

# SafeNet Authentication Service (SAS)

Push OTP Solution Guide

All information herein is either public information or is the property of and owned solely by Gemalto 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.

© 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto 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:** 007-013306-001, Rev. F

**Release Date:** May 2017

# Contents

<b>Preface</b> .....	<b>5</b>
Introduction .....	5
Audience .....	5
Terminology .....	5
Support Contacts .....	7
<b>1 Overview</b> .....	<b>8</b>
Why Push OTP? .....	8
Improved User Experience.....	8
Automatic, Out-of-Band OTP Delivery .....	9
Push OTP Authentication Flow Diagram.....	9
<b>2 Getting Started</b> .....	<b>10</b>
Requirements and Considerations .....	10
Application Integration.....	11
Deployment Considerations .....	11
Token Types and Licenses .....	12
Checklists .....	13
<b>3 Enable Push OTP and MobilePASS+ for the Virtual Server</b> .....	<b>15</b>
Enable the Push OTP Policy .....	15
Set Policies .....	16
Set the Allowed Targets Policy .....	16
Set the Push OTP Rejection Policy (Optional).....	17
Set the Operator Policy (Optional) .....	19
Customize Push Notifications .....	20
Set the Custom Organization Name .....	20
Set the Auth Node Resource Name.....	21
Customize the Push Notification Rejection Alert for the User (Optional) .....	22
Customize the Push Notification Rejection Alert for the Internal Operator (Optional).....	23
Customize the Self-Enrollment Email Template and Self-Enrollment Page (Optional).....	23
<b>4 Set Up Applications for Push OTP</b> .....	<b>24</b>
Agents with Rich User Experience .....	24
SAS Cloud SAML Service Configuration .....	25
AD FS Agent Configuration .....	25
SAS Cloud RADIUS Service.....	26
SAS Cloud RADIUS Configuration.....	26
Agents with Simple Mode User Experience .....	27
SAS Agent for NPS 2.0 Configuration.....	27

<b>5</b>	<b>Token Management and Enrollment .....</b>	<b>28</b>
	Token Enrollment Process.....	28
	Viewing Device Information About MobilePASS Tokens .....	29
	Token Reports .....	30
	Users – With Tokens Report .....	30
<b>6</b>	<b>Push OTP Authentications .....</b>	<b>31</b>
	Triggering Push Notifications in the Agent .....	31
	Simple Mode .....	31
	Rich User Experience.....	32
	Push Notification Contents .....	33
	What Happens... .....	34
	...when a user accepts a push notification? .....	34
	...when a user denies a push notification? .....	34
	...if a push notification times out? .....	34
	...if a user is challenged for an OTP to re-sync the token? .....	34
	Authentication Activity Logging.....	35
	Push Notification Reports .....	35
	Push OTP Authentication History Report.....	35

# Preface

## Introduction

This document provides an overview of the Push OTP solution in SAS, highlights what you will need to get started, and the detailed steps to enable the end-to-end solution.

For comparative information on MobilePASS vs. MobilePASS+, migration details, deployment considerations, and MobilePASS+ FAQs (ordering, licensing, allocation, token enrollment, etc.), please refer to the *Push OTP Planning Guide*.

## Audience

This guide is intended for SafeNet Authentication Service system administrators who want to deploy Push OTP for their users.

## Terminology

Term	Definition
<b>Agent</b>	<ul style="list-style-type: none"> <li>The software from which the authentication operation enters the SAS system. It can be an agent deployed in the SAS Cloud service, or an on-premises agent.</li> </ul>
<b>MobilePASS App</b>	<ul style="list-style-type: none"> <li>This is an application that turns your mobile phone into a two-factor authentication device. This mobile app acts as a container for the tokens used for authentication for one or more users. An integrated support feature allows administration directly from the <b>Token Management</b> module in the SAS Management Console. <b>MobilePASS</b> allows users to enroll, activate, and use their tokens without administrative assistance.</li> <li>There are two variations of MobilePASS:</li> <li><b>MobilePASS 8</b>: Supports manual OTP on iOS, Android, BlackBerry, Mac OS X, and Windows platforms.</li> <li><b>MobilePASS+</b>: Supports manual OTP as well as Push OTP, which is the ability to accept push notifications and then, in turn, generate and push a one-time password (OTP) back to SAS. Supported on iOS and Android platforms.</li> </ul>
<b>MobilePASS Token</b>	<ul style="list-style-type: none"> <li>A token that is provisioned onto the MobilePASS or MobilePASS+ app. Each token is related to an account and its associated parameters, such as name, user PIN, enrolled keys, and PIN policy.</li> <li>A MobilePASS token has a unique value (seed) used to generate an OTP value for authentication. When the token is enrolled, it is associated with a user on SAS.</li> </ul>
<b>OTP (One-time Password)</b>	<ul style="list-style-type: none"> <li>An automatically generated password (also referred to as a <i>passcode</i>), consisting of a 6- or 8-digit code, which is used as a second factor during authentication. With Push OTP, the passcode is sent automatically—there is no</li> </ul>

Term	Definition
	need for the user to manually open the MobilePASS app and type the passcode into the agent.
<b>Protected Resource</b>	<ul style="list-style-type: none"><li>Any part of a computer system or network, such as a web page, cloud, or VPN, requiring authentication to enable access.</li></ul>
<b>Push Notification</b>	<ul style="list-style-type: none"><li>An authentication request that is sent to the user's mobile device. The user can respond to the request directly with the push notification, or by tapping on the push notification to open the MobilePASS+ application, and then responding within the app. This authentication request includes user actions to either accept or reject the notification. Choose Accept to automatically send the generated OTP to SAS.</li></ul>
<b>Push Notification Service Provider</b>	<ul style="list-style-type: none"><li>Apple or Google. They provide the service that delivers a Push Notification message to an application on the user's mobile phone (in our case, to MobilePASS+).</li></ul>
<b>Push OTP</b>	<ul style="list-style-type: none"><li>The On-the-Go (OTG) solution in SAS to send push notifications and process responses. Push OTP simplifies the process of accessing a protected resource, such as a web page, cloud, or VPN.</li></ul>
<b>User</b>	<ul style="list-style-type: none"><li>A user on an instance of a Virtual SAS Server. A user can be provisioned with one or more MobilePASS tokens.</li></ul>

## 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	
<b>Address</b>	<ul style="list-style-type: none"> <li>• Gemalto</li> <li>• 4690 Millennium Drive</li> <li>• Belcamp, Maryland 21017, USA</li> </ul>	
<b>Phone</b>	• US	1-800-545-6608
	• International	1-410-931-7520
<b>Technical Support Customer Portal</b>	<ul style="list-style-type: none"> <li>• <a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></li> <li>• 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.</li> </ul>	

# 1 Overview

## Why Push OTP?

### Improved User Experience

The Push OTP solution leverages out-of-band communication channels to provide a frictionless user experience around two-factor authentication with a mobile phone.

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. The addition of out-of-band delivery of passcodes takes convenience one step further—it means users no longer have to manually find the application to open it and then type anything in. 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.

### How Does Login with Push OTP Work?

When a user wants to access an application that supports Push OTP, he makes the choice to login with push OTP by either selecting the option, or by leaving the OTP field empty or typing a 1-character passcode. (Refer to “Triggering Push Notifications in the Agent” on page 31 for details.) This cues SAS to send a push notification out-of-band to the user’s mobile device requesting for login authorization. When the push notification arrives on the user’s mobile device, he can respond to the request directly on the push notification, or tap on the notification to load additional request details within the MobilePASS+ application, and then respond.



**NOTE:** The login method will depend on the integration—refer to “Set Up Applications for Push OTP” on page 24 for details.

The SAS login request requires the user to either accept or reject the notification. Accepting the notification will automatically generate an OTP and send it to SAS via a secure out-of-band communication channel. (The ability to respond directly on the push notification is largely dependent on the operating system of the mobile device. Later versions of the OS have this capability, while earlier ones may not.) Once the OTP authentication is validated by SAS, access to the requesting application will automatically be granted.

See “Push OTP Authentication Flow Diagram” on page 9.



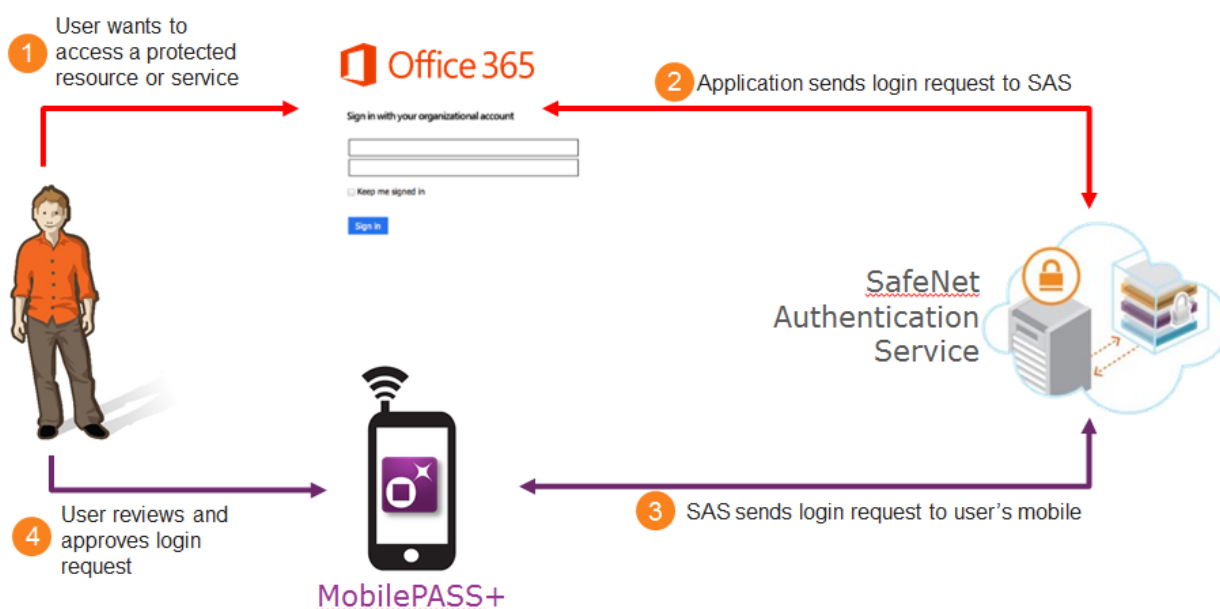
## Automatic, Out-of-Band OTP Delivery

Using out-of-band (OOB) authentication provides improved usability compared to traditional offline or disconnected authentication methods, without compromising security.

With Push OTP, there is no longer the need to manually type in a 6- or 8-digit OTP to access a protected application every time. Now, a user can verify the validity of a pending authentication request directly on his mobile device, and approve it with one tap. Approval automatically triggers an OTP to be delivered to SAS through an OOB channel.

## Push OTP Authentication Flow Diagram

The image below describes the Push OTP authentication flow. Some applications will work by leaving the OTP field empty or by typing a 1-character passcode, while others will work by presenting the user with a choice on the login screen. This will vary, based on the integration. (Refer to “Triggering Push Notifications in the Agent” on page 31 for details.)



1. The user wants to access an application which requires two-factor authentication (for example, Office 365). He provides his user name and password, and then clicks the **Sign In** button.
2. The application sends the login requests to the server, which identifies the user and his mobile device.
3. The server will directly trigger an on-the-go authentication request. If push is used, the user receives a push notification on his mobile to indicate there is a login request pending.



**NOTE:** The integrated application (for example, Office 365) determines if it supports push or not. If it does, then a push is triggered.

4. The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request. (In some cases, the user may need to provide an additional PIN before he is permitted to view and respond to the login request.) The response (with a passcode attached) is sent back to the server, where it is validated, and when the authentication succeeds, the application is automatically refreshed, and access is granted to the user.

# 2

## Getting Started

### Requirements and Considerations

- Push OTP is supported in SAS Cloud version 3.5 or later.
- MobilePASS is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x, 5.x
    - iOS 7+
  - MobilePASS 8 (**no** Push OTP support)
    - Android 2.3+
    - BlackBerry 10 10.2+
    - BlackBerry Java
      - BB Curve 9320/OS 7.1
      - BB Torch 9800/OS 6.0
      - BB Bold Touch 9900/OS 7.0
      - BB Torch 9860/OS 7.1
      - BB 9700 (Bold)/running v5.0.0.979
      - BB 9810 (Torch)/running v7.1.0.714
      - BB 9900/OS 7.1
    - iOS 6+
    - Mac OS X 10.9 and 10.10
    - Windows 7, 8, 8.1, and 10
    - Windows Phone 8.1+
    - Windows RT 8.1+
- Network access to use push and grant push permissions is required.
- SAS cannot guarantee the delivery of a push notification, since this is under the control of the push notification service providers (Apple and Google), as well as other factors, such as network connectivity. If a push notification is not delivered, users can always fallback to manual OTP authentication.
- **For existing customers:** A new token **must** be enrolled on MobilePASS+ to be able to use push.

## Application Integration

Any application that is integrated through SAS Cloud RADIUS Service (FreeRADIUS), SAS Cloud SAML Service, or AD FS Agent can support Push OTP. Note that the new SAS AD FS Agent **must** be installed. For additional details, please refer to “Set Up Applications for Push OTP” on page 24.

The following table is a list of applications that currently have integration guides available for Push OTP. These documents describe how to deploy multi-factor authentication (MFA) options in third-party applications using MobilePASS+ managed by SAS.

Simple mode is available for all SAS Cloud RADIUS Service integrations. With simple mode, if Push OTP is enabled, the user can trigger a push notification by leaving the passcode field empty, or by entering any 1-character passcode (excluding “s” or “g” if either SMS or Gridsure tokens are present). Refer to “Triggering Push Notifications in the Agent” on page 31 for details.

Third-party	Integration Guide Description
<b>Blue Coat</b>	<ul style="list-style-type: none"> <li>Push OTP Integration Using RADIUS Protocol for Blue Coat Proxy SG</li> </ul>
<b>Check Point</b>	<ul style="list-style-type: none"> <li>Push OTP Integration Using RADIUS Protocol for Check Point Security</li> </ul>
<b>Cisco</b>	<ul style="list-style-type: none"> <li>Push OTP Integration Using LDAP and RADIUS Protocol for Cisco</li> </ul>
<b>Citrix</b>	<ul style="list-style-type: none"> <li>Push OTP Integration Using RADIUS Protocol for Citrix NetScaler Access Gateway 11</li> </ul>
<b>F5</b>	<ul style="list-style-type: none"> <li>Push OTP Integration Using RADIUS Protocol for F5 BIG-IP APM</li> </ul>
<b>Microsoft</b>	<ul style="list-style-type: none"> <li>Push OTP Using SafeNet Authentication Service as an Identity Provider for:               <ul style="list-style-type: none"> <li>Microsoft Office 365</li> <li>Microsoft Office 365 ProPlus</li> <li>Microsoft Dynamics CRM</li> </ul> </li> </ul>
<b>Pulse Secure</b>	<ul style="list-style-type: none"> <li>Push OTP Integration Using RADIUS Protocol for Pulse Connect Secure</li> </ul>
<b>SonicWall</b>	<ul style="list-style-type: none"> <li>Push OTP Integration Using RADIUS Protocol for SonicWALL Secure Remote Access</li> </ul>

## Deployment Considerations

Before deploying MobilePASS+ with Push OTP, consider the following:

- If your users are primarily Android and iPhone users, then deploy MobilePASS+.
- If your apps are listed in the integration table (in the previous section), or integrated using SAML, then deploy MobilePASS+.
- If your users or apps do not, or only possibly meet the criteria above, then clarify the scope. For example, if your users are iPhone and BlackBerry users, then Push OTP is only available to your iPhone users, and BlackBerry users must continue to use MobilePASS 8.

If this is acceptable, then deploy MobilePASS+ for your iPhone users.

- How do I migrate current users?

Existing MobilePASS tokens on MobilePASS 8 cannot be used for MobilePASS+. Users who are currently using MobilePASS tokens will need to enroll new MobilePASS tokens on MobilePASS+ in order to use Push OTP.

You will need MobilePASS tokens in inventory to migrate users from MobilePASS 8 to MobilePASS+. After users have enrolled new tokens in MobilePASS+, you can revoke their tokens in MobilePASS 8, return them to inventory, and then reuse them to migrate more users from MobilePASS 8 to MobilePASS+.

## Token Types and Licenses

There is no difference between MobilePASS+ and MobilePASS 8 token types, or in terms of commercial license and pricing, allocations, provisioning tasks, and auto-provisioning rules.

## Checklists

### Set Up Push OTP for New Accounts Created in SAS 3.5

<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Review/select the <b>Allowed Targets Settings</b> in the SAS Management Console.</li> <li>• By default, <b>all</b> platforms are configured to MobilePASS 8. For MobilePASS+, make any changes to the platform(s) you want to deploy Push OTP on.</li> <li>• See “Set the Allowed Targets Policy” on page 16.</li> <li>• Note that one MobilePASS application per OS type can be selected. For example, you can enable iOS for either MobilePASS+ or MobilePASS 8, but not both.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• (Optional) Configure user and operator policies for rejected push notifications.</li> <li>• See “Set the Push OTP Rejection Policy (Optional)” on page 17.</li> <li>• See “Set the Operator Policy (Optional)” on page 19.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Allocate MobilePASS tokens. MobilePASS 8 and MobilePASS+ use the same token type.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• (Optional) Customize the user and operator push notification rejection alert messages, and the email template and self-enrollment page.</li> <li>• See “Customize the Push Notification Rejection Alert for the User (Optional)” on page 22.</li> <li>• See “Customize the Push Notification Rejection Alert for the Internal Operator (Optional)” on page 23.</li> <li>• See “Customize the Self-Enrollment Email Template and Self-Enrollment Page (Optional)” on page 23.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Configure application integrations to support Push OTP by one of the following:</li> <li>• Install and configure the new SAS AD FS Agent 2.0.</li> <li>• Set the combination of RADIUS timeout and retry values to at least 60 seconds for SAS Cloud RADIUS Service (FreeRADIUS). For example:             <ul style="list-style-type: none"> <li>○ Multiple NPS servers (backup/failover):                 <ul style="list-style-type: none"> <li>▪ Timeout: 60 seconds</li> <li>Retries: 1</li> </ul> </li> <li>○ Single NPS server:                 <ul style="list-style-type: none"> <li>▪ Timeout: 20 seconds</li> <li>Retries: 3</li> </ul> </li> </ul> </li> <li>• Configure SAML services to display Push OTP user controls on the SAML <b>Login</b> page.</li> <li>• Deploy SAS Agent for NPS 2.0.</li> </ul> <p>See “Set Up Applications for Push OTP” on page 24.</p>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Provision MobilePASS tokens to users.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Users must download the MobilePASS+ app and complete the self-enrollment. See “Token Management and Enrollment” on page 28. Refer also to the <i>MobilePASS+ User Guide</i> for details.</li> </ul>

## Set Up Push OTP for Existing Accounts

<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Enable Push OTP. By default, the feature is disabled. See “Enable the Push OTP” on page 15.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Review/select the <b>Allowed Targets Settings</b> in the SAS Management Console.</li> <li>• By default, <b>all</b> platforms are configured to MobilePASS 8. For MobilePASS+, make any changes to the platform(s) you want to deploy Push OTP on.</li> <li>• See “Set the Allowed Targets Policy” on page 16.</li> <li>• Note that one MobilePASS application per OS type can be selected. For example, you can enable iOS for either MobilePASS+ or MobilePASS 8, but not both.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• (Optional) Configure user and operator policies for rejected push notifications.</li> <li>• See “Set the Push OTP Rejection Policy (Optional)” on page 17.</li> <li>• See “Set the Operator Policy (Optional)” on page 19.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Allocate additional MobilePASS tokens. MobilePASS 8 and MobilePASS+ use the same token type.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• (Optional) Revoke MobilePASS 8 tokens that are no longer needed.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Enroll a new token on MobilePASS+ to use Push OTP.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• (Optional) Customize the user and operator push notification rejection alert messages, and the email template and self-enrollment page.</li> <li>• See “Customize the Push Notification Rejection Alert for the User (Optional)” on page 22.</li> <li>• See “Customize the Push Notification Rejection Alert for the Internal Operator (Optional)” on page 23.</li> <li>• See “Customize the Self-Enrollment Email Template and Self-Enrollment Page (Optional)” on page 23.</li> </ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Configure application integrations to support Push OTP by one of the following: <ul style="list-style-type: none"> <li>• Install and configure the new SAS AD FS Agent 2.0.</li> <li>• Set the combination of RADIUS timeout and retry values to at least 60 seconds for SAS Cloud RADIUS Service (FreeRADIUS). For example: <ul style="list-style-type: none"> <li>○ Multiple NPS servers (backup/failover): <ul style="list-style-type: none"> <li>▪ Timeout: 60 seconds</li> <li>Retries: 1</li> </ul> </li> <li>○ Single NPS server: <ul style="list-style-type: none"> <li>▪ Timeout: 20 seconds</li> <li>Retries: 3</li> </ul> </li> </ul> </li> <li>• Configure SAML services to display Push OTP user controls on the SAML <b>Login</b> page.</li> <li>• Deploy SAS Agent for NPS 2.0.</li> </ul> <p>See “Set Up Applications for Push OTP” on page 24.</p> </li></ul>
<input type="checkbox"/>	<ul style="list-style-type: none"> <li>• Users must download the MobilePASS+ app and complete the self-enrollment. See “Token Management and Enrollment” on page 28. Refer to the <i>MobilePASS+ User Guide</i> for details.</li> </ul>

# 3

## Enable Push OTP and MobilePASS+ for the Virtual Server

For Push OTP to be permitted during authentication, the Push OTP feature must be enabled, and the user must have a token on the MobilePASS+ application. Furthermore, the user must have permitted MobilePASS+ push notifications for their mobile devices to receive push notifications.

### Enable the Push OTP Policy

---

The Push OTP functionality is enabled by default for newly created accounts, and disabled by default for upgraded accounts. Push OTP can be enabled (or disabled) at any time.

When Push OTP is disabled on the virtual server side, the MobilePASS+ application will not ask the user to grant push permissions. Enabling Push OTP is independent per virtual server. Complete these steps on any virtual server that should support Push OTP:

1. Go to **POLICY > Token Policies**.
2. Click **Software Token Push OTP Setting**.
3. Select **Enable Push OTP communication with MobilePASS+**.
4. Under **Allowed Targets Settings > MobilePASS+**, select:
  - **iOS** to enable MobilePASS+ on iOS devices and support features such as Touch ID for iOS.
  - **Android** to enable MobilePASS+ on Android devices and support features such as Biometric PIN.
5. Click **Apply**.

**Token Policies**
i - ?

Use these policies to customize the operation of tokens and how they interact with the authentication service.

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

**Software Token Push OTP Setting**

Apply
Cancel
Change Log

Enable Push OTP communication with MobilePass+

---

**Allowed Targets Settings**

**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.


## Set Policies

### Set the Allowed Targets Policy

For Push OTP to be permitted during authentication, the user must have a token enrolled in the MobilePASS+ application. The settings that you enable in this policy will determine which targets are presented to users during the self-enrollment of MobilePASS tokens. You can restrict the OS types on which MobilePASS tokens are allowed to be activated/enrolled. The default settings on this screen will depend on whether your account is newly created or upgraded.

1. Go to **POLICY > Token Policies**.
2. Click **Allowed Targets Settings**.
3. On the **MobilePASS** tab, select the desired OS types as allowed targets. Then click **Apply**.  
 For iOS and Android, you can choose between MobilePASS 8 and MobilePASS+.  
 By default, **all** platforms are selected to deploy for MobilePASS 8. Enable **iOS** or **Android** (or both) for MobilePASS+ in order to use Push OTP.





**For newly created accounts:** Review/select the platform assignments. By default, **iOS** and **Android** are configured to MobilePASS+, and all other platforms are configured to MobilePASS 8. Make any changes to the platform(s) you want to deploy MobilePASS tokens on.

**For upgraded accounts:** Review/select the platform assignments. By default, **all** platforms are selected to deploy for MobilePASS 8. You will need to enable **iOS** or **Android** (or both) for MobilePASS+ in order to use Push OTP.



**NOTE:** One MobilePASS application per OS type can be selected. For example, you can enable **iOS** for either MobilePASS+ or MobilePASS 8, but not both.

You can enroll a new MobilePASS+ token in parallel to an existing MobilePASS 8 token.

## Set the Push OTP Rejection Policy (Optional)

Push notifications are only sent to registered devices with currently active, push-enabled tokens. If a user receives a push notification that he or she did not initiate and the notification is rejected, setting this user policy will automatically email a Push Notification Rejection Alert to the user (see example below). If the user's account gets locked due to this Push OTP rejection, the body of the Push Notification Rejection Alert is appended to the User Lockout Alert that is sent to the user.



**NOTE:** You can customize the contents of the alert email in **COMMS > Communications > Email Messages**. See “Customize the Push Notification Rejection Alert for the User (Optional)” on page 22.

1. Go to **POLICY > User Policies**.
2. Select **Push OTP Rejection Policy**.
3. Select **Alert user on OTP push notification rejected**, and then click **Apply**.

**User Policies**

Use these policies to set users' access to the authentication service.

Task	Description
<a href="#">Account Lockout/Unlock Policy</a>	Set the conditions under which the server will automatically lock and/or unlock a user account.
<a href="#">Dormant Account Lockout Policy</a>	Set conditions for locking accounts which have become dormant.
<a href="#">Push OTP Rejection Policy</a>	Enable sending email alerts when users reject OTP push notifications.

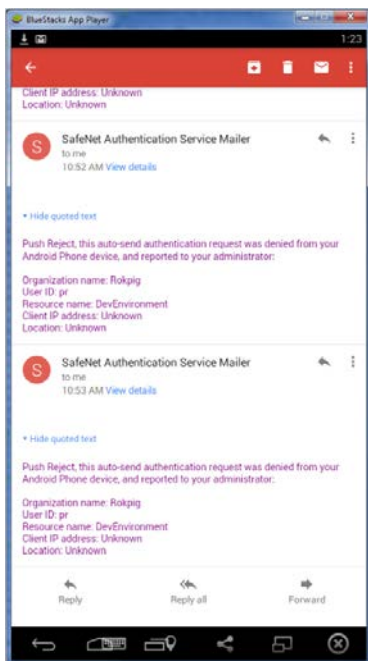
**Push OTP Rejection Policy**

Apply Cancel Change Log

The policy determines if an email alert is sent when user rejects an OTP push notification.

Alert user on OTP push notification rejected

### Sample Push Notification Rejection Alert to User



## Set the Operator Policy (Optional)

If a user receives a push notification that he or she did not initiate and the notification is rejected, setting this operator policy will automatically send a Push Notification Rejection Alert to the operator so that logs can be investigated if necessary.



**NOTE:** You can customize the contents of the alert email in **COMMS > Communications > Email Messages**. See “Customize the Push Notification Rejection Alert for the Internal Operator (Optional)” on page 23.

1. Go to **POLICY > Role Management > Alert Management**.
2. Click the corresponding **Edit** hyperlink for a role.
3. Select **Push Notification Rejection Operator Alert** for the desired delivery method(s), and then click **Apply**.

**Role Management**

Use these policies to set operator roles and the appearance of the Administration console.

Task	Description
<a href="#">Role Management</a>	Create roles by grouping management functions found on tabs and modules.
<a href="#">Alert Management</a>	Set which email and/or SMS event alerts that operators will receive, according to their role.
<a href="#">External Alerts Recipients</a>	Create a list of external recipients for email and/or SMS event alerts.
<a href="#">Event Thresholds</a>	Set the conditions under which alerts will be sent.
<a href="#">Language</a>	Set the language
<a href="#">Allowed Management IP Range</a>	Restrict logon to an account's SAS management UI to a specified IP range

**Alerts Management:**

[Cancel](#)

Name	Description	<a href="#">Edit</a>
Operator	Grants unrestricted rights to manage this authentication service. (Default)	<a href="#">Edit</a>

Displaying: 1 to 1 of 1

**Alerts Settings: Operator**

[Apply](#) [Cancel](#)

E-mail	SMS	Event Name
<input type="checkbox"/>	<input type="checkbox"/>	Organization Capacity
<input type="checkbox"/>	<input type="checkbox"/>	Account SMS Credits
<input type="checkbox"/>	<input type="checkbox"/>	Operator Status Change
<input type="checkbox"/>	<input type="checkbox"/>	Expired Reservation
<input type="checkbox"/>	<input type="checkbox"/>	Enrollment Lock out
<input type="checkbox"/>	<input type="checkbox"/>	Hardware Assignment Notification
<input type="checkbox"/>	<input type="checkbox"/>	Hardware Provisioning Notification
<input type="checkbox"/>	<input type="checkbox"/>	LDAP Sync Notification
<input type="checkbox"/>	<input type="checkbox"/>	Service Notifications
<input type="checkbox"/>	<input type="checkbox"/>	Provisioning Notification
<input type="checkbox"/>	<input type="checkbox"/>	Operator Lockout Alert
<input type="checkbox"/>	<input type="checkbox"/>	Operator Unlock Alert
<input type="checkbox"/>	<input type="checkbox"/>	Auth Node Changes
<input type="checkbox"/>	<input type="checkbox"/>	Allocation/Deallocation Alert
<input type="checkbox"/>	<input type="checkbox"/>	Lost Token Report
<input type="checkbox"/>	<input type="checkbox"/>	Dormant Account Alert
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Organization Stop Date
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sync Host Notification
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Push Notification Rejection Operator Alert

## Sample Push Notification Rejection Alert to Operator



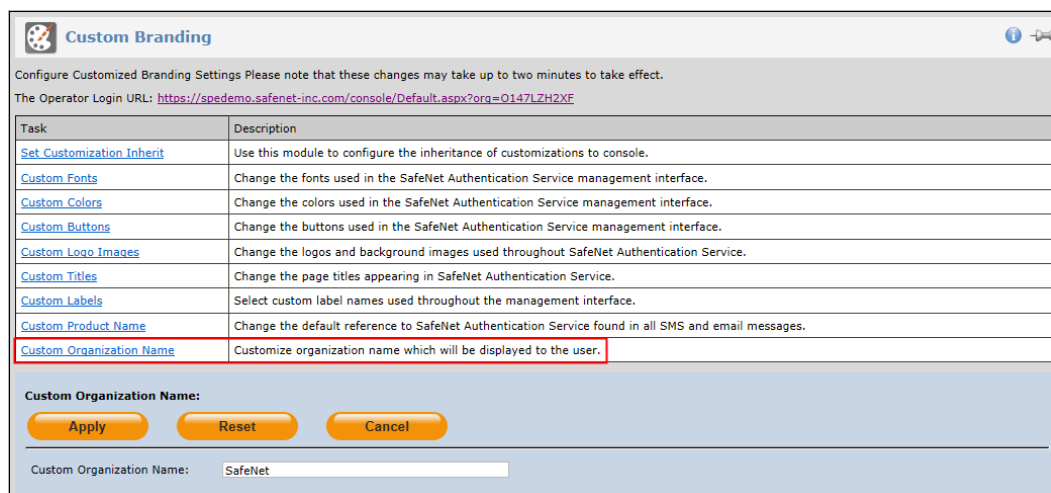
## Customize Push Notifications

### Set the Custom Organization Name

A **Custom Organization Name** is defined for each virtual server. By default, the **Custom Organization Name** is the existing operator-facing account name, and it does not have to be unique if there are multiple virtual servers. This name is included in the login request details on a user's mobile device.

Complete these steps to change the organization name on each virtual server:

1. Go to **COMMS > Custom Branding**.
2. Select **Custom Organization Name**.
3. Enter the desired organization name, and then click **Apply**.



## Set the Auth Node Resource Name

In a push notification, the **Resource Name** identifies which authentication node it relates to, so the user can be sure he is authenticating a valid node. Refer to “Push Notification Contents” on page 33 to see an example.

By default, the **Resource Name** is the existing operator-facing **Auth Node Name** (this field was formerly called **Agent Description**). Unlike the **Auth Node Name**, the **Resource Name** does not have to be unique.



**NOTE:** For SAML services, the **Resource Name** is configured per SAML service. Refer to “SAS Cloud SAML Service Configuration” on page 25 for configuration details.

To customize the name:

1. Go to **COMMS > Auth Nodes**.
2. Click the **Auth Nodes** hyperlink.
3. Click **Edit** for the auth node to customize.
4. On the **Auth Nodes** tab, enter the **Resource Name**, and then click **Save**.

The screenshot shows the 'Auth Nodes' configuration page. At the top, there's a table with columns 'Task' and 'Description'. Below that, there's a section for 'Auth Nodes' with buttons for 'Add', 'Change Log', and 'Cancel'. A table lists existing auth nodes with columns for Index, Auth Node Name, Host Name, IP Address, FreeRADIUS Synchronization, Edit, and Remove. The 'Edit Auth Node' form is open, showing the 'Resource Name' field highlighted in red. The form includes fields for Auth Node Name, Resource Name, Host Name, Low IP Address In Range, High IP Address In Range, Shared Secret, and Confirm Shared Secret. There are also checkboxes for 'Exclude from PIN change requests' and 'Configure FreeRADIUS Synchronization'.



**NOTE:** An Auth Node Change alert is generated if the **Resource Name** is changed.

## Customize the Push Notification Rejection Alert for the User (Optional)

1. Go to **COMMS > Communications > Email Messages**.
2. Under **Customize Email Messages**, click **Custom**.
3. Select **Push Notification Rejection User Alert** from the **Email Message Type** menu.

Configure email and SMS communication settings.

Task	Description
<a href="#">SMS Settings</a>	Configure the settings for SMS plugins.
<a href="#">Email Settings</a>	Configure connection settings for the email server.
<a href="#">SMS Messages</a>	Customize the text and formatting of SMS messages.
<b><a href="#">Email Messages</a></b>	Customize the text and formatting of email messages.
<a href="#">LDAP Sync Server Settings</a>	Set URL and port for the LDAP Sync Server.
<a href="#">FTP/SFTP/SCP Settings</a>	Customize the settings for FTP/SFTP/SCP transfer of reports.
<a href="#">Logging Agent Server Settings</a>	Set URL and port for the Logging Agent Server.

**Customize Email Messages**

Default  Custom  
Applying defaults (clicking Default then Apply) resets all messages to those of your parent service provider.

Email Message Type: Push Notification Rejection User Alert

Format:  Text  HTML

Subject:

Body:

SMS Content: 
 Max 160 chars.

4. Modify the contents as needed, and then click **Apply**.

## Customize the Push Notification Rejection Alert for the Internal Operator (Optional)

1. Go to **COMMS > Communications > Email Messages**.
2. Under **Customize Email Messages**, click **Custom**.
3. Select **Push Notification Rejection Internal Operator Alert** from the **Email Message Type** menu.

The screenshot shows the 'Communications' configuration page in the SAS Self-Service Administrator. The 'COMMS' tab is active. Under 'Customize Email Messages', the 'Custom' radio button is selected. The 'Email Message Type' dropdown menu is set to 'Push Notification Rejection Internal Operator Alert'. The 'Format' is set to 'Text'. The 'Subject' field contains the placeholder text: '<productName /> Push Notification Rejection Alert'. The 'Body' field contains the following text: 'The user account <userName /> in organization <organization /> denied and reported a push notification: Organization name: <organizationName /> Resource name: <resourceName /> Client IP address: <clientIP /> Location: <clientLocation />'. The 'SMS Content' field contains: 'Account <userName /> in <organizationName /> denied and reported a push notification. Max 160 chars.'

4. Modify the contents as needed, and then click **Apply**.

## Customize the Self-Enrollment Email Template and Self-Enrollment Page (Optional)

If desired, you can customize the Self-Enrollment email template and Self-Enrollment page. Please refer to the *SAS Self-Service Administrator Guide*, and either the *Service Provider Administrator Guide* or *Subscriber Account Operator Guide* for details.

## 4

# Set Up Applications for Push OTP

Any application that is integrated through SAS Cloud RADIUS Service (FreeRADIUS), SAS Cloud SAML Service, AD FS Agent, or SAS Agent for NPS 2.0 can support Push OTP. The agents provide two user interaction models:

- Rich user experience, which is provided by the SAS Cloud SAML Service and AD FS Agent
- Simple mode, which is provided by the SAS Cloud RADIUS Service



**NOTE:** Some of the web-based RADIUS clients (for example, F5, NetScaler, Citrix, etc.) require application integration. Please refer to the appropriate integration guide for details (see the list in “Application Integration” on page 10).

## Agents with Rich User Experience

SAS Cloud SAML Service and agents such as AD FS provide a rich user experience, as compared to the simple mode in the SAS Cloud RADIUS integration.

With the rich user experience, logging into a protected application will redirect the user to a modified login screen, which presents options to choose between push or manual passcode entry. In addition, users have the ability to cancel a push notification.



Figure 1 - AD FS Agent

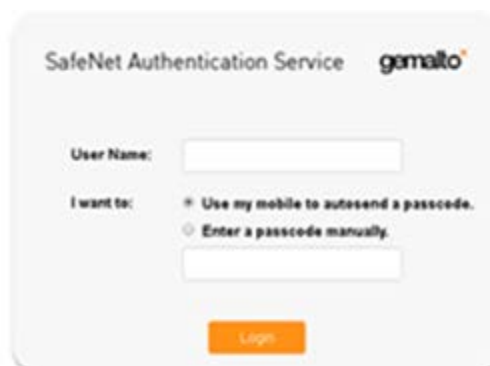


Figure 2 - SAML Service



**NOTE:** The passcode triggers to override Push OTP (described in “Triggering Push Notifications in the Agent” on page 31) apply to the push behavior for AD FS Agent and SAML login.



## SAS Cloud SAML Service Configuration

A SAML service can be customized to change how Push OTP is displayed on the SAML **Login** page.

1. In the SAS Management Console, enable and customize Push OTP text for the SAML **Login** page.
  - Go to **COMMS > SAML Service Providers > SAML 2.0 Settings**.
  - Under **Custom Login UI**, select the **Enable Push/Manual OTP Selector** check box to display controls on the SAML **Login** page for selecting between Push OTP and manually entering the OTP.
  - Optionally, modify the following descriptors to customize the SAML **Login** page:
    - **Push/Manual OTP Selector Text**: Enter the text to replace “**I want to:**”
    - **Push OTP Button Text**—Enter the text to display for the option to use Push OTP.
    - **Manual OTP Button Text**—Enter the text to display for the option to use a manual OTP.
  - Customize the remaining Push OTP processing, cancellation, and authentication descriptors, as needed.



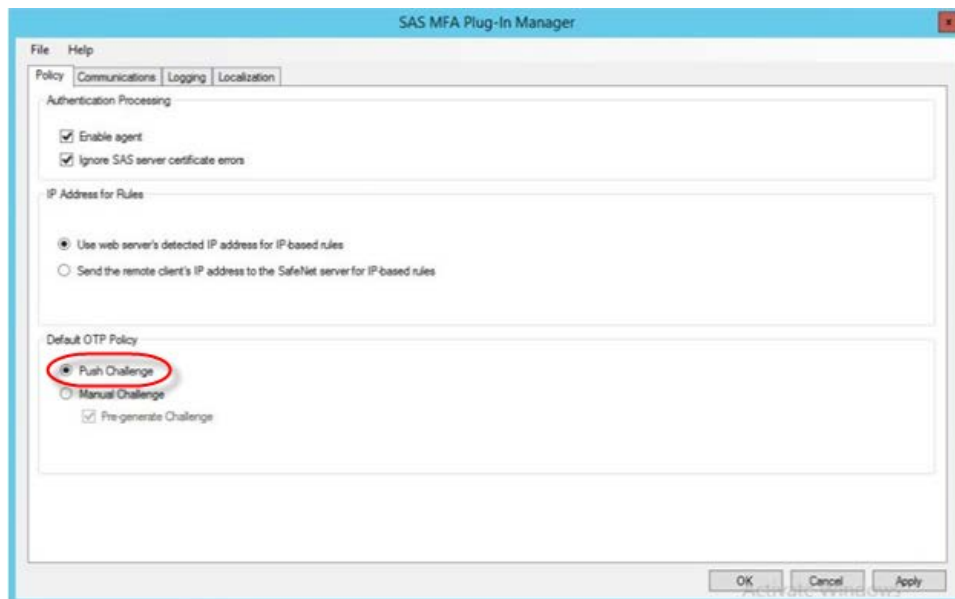
**NOTE:** If the **Enable Push/Manual OTP Selector** option is disabled, the user can still trigger push or another challenge/response method with an empty passcode. Refer to “Triggering Push Notifications in the Agent” on page 31 for details.

## AD FS Agent Configuration

1. Install the new **SAS AD FS Agent v2.0** with Push OTP support.
2. Configure the SAS AD FS Agent to use Push OTP.
  - a. Select **Start > All Programs > SafeNet > Agents > ADFS Agent** (run as administrator).
  - b. On the **SAS MFA Plug-In Manager** window, click the **Policy** tab.
  - c. Under **Default OTP Policy**, click **Push Challenge**, and then click **Apply**.



**NOTE:** By choosing the **Push Challenge** option, the AD FS integration will automatically promote push. The user will be presented with the option to use either push or manual passcode entry.



For additional information, please refer to the *SafeNet Authentication Service AD FS Agent Configuration Guide* and the *AD FS Customer Release Notes*.

## SAS Cloud RADIUS Service

This type of application integration presents a simple user experience, which cannot be modified. Please note the following behavioral changes:

- Unlike the AD FS Agent, the login screen cannot be modified. Therefore, users will not be presented with options to either select push or use manual passcode entry. To trigger Push OTP, users will need to be instructed to leave the password field empty, or type any 1-character passcode on the login screen.
- If your users were previously using GrIDSure or SMS: Note that when deploying Push OTP (and it is enabled for the virtual server), once users have enrolled a token on MobilePASS+, they will have the option to either authenticate with Push OTP, or use another authentication method by using a passcode trigger. Refer to “Triggering Push Notifications in the Agent” on page 31 for details.



**NOTE:** Passcode triggers are not case-sensitive.



**NOTE:** RADIUS applications which are integrated to SAS through the NPS Agent cannot use Push OTP.

## SAS Cloud RADIUS Configuration

The only configuration requirement to support the SAS Cloud RADIUS service is to set the RADIUS timeout value to at least **60** seconds on the client machine.

---

## Agents with Simple Mode User Experience

---

This type of application integration presents a simple user experience, which cannot be modified. Please note the following behavioral changes:

- Unlike the AD FS Agent, the login screen cannot be modified. Therefore, users will not be presented with options to either select push or use manual passcode entry. To trigger Push OTP, users will need to be instructed to leave the password field empty, or type any 1-character passcode on the login screen.
- If your users were previously using Gridsure or SMS: Note that when deploying Push OTP (and it is enabled for the virtual server), once users have enrolled a token on MobilePASS+, they will have the option to either authenticate with Push OTP, or use another authentication method by using a passcode trigger. Refer to “Triggering Push Notifications in the Agent” on page 31 for details.



**NOTE:** Passcode triggers are not case-sensitive.

---

## SAS Agent for NPS 2.0 Configuration

1. Install SAS Agent for NPS 2.0 with Push OTP support.
2. Configure the SAS Agent for NPS 2.0 to use Push OTP.
  - a. Enable Push Notifications in POLICY > Token Policies.
  - b. Set MobilePASS+ as the Allowed Target in POLICY > Token Policies.
3. Set the NPS 2.0 timeout value on the client machine such that the product of ((time-out) x (number of retransmissions)) is at least **60** seconds. For example, if retransmissions is set to 6, then set time-out to 10 seconds or greater.

## 5

# Token Management and Enrollment

For existing customers who are currently using MobilePASS tokens, you'll need to provision new MobilePASS tokens on MobilePASS+ after the upgrade. The same MobilePASS token type is used for allocation.

Users will need to enroll a new MobilePASS+ token. Once enrollment is complete, users will also need to be aware of the applications for which they can use their MobilePASS+ tokens for Push OTP.

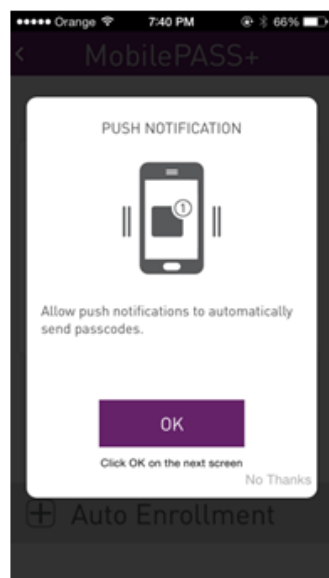
After users have enrolled new tokens in MobilePASS+, you can revoke their tokens in MobilePASS 8, return them to inventory, and then reuse them to migrate more users from MobilePASS 8 to MobilePASS+.

## Token Enrollment Process

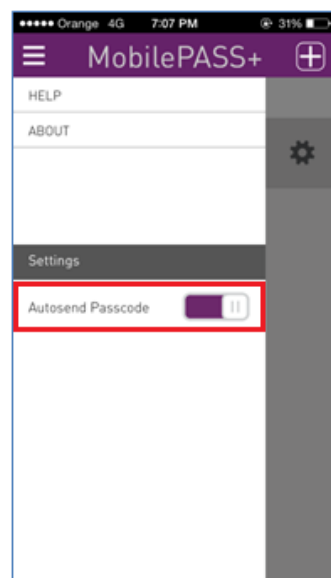
The token enrollment process on the mobile device is largely unchanged from previous versions. After the SAS operator provisions a user a MobilePASS token, the user will receive an enrollment email. The user can enroll the token by opening the enrollment email on an iOS or Android device, following the instructions to download MobilePASS+, and then clicking the auto-enrollment link on the self-enrollment page.

During enrollment, users will be asked whether to permit push notifications in MobilePASS+ on their device, as shown in the image below, left. If they choose to opt-out (choose **No Thanks**) during the enrollment, they can grant permission through the MobilePASS+ app later, by sliding the **Autosend Passcode** button to the right (purple indicates that Push OTP is activated) on the MobilePASS+ Information screen.

### During Enrollment



### Later in the MobilePASS+ App



For additional details, please refer to the *MobilePASS+ User Guide*.

## Viewing Device Information About MobilePASS Tokens

SAS operators can inspect on which device a MobilePASS token was provisioned, and whether Push OTP is enabled.

To view the MobilePASS token details:

1. Go to **TOKENS > Tokens**.
2. Under **Token List**, click on a token serial number to view. The **Token Detail** for the token is displayed.

The **Mobile App** section includes the following details:

- **Target**—This field displays the device OS on which the MobilePASS token is enrolled.
- **Device Type**—This field displays the type of device on which the MobilePASS token is enrolled.
- **Push OTP**—This field displays one of the following states:
  - **Enabled**—This state is displayed if the user has permitted Push OTP notifications on the device.
  - **Disabled**—This state is displayed if the user has not permitted Push OTP notifications on the device, but the application is push capable (i.e., on MobilePASS+).
  - **Not Applicable**—This state is displayed if the application is not push capable for the provisioned token (i.e., on MobilePASS 8).

Token Detail: 1000010158				
<b>Status:</b>	Type:	MobilePASS	In Service:	8/4/2015 10:17:41 PM
	State:	Active Token	Last Initialized:	9/4/2015 7:15:09 PM
	Last State Change:	9/4/2015 7:15:44 PM	Activated:	8/4/2015 10:17:41 PM
	Next PIN Change:		ICE Token:	
<b>Metrics:</b>	Last Auth Date:		Total OTP Pass:	0
	Result:		Total OTP Fail:	0
	Last Fail Date:		Total Auth:	0
<b>Passcode:</b>	Encryption:	SHA-256	Length:	6 characters
	Mode:	Quick Log	Display Mask:	None
	Complexity:	Decimal	OTP/Cycle:	Single
	Synchronization:	Event-based		
<b>PIN:</b>	PIN Type:	User-selected PIN	Max. PIN Attempts:	3 Attempts
	Min. PIN Length:	4	Initial PIN:	
	Complexity:	Decimal		
<b>Operation:</b>	Manual Shut-off:	Disabled	Auto Shut-off:	30 seconds
<b>Tracking:</b>	Provider:	root	Type:	Rental
	Allocation Date:	2015/08/28	Transaction ID:	1677228
<b>Mobile App</b>	Target:	Android	Device Type:	Tablet
	Push OTP:	Enabled		



**NOTE:** In the **Token Details** panel, the Push OTP state in the **Mobile App** section only displays the Push OTP state at the time of token enrollment.



**NOTE:** This token detail can also be viewed in **ASSIGNMENT > Tokens**.

## Token Reports

---

### Users – With Tokens Report

This report can help track MobilePASS+ and Push OTP deployment. It includes Token Details information—OS Type, Device Type, and Push OTP state—for MobilePASS tokens for all users in a virtual server.

## 6

# Push OTP Authentications

## Triggering Push Notifications in the Agent

The agents provide two user interaction models:

- Simple mode, which is provided by the SAS Cloud RADIUS Service or SAS Agent for NPS 2.0
- Rich user experience, which is provided by the SAS Cloud SAML Service and AD FS Agent.

### Simple Mode

With **simple mode**, if Push OTP is **enabled**, the user can trigger a push notification by:

- leaving the passcode field empty, or
- entering any 1-character passcode (excluding “s” or “g” if other authentication methods are present)

To override push and use another authentication method (if present), the user can:

- enter “s” to trigger SMS, or
- enter “g” to trigger GrIDSure

If Push OTP is **disabled** for the virtual server, an empty or any 1-character passcode will trigger an SMS challenge/response or GrIDSure, depending upon the token type the user has enrolled.



**NOTE:** Passcode triggers are not case-sensitive.



**NOTE for MS-CHAPv2 encryption:** Instead of “any 1-character” as stated in the rules above, the only passcode triggers that are allowed are “p,” “s,” “g,” or a space. Using any other character will fail the authentication.

## Rich User Experience

With the **rich user experience** provided by the SAS Cloud SAML Service and AD FS Agent, if Push OTP is **enabled**, the user is presented with the option to choose between using his mobile device to automatically send a passcode, or manually entering a passcode, as shown in the examples below.



Figure 1 - AD FS Agent



Figure 2 - SAML Service

To override push and use another authentication method (if present), the user can:

- Choose **Enter a passcode manually**, and then:
  - enter “s” to trigger SMS, or
  - enter “g” to trigger GrIDSure

If Push OTP is **disabled** for the virtual server, an empty or any 1-character passcode will trigger an SMS challenge/response or GrIDSure, depending upon the token type the user has enrolled.



**NOTE:** Passcode triggers are not case-sensitive.



**NOTE for MS-CHAPv2 encryption:** Instead of “any 1-character” as stated in the rules above, the only passcode triggers that are allowed are “p,” “s,” “g,” or a space. Using any other character will fail the authentication.



## Push Notification Contents

Push notification includes the following content:

- **Resource Name**—This is the application where the login request originated.
- **Organization Name**—This matches the **Custom Organization Name** defined in SAS (see “Set the Custom Organization Name” on page 5).
- **User Name**—This is the user who made the request (this name should match what was typed in during login on the application).
- **Timestamp**—This is the login request start time, localized for display on the phone.
- **Geolocation/IP Address**—This is the location and the User IP address where the requested originated. For web-based agents, this is the browser IP, and for logon agents, this is the machine IP. User IP is not supported for SAS Cloud RADIUS service.



---

## What Happens...

---

### ...when a user accepts a push notification?

When a user receives a login request on his phone, and taps **APPROVE**, the notification will automatically generate an OTP and send it to SAS. When the authentication succeeds, access to the protected resource is granted to the user.

### ...when a user denies a push notification?

When a user receives a login request on his phone and taps **DENY**, two options are presented:

- **It wasn't me!**—Tapping this option will end the authentication, and treat it as a failed authentication (as if the user had typed the wrong passcode).
- **I made a mistake**—Tapping this option will end the authentication. This is treated the same as a timeout/expired notification.

If configured, rejecting a notification will send a push notification rejection alert email to the user and the Operator. If the user's account gets locked due to this Push OTP rejection, the body of this alert is appended to the User Lockout Alert that is sent to the user.

See the push notification customization procedures on pages 22 and 23.

### ...if a push notification times out?

If a push notification times out, the user can either initiate push again, or manually enter a generated OTP.

### ...if a user is challenged for an OTP to re-sync the token?

If a user is challenged for an OTP to re-sync the token, the OTP is not automatically sent and has to be entered manually. In the SAS Management Console in **SNAPSHOT > Authentication Activity**, this is logged as an **Outer Window Authentication** event in the **Result** column, and the user will need to resynchronize the token by manually entering a new OTP.

## Authentication Activity Logging

Push log activity can be viewed in the SAS Management Console in **SNAPSHOT > Authentication Activity**.

Timestamp	User ID	Actions	Result	Serial #	IP	Message
2/18/2016 6:00:02 PM	push_user1	Authentication	Success	1000011646	192.43.161.1	
2/18/2016 5:59:43 PM	push_user1	Authentication	Challenge		192.43.161.1	Push OTP request from client IP 137.122.192.40 at Ottawa.ON.CA to resource 192.43.161.1 at Helen_Inc.
2/18/2016 5:59:22 PM	push_user1	Authentication	Challenge		192.43.161.1	Push OTP request from client IP 137.122.192.40 at Ottawa.ON.CA to resource 192.43.161.1 at Helen_Inc.
2/18/2016 5:58:34 PM	push_user1	Authentication	Success	1000011646	192.43.161.1	
2/18/2016 5:57:49 PM	push_user1	Authentication	Challenge		192.43.161.1	Push OTP request from client IP 137.122.192.40 at Ottawa.ON.CA to resource 192.43.161.1 at Helen_Inc.
2/18/2016 5:57:39 PM	push_user1	Authentication	Success	1000011646	192.43.161.1	
2/18/2016 5:56:54 PM	push_user1	Authentication	Challenge		192.43.161.1	Push OTP request from client IP 137.122.192.40 at Ottawa.ON.CA to resource 192.43.161.1 at Helen_Inc.
2/18/2016 5:53:50 PM	push_user1	Authentication	Challenge		192.43.161.1	Push OTP request from client IP 137.122.192.40 at Ottawa.ON.CA to resource 192.43.161.1 at Helen_Inc.
2/18/2016 5:50:13 PM	push_user1	Authentication	Challenge		192.43.161.1	Push OTP request from client IP 137.122.192.40 at Ottawa.ON.CA to resource 192.43.161.1 at Helen_Inc.
2/18/2016 5:49:39 PM	push_user1	Authentication	Challenge		192.43.161.1	Push OTP request from client IP 137.122.192.40 at Ottawa.ON.CA to resource 192.43.161.1 at Helen_Inc.

- Push notifications are listed in the **Result** column as **Challenge**, and are displayed with the same information that is included in the push notification to the user.
- Push notifications that are accepted (“approved”) by the user are listed in the **Result** column as **Success**.
- Push notifications that are rejected (“deny & report”) by the user are listed in the **Result** column as **Failure**, with a message to indicate that it was due to user rejection.
- Push notifications that are ignored by the user do not result in another entry after the **Challenge**.

## Push Notification Reports

### Push OTP Authentication History Report

This report lists Push OTP transactions and their outcome in chronological, descending order.