Dual Channel

Overview

Dual Channel refers to two lines of communication and authentication and is usually made in reference to the sending of SMS text messages or Voice Calls:

1. Authentication details are sent by SMS/Phone Call across the mobile phone network.

2. Authentication is made using the internet

Alternatives to Dual Channel communications are Single Channel or without communication where the One Time Code is predicted using mathematical means based on events or time, see Token.

Swivel version 3.10.2 onwards allows PIN protection for Single Channel communications and PINless for dual channel authentication.

Configuration

On Demand Authentication

On Demand Delivery

Allow message request by username: default Yes, allows username to be used to request an SMS, otherwise SessionID is required. The format is:

Virtual or hardware appliance: https://Swivel-server:8443/proxy/DCMessage?username=test

Software only: http://Swivel-server:8080/pinsafe/DCMessage?username=test

Allow alternative usernames: default No, allow the user of alternative usernames

Alternative username attributes: the alternative attributes that are permitted, for multiples seperate with a comma ','

Multiple authentications per String: default No, Allow the One Time Code to be resubmitted

Confirmation image on message request: default Yes, see Dual Channel Confirmed Message

In Bound OTC Rule: default None, Options:

- None, No inbound rules
- Match, OTC is submitted both at the authentication point sent by SMS and must be the same
- Message, OTC is just used in SMS message and not the login page
- Confirm Key, used with the below key to define a key to indicate that the message has been received

[server_dualchannel_inboundconfirmkey]: default 1

[server_dualchannel_inboundcallgap]: default 10

In Bound SMS Timeout (ms): default 500