

Swivel Authentication Version 3.9.6

Release Bulletin

Introduction

This release bulletin relates to Version 3.9.6 of the Swivel Authentication Platform.

This latest release brings with it new product enhancements to the Swivel Core and user experience. 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.

Feature Overview

Product Enhancements

- OATH Support

Other Enhancements

- Admin Console Re-direction
- Sync Job Enhancements
- RADIUS authentication Enhancements
- New mobile functionality
- Upgrade to Share Point Filter
- Site ID Enhancements
- SMS Support

Bug Fixes

- Android Phone
- Core

Feature Details

Product Enhancements

OATH Support

The addition of OATH support means that the Swivel Platform really is the only authentication solution you will ever need.

This removes a number of barriers to Swivel deployment, for example:

- Where two-factor authentication is required and mobile-phone cannot be used (e.g. in call centre)
- Where customers seek standards compliance (OATH)
- Where customers have invested in tokens and want to migrate

The tokens supported by Swivel are OATH HOTP tokens and are event-based tokens.

The Swivel Core server can be configured to treat members of a certain repository group as being able to authenticate using an OATH HOTP token; when the repository is synchronised users that are members of that group will be marked as being OATH Token users.

Token administration

Tokens are provisioned onto your Swivel Core Platform by uploading the seeds and serial number data via the admin console.

Tokens are identified via a visible serial number and secret seed. Your token provider can provide you with a list in electronic format that highlights which serial number relates to which seed.

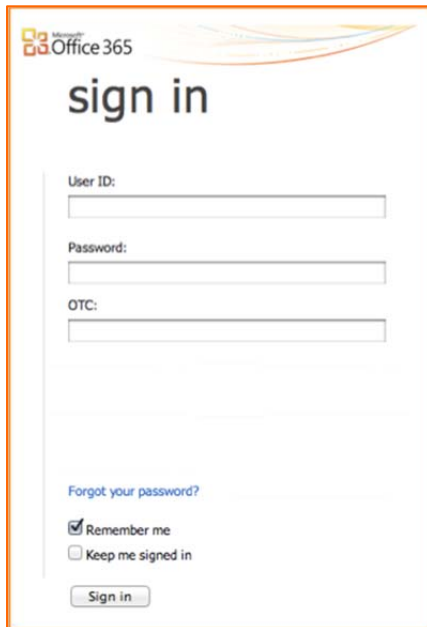
The Swivel administrator can upload this data to the Swivel Core in order for the Swivel Core to store serial-number & seed information. (Token seed information can also be manually entered). See information is stored on the database in an encrypted format.

Once the seed information is stored on the Swivel platform, tokens are then referred to by their visible token serial number.

The token-admin screens show which user has which token and will also list unallocated tokens in order for them to be allocated.

A user (or administrator) may wish to synchronise a token. To do this they enter two successive OTPs. This allows the Swivel platform to calculate (and store) the number of events that the token has been used for.

User Authentication Process



Microsoft Office 365
sign in

User ID:

Password:

OTC:

[Forgot your password?](#)

Remember me
 Keep me signed in

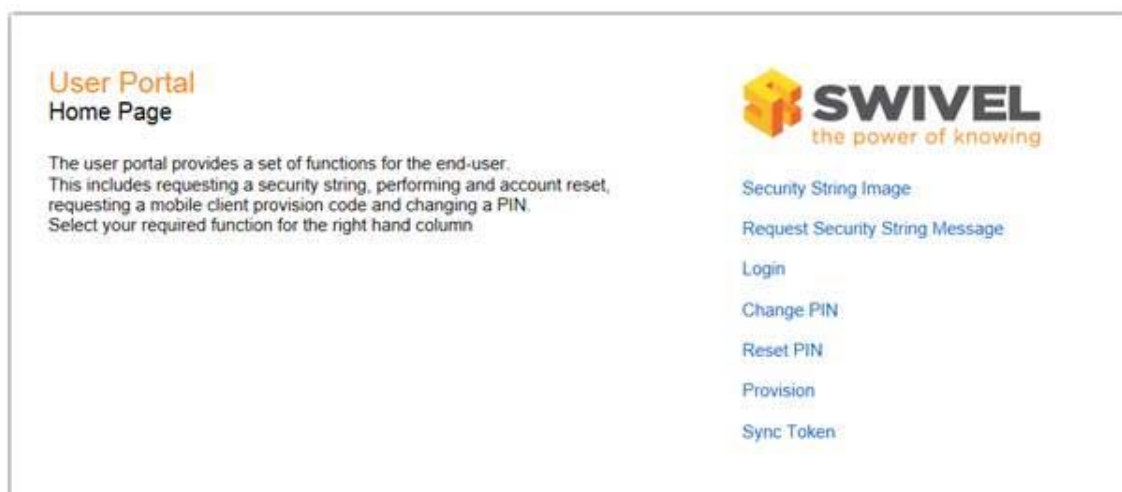
A user allocated a token will need to have the token present at the time of login, in order for them to authenticate.

The token generates a unique 6 digit number (OTC) which expires after about 10 seconds. This OTC will be entered at the time of login in order for the user to be authenticated.

The user will enter their username, password, and then simply enter the 6 digit code provided by the token into the OTC box.


Token Synchronisation

If a user loses the ability to login even though they are using the correct OTC from the token then it's possible that the token has become de-synced. If this happens the user will need to re-sync by going to the Swivel User Portal. The option "Sync Token" has been added to the User Portal:



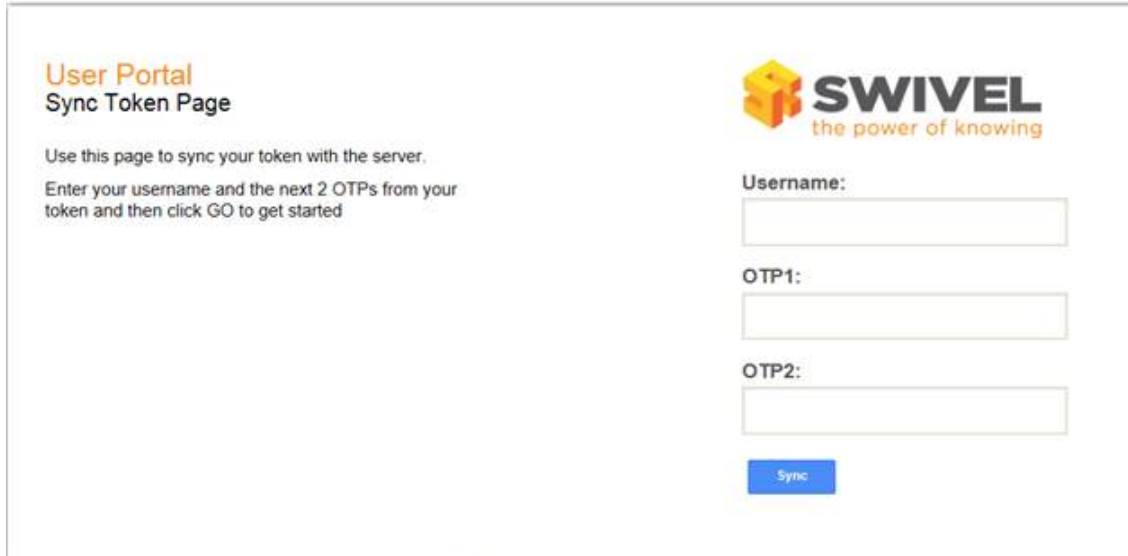
User Portal
Home Page

The user portal provides a set of functions for the end-user. This includes requesting a security string, performing and account reset, requesting a mobile client provision code and changing a PIN. Select your required function for the right hand column.

 **SWIVEL**
the power of knowing

- [Security String Image](#)
- [Request Security String Message](#)
- [Login](#)
- [Change PIN](#)
- [Reset PIN](#)
- [Provision](#)
- [Sync Token](#)

If the user clicks on this option they will be taken to the following screen:



The screenshot shows a web page titled "User Portal Sync Token Page". On the left, there is instructional text: "Use this page to sync your token with the server. Enter your username and the next 2 OTPs from your token and then click GO to get started". On the right, there is a form with the SWIVEL logo at the top. The form contains three input fields labeled "Username:", "OTP1:", and "OTP2:". Below these fields is a blue button labeled "Sync".

The user will need to input their username followed by the next two consecutive OTCs. This will re-sync the token and allow them to log in. A user account may have been locked due to too many failed login attempts - this will need to be resolved by a helpdesk user.

The server will recognise the two consecutive numbers and synchronise with the token.

Policy options:

If required, a policy control may be set to force a user to enter their PIN directly after the OTC generated by the token. The user will append their PIN to the generated token code, they will need to include the PIN at the end of the 6 digits without any decoration (i.e. “,”)

Other Enhancements

Admin Console Re-direction

To enhance usability, the option to redirect to another page if access to the admin console is not allowed has been added.

Sync Job Enhancements

Improvements have been made to increase the efficiency of the Sync Job. This means that changes made on the transport screen will now take immediate effect without the need for a User Sync. In addition to this, when changes are made to a user on the user edit screen an asterisk (*) will be shown next to the user name to indicate that a User Sync needs to take place in order to sync the changes into the database.

RADIUS authentication Enhancements

Enhancements have been made to the two-stage RADIUS authentication facility to provide increase flexibility and the following admin options are now available:

- Option to not automatically send a security string after the first stage.
- Option to allow unknown users to authenticate using only repository password.
- Option to allow different challenges to be sent after the first stage, based on group membership.

SMS Support

New SMS support added for SMS service provider Packet Media and Phonovation

Site ID Enhancements

Facility to allow the Site ID to be stored within Swivel, and accessed in a Transport by a name, as opposed to manually entering the ID number. Facilitates reuse of the ID without introducing typos.

Mobile - new functionality

SMS Security String Usage

Users now have the ability to move back and forward through the security strings provided by Swivel, and are no longer required to use them in the specified order they arrive. This provides additional usability for working with secure RADIUS protocols such as CHAP.

Client provision Process



It is now possible to automatically provision new users via an SMS link. This new functionality is supported for Android and iPhones.

Bug Fixes

Android - bugs fixed

- Icon on android desktop has been corrected

Swivel Core - bug fixes

User history- now includes the latest event of each type, from the activity table, if no events of that type have occurred in period covered by the audit table.

User Attributes - When default value for a particular user attribute in a particular repository type is not empty (which is the case for all repository types except DB), they can now be not included.

User Credential Send Issues - Credentials will now always be sent to new users even if re-send credentials have been disabled on transport change.

Admin XML - XML has now been amended to ensure that special characters are correctly encoded.

The Helpdesk API - Customer messages can now be sent to any user and is not limited to users in agent based repositories.

NAS Entry Issue - The issue relating to creation of a NAS entry that was too long for the audit table has been resolved.

PIN Expiry Check Failure - The issue relating to PIN expiry checks failing if either last PIN change or last admin reset was null has been resolved.

Support for PostgreSQL Database - Support for the PostgreSQL database has been removed.