

## Swivel Authentication Version 3.10

### Release Bulletin

#### **Introduction**

This release bulletin relates to Version 3.10 of the Swivel Authentication Platform.

This latest release brings with it new product enhancements to the Swivel Core, user experience and integrations. Full feature information and details are set out in this document.

We strongly recommend that all our customers upgrade to the latest version as soon as possible. Upgrades are included as part of your annual maintenance renewal and are free of charge.

## Feature Overview

Introduction.....	1
Product Enhancements.....	3
Enhanced SAML Solution for Google Docs – New Functionality.....	3
Mobile – new functionality .....	3
Swivel Core - New functionality .....	4
Configuration replication - Shared Secret.....	4
Voice Support Transport .....	4
Reports by Email.....	4
Comma policy removal for mobile client.....	4
Swivel Core – Bug Fixes.....	4
Inbound Servlet Issues.....	4
Session sync default shared secret Issues .....	4
Display Issues with PINpad Images.....	4
Wrong Index on User Attributes Table .....	4
Log Viewer Screen Sizing.....	4
HTML / Plain Text Security Strings.....	4
Sub menu Ordering.....	5
Token Data Migrating Issues.....	5
User Exists for alternative Usernames .....	5
Replace PINsafe with Swivel.....	5
TokenIndexImage and TokenIndex.....	5
Group Names.....	5
Generic Error Trapping.....	5
Session Replication Errors.....	5

## Product Enhancements

### Enhanced SAML Solution for Google Docs – New Functionality

This is a fully working SAML based solution that works as an Identity Provider for Google-Docs. It enables clients to specify authentication rules for accessing Google-Docs.

When a user tries to access Google-Docs the authentication process can now be set out as follows:

- If accessed from a trusted IP address range (as specified in the configuration) the user will be prompted for their Active Directory Username and password. If these are correct their login will succeed and they will be redirected to Google-Docs and “logged in”.
- If accessed from an untrusted IP address range the user will be prompted for their AD Username, password and an additional Swivel credential. If these are correct their login will succeed and they will be redirected to Google-Docs and “logged in”.

Other scenarios can be supported, for example access from a trusted IP address may be allowed with PINpad based authentication whereas access from untrusted IP may require full two-factor authentication

This solution can also be applied to other SAML based integrations

### Mobile – new functionality

New mobile phone clients have been created across all mobile platforms. The following new functionality has been added:

- Easy provisioning through URL scheme, with a single URL. User just needs to click on one url
- Same user interface for all mobile platforms
- Introduction Wizard
- Add new policies from core
- Internationalization for all text
- Enhanced support for iPad
- Available to Blackberry 10 users.

## Swivel Core - New functionality

### Configuration replication - Shared Secret

Building on the 'Configuration Replication' introduced in the last version, additional security has now been added requiring the use of a 'Share Secret' between appliances in order to allow configurations to replicate.

### Voice Support Transport

Functionality has been added to support voice based authentication. An administrator can now define if a user is to be called, and set the company that will make the call. See here for user guide:

<https://kb.swivelsecure.com/wiki/images/1/11/NexmoVoiceSetup.pdf>

### Reports by Email

Administrators now have the option to email scheduled reports and add logic to reports if required.

### Comma policy removal for mobile client

The use of the new Mobile Apps with this current version of Swivel has eliminated the need for users to enter a comma as part of the OTC. See here for user guides and video demonstrating the new quick provisioning user experience. The refactoring of this element of the core has also fix a number of issues related to some modes of RADIUS-based Token authentication:

[https://kb.swivelsecure.com/wiki/index.php/IFhone\\_2.0](https://kb.swivelsecure.com/wiki/index.php/IFhone_2.0)

or

[https://kb.swivelsecure.com/wiki/index.php/Mobile\\_Phone\\_Client\\_2.0](https://kb.swivelsecure.com/wiki/index.php/Mobile_Phone_Client_2.0)

## Swivel Core – Bug Fixes

### Inbound Servlet Issues

Agent-XML API calls changed to reflect new database schema

### Session sync default shared secret Issues

Admins can now sync sessions with any password set.

### Display Issues with PINpad Images

An issue relating to PINpad images not showing correctly has now been resolved

### Wrong Index on User Attributes Table

Issues relating to the wrong index being used on the user attributes table, which impacted performance of on retrieving user attributes have now been resolved.

### Log Viewer Screen Sizing

Screen sizing issues, which left links showing off the side of the screen, have now been resolved.

### HTML / Plain Text Security Strings

An issue relating to plain text security strings being sent after HTML has been enabled has now been resolved.

**Sub menu Ordering**

Sub menu items are now correctly configured to order numerically.

**Token Data Migrating Issues**

The issue relating to token data not migrating across from MySQL correctly has been rectified and the token table is now include correctly in the sync.

**User Exists for alternative Usernames**

User exists functionality (via API or for RADIUS proxying) now works with alternative usernames

**Replace PINsafe with Swivel**

PINsafe has been replaced with Swivel on default messages and field descriptions.

**TokenIndexImage and TokenIndex**

TokenIndexImage and TokenIndex are now accessible through the appliance proxy.

**Group Names**

Group names which include # in the path can now be included in LDAP repositories.

**Generic Error Trapping**

Prevent stack traces from showing to the user

**Session Replication Errors**

Errors which lead to sessions being deleted when two cores were working in sync has been resolved.