Technical Bulletin, November 2014

Introduction

This release bulletin relates to Version 3.10.3 of the Swivel Authentication Platform.

Feature Overview

Core Enhancements Version 3.10.3

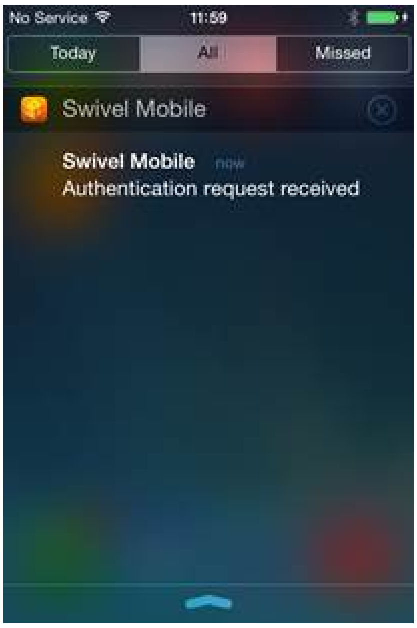
Send Dual Channel String

The behaviour when a user failed an authentication was changed in 3.10 so that under certain circumstances if a dual-channel user failed an authentication they were not sent a new security string. This was a change to 3.9 and earlier versions.

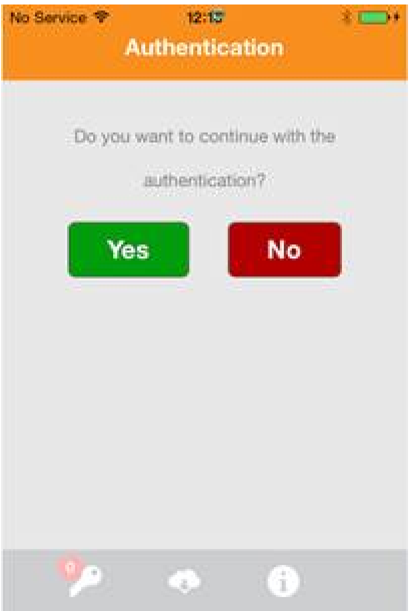
This anomaly has been rectified in 3.10.3 (a change that has also been back-ported to version 3.10 and 3.10.2) so that when a dual-channel user fails an authentication they are sent a new security string.

New OneTouch iPhone Client

Swivel has developed a new iPhone Mobile client that makes authentication as easy as pressing a button on your iPhone. The use case is that the user goes to the service to which the wish to authenticate. The user enters their username (and optional password). At this point a notification is sent to their Swivel Mobile Phone Client which prompts the user to confirm that they wish the authentication to continue.



Swivel Mobile now
Authentication request received



Do you want to continue with the authentication?

All the user has to do to complete the authentication process is click YES. This will cause the form to submit and the authentication to complete (assuming the password is correct)

This brings the same one-touch authentication model that Swivel offers via telephony, to the mobile client

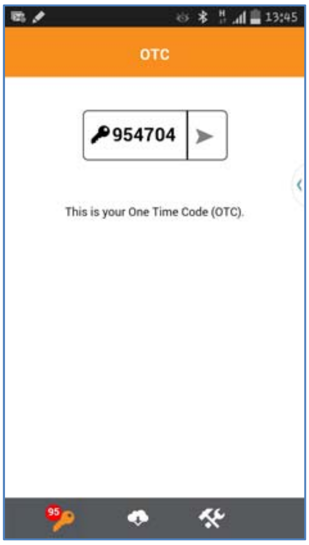
If the user has not instigated the authentication then theycan press NO to prevent the authentication continuing.

This feature adds a new, very easy to use, form of two-factor authentication. This feature will be made available to other mobile clients (Android, Windows, Blackberry) later in 2014.

All versions of the mobile app will use the relevant push platform provided by the respective mobile phone platform.

Keys remaining badge

One change available across all mobile phone clients is a badge (the name for the circle that appears by or within an application) that indicates the number of keys, or security strings, stored on the client. This helps the user decide when the best time to top-up is.



954704

This is your One Time Code (OTC).

On the Windows and iPhone versions of the client the badge also appears on the application icon on the phone home screen.

Two-stage RADIUS with no password

Until this version of the core product, in order for two-stage RADIUS authentication to work, a password had to be provided at stage 1. This limitation no longer applies. So now two stage authentication can be used if the only credential required to authenticate is a Swivel One-Time Code.

The resultant use case is

1) User enters their username on VPN, clicks submit
2) The VPN displays an additional (2nd Stage) login form
3) In the meantime the user receives a security string (or one-time code)
4) User enters their one-time code into the 2nd stage login page to authenticate.

Third Party Authentication

When using third-party authentication (required for the Swivel authentication provider to use Swivel on a Windows Desktop) it is now possible to apply this additional authentication to all users, just a group of users or no users.

Admin API "List All Detailed"

The API call now is extended to include users created via the Agent XML as well as those user created via synchronisation with a repository

Other Enhancements

OWA Change PIN

The change PIN process supported by the OWA filter has been improved to make the user flow more logical and easier to follow.

Bug Fixes

Synchronised mobile client could not retrieve security strings via the appliance proxy. FIXED.

When using MSCHAP, tokens could lose synchronisation and not regain it. FIXED.