How To Configure Push Mobile

Contents

Overview

Push (or OneTouch) authentication allows a mobile device to be prompted by the Swivel server to let the user authenticate by pressing a confirm button on the mobile device screen, via a Swivel mobile application. You can see how that works on the following video:

Prerequisites

Swivel AuthControl Sentry v4 onwards

Swivel Mobile Phone Client Version v4 for One Touch Mobile client based solution.

Swivel Server Details SSD for mobile client with OneTouch enabled.

Swivel Server will need connection with Google and Apple servers: android.googleapis.com:443, fcm.googleapis.com:443, gateway.push.apple.com:2195, feedback.push.apple.com:2196

Swivel core configuration

In order for a user to receive the Push / OneTouch Mobile push message they must be allocated the right to use the OneTouch mode of operation. This is done by ensuring that they are a member of a group that has this right.

In addition they must be in a group associated with an Push / OneTouch transport. The transport must be the PNA (push notification authentication) Transport for Push / OneTouch Mobile client users.

Push / OneTouch Mobile client users must install the Swivel Mobile Phone Client from the app store. You can see how that works on the following videos:

Configuring Dual Channel settings

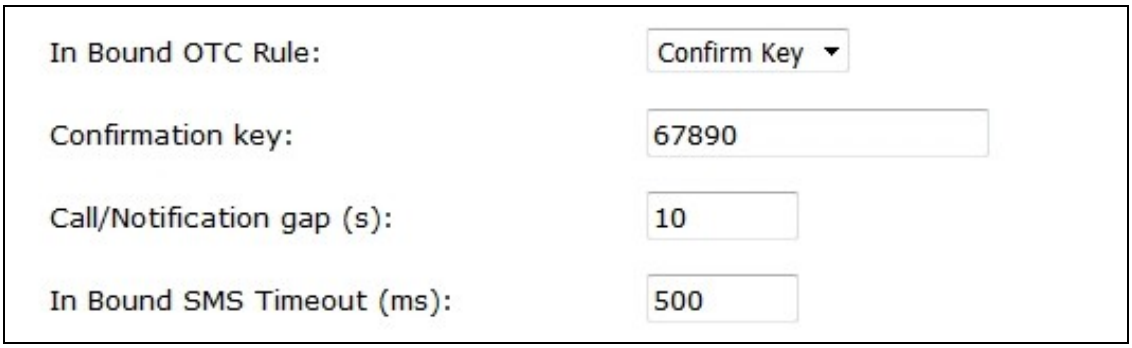
On the Swivel Administration console select Server/Dual Channel and ensure the below settings are configured:

Set **On-Demand Delivery** to Yes

Set **Allow message request by Username** to Yes

In Bound OTC Rule: Confirm key - enter the digits defined under Confirm Key to authenticate, example: if 1234 is entered then confirm by entering 1234 on the telephone keypad. OneTouch Mobile client solution currently only supports the confirm key mode of operation Confirmation key: (may be shown as [server_dualchannel_inboundconfirmkey]): The key(s) to be pressed to confirm authentication Call/Notification gap(s) (may be shown as [server_dualchannel_inboundcallgap]):

Domain Allowed to get OTC: Indicates the domain (e.g. http://localhost:8080, http://domain) authorized to get OTC. That is used by 2 way transport like Push Voice telephone or Push Mobile PNA (push notification authentication). The domain will correspond with the domain client (e.g. AuthControl Sentry, OnePushDemo, ...). If the value is * it will allow all the domains.



Define a group of Push Users

On the Swivel Administration console, select a group of users that will be using Push authentication and ensure that the Push box is ticked then click Apply.

Push Mobile Users

Repository>Groups

Please enter the repository group information to be used by the Swivel server.
This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy

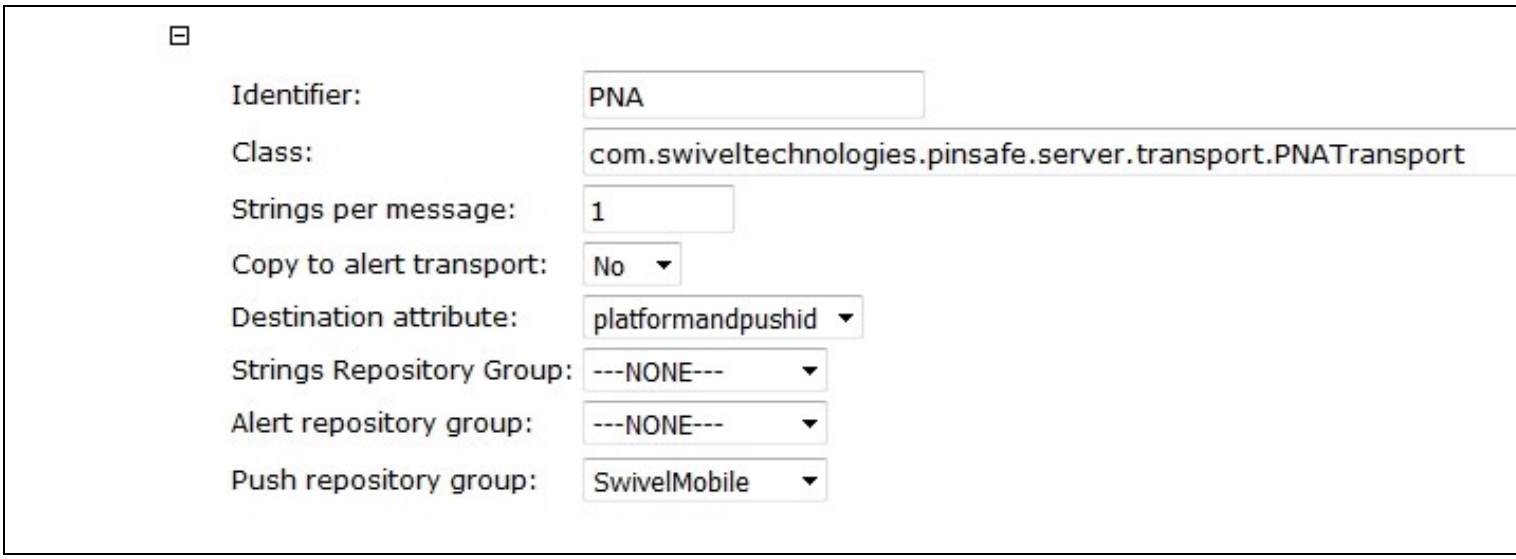
		Single	Dual
Name:	SwivelAdmin	☑	☑
Definitions:			
repoTest:	SwivelAdmin		
Name:	SwivelImage	☑	☐
Definitions:			
repoTest:	SwivelImage		
Name:	SwivelHelpDesk	☑	☑
Definitions:			
repoTest:	SwivelHelpDesk		
Name:	SwivelMobile	☐	☑
Definitions:			
repoTest:	SwivelMobile		
Name:	SwivelSMTP	☐	☐
Definitions:			
repoTest:	SwivelSMTP		
Name:	SwivelToken	☐	☑
Definitions:			
repoTest:	SwivelToken		

Define a Push Transport

On the Swivel Administration console, select or create a Push Transport

For OneTouch Mobile Client this will be the PNA (push notification authentication) Transport

Push Mobile Client Transport



Configure Push Transports Configure a One Touch Mobile Client (PNA) Transport

The PNA (push notification authentication) Transport is preconfigured, no configuration changes are required unless requested by Swivel support

Timeout (ms): default 30000. Notification timeout. If the notification is pressed or arrives after the specified time, a message will be shown to the user to indicate that the Authentication Request has expired. 0 is no Timeout.

Notification title: Text displayed on the device notification.

Notification body: Text displayed on the authentication screen of the Swivel Mobile App.

iOS cert password: iOS certificate password which should correspond with the kind of certificate that is being used: production or development. The certificate used will depend of the attribute 'Production environment'.

BB URL: Push URL for BB10 Swivel Mobile App.

BB application id: BB10 Swivel Mobile App's identifier.

BB password: Push password for BB.

Android key: Key related with the Swivel Mobile app used.

Production environment: Indicates if the current environment is development or production. Depending of this value the certificate used to send the notification to the device will be the production one or the development one.

PNA configuration

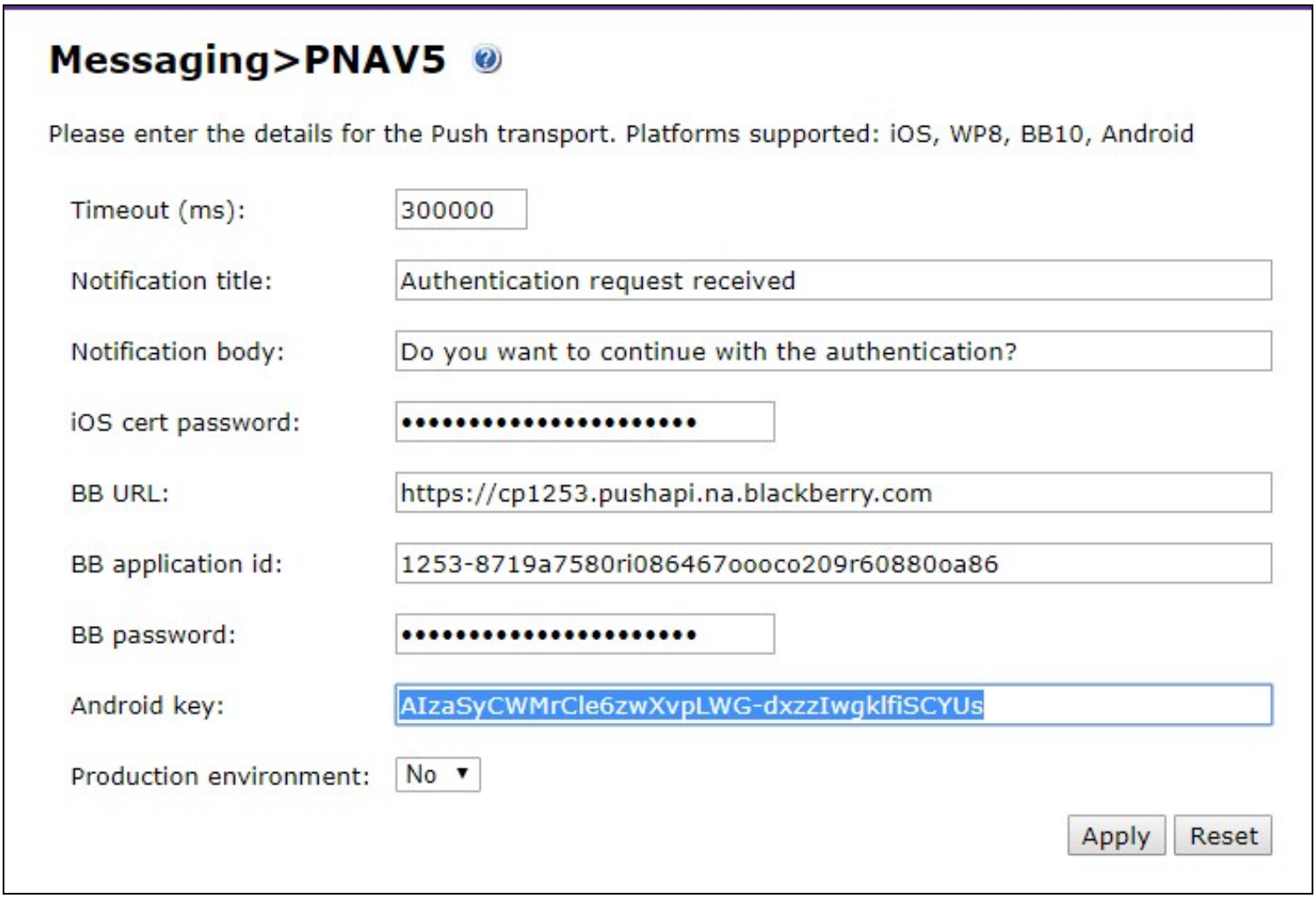
Messaging>PNA

Please enter the details for the Push transport. Platforms supported: iOS, WP8, BB10, Android

Timeout (ms):	300000
Notification title:	Authentication request received
Notification body:	Do you want to continue with the authentication?
iOS cert password:	••••••••••••••••••••••
BB URL:	https://cp1253.pushapi.na.blackberry.com
BB application id:	1253-8719a7580ri086467oooco209r60880oa86
BB password:	••••••••••••••••••••••
Android key:	AIzaSyAi-Kc1VQmQr7frrgMeHWVqxg8RdWGc3Ow
Production environment:	Yes

Apply Reset

PNA V5 Configuration



iOS Users

A renewal of the certificate might be due to happen from time to time as for now this is a non permanent certificate. Instructions and file: APNS Push Certificates

Bear in mind that v4 has an Update available but for internal database type we suggest that you either update the appliance and get the newer version (4.0.5) or if you decide to go for the manual option we strongly advise you to change from Internal to Appliance Database - there is a known bug when tomcat is restarted for v4.0.4 using the Internal database - check: https://kb.swivelsecure.com/w/index.php/Migrate_How_to_guide

Android Users

For AuthControl Mobile App v5 please ensure you create a PNA_V5 as Push Transport. Open it and replace the Android key by the following: AIzaSyCWMrCle6zwXvpLWG-dxzzIwgklfiSCYUs

Testing

For testing OneTouch you can use AuthControl Sentry adaptative authentication system or RADIUS with OneTouch enabled.

Troubleshooting

Check the Swivel logs for error messages

Error Messages:

Calling or sending notification to user "push" failed, error: The transport destination is empty.

This error can be seen where the user is authentication with the PNA and if the Mobile device has not been provisioned.

Authentication failure. Please Reprovision the device

The mobile device needs to be provisioned.

The authentication request expired

The authentication request took too long to reach the Mobile Client and is no longer valid. A large time difference between the mobile client and the Swivel server can cause this error. To increase the value, change the PNA Transport Timeout (ms): to a larger value or to 0 to prevent timeout.

PNA user id error

The wrong User is associated with the Provisioned mobile device. Provision with the correct user.

Calling or sending notification to user "gfield" failed, error: The transport destination is empty.

This can be caused wherethe SSD has a value of false for Push. To allow OneTouch Mobile this value needs to be true. To check this, verify on the Swivel Administration Console User Administration, View by Attributes to see platformandpushid.