 'Netmask/Prefix Length', and 'Allow/Deny' is shown. The 'Allow/Deny' column has 'Allow' and 'Deny' radio buttons, with 'Allow' selected. An 'Add' button is to the right of the table. A note at the bottom states: 'Note: This restriction will not be enforced if no IP addresses are listed. Add one or more source IP addresses from which users are allowed to sign in or denied access.' A 'Save Changes' button is at the bottom.

(The screen image above is from Pulse Secure®. 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)**

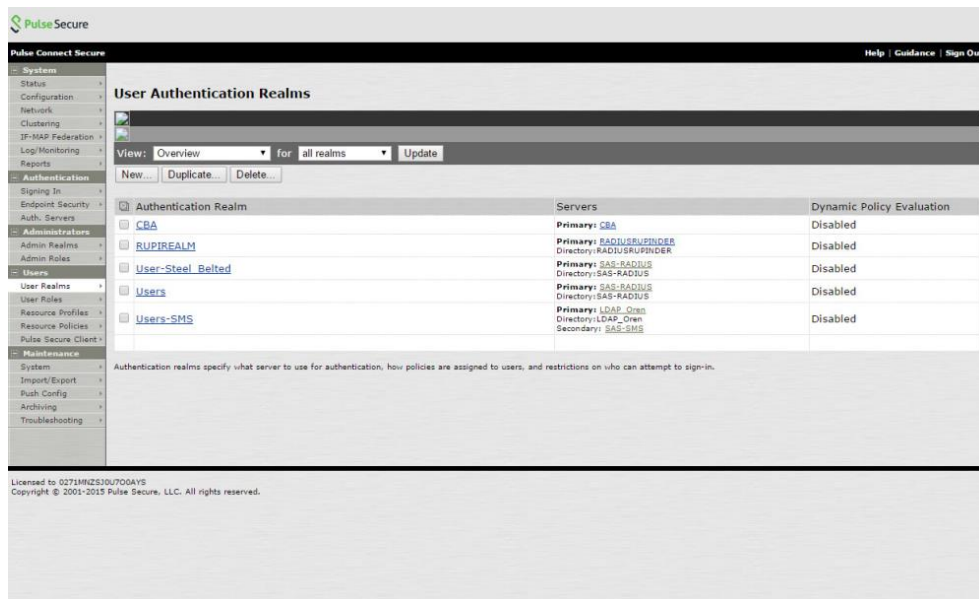
The screenshot shows the Pulse Connect Secure web interface, similar to the previous one, but with the 'Password' sub-tab selected under 'Authentication Policy'. The 'Options for primary authentication server' section has two radio buttons: 'Allow all users (passwords of any length)' (selected) and 'Only allow users that have passwords of a minimum length:'. Below the second option is a 'Minimum Length' field with the value '4'. The 'Enable Password Management' checkbox is checked. Below it, text says 'This option enables the device to relay vital password information to users and enables users to change their passwords.' and 'Display warning 14 day(s) before password expires'. A note at the bottom says: 'Note: Administrators may need to enable and configure LDAP authentication on the [LDAP server configuration page](#).' The 'Options for additional authentication server' section also has two radio buttons: 'Allow all users (passwords of any length)' (selected) and 'Only allow users that have passwords of a minimum length:'. Below the second option is a 'Minimum Length' field with the value '4'.

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

Configuring Push OTP Hybrid Mode

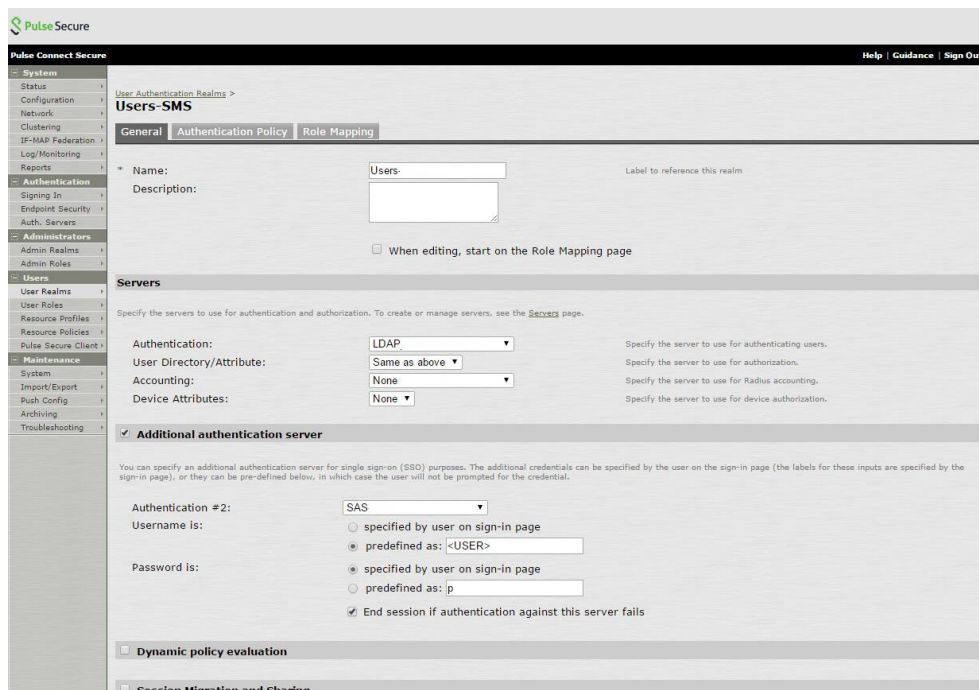
To configure Pulse Connect Secure to support Push OTP Hybrid mode, you will need to configure Pulse Connect Secure to support an additional authentication field, and then upload the login page package to replace the default login page.

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



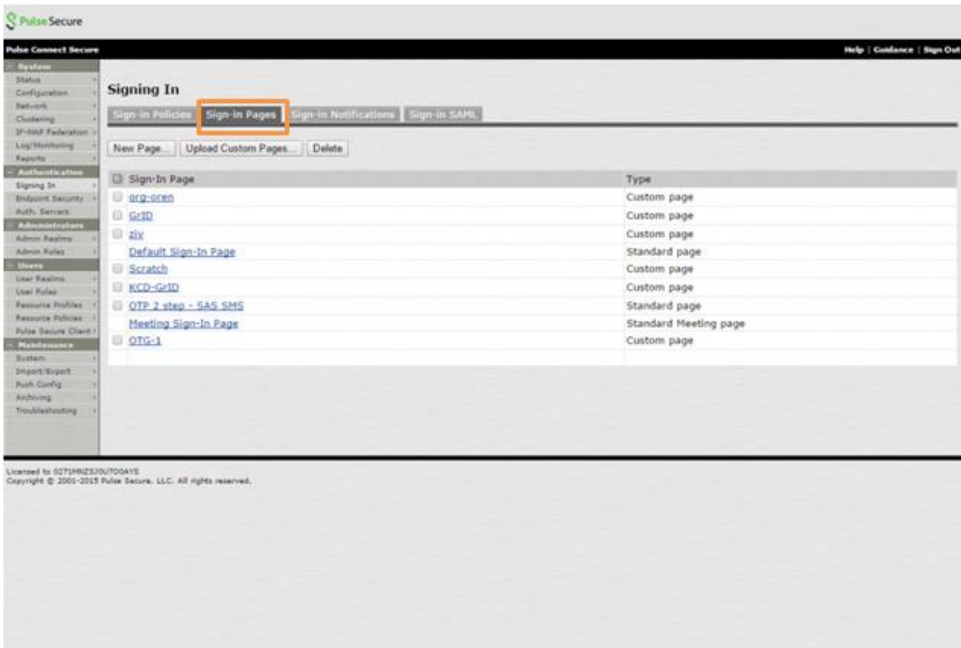
(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)

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.



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

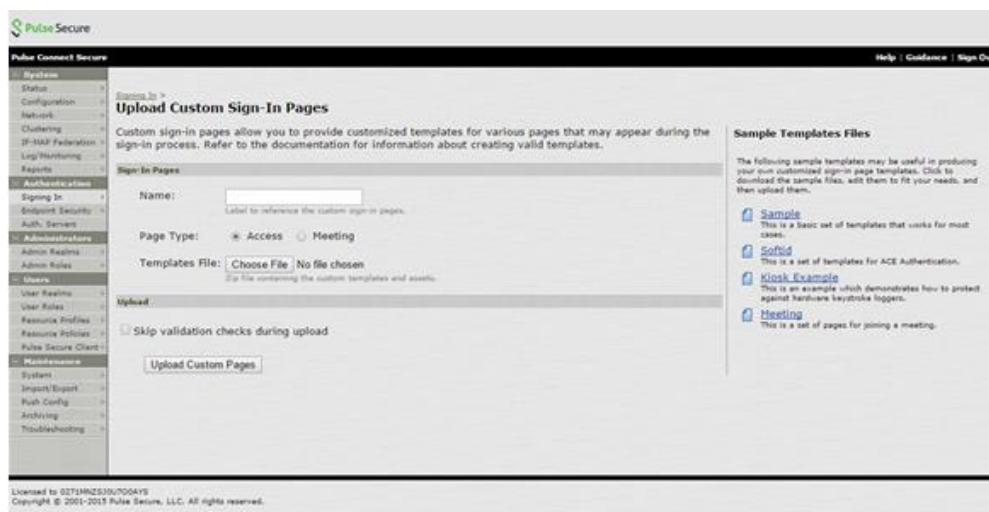
- Next, upload the login page package to replace the default page. In the left pane, select **Authentication > Signing In**, and then click the **Sign-in Pages** tab.



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

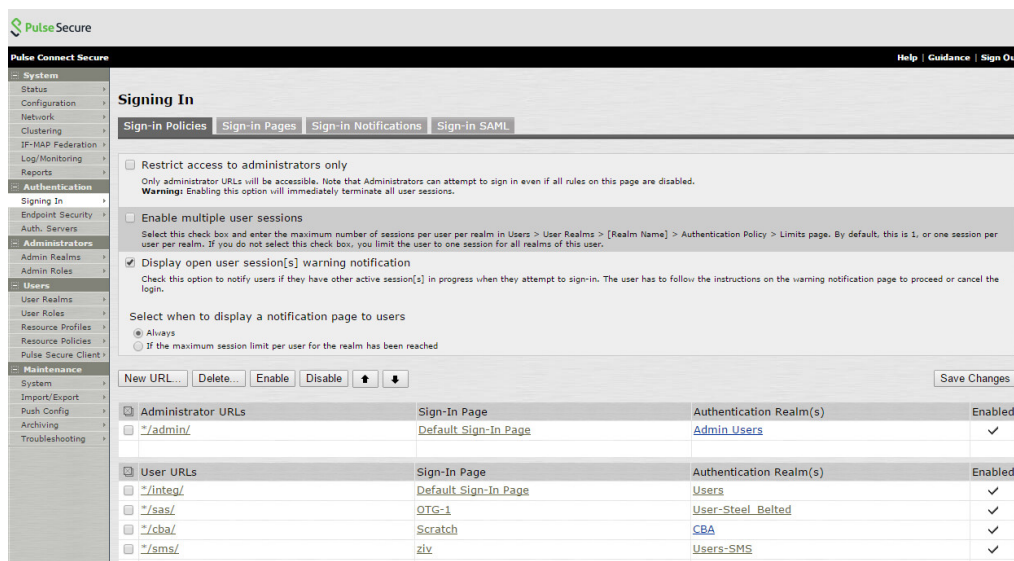
- Click **Upload Custom Pages**.
- On the **Upload Custom Sign-In Pages** window, complete the following, and then click **Upload Custom Pages**:

Name	Enter a name for the custom sign-in page.
Templates File	Click Choose File , and then select the following zip file: Sample.ZIP (can be downloaded from inquirea TE2501 - https://kb.safenet-inc.com/resources/sites/SAFENET/content/staging/TECH_NOTES/2000/TE2501/en_US/2.0/sample_Pulse.zip)
Skip validation checks during upload	Select this check box.



(The screen image above is from Pulse Secure®. 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.



(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**.

Pulse Secure

Pulse Connect Secure Help | Guidance | Sign Out

System

- Status
- Configuration
- Network
- Clustering
- IP-Map Federation
- Log/Monitoring
- Reports

Authentication

- Signing In
- Endpoint Security
- Auth. Servers

Administrators

- Admin Realms
- Admin Roles

Users

- User Realms
- User Roles
- Resource Profiles
- Resource Policies
- Pulse Secure Client

Maintenance

- System
- Import/Export
- Push Config
- Archiving
- Troubleshooting

Signing In > */sms/

[Save Changes](#)

User type: ☒ Users ☐ Administrators ☐ Authorization Only Access

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

Description: SMS for OTG

Sign-in page: OTG-1 To create or manage pages, see [Sign-In pages](#).

Meeting URL: */meeting/

Authentication realm

Specify how to select an authentication realm when signing in.

☐ 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 manage realms, see the [User Authentication](#) page or the [Administrator Authentication](#) page.

Available realms: CBA, RUPREALM, User-Steel_Belted, Users

Add -> Remove

Selected realms: Users-SMS

Move Up Move Down

Configure Sign-in Notifications

☐ Pre-Auth Sign-in Notification

☐ Post-Auth Sign-in Notification

Save changes?

[Save Changes](#)

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

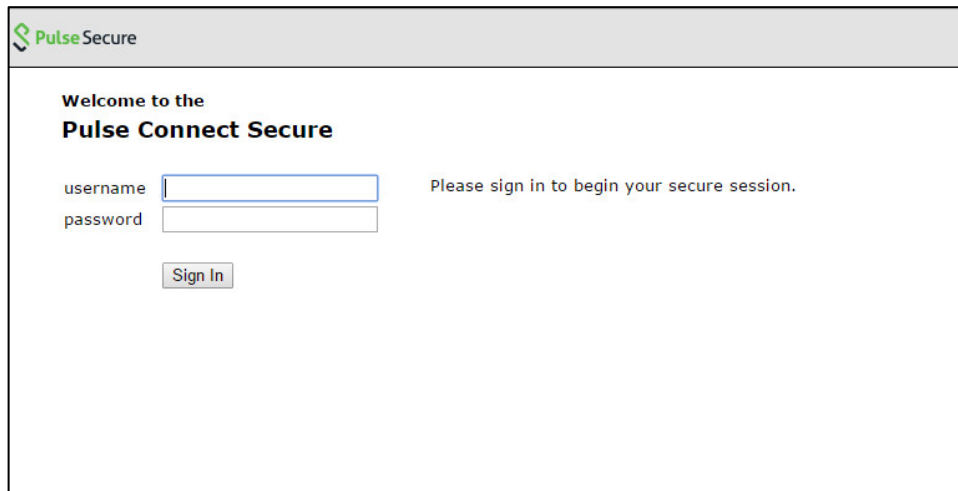
Running the Solution

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.



Pulse Secure

Welcome to the
Pulse Connect Secure

username

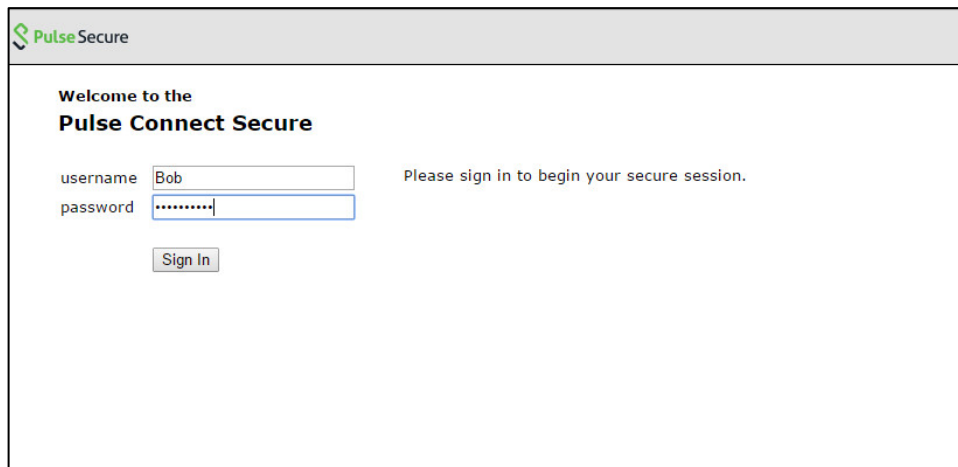
password

Please sign in to begin your secure session.

Sign In

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

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



Pulse Secure

Welcome to the
Pulse Connect Secure

username

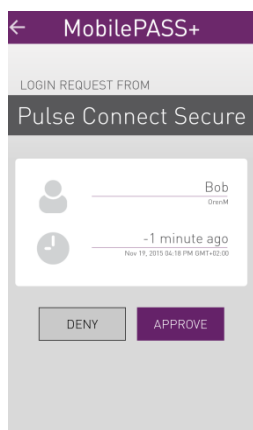
password

Please sign in to begin your secure session.

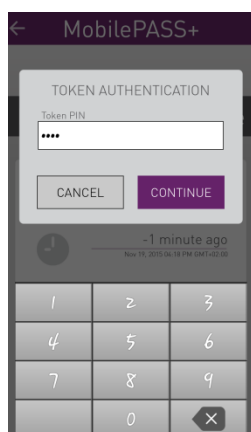
Sign In

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

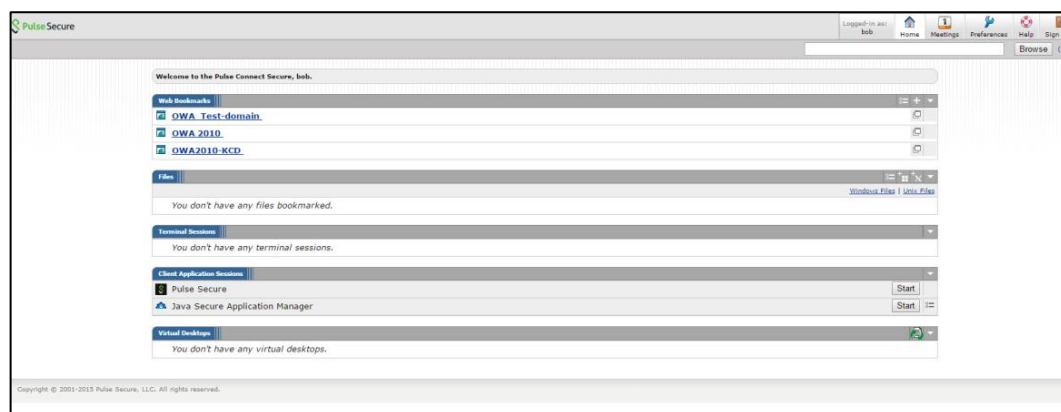
3. You will then receive a push notification on your mobile. Tap **Approve**.



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



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

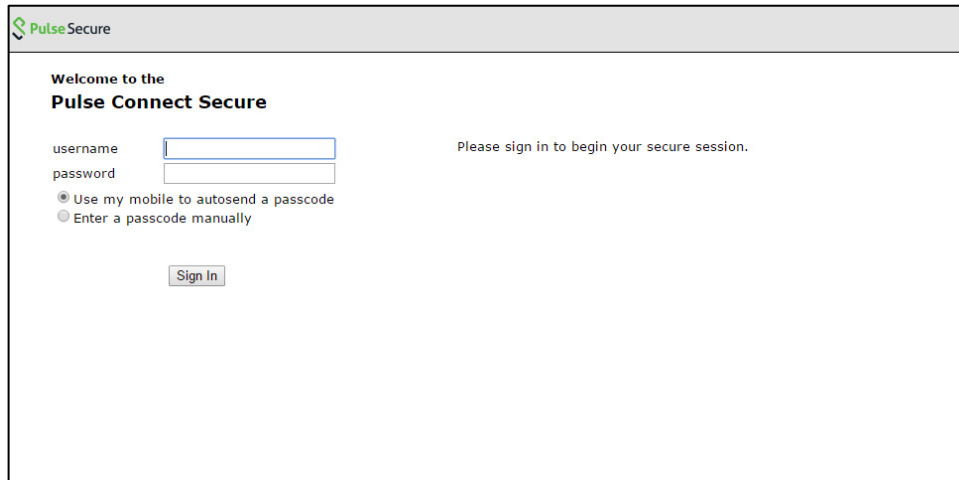


(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)

Connecting to the Pulse Connect Secure Portal using Hybrid Mode

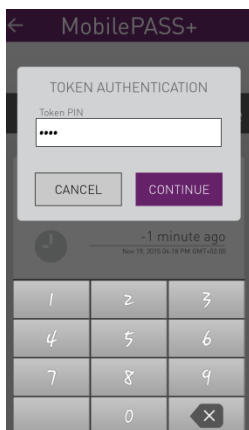
In the following scenario, the hybrid mode login screen is used, and you will have the option to choose between authentication using the Push OTP notification message, or manually typing a passcode.

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

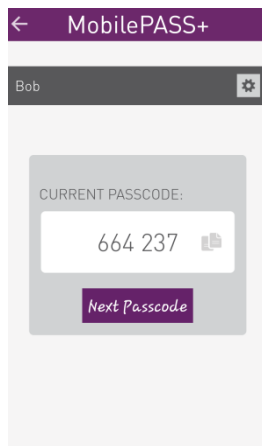


(The screen image above is from Pulse Secure®. Trademarks are the property of their respective owners.)

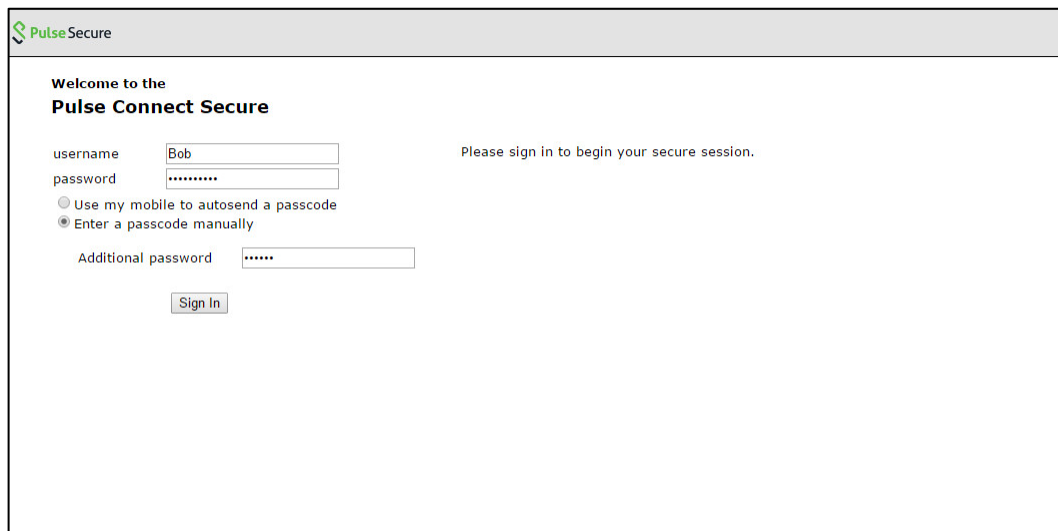
2. Enter your LDAP credentials, and then choose one of the following:
 - **Use my mobile to autosend a passcode**—If you choose this option, a push notification will be sent to your mobile. Follow the steps as described in the previous scenario.
 - **Enter a passcode manually**—If you choose this option, 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**.



- You will receive a passcode.

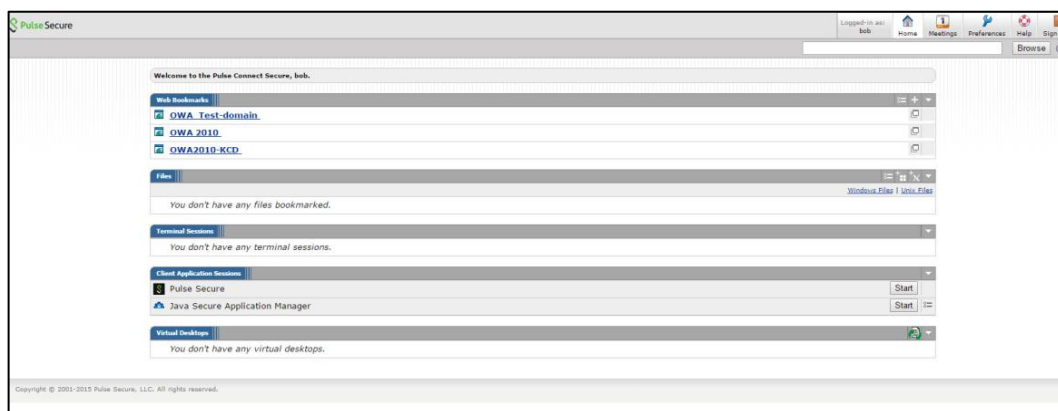


- In the Pulse Connect Secure console, in the **Additional password** field, enter the passcode, and then click **Sign In**.



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

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



(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
	International	1-410-931-7520
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.	