SafeNet Authentication Service

Push OTP Solution Guide

gemalto
security to be free

Document Number: 007-013306-001, Rev. H

Release Date: January 2018

Contents

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
Agent	• 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.
MobilePASS App	• 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 **Token Management** module in the SAS Management Console. **MobilePASS** allows users to enroll, activate, and use their tokens without administrative assistance. • There are two variations of MobilePASS: • **MobilePASS 8**: Supports manual OTP on iOS, Android, BlackBerry, Mac OS X, and Windows platforms. • **MobilePASS+**: 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.
MobilePASS Token	• 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. • 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.
OTP (One-time Password)	• An automatically generated password (also referred to as a *passcode*), 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

Term	Definition
	need for the user to manually open the MobilePASS app and type the passcode into the agent.
Protected Resource	• Any part of a computer system or network, such as a web page, cloud, or VPN, requiring authentication to enable access.
Push Notification	• 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.
Push Notification Service Provider	• 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+).
Push OTP	• 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.
User	• A user on an instance of a Virtual SAS Server. A user can be provisioned with one or more MobilePASS tokens.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to 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.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

Region	**Telephone number** (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1-410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421
Japan	0066 3382 1699
Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608

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 30 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 23 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.

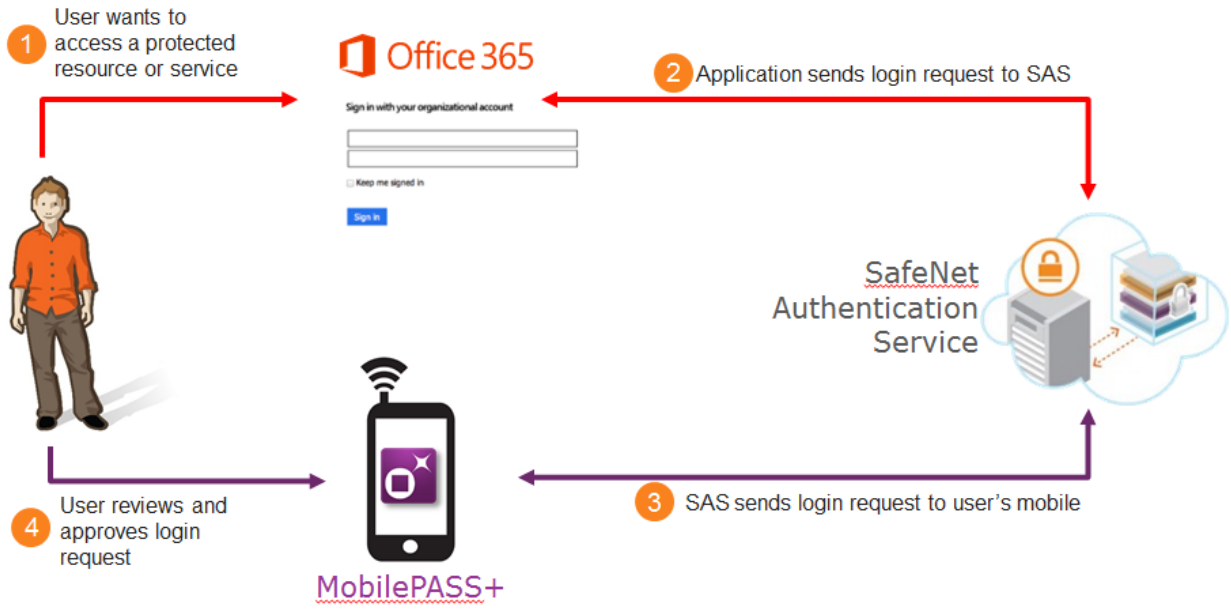
Automatic, Out-of-Band OTP Delivery

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 30 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+ Push OTP is supported on the following OS platforms:
  - Android 4.0 or later
  - iOS 8 or later
- MobilePASS 8 does **not** support Push OTP.
- 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.

NOTE: 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 23.

Integration guides for Push OTP, describing how to deploy multi-factor authentication (MFA) options in third-party applications using MobilePASS+ managed by SAS are available in the knowledge base section of the Customer Support Portal.

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 30 for details.

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 Cloud

❑	• Review/select the **Allowed Targets Settings** in the SAS Management Console. • By default, **all** platforms are configured to MobilePASS 8. For MobilePASS+, make any changes to the platform(s) you want to deploy Push OTP on. • See "Set the Allowed Targets Policy" on page 15. • 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.
❑	• (Optional) Configure user and operator policies for rejected push notifications. • See "Set the Push OTP Rejection Policy (Optional)" on page 16. • See "Set the Operator Policy" on page 18.
❑	• Allocate MobilePASS tokens. MobilePASS 8 and MobilePASS+ use the same token type.
❑	• (Optional) Customize the user and operator push notification rejection alert messages, and the email template and self-enrollment page. • See "Customize the Rejection Alert for the User" on page 21. • See "Customize the Rejection Alert for the Internal Operator" on page 22. • See "Customize the Self-Enrollment Page and Email Template" on page 22.
❑	• Configure application integrations to support Push OTP by one of the following: • Install and configure the new SAS AD FS Agent 2.0. • Set the combination of RADIUS timeout and retry values to at least 60 seconds for SAS Cloud RADIUS Service (FreeRADIUS). For example: o Multiple NPS servers (backup/failover): ▪ Timeout: 60 seconds Retries: 1 o Single NPS server: ▪ Timeout: 20 seconds Retries: 3 • Configure SAML services to display Push OTP user controls on the SAML **Login** page. • Deploy SAS Agent for NPS 2.0. • See "Set Up Applications for Push OTP" on page 23.
❑	• Provision MobilePASS tokens to users.
❑	• Users must download the MobilePASS+ app and complete the self-enrollment. See "Token Management and Enrollment" on page 27. Refer also to the *MobilePASS+ User Guide* for details.

Set Up Push OTP for Existing Accounts

❑	• Enable Push OTP. By default, the feature is disabled. See “Enable the Push OTP” on page 14.
❑	• Review/select the **Allowed Targets Settings** in the SAS Management Console. • By default, **all** platforms are configured to MobilePASS 8. For MobilePASS+, make any changes to the platform(s) you want to deploy Push OTP on. • See “Set the Allowed Targets Policy” on page 15. • 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.
❑	• (Optional) Configure user and operator policies for rejected push notifications. • See “Set the Push OTP Rejection Policy (Optional)” on page 16. • See “Set the Operator Policy” on page 18.
❑	• Allocate additional MobilePASS tokens. MobilePASS 8 and MobilePASS+ use the same token type.
❑	• (Optional) Revoke MobilePASS 8 tokens that are no longer needed.
❑	• Enroll a new token on MobilePASS+ to use Push OTP.
❑	• (Optional) Customize the user and operator push notification rejection alert messages, and the email template and self-enrollment page. • See “ • Customize the Rejection Alert for the User” on page 21. • See “Customize the Rejection Alert for the Internal Operator” on page 22. • See “Customize the Self-Enrollment Page and Email Template” on page 22.
❑	• Configure application integrations to support Push OTP by one of the following: • Install and configure the new SAS AD FS Agent 2.0. • Set the combination of RADIUS timeout and retry values to at least 60 seconds for SAS Cloud RADIUS Service (FreeRADIUS). For example: o Multiple NPS servers (backup/failover): ▪ Timeout: 60 seconds Retries: 1 o Single NPS server: ▪ Timeout: 20 seconds Retries: 3 • Configure SAML services to display Push OTP user controls on the SAML **Login** page. • Deploy SAS Agent for NPS 2.0. • See “Set Up Applications for Push OTP” on page 23.
❑	• Users must download the MobilePASS+ app and complete the self-enrollment. See “Token Management and Enrollment” on page 27. Refer to the *MobilePASS+ User Guide* for details.

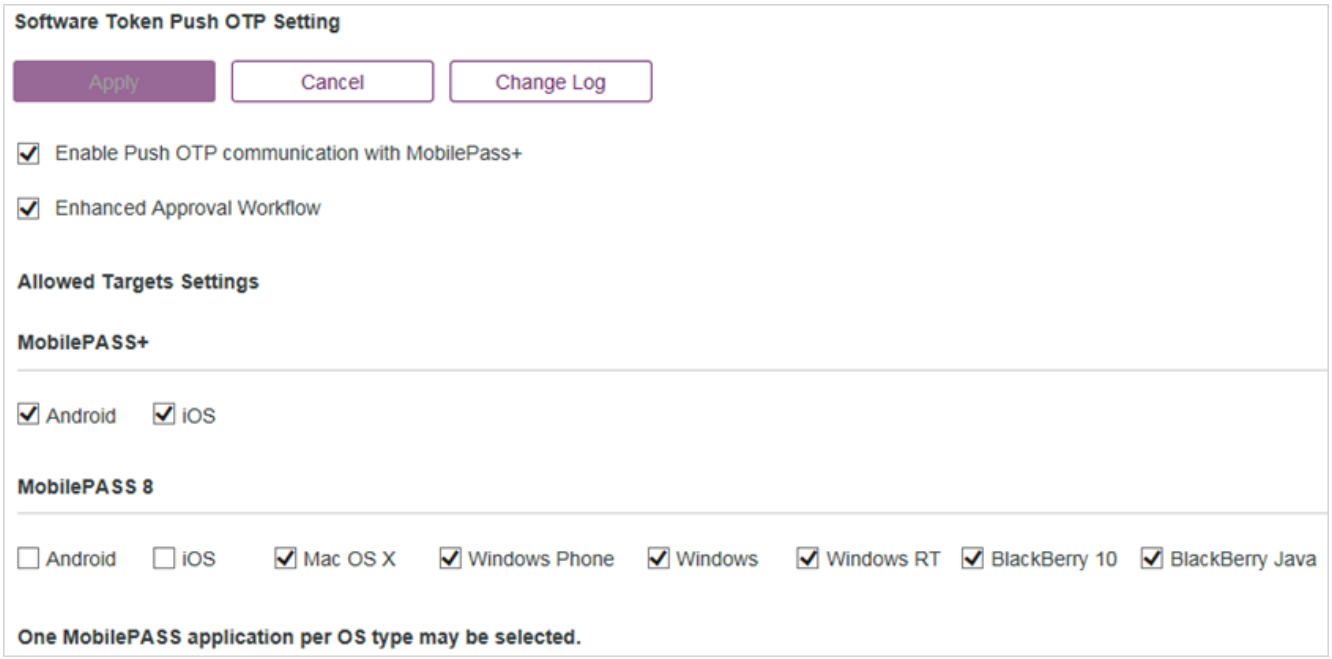
3
Enable Push OTP and MobilePASS+

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

Push OTP functionality is enabled by default for newly created accounts, and disabled by default for upgraded accounts. Push OTP is independent per virtual server and 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.

To significantly accelerate the authentication process for MobilePASS+ (version 1.4 or higher) tokens and to enable users to manage push login requests without unlocking their mobile device, select **Enhanced Approval Workflow**.



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. Select **Enhanced Approval Workflow**.

NOTE: It is highly recommended that you either enforce a device PIN or enable a PIN setting in the MobilePASS token template so that only the device owner or token assignee can approve a push request.

NOTE: If Enhanced Approval Workflow is enabled, users with incompatible versions of MobilePASS+ will receive an error message when the application opens. Enhanced Approval Workflow can be disabled at any time, restoring full functionality with earlier MobilePASS+ versions.

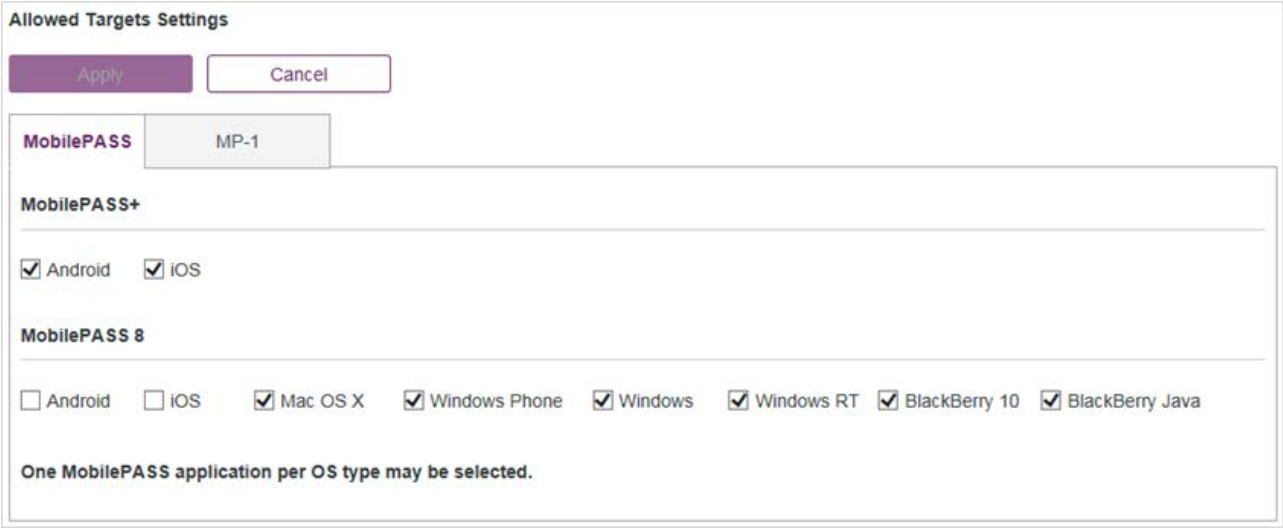
5. Under **Allowed Targets Settings > MobilePASS+**, select:
   - **iOS** to enable MobilePASS+ on iOS devices and support features such as Touch ID for iOS.
   - **Android** to enable MobilePASS+ on Android devices and support features such as Biometric PIN.
6. Click **Apply**.

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.

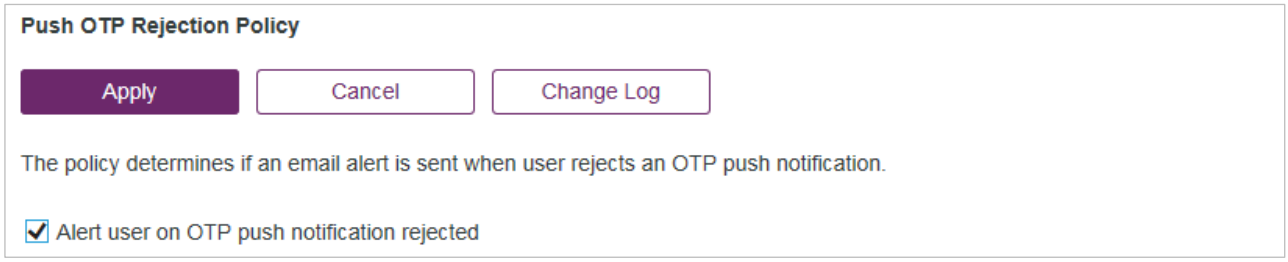
Set the Push OTP Rejection Policy (Optional)

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.

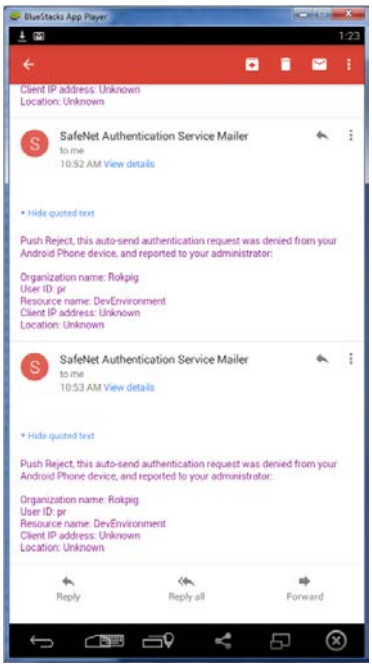
NOTE: You can customize the contents of the alert email in **COMMS > Communications > Email Messages**. See "

Customize the Rejection Alert for the User" on page 21.

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**.



Sample Push Notification Rejection Alert to User

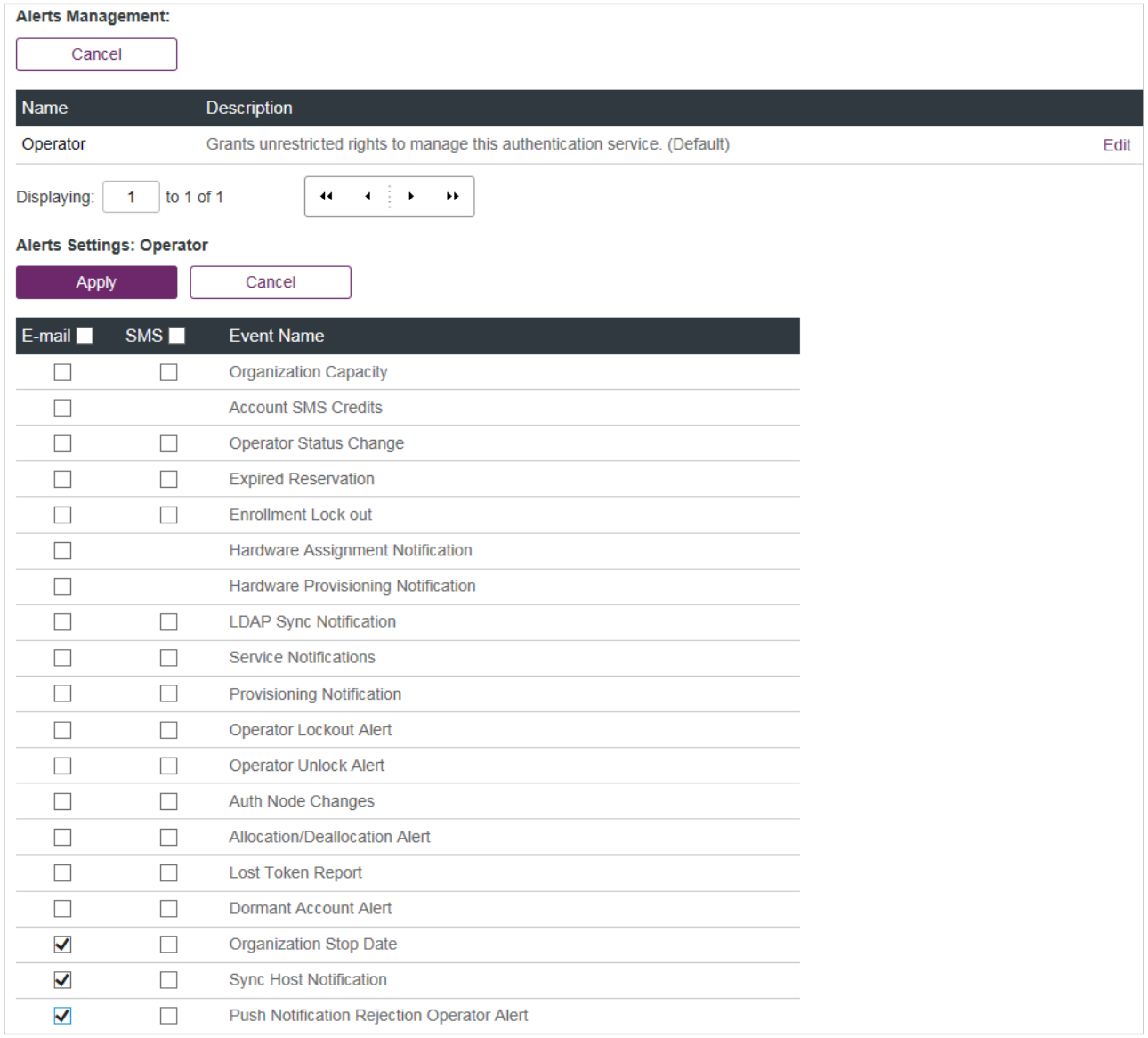


Set the Operator Policy

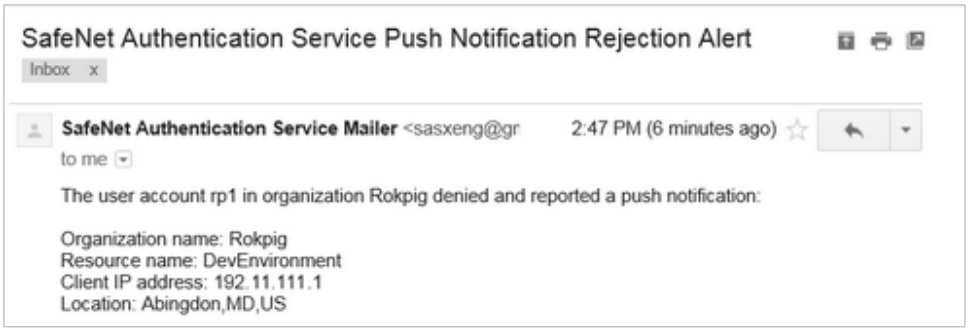
You can optionally send a Push Notification Rejection Alert to the operator if a user rejects a push notification that they did not initiate; so that the log files can be investigated if necessary.

NOTE: You can customize the contents of the alert email in **COMMS > Communications > Email Messages**. See "Customize the Rejection Alert for the Internal Operator" on page 22.

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**.



Sample Push Notification Rejection Alert to Operator



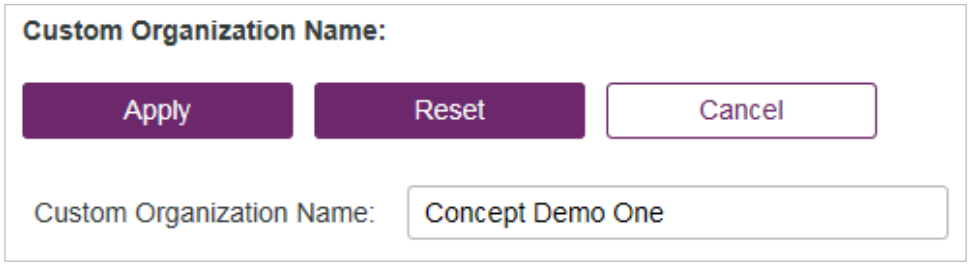
Customize Push Notifications

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

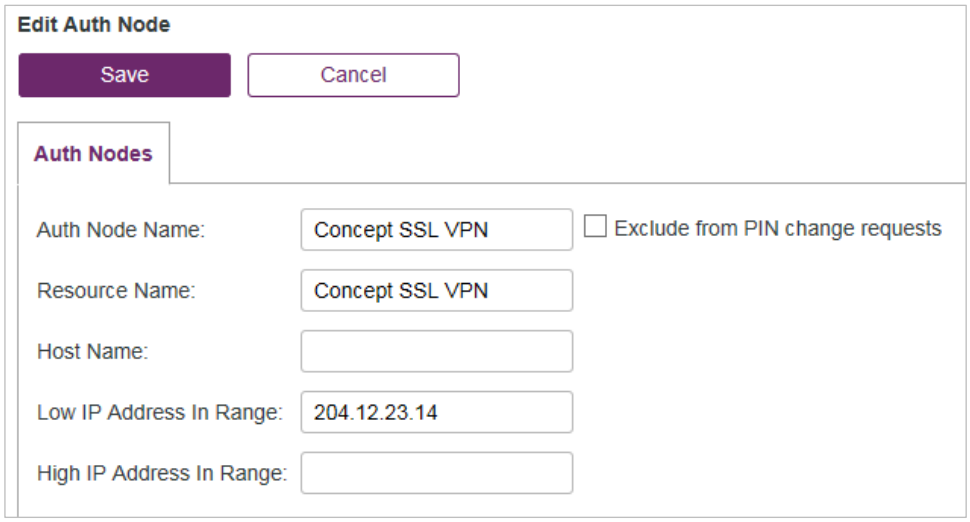
In a push notification, the **Resource Name** identifies which authentication node it relates to, so the user can be sure he is authenticating a valid node. Refer to “Push Notification Contents” on page 32 to see an example.

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 24 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**.

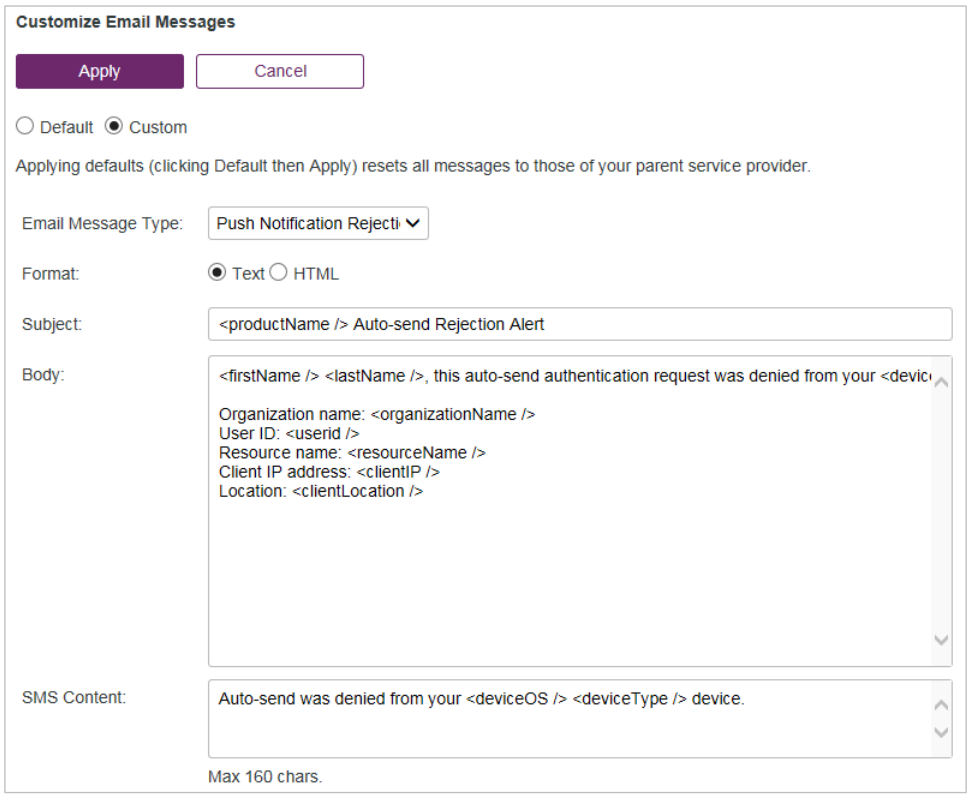


> **NOTE:** An Auth Node Change alert is generated if the **Resource Name** is changed.

Customize the Rejection Alert for the User

You can optionally customize the push notification rejection alert for the user:

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.

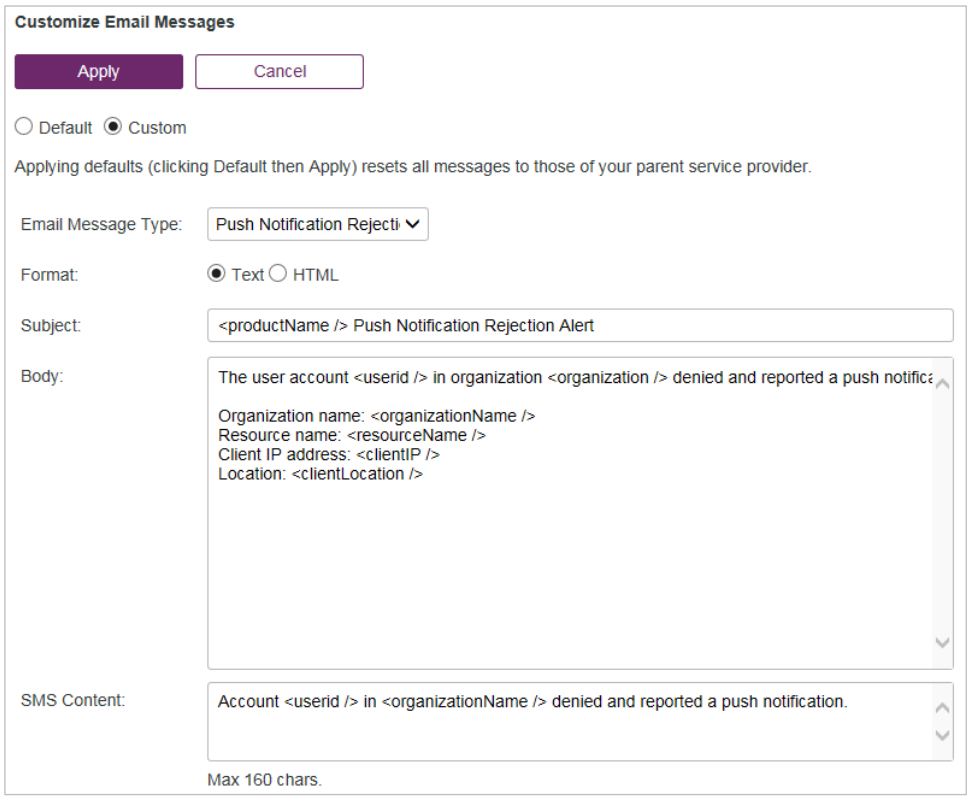


4. Modify the contents as needed, and then click **Apply**.

Customize the Rejection Alert for the Internal Operator

You can optionally customize the push notification rejection alert for the internal Operator:

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.



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

Customize the Self-Enrollment Page and Email Template

You can optionally 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 30) 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.

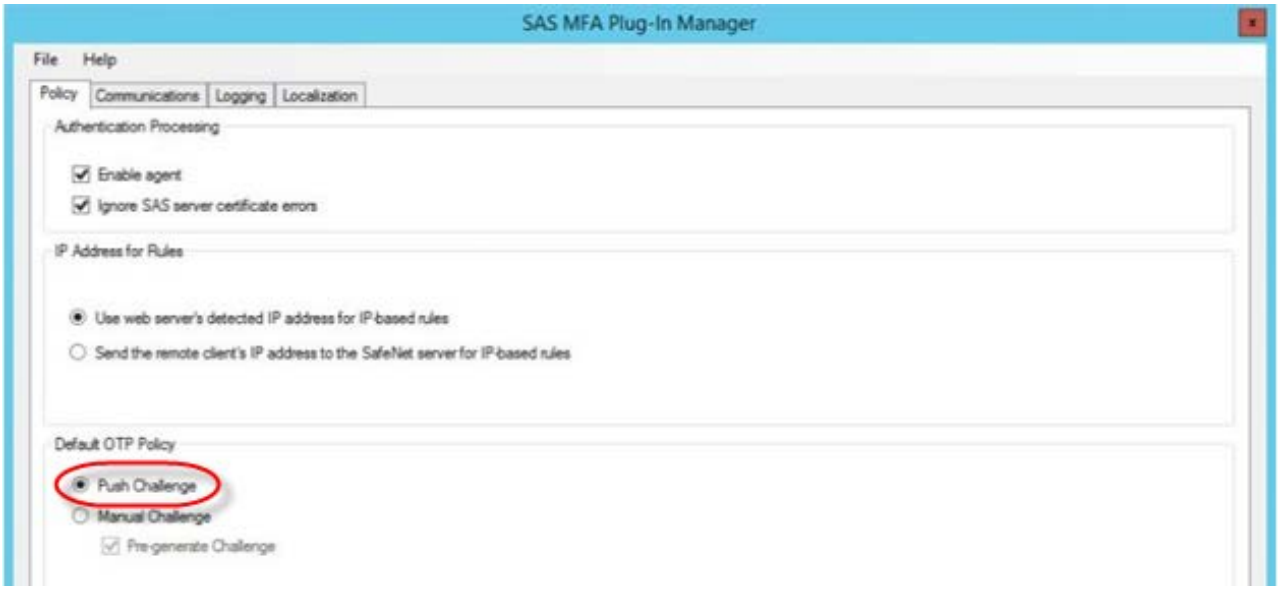
1. In the SAS Management Console, enable and customize Push OTP text for the SAML **Login** page.
   - Go to **COMMS > SAML Service Providers > SAML 2.0 Settings**.
   - Under **Custom Login UI**, select the **Enable Push/Manual OTP Selector** check box to display controls on the SAML **Login** page 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 30 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 30 for details.

NOTE: Passcode triggers are not case-sensitive.

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 30 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.

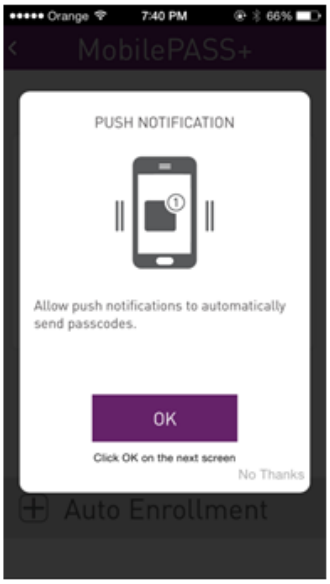
After users have enrolled new tokens in MobilePASS+, you can revoke their tokens in MobilePASS 8, return them to inventory, and then reuse them to migrate more users from MobilePASS 8 to MobilePASS+.

Token Enrollment Process

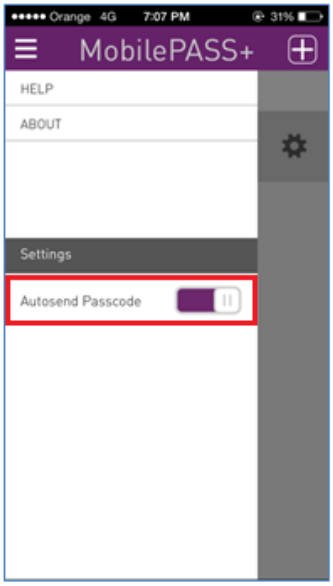
The token enrollment process on the mobile device is largely unchanged from previous versions. After the SAS operator provisions a user a MobilePASS token, the user will receive an enrollment email. The user can enroll the token by opening the enrollment email on an iOS or Android device, following the 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).

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.

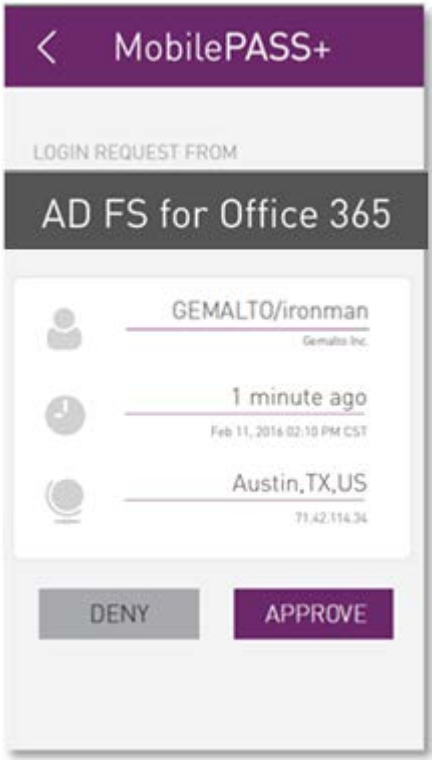
NOTE: Passcode triggers are not case-sensitive.

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 21 and 22.

...if a push notification times out?

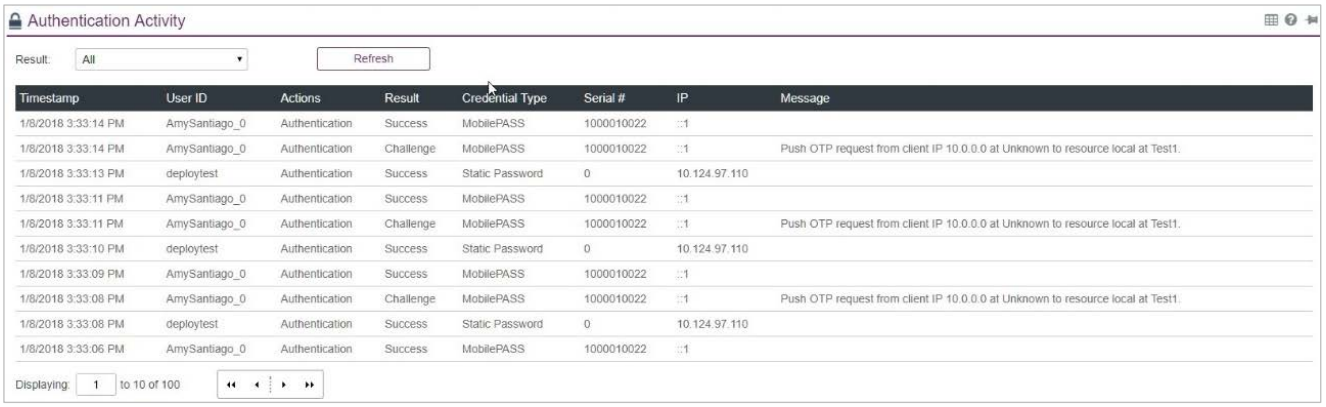
If a push notification times out, the user can either initiate push again, or manually enter a generated OTP.

...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**.



- 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.