Swivel Authentication Version 3.9.1

Release Bulletin

Introduction

This release bulletin relates to Version 3.9.1 of the Swivel Authentication Platform.

There have been a number of changes at Swivel Secure recently. One of the most important changes for our customers is the way we continue to develop our authentication platform.

Swivel has moved to the agile development process and will be working to much shorter release cycles. This change will enable us to deliver new product features and enhancements to our customers through product updates every 6 to 8 weeks.

This latest release comes hot on the heels of version 3.9 and brings with it some key product attributes. A significant change of great importance to our customers is the way the Swivel authentication platform is structured. This change, once implemented will streamline and simplify the upgrade process of the Swivel platform.

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

- Simplification of the Swivel upgrade process
- Federated identity support
- Viewing of queue sizes on status page

Other Enhancements

- Pin Reset
- Lockout
- Issues with Reactivated users
- Phone prefix issues
- Issues with log viewer
- Errors in cron string management
- AdminXML federatedID issues
- Stack overflow error in log viewer
- RADIUS MSCHAP
- User sync failures
- User attributes visibility issues

Feature Details

Product Enhancements

Simplification of the Swivel upgrade process

From version 3.9.1 Swivel upgrades will only require replacing the Swivel software. Configuration data will now be held outside of the main product distribution, which will simply the upgrade and install process.

Simplifying the upgrade route, will allow users to easily migrate and update to the latest release, thereby taking advantage of the new release schedule that Swivel are adopting. This will allow future enhancements of the product to be easily recognised.

Federated identity support

Swivel now supports multiple login credentials for a single licensed user. This new feature provides user with the flexibility to use both AD account names, and services (i.e. cloud), which predominantly use an email address as the login credential. User will now be able to access multiple services, using their Swivel PIN code.

Viewing of queue sizes on status page

The number of pending messages on each transport queue can now be viewed at the bottom of the status page. Updated counts from static display can be viewed on completely a page refresh.

Other Enhancements

Pin Reset
Resolves the issue relating to different expiry times being set depending on if a user resets their pin or if an admin/helpdesk user resets the user's pin.

Lockout
Resolves issue whereby, under certain circumstances, a user could be locked out incorrectly due to incorrect checking of dual channel and mobile rights.

Issues with Reactivated users
Resolves issue whereby reactivated users could be re-marked as inactive before they had a chance to login.

Phone prefix issues
Resolves issue whereby, under certain circumstances when using AD repositories, the phone prefix was not being removed.

Issues with log viewer
Resolves issue whereby, under certain circumstances, the pin of a security string message could be seen in the log viewer. The value shown was not correct so no security problem existed but this display has been corrected.

Errors when scheduling reports, and repository synchronisations
Specifying multiple days of the week now correctly shows as custom entry.
Specifying an invalid schedule (cron job) now correctly shows an error.

AdminXML federatedID issues
Resolves an issue when retrieving the user's e-mail address to use as a federatedID. Now retrieves the e-mail when either the string transport or alert transport uses an e-mail address.

Stack overflow error in log viewer
Resolves an issue whereby under certain circumstances a stack overflow error occurs in the log viewer.

RADIUS MSCHAP
Resolves an issue whereby when using RADIUS MS-CHAP protocol a user could be authenticated to PINsafe with any OTC.

User sync failures
Resolves issue whereby, under certain circumstances, attributes are not loaded correctly on startup.
Resolves issue whereby, under certain circumstances, the user sync would fail after upgrading to 3.9.

User attributes visibility issues
Resolves issue that caused user attributes not to be shown on the edit screen after adding a new user to an OpenLDAP writeable repository.