OneTouch Mobile

Contents

Overview

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.

For other forms of authentication see: Transports How To Guide and OneTouch Voice

Prerequisites

Swivel 3.10.4 onwards

Swivel Mobile Phone Client Version 2.1.2 for One Touch Mobile client based solution.

Latest version of the Swivel Appliance Proxy available from Downloads

Swivel Server Details SSD for mobile client with OneTouch Push enabled

Swivel SSD Configuration

Swivel Mobile Phone Client must be configured to obtain its details from the Swivel SSD. For the configuration options see SSD.

Swivel core configuration

In order for a user to receive the 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 OneTouch transport. The transport must be the PNA (push notification authentication) Transport for OneTouch Mobile client users.

OneTouch Mobile client users must install the Swivel Mobile Phone Client from the app store.

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

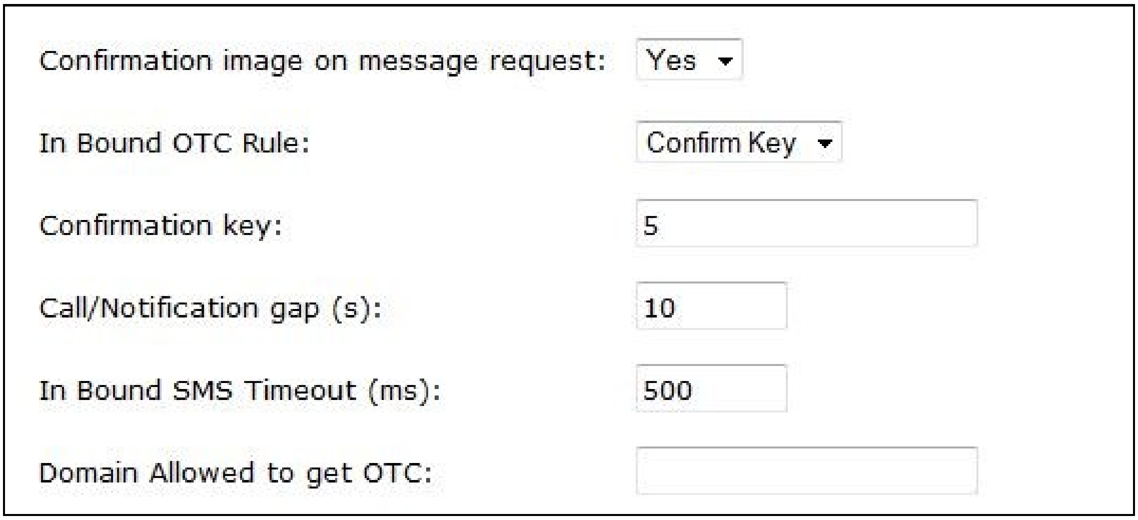
In Bound OTC Rule:

- 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 OneTouch Voice telephone or OneTouch Mobile PNA (push notification authentication). The domain will correspond with the domain client (e.g. Userportal, Juniper, ...). If the value is * it will allow all the domains.

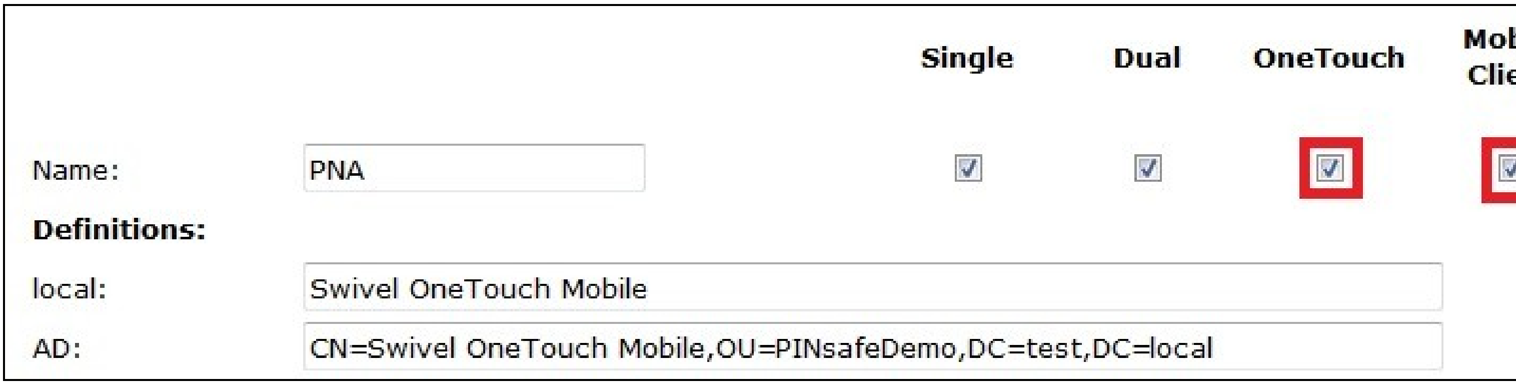


Confirmation image on message request:	Yes ▾
In Bound OTC Rule:	Confirm Key ▾
Confirmation key:	5
Call/Notification gap (s):	10
In Bound SMS Timeout (ms):	500
Domain Allowed to get OTC:	

Define a group of OneTouch Users

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

OneTouch Mobile Users



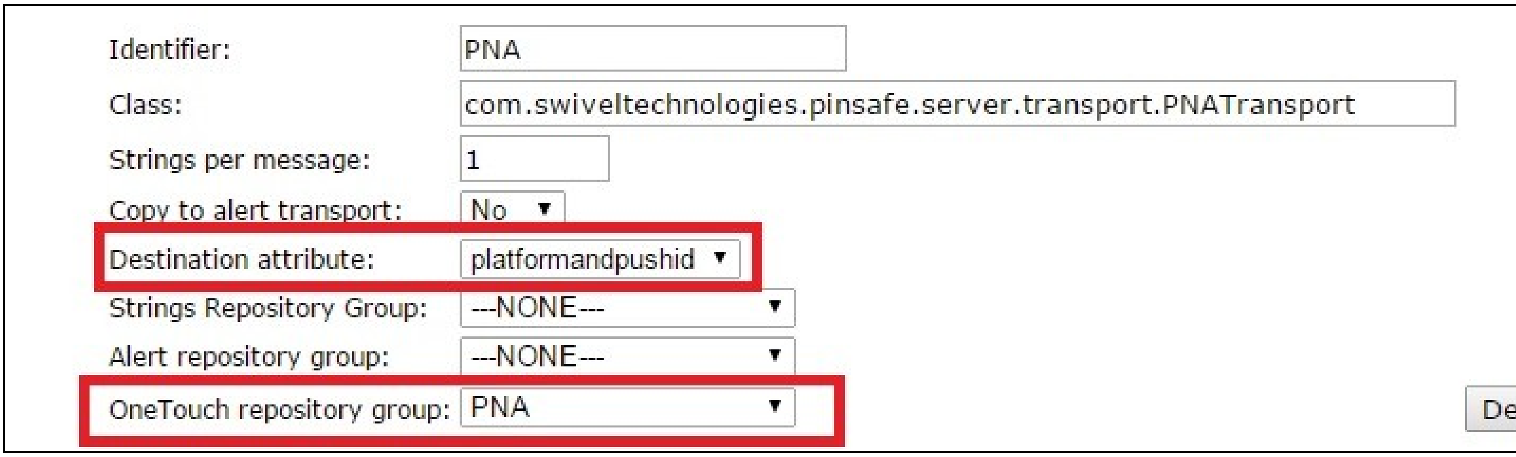
		Single	Dual	OneTouch	Mob Clie
Name:	PNA	☑	☑	☑	☑
Definitions:					
local:	Swivel OneTouch Mobile				
AD:	CN=Swivel OneTouch Mobile,OU=PINsafeDemo,DC=test,DC=local				

Define a OneTouch Transport

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

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

One Touch Mobile Client Transport



Identifier:	PNA
Class:	com.swiveltechnologies.pinsafe.server.transport.PNATransport
Strings per message:	1
Copy to alert transport:	No ▾
Destination attribute:	platformandpushid ▾
Strings Repository Group:	---NONE--- ▾
Alert repository group:	---NONE--- ▾
OneTouch repository group:	PNA ▾

Configure OneTouch 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'.

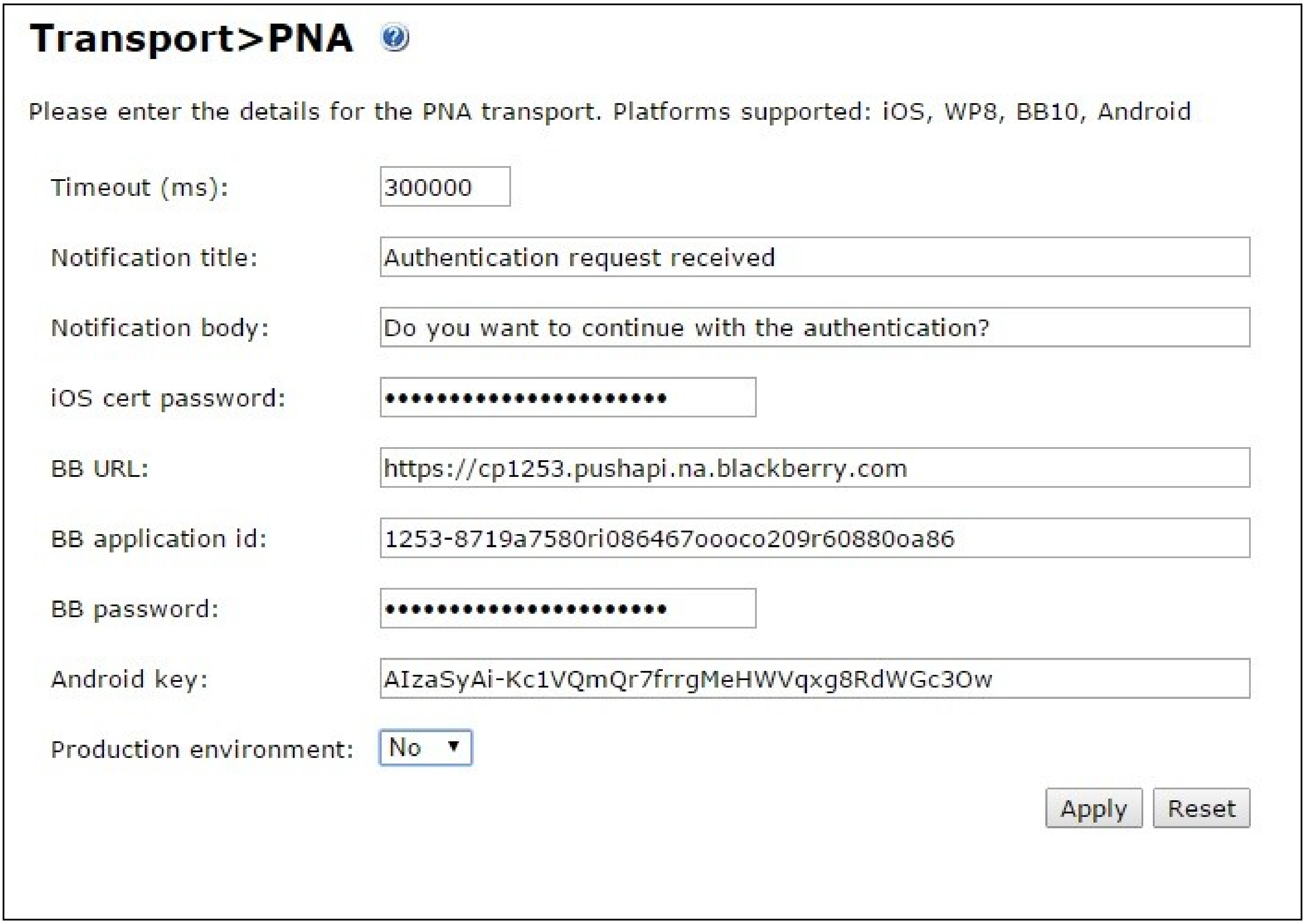
BB URL: Push URL for BB10 Swivel Mobile App.

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.



Transport>PNA

Please enter the details for the PNA 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: No ▾

Testing

The Swivel OneTouch can be configured to work with a test authentication page available for download.

Configuring the Test Page

Edit the userportal/js/ajax.js file and make sure the top line has the serverContext variable set

var serverContext = https://localhost:8080/pinsafe

If it is installed on a different server then a Hostname or IP address will need to be specified. If HTTP is used instead of HTTPS then this may need to be changed.

Integrating OneTouch

The OneTouch Mobile can be initiated in much the same way as the sending of an SMS message.

The login page needs to start an authentication session then include a GET request to TCImageCall servlet passing in the session ID. This generates the call.

The login page can also include logic to detect when the core platform has received the user?s response.

Once the user response has been received the form can be submitted, using the sessionID as the users? one-time code.

An example OneTouch login page is available for Juniper.

VPN Integration

As it may not be possible to perform some of the stages of the integration within the constraints of a VPN login page, we have developed a different approach for OneTouch integration with VPNs.

Rather than creating a login page that handles the authentication we have created a custom VPN login page that redirects the user to a different server that hosts the OneTouch login page.

The user enters their username and password on this page and this page requests the push-message/call. When this page detects that the user has responded it redirects the user back to the VPN login page, complete with username, password and session ID. The modified login page automatically submits the form and the authentication then proceeds.

Known Issues

Troubleshooting

Check the Swivel logs for error messages

Error Messages

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

This error can be seen where the user is authenticationg 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**.