# Transports How To Guide

## Contents

# Overview

This document is an overview of the available transports, for troubleshooting information see Symptoms.

Each Swivel user can be configured to receive authentication and account information.

**User Alerts** are notifications about the user account, such as PIN numbers, passwords, account locked, PIN changed, PIN change required, etc.

**Security Strings** or **One Time Code** is the authentication information.

# Transport Methods

Swivel can send Alerts, Security Strings and One Time Codes in a variety of methods, these include:

## Alerts, Security Strings and One Time Codes

- SMS and where supported SMS Flash see Transport Configuration
- SMTP (Email) see Transport Configuration

If the users alert type is changed then a new welcome message is sent to the user.

## Security Strings and One Time Codes

- Single Channel Graphical Images (TURing, PATtern, BUTton, PINpad)
- SMS, see Transport Configuration
- Mobile Phone Client
- SMTP, see Transport Configuration
- Hardware or software Token

Each of these methods are described below:

For further information on configuring Transports see Transport Configuration

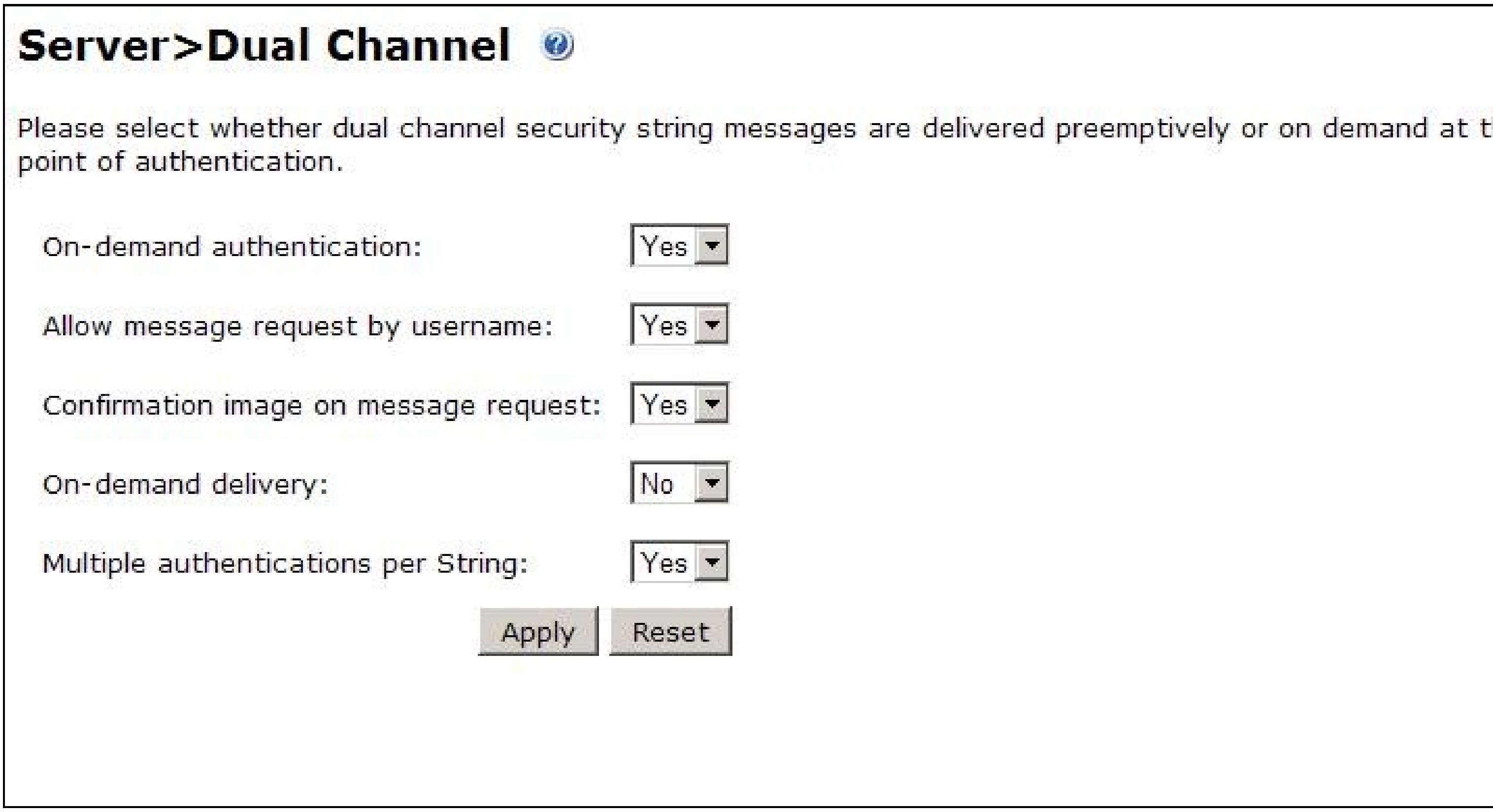
# Dual Channel

A text message sent from an SMS gateway or GSM modem (see GSM Modem How To Guide). This is known as Dual Channel authentication as the user receives their security string by one method (the mobile phone network), and authenticates by another channel (the internet). PINsafe also supports the sending of Multiple Security Strings, see Multiple Security Strings How To Guide, and the sending of One Time Codes without PIN extraction, see PINless How To Guide. Possession of the mobile phone acts as a **Something you have** for Two Factor Authentication.

There are two delivery methods for Dual Channel messages, standard delivery, and On Demand Authentication:

**Standard Delivery:** When a user account is created the user is sent a security string. When the user passes or fails an authentication, a new security string is sent to the user. Where 'On Demand' delivery is used a button can be added to the login page to request a new SMS message.

**On Demand Authentication:** An SMS message is sent to the user only when it is requested. A button is usually created for the user to request the SMS. Where it is supported by the Access device Challenge and Response authentication' can be used where a password is entered before an SMS is sent to the user, see Juniper Two Stage Challenge and Response for a sample of how to do this. On demand security strings are only valid for a limited time span, see Session Cleanup.



Server>Dual Channel

Please select whether dual channel security string messages are delivered preemptively or on demand at t
point of authentication.

On-demand authentication: Yes

Allow message request by username: Yes

Confirmation image on message request: Yes

On-demand delivery: No

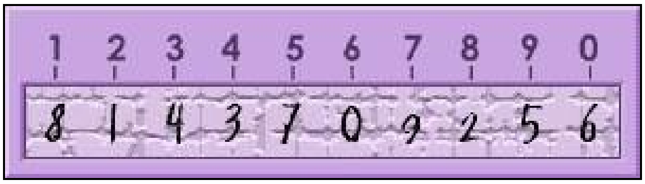
Multiple authentications per String: Yes

## Single Channel

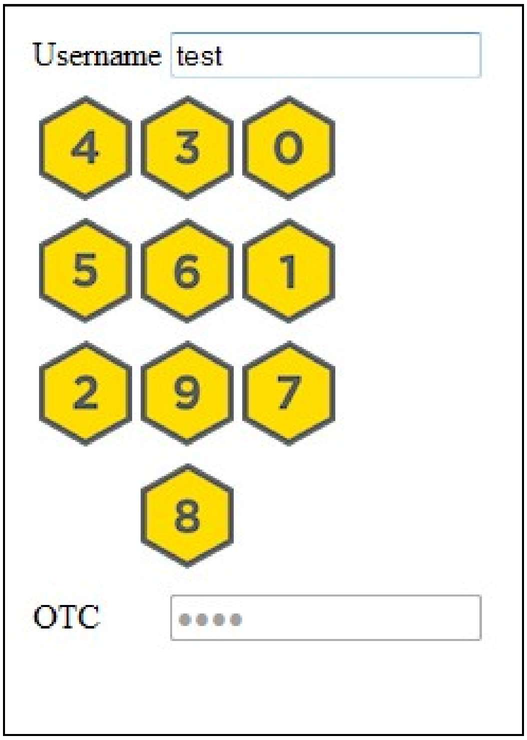
This is where the user receives their security string and authenticates by the same channel (i.e. the internet). The Image is normally embedded into the login page, where this is not possible a Taskbar application is available, see Taskbar How to Guide. Single Channel images are only valid for a limited timespan, see Session Cleanup. The users PIN is **Something you know** as one part of Two Factor Authentication.

Swivel offers a variety of methods including:

**Turing Image** The first line is a place holder the second line is the numbers or letters for the PIN extraction. Each image is unique and the numbers change position each time.



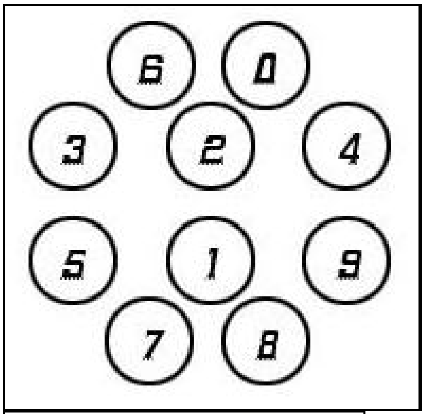
**Pinpad**, the user would click on the numbers corresponding to their PIN number. Each image is unique and the numbers change position each time.

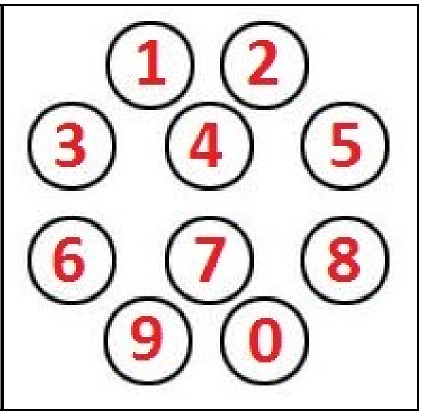


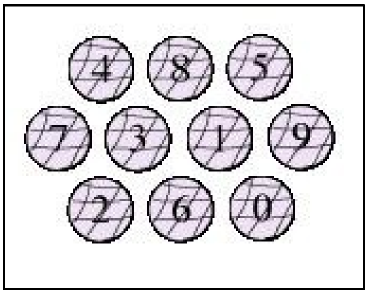
Username test

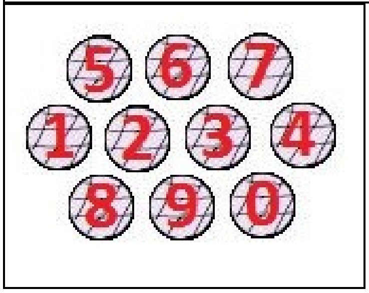
OTC ••••

**PATTern Image**, designed so that a user remembers a pattern rather than a PIN. The red numbers show the default PIN number settings and map a PIN to the pattern. The One Time Code is derived from the numbers displayed in their pattern. Each image is unique and the numbers change position each time. (Note PATtern is not related to the Pinpad).

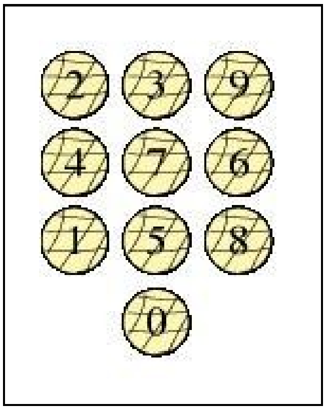


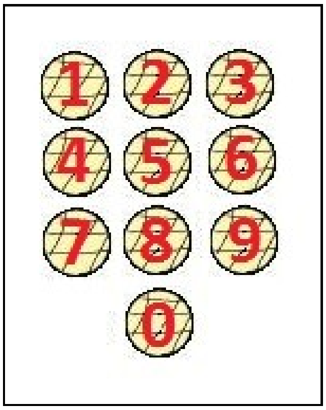






BUTton Image, the PIN is arranged as a telephone keypad, and the PIN extraction relates to the PIN numbers in the pad. The red numbers show the default PIN number settings. The One Time Code is derived from the numbers displayed in their pattern. Each image is unique and the numbers change position each time. (Note BUTton is not related to the Pinpad).



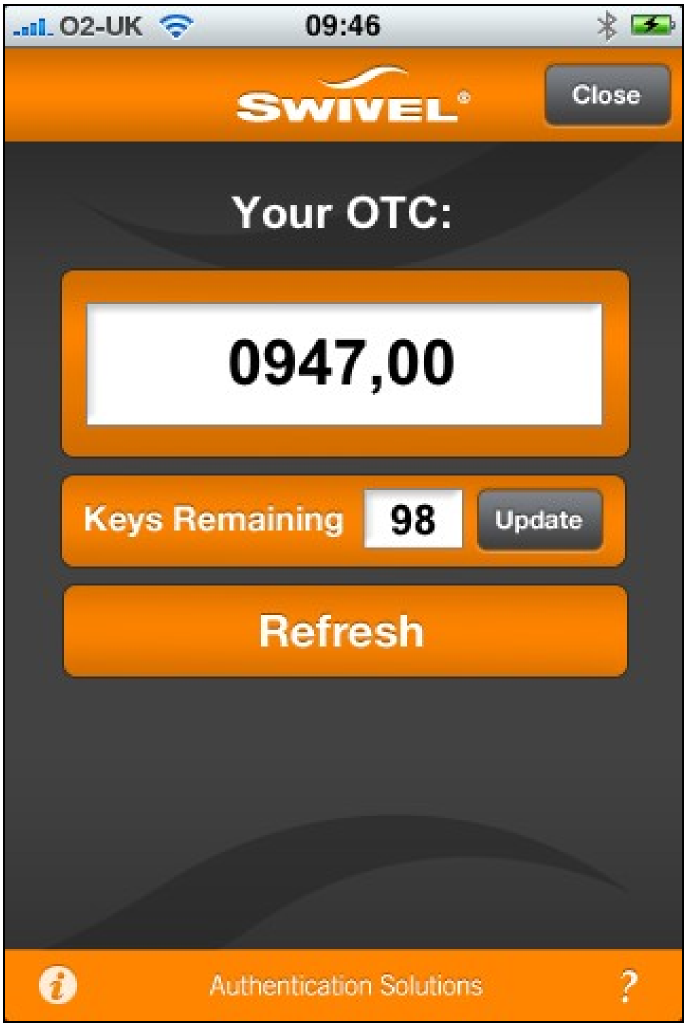


Also see: Single Channel Customisation How to Guide

## Mobile Phone Application

This is where the Mobile Phone Client requests a number of security strings, it is normally dual channel authentication, as the security strings are requested from the Swivel server across the wireless network. Possession of the mobile phone acts as a **Something you have** for two factor authentication.

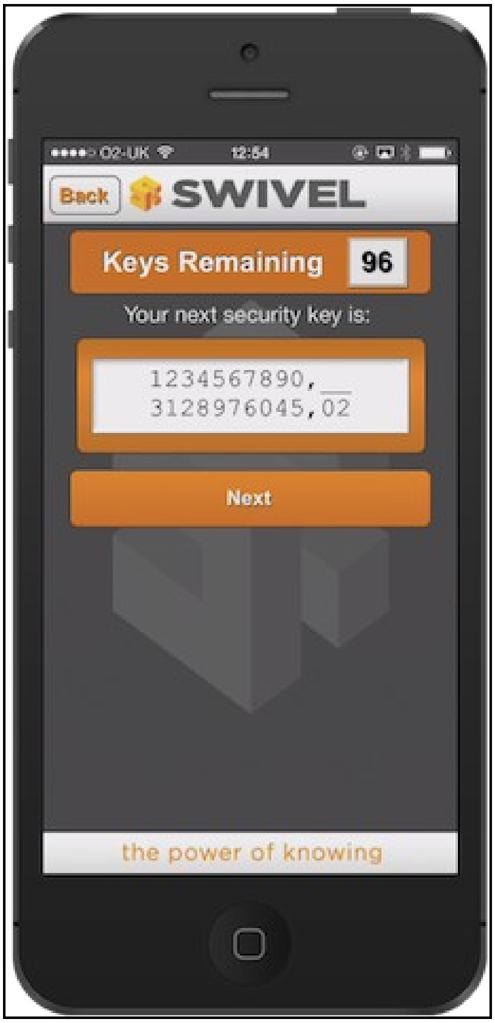
For more information see Mobile Phone Guides



Your OTC:

0947,00

Keys Remaining 98



Keys Remaining 96

Your next security key is:

1234567890,__
3128976045,02

## Hardware Token

Swivel version 3.9.6 adds support for OATH Tokens. These use event based authentication using the Swivel OATH HOTP Hardware Token and Time based with the Swivel OATH HOTP Hardware Token and also OATH OCRA. Possession of the hardware token acts as a **Something you have** for two factor authentication. For further information see Token.

## SMTP (Email)

SMTP can be Dual or Single Channel authentication. Where it is sent directly to a mobile phone by wireless transmission (e.g. a Blackberry), it is Dual Channel, where it is sent across the internet to the user it is singe channel. See also SMTP solutions