# Versions FAQ

## Contents



# Overview

This FAQ outlines the different features brought in by the differing versions of Swivel. Some releases contain some bug fixes and these are not generally listed below. Unless there is a specific requirement, an upgrade would usually be made to the latest version. To find your version see Version Information.

# Prerequisites

The Swivel software is only provided as part of an appliance installation. Direct software installation on a Windows or Linux server is not supported by Swivel as a production deployment environment.

For Sales or technical help with an appliance please contact sales@swivesecure.com

# News and Updates

For information on receiving details of new versions and news see Contact Details.

## Swivel Virtual or hardware Appliance Upgrades

When upgrading Swivel on virtual or hardware appliances do not use these files unless directed by suppport, instead see Patch Swivel Install. Swivel updates for appliances are contained within patch files, for information on specific patch versions see Appliance Swivel Core Patch File Verions FAQ.

For information on upgrading Swivel on virtual or hardware appliances see Patch Swivel Install or for software only see Upgrade PINsafe. To find your version see Appliance Versions FAQ.

## Swivel Core Update Information

### AuthControl Sentry 4.2.3 (7074)

Released: March 2024

**IMPORTANT FOR Active Directory Repositories:** As well as updating the Core software, we have also updated the Java version. Unfortunately, this means that there are stricter controls on LDAPS connections. This means that it is no longer possible to connect to the domain controller using an IP address, unless the TLS certificate on the domain controller contains a Subject Alternate Name for the IP address. The simpler alternative is to use the hostname in preference to the IP address. This may require changes to the DNS settings for the appliance, if it does not recognise the host name.

- Fixed authentication issues when using mobile app for PINless users
- Only send one message when users are locked/unlocked using the API
- Better detection of invalid characters when writing API errors to the logs
- Fixed password authentication for users not known to Sentry, if permitted
- Added the latest Apple Push certificates

### AuthControl Sentry 4.2.3 (7040)

Released: January 2024

- Fixed issue with authenticating when using mobile app with a password
- Updated version of ActiveMQ due to reported vulnerability

### AuthControl Sentry 4.2.3 (6939)

Released: October 2023

- Apply SMTP Changes Without Restarting Tomcat: in the previous version, SMTP configuration changes did not take effect until Tomcat was restarted. This issue has now been resolved.
- Date Filters in Log Viewer (Bug): Date filters in the log viewer were not functioning as expected. This issue has been fixed, and date filters now accurately filter log entries.
- SMTP Logging Issue (Bug): SMTP logging was not functioning correctly, leading to a lack of log records. This issue has been addressed, and SMTP logging now works as intended.
- Disabling XML Logging (Bug): Disabling XML logging also disabled other log types, which was not the intended behavior. This issue has been rectified, and disabling XML logging now affects only XML logs.
- PINless Users in ACD with PINless TURing (Bug): PINless users were able to log into ACD with PINless TURing, which was not intended. This security concern has been addressed, and PINless users can no longer access ACD without proper authentication.
- Append PIN to OATH Fails in RADIUS (Bug): The process of appending a PIN to OATH tokens in RADIUS was failing. This issue has been resolved, and the PIN append functionality now works correctly.
- Circular Definition in XSL (Bug): A circular definition issue in XSL has been identified and fixed. XSL definitions no longer result in circular references.
- ConcurrentModificationException in ActiveMQManager (Bug): An issue causing ConcurrentModificationException in ActiveMQManager when accessing statistics for all transport queues has been addressed. The software now handles concurrent access without errors.
- ActiveMQ Failure - "Timer Already Cancelled" (Bug): An issue related to "Timer already cancelled" failures in ActiveMQ has been fixed. These errors no longer occur.
- Configuration Sync Group Names Display (Bug): Configuration sync group names were not displayed in the Status page, making it challenging to track configuration changes. This issue has been resolved, and sync group names are now visible.
- SMTP to SMSGateway Start TLS (Bug): The SMTP to SMSGateway transport did not allow the use of Start TLS for secure communication. This limitation has been removed, and Start TLS is now supported.
- Reprovision OATH Token in Mobile App (Bug): Users encountered difficulties when attempting to reprovision OATH tokens in the mobile app. This issue has been fixed, and token reprovisioning is now seamless.
- Assigning Tokens to Users with \\ in Their Names (Bug): Assigning tokens to users with backslashes \\ in their names resulted in errors. This issue has been resolved, and tokens can now be assigned to users with special characters in their names.
- OATH Tokens Page for Helpdesk Users (Bug): Helpdesk users were unable to access the OATH tokens page. This issue has been addressed, and the OATH tokens page is now accessible to helpdesk users.

### AuthControl Sentry 4.2.2 (6854)

Released: June 2023

**New Features**:

- Log4j Update: The update of log4j to version 2.19.0 in this release is an important and necessary step in ensuring the security and stability of our software. With the recent discovery of vulnerabilities in log4j version 2, it is imperative to take measures and mitigate any potential risks. Updating log4j is not only a matter of addressing security concerns but also to ensure that the software remains up-to-date and compatible with other systems or dependencies. In addition, the update done stores logs directly in a database, making the stand-alone logviewer obsolete, and making log searching much faster.

- Spring Framework Update: This release features an important update to the Spring Framework, which addresses vulnerabilities present in previous versions. The Spring Framework is a widely-used Java-based framework that provides developers with an extensive set of tools and features for building enterprise-grade applications. This update ensures that the software remains secure and stable, providing customers with greater peace of mind. By mitigating these vulnerabilities, the update protects the application and ensures the integrity of customer systems.

The update also ensures that the software remains compatible with other systems and technologies, providing a seamless experience for customers. Overall, this update to the Spring Framework represents a significant step in the commitment to providing secure and reliable software solutions.

- New transport integration with SaudiAlert: This release features an exciting new integration with Saudialert, a leading cloud-based SMS gateway provider based in Saudi Arabia. This integration enables Middle East customers to leverage Saudialert's reliable SMS infrastructure directly from the software, allowing them to send SMS alerts and notifications with ease. This integration also offers greater flexibility and customization options for customers in the Middle East, allowing them to tailor their SMS messages to specific regions and languages. Overall, the integration with Saudialert SMS gateway provider provides a powerful and efficient SMS solution for Middle East customers to enhance their communication efforts.

- New Reports Available: This release includes the addition of new reports in Sentry, following several customer requests. These reports provide customers with valuable insights and analytics on their data, allowing them to make more informed decisions. The new reports cover a range of topics and have been designed to be user-friendly and intuitive. Customers can customize and filter the reports to meet their specific needs, and can easily export the data for further analysis. This new feature is a valuable addition to the application and demonstrates the commitment to meeting customer needs and providing a superior user experience.

- Appliance Identification: This release includes an important new feature for customers using the high-availability architecture of the product. The feature enhances the ability to identify whether writing to a shared database is being done by the primary or standby appliance. This is accomplished through the identification of the appliance in logs whenever a write occurs. In addition, the feature includes the ability to set different default configurations for scheduled jobs where required. This provides customers with greater visibility and control over their high-availability architecture, enabling them to monitor and manage the appliances more effectively.

**Improvements**:

- Enhanced Authentication Error Messages: This release includes an important improvement to authentication error messages. Authentication errors are now more explicit and informative, providing administrators with a clearer understanding of the reason for the failed authentication. This feature provides system administrators with greater visibility into the cause of authentication failures, enabling them to more effectively manage user accounts and ensure the security of the system.

- Enhanced SCPinPad parameter handling: This release includes an enhancement in the SCPinPad API?s parameter handling. The padno parameter, which was originally intended to distinguish between multiple requests for the same username, has been updated to support a new behavior. These updates will provide improved flexibility and usability for integrations using the SCPinPad API.

**Bug Fixes**:

- User Exist API fix: The User Existence API has been fixed to address an issue where it would check all user attributes, leading to inconsistencies or false positives. With this update, the API will only check for the username or altusername attribute, ensuring accurate results and reducing the potential for errors. It will also check any attributes defined as alternative usernames for the Agent making the request. This fix improves the reliability and accuracy of the User Existence API.

- API Improved Error Response: This issue was related to an API that previously would not provide a clear and descriptive error response when the request structure was incorrect. Instead, logs would print a Java error due to the lack of XML content in the response. With the bug fix, the API now provides an XML response that is more user-friendly and that indicates the reason for the error, making it easier to diagnose and address any issues.

- Database Pooled Connection Error: This bug fix addresses an issue where the application logs were throwing an error due to a null pointer exception caused by a missing object in a specific scenario. The fix corrects the code to properly handle the missing object and prevent the error message.

- Fixed User Sync Crashing due to license limit: Previous Sentry versions would crash the user sync service when the user license limit was reached. However, this issue has been resolved in the current version, and the user sync service will no longer crash when the user license limit is reached.

- Append PIN option not copied to TOTP on upgrade: In the previous version, the Append PIN option for OATH policies was only copied to HOTP on upgrade and not to TOTP. This led to inconsistencies in policy settings and configuration issues. With the latest bug fix this is properly copied to both HOTP and TOTP during upgrades, ensuring consistent policy settings for both types of OATH policies.

- Fixed incorrect message sent to user upon undelete or un-disable: In previous versions, when a user was undeleted or un-disabled, an incorrect message stating that the user was "unlocked" was sent. This has now been fixed, and the proper message is now sent to the user. This ensures that users receive accurate and appropriate messages, improving the overall user experience.

- Fixed issue with OATH and MobileApp: Previously, if a user with an OATH token entered a mobile app code, the OATH would fail and the logic would assume that the mobile app code was not applied. This issue has been fixed, and users with OATH tokens can now enter mobile app codes without any issues.

- Issues after switching from Shipping Database: A fix has been implemented for an issue related to switching from shipping database mode. The issue was caused by new flags in the database which required a tomcat restart. The issue has now been resolved and switch from shipping database mode will not cause previous issue.

- API locked policy: In Sentry last version, AdminAPI status flags had changes and "locked" attribute was no longer valid. Instead, the attribute "lockedByAdmin" should be used. For backward compatibility, both attributes will be accepted.

- HTML Message Preview not deconding: In Sentry last version, HTML preview doesn't decode from base64 and messages were not properly previewed in browser. This issue has been fixed.

## AuthControl Sentry 4.2.1 (6751)

Released: January 2023

**New Features**:

- OATH code visibiity (past, present and future) in User strings / Administrators can have a pick in the past OTCs and futures OTCs. This feature is helpful to fully understand the policies applied to OATH and possible issues that could be resolved with policies.
- Customization and logs insertion for new modules and features in Sentry logs / New availability to add logs to Sentry; tailor made solutions will have even more information added to the logs
- Addition of dedicated policies for TOTP and HOTP token / New customization for specific types of token configured. Dedicated policies helps administrators to setup and define configuratio of token types
- MDM available in AuthControl Sentry to control AuthControl Desktop in domained workstations / Similar to user synchronisation, this new module allows Sentry to sync computers in domain to remotely install AuthControl Desktop, manage availability of MFA on workstations, enable and disable agent remotely along with a dedicated Dashboard related to workstations authentication activities

- Tomcat update to version 9.0.68 / Upgrading to version Sentry 4.2.1 updates Tomcat to version 9.0.68 which have important security updates. Please refer to release notes of Tomcat 9.0.68
- PIN expiry management / Ancillary application to help on PIN expiry-renewal process using Sentry APIs 2.2

**Bug Fixes**:

- Last OTP sessions synchronisation fix / Correction to SyncXML so that Last OTP replicates on standby appliance
- User lock flag adjustments / Fix on previous update which marks deleted users as locked instead of deleted
- Appliances with zipped logs boot fix / Fixed issue that happened in some cases starting the appliance when there are too many zipped log
- OATH authentication fix for users with PINless policy / Issue fixed for users using PINless and OATH privileges
- Database upgrade fixes (NAME_ID_FORMAT) / Database upgrade script in some cases would not add the required column which is now fixed in this version
- Fail logins message adjustments / Messages adjustments to properly identify the reason why authentication has failed
- Mobile app policies initialisation fixes / Duplicated entries in Mobile App policies fix
- Fix for password field not displayed for admin login after logout / Password field was not coming to display after admin logout the web application
- Fix logs with LOCK_USER messages / Fixed logs being filled with unnecessary information of LOCK_USER
- Fix for Helpdesk policy on users creation / Helpdesk policy fix to allow helpdesk user to create users
- New dispatcher-servlet.xml to fix deployment of appliance web apps / File update to fix some cases that SSO Portal would not start properly
- Fix characters display of appliance web apps / Special characters adjustments
- Session start fix to point to imageserver / Fix for session start that was pointing to pinsafe server instead of image server
- Account unlocked audit message uses wrong subject fix / Mailing fix to set subject properly for accounts unlocked
- Refactoring of libraries / Duplicated libraries and old version libraries refactor

## AuthControl Sentry 4.2.0 (6612)

Released: 1st June 2022

**Sentry Core** :

- Push notification authentication can now be configured using reverse proxy
- Database migration process from older appliances is improved
- Database migration process from older MSSQL databases is improved
- Login sessions now sync via database
- IP addresses reserved for user VPN account can be sent via RADIUS and retrieved from AD
- Reporting now includes source IP and authentication method used by the user
- Group display order is now consistent across all screens
- Policy for account lockout time
- AD password management in User Portal
- Account ?claim code? feature for users with no email or telephone in repository
- Self management: users can now change their PIN with account locked
- Self management: users can now unlock the account with Reset PIN or Change PIN option

**AuthControl Single Sing-On Portal** :

- Local applications can be defined in SSO portal with new PAM method / user known credential storage
- Local applications can be defined in SSO portal with new P2AM method / user will never know credentials
- Web applications supporting OAUTH2 can be integrated in SSO portal
- Web applications supporting OpenID can be integrated in SSO portal

**Bug Fixes**:

- Log4J updated to 2.17.1 and necessary maintenance undertaken to make this compatible
- Name ID format now available in SAML SSO integrations
- PINless policy and PINpad implementation caused duplicated digits to be displayed, now handled
- Handling of special non UTF-8 digits in passwords to avoid invalid characters logging
- Reset password option was ignored unless policy indicated that password is required. Fixed option by resetting password irrespective of whether password required policy is set / not set.
- User groups with . character in the name were not being assigned to repository on first sync
- Connectivity loss during User Sync now results in aborted sync
- Latest ActiveMQ libraries updated to fix vulnerabilities
- App provision issues for usernames containing spaces rectified by URL decode fix
- Fixed reported behaviour conflict of timed lock-out policy with other policies

**Recommendation**:

- Any reports that reference the policy flags table, PINSAFEC, will not work with Sentry version 4.2 or later, and must reference the new status flags table, PINSAFES.

## AuthControl Sentry 4.1.3 (6502)

- Updated SMTP client libraries to support TLS 1.2.

## AuthControl Sentry 4.1.3 (6487)

Released: 8th December 2021

**Sentry Core**:

- Abort user sync if there is an error connecting to LDAP.
- Fixed error with Push response when used with AuthControl Desktop
- Changes to Simple LDAP repository to improve compatibility
- Allow provisioning of mobile app for usernames containing spaces
- Fixed compatibility of 4.1.3 with MS SQL Server
- Further correction to SMPP transport
- Restored the previous Secure SMTP transport as a custom instance of SMTP transport

## AuthControl Sentry 4.1.3 (6442)

Released: 1st October 2021

**Sentry Core**:

- Active Directory Agent for multiple endpoints
- Support for authentication with multiple repository servers
- PINpad and PICpad added to Sentry login page
- Security improvements : Tomcat 9.0.48
- Improved Push notification with Firebase for Mobile applications.
- Random password generation for selected repositories
- Improved transport for HTTP GET and SOAP
- Syslog improvement for remote server logging
- Offline strings remaining count for WCP
- Addition of Purge users options as a scheduled service
- Voice transport and Push transport view in User Administration
- Improvements to SMS transport
- User history with authentication method information
- Improvements on welcome page in User Portal
- Push notification with Biometrics, Confirmation or a combination of both
- RADIUS Push notification improvement
- SMTP service unified for SSL and TLS protocols
- Upgrade of the security in provision codes

## AuthControl Sentry 4.1.2 (6330)

Released: 7th April 2021

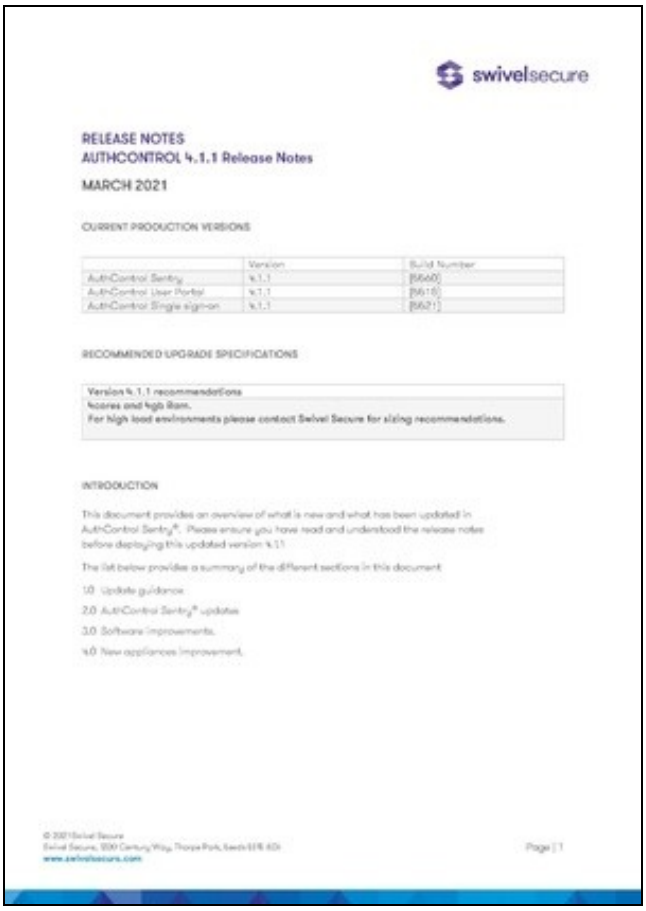
**Sentry Core**:

- RADIUS NAS entries can now specify a range of IP addresses, using CIDR notation.
- It is possible to specify how many re-uses of an OATH OTP are allowed. Our latest release 4.1.1, removed re-use altogether, but this causes problems where the OTP is specified correctly but authentication fails for other reasons.
- An error is shown on the User Administration page when attempting to reprovision a user that has an OATH token allocated. It is not permitted to have both an OATH token and an OATHbased mobile app, but previously this error was logged silently and reprovision appeared to have failed.
- A bug has been fixed whereby transports were not shown in the user administration in certain circumstances.
- The API call to initiate user sync has now been fixed.
- More improvements to session replication
- Password checking for Simple LDAP repository has been fixed.
- An option has been added to generate a random password for new users per repository.
- The RADIUS server is no longer restarted when certain irrelevant configuration changes are made.
- Sending security strings by email has been fixed.
- Line breaks in the FoxBox transport have been fixed.
- Timeout options have been added to more transports that previously would hang indefinitely.
- Support has been added for Push feature in future mobile apps, and it has been made easier to update these for future support.
- Support has been added for future versions of the mobile app that allow multiple accounts.

**User Portal**:

- Added Japanese translation.
- Improved support for internationalisation.
- Fixed security hole that allowed users access to user portal without authentication in some circumstances.

## AuthControl Sentry 4.1.1



swivelsecure

RELEASE NOTES
AUTHCONTROL 4.1.1 Release Notes
MARCH 2021

CURRENT PRODUCTION VERSIONS

| | Version | Build Number |
|---|---|---|
| AuthControl Sentry | 4.1.1 | [6660] |
| AuthControl User Portal | 4.1.1 | [6615] |
| AuthControl Single sign-on | 4.1.1 | [6621] |

RECOMMENDED UPGRADE SPECIFICATIONS

| Version 4.1.1 recommendations |
|---|
| 4cores and 4gb Ram. |
| For high load environments please contact Swivel Secure for sizing recommendations. |

INTRODUCTION

This document provides an overview of what is new and what has been updated in AuthControl Sentry®. Please ensure you have read and understood the release notes before deploying this updated version 4.1.1

The list below provides a summary of the different sections in this document

1.0 Update guidance
2.0 AuthControl Sentry® updates
3.0 Software improvements
4.0 New appliances improvement

© 2021 Swivel Secure


## AuthControl Sentry 4.1.0 (6095)

Released 4th March 2020

**Bug fixes**:

- RADIUS repository password check was not working since build 6062. Now fixed.
- Whole CSV import failed if one user failed to import. Now logs single user failure but continues.

**Security improvements**:

- Tomcat 9.0.31

## AuthControl Sentry 4.1.0 (6082)

Released 23rd January 2020

**Bug fixes**:

- NAS identification fix in previous release was incomplete. Now fixed.
- PIN expiry no longer uses timed lockout: users are locked on PIN expiry until released by helpdesk.

**Security improvements**:

- Tomcat 9.0.30

## AuthControl Sentry 4.1.0 (6074)

Released 15th January 2020

**Bug fixes**:

- RADIUS NAS identification now checks both IP address and NAS Identifier
- Deleting repository groups or attributes no longer causes errors

## AuthControl Sentry 4.1.0 (6062)

Released 19th December 2019

**New Features**:

- Multi NAS RADIUS capability
- RADIUS VIP for HA environments
- Push and NEXMO-VOIP on the same core is now supported
- Disk Space Check before config operation

**Bug fixes**:

- Non ASCII characters on HTML messages (Japanese, Chinese, Arabic, Cyrilic)
- PIN change not requiring upper/lower case matching on userportal (now coherent with the core authentication)
- User Portal Confirmation code is now supported on non persistent sync (appliance sync)
- Auto reconnect on Repository Sync Job connection drop

**Security improvements**:

- Tomcat 9.0.29
- Customized error pages (information disclosure control)

## AuthControl Sentry 4.1.0 (5995)

Released 9th August 2019

**Bug fixes**:

- Fixed Android push error
- Fixed Provisioning URL in SMTP transport

## AuthControl Sentry 4.1.0 (5974)

Released 5th August 2019

**Release notes**: [1]

**NOTE**: from version 4.1, the appliance database service is required for the user portal as well as Sentry SSO. If you are not using Sentry SSO and are using an external database for the Sentry Core, you will need to ensure that the appliance database service is running BEFORE updating.

## AuthControl Sentry 4.0.5 (5560)

Released 19th September 2018

**Maintenance update**:

- Renewed Apple push certificates

## AuthControl Sentry 4.0.5 (5535)

Released 29th August 2018

**Bug Fixes**:

- Fixed error using MSSQL Server and Oracle Databases regarding Attribute column size being to large

## AuthControl Sentry 4.0.5

Released 27th July 2018

**Version 4.0.5 introduces new features and fixes others**

**New Features**:

AuthControl Desktop (requires WCP v5.4.2.1)

- Biometric Fingerprint for Windows Credential Provider - Now WCP can enrol fingerprint and can identify users and be used to authenticate as 2FA. (Requires: Nitgen biometric reader or Windows 10 biometric authentication with integrated fingerprint reader)
- WCP is configurable as 2FA with RBA rules.

Sentry Core

- Generate random pin for Helpdesk in user management
- Mobile app settings were removed and are no longer used: ?Allow user to choose how to extract OTC?, ?Provision is numeric?, ?VPN URL Scheme?
- Provision code will always be numeric
- New transport: ReachData SMS Transport, MEO SMS Gateway Transport, Rand and Rave (Rapide) SMS Transport
- Possibility to limit SC and DC String Requests by time, if many requests are done in a period of time, access will be denied
- Added Fingerprint remove option (User Management -> View -> Attributes)
- Added new vendor radius Sophos
- Improved HTTP requests with HSTS, CSRF and XSS security handling
- Tomcat 9.0.10 support
- Added Trademark Registration
- Added possibility to view current OATH token to User Administration -> View Strings

User Portal changes

- Login with Confirmation code to increased security. Needs to be enabled in .swivel/user-portal/settings.properties with ?showconfirmationcode=true?
- Confirmation code blocked after too many attempts
- Change Pin now requires entering new pin twice and shows policy errors

Sentry SSO changes

- Authentication before Applications list (configurable by admin)
- Now SSO can show Applications by user group
- Added logout button
- Password field is now configurable to show or not
- Windows Credential Provider integration (for RBA only)
- Azure AD Integration (without federation)
- Possibility to add custom SAML Attributes per application. For more details: https://kb.swivelsecure.com/w/index.php/Authcontrol_v4_Sentry_SSO_and_Adaptive_Authentication#Defining_Applications
- Added Trademark Registration

**Bug Fixes/ Enhancements to Existing Features**:

- Fixed Session Sharing issues in HA
- User Portal: fixed visual issues in IE with compatibility mode, fixed issue with QR Code not working
- Fixed RADIUS with Push not working on some VPNs
- Fixed RADIUS change PIN not being able to change the length of the PIN
- Fixed Bulk Provisioning in Oracle database
- Fixed OATH tokens not being assigned on user sync from AD
- Fixed OATH tokens to remove existing allocations before assigning new token to user.
- Fixed Clickatell Transport not working due to API change
- Fixed PacketMedia Transport not working due to API change
- Fixed IPModem Transport crash if no response received from modem

## AuthControl Sentry 4.0.4

Released 27 March 2017

**Version 4.0.4 introduces new features and fixes another**

Note: A new licence key will be required to run the new features that have been rolled out in June 2016 To request a new licence key please go to https://supportdesk.swivelsecure.com and create a new ticket, quoting the name that your current licence is issued in.

**New Features**:

- Adaptive Authentication and Single Sign On: This is a means by which you can manage the way users access a range of on-premise and cloud applications. Specifically, if and how they need to authenticate in order to gain access to those services. For more details: https://kb2.swivelsecure.com/index.php/Sentry_User_Guide.
- New Branding, colours and logos on the Swivel Core have changed.
- New Name: ?pinsafe? is now ?sentry?.The main effect on existing users is that the context path for web URLs is now ?sentry?, rather than ?pinsafe?. When integrating with existing products, you will need to change the context from the default. As integration products are updated, the default context will be changed to fit with the new naming.
- AuthControl Mobile App is the new naming of the mobile app
- This version allows the Swivel Mobile App to be configured as an OATH token
- Default SMTP templates for Credentials and App Provisioning have been added. A new option on the menu has been added to allow customers to replace or add new images to the templates
- Defined default configuration for single instances
- A new policy has been included on Policy > Password that allows to hide the Reset Password button from Admin Console
- Admin and Helpdesk users can invalidate a user session from User Admin, View Strings screen. The sessions that can be invalidate are the single and on-demand dual channel ones
- Log Viewer Standalone version that automatically imports the logs from Swivel Core and stores them on a database

**Bug Fixes/ Enhancements to Existing Features**:

- Deleting Agents no longer causes errors
- Sending Message for Alternative Username
- Deleting users with repository doesn't delete them from the Swivel Core when the policy Delete Users with repository is set to NO
- Allow expired passwords set to NO doesn't allow authentication
- Positive ID is not supported anymore and it has been removed from Messaging Screens
- Removed Manual App Provisioning action

**Updated terminology**:

- Transports is now called Messaging
- OneTouch is now called Push
- Mobile Client is now Mobile App.
- Quick Provision is now App Provision

For more details, see the Release Notes.

There was a beta release 4.0.3 and updating it to 4.0.4 enhances it

## Swivel 3.11.5

**Version 3.11.5 introduces 1 new feature and enhances/fixes another**

NOTE: Swivel Secure software versions 3.x are not compatible with Java version 8.

**Changes**:

- Support for One Touch over RADIUS PAP
- Fix for SecureSMTPTransport and Support for Start TLS

For more details, see the Release Notes.

## Swivel 3.11.4

**Version 3.11.4 introduces 4 new features, and 2 bug fixes**

**New Features**:

- RADIUS vendor class to support ACL on Cisco
- RADIUS vendor class for Dell SonicWall
- RADIUS vendor class to return a single group: primarily aimed at Juniper Pulse
- Bulk mobile client provision feature

**Bug Fixes**:

- The database upgrade code for Oracle database now works correctly
- The option to allow self-signed certificates for LDAPS on Active Directory and Simple LDAP now works.

For more details on the changes, please see the release notes

## Swivel 3.11.3

**Version 3.11.3 is a bug-fix release for issues found in 3.11.2 and earlier versions**

**Network connections now closed promptly on error**

It was found that, if network connections failed for whatever reason, the connections were not closed immediately, but were left to be closed by Tomcat automatically. As this could take some time, in a busy environment this could result in connections running out, or depending on the environment, running out of memory or database failures. This fix ensures that, if a connection fails for any reason, it is closed immediately.

**SMTP authentication now works**

Due to a typographical error, authentication to the SMTP server was never applied in versions 3.10.6 and 3.11.2. This has now been corrected.

**SMTP connection pooling is now configurable**

SMTP connection pooling was introduced in versions 3.10.6 and 3.11.2. Unfortunately, the default settings meant that connections in the pool could expire and so SMTP messages fail. In this version, 3 new options were added:

- Use Connection Pooling: this allows administrators to enable or disable connection pooling. However, disabling pooling could mean that some messages may fail if a large number of messages are sent in a short time.
- Connection Idle Timeout: this sets the length of time a connection remains valid after being used. The default is 30 seconds, but individual administrators may need to experiment, based on mail server settings.
- Max. No. Messages per Connection: this sets the maximum number of messages that will be sent by a single connection. The default is 10. The setting for this will depend on mail server settings.

**Deleting Agents no longer causes errors**

It was found that deleting several Agents could cause the Agents configuration screen to crash, although the Agents were deleted. Restarting Tomcat fixed this problem, but this is not convenient. This release fixes this problem.

**Changes to RADIUS authentication for unknown users**

- Now uses the correct username to pass to LDAP

The feature that allows users not in the Swivel database to authenticate through RADIUS using repository password only only worked if the username used to authenticate to the repository was the primary username for the repository. In other words, the attribute for authenticating unknown users, set in the NAS, was not used. There was a workaround: to create an Agent with exactly the same name as the NAS and set the attribute on that. However, when checking unknown users, RADIUS authentication now correctly checks the NAS username attribute, rather than the Agent attribute.

- Uses domain prefix to select repository

Previously, the ability to authenticate unknown users to the repository was restricted to one named repository. Now, if the username is entered in the form ?domain\username?, Swivel will attempt to identify the repository from the domain prefix. It first checks against any domain prefix specified for the repository, and if there is no match, against the repository name. If the domain does not match, it is simply ignored, and the default repository is used.

**Reset PIN without Resetting Password**

The API call to reset PIN using a confirmation code now takes an additional option to specify whether or not the user?s Swivel password should also be reset. Previously, if the user had a Swivel password, it would always be reset along with the PIN. Now, it is possible to reset just the PIN. As this is an API call, it requires that client applications, such as the User Portal, should be updated to support this option.

## Swivel 3.11.2

**Version 3.11.2 supports both the previous and new licencing method. Customers on versions 3.10.5 or below do not need to update their licence immediately unless Sentry is being added to the licence. Version 3.11.2 also includes the changes in 3.10.6.**

## Swivel 3.11

**Version 3.11 requires a different licence key to previous versions, please ensure you obtain a 3.11 licence key before updating any production instances. However, 3.11.2 onwards supports both licences**

This is a new full release, but because of the requirement for a new licence key upgrades will require you to contact Swivel prior to completing the upgrade.

New licence keys are free to customers with fully paid support.

NOTE: 3.11 is based on 3.10.5, and does not include any changes made in 3.10.6.

**New Licence Model**

- Install new licence key
- Any upgrades you purchase will be added to your Swivel installation without the need for you to install new licence key
- Swivel core needs to be able to contact Swivel Licence server to be updated

**Mobile Client Local Mode**

- Deploy client in local mode
- Client never needs to contact the Swivel Core Server
- Swivel Client generates its own security strings locally

**Mobile Client Index**

- Mobile client stays in sync if user accidentally enters an index greater than the one expected (and the authentication fails)

**New Transports**

- Nexmo SMS supported
- SMTP over TLS supported

**Bug Fixes**

- View Strings for Mobile client no works for non-dual channel users
- User admin screen speed issues for MS SQL installations resolved
- Timed lock-out issues remedied
- Session replication over TLS on V3 Appliances fixed

## Swivel 3.10.6 (3476)

Released 4th February 2016

NOTE: version 3.10.6 is later than version 3.11, but does not include support for the new licence format.

- Fixed bug when attempting to log on with no security string

**Swivel 3.10.6 (3395)**

Released 13th January 2016

- Fixed count limit when syncing ADAM repository
- Fixed speed issue viewing User Administration page
- Removed Repository view from Editable repositories, because of speed issues
- Automatic single-user sync in Editable repositories
- Refactored User Sync Job to improve speed

## Swivel 3.10.5 (3030)

Fully released. 12th October 2015

**Oath Tokens**

- The dates on which tokens are imported and allocated to users are now recorded
- Reporting options now available for tokens
- Tokens can now be allocated using Active Directory attributes
- Helpdesk users can be permitted to administer tokens

**User Administration**

- There is a new Repository view in the User List page
- User edit for helpdesk users fixed

**Custom Attributes**

- The domain qualifier can be added to any attribute, not just the username
- Option not to synchronise attributes with repository now works correctly

**General**

- Optionally, a new dual-channel string will not be sent if the user already has a valid string
- Optionally, repository password will still validate even if the user?s password has expired
- Special security string image for sight-impaired users
- Account locked message will now only be sent once each time a user is locked
- Enhancements to Modem transport, including flash support
- Clickatell transport now supports flash SMS

**Bug Fixes**

- Fixed problem where HTML messages could break the configuration
- RADIUS NAS entries now correctly support alternative attributes
- Date format for report parameters now respects the global date format

## Swivel 3.10.4 (2701)

released: 18th June 2015 Release Bulletin

- OneTouch Out of band Mobile APP and OneTouch Voice Authentication
- Provision Mobile Client using a QR Code Provision
- User Attributes Synchronisation
- Swivel Remote Sync Client
- Mobile Client fingerprinting options
- Helpdesk API token allocation
- API token allocation
- Restore original license if new license fails to install
- MSCHAP RADIUS fix
- XML Repository username with a '_' purge fix
- User Administration Search fixes
- Username containing '\' fix for domain\username
- SQL DB Attribute field database fix
- RADIUS fix secret when existing NAS is deleted
- Deleting multiple items from a list no longer causes crashes
- Add Prefix for Telephone number bug fix
- Fix for user sync when users are not marked as deleted
- Fix for log viewer issues

## Swivel 3.10.3 (2014)

released: 29th October 2014 Release Bulletin

- Send Dual Channel string - failed authentication sends out a new string fix.
- One Touch iPhone Client.

- Mobile Clients - Remaining Keys badge indicating the number of keys or security strings stored.
- Two-stage RADIUS with no password.
- Third Party Authentication.
- Synchronised Mobile Client could not retrieve strings via the Appliance proxy - Fixed.
- Using MSCHAP, tokens could lose sync and not regain sync - Fixed.

### Swivel 3.10.2 (1950)

released: 12th September 2014 Release Bulletin (3.10.1 and 3.10.2 release information)

- Users can be Pinned for Single Channel (TURing, PINpad) and Pinless for dual channel (SMS, Mobile Phone Client)
- Alpanumeric strings can be used for TURing, SMS and Mobile Phone Apps and still allow the numeric PINpad to still function
- OATH OCRA Token API support
- Test Sync button
- Auto Provision Mobile alert on user creation option
- Mobile Client Policy to show/hide policies on the Mobile Phone Client
- Mobile Client Policy to allow Mobile Phone Client to show synchronisation status and keep existing security strings if the server is not reachable
- Provision code for Mobile Phone Client on account creation policy
- Accounts Marked as deleted cannot become locked
- OATH works now with MSCHAP
- Helpdesk Groups can optionally be administered by Helpdesk users
- PINpad now logs one session start instead of ten
- Helpdesk Admin Pin reset message corrected
- MIGRATE issues from Internal to Oracle, MySQL, MSSQL resolved
- MySQL user creation initial imported credential issue resolved
- Group Membership rule added to SAML integration (Authentication Manager)

Patched release (build 1950 - Sep 25, 2014):

- Fix for non-sending of security strings

### Swivel 3.10.1 (1701)

released: Internal only release 29th July 2014

- OATH TOTP Token support
- Agent XML Extended User Attribute support
- Phone number prefix remove/replace fix
- Non ASCII characters for XML repository fix
- You are now able to purge token users
- Sync job deleting users fix
- Helpdesk users can manage other helpdesk users

Related Updates

- Swivel Remote Sync Client (SRSC)
- User Portal transient data storage deployment
- USAM IDP X509 certificate verification

### Swivel 3.10 (1947)*Patched: 25th Sept 2014*

build 1703 released: 9th June 2014 Release Bulletin

- Mobile App One Click Provisioning and in API
- Mobile App new unified Wizard interface
- Mobile App Blackberry 10 support
- Mobile App enhanced iPad support
- Mobile App ',' removed in need for authentication
- Enhanced SAML - Untrusted IP source users are prompted for Swivel authentication, trusted users can use just Username and Password
- User Administration Quick Provision, sends out a URL to configure and provision the mobile in one click
- User Administration Manual Provision, send the user a SiteID and Provision code to manually provision the mobile
- Configuration replication shared secret added
- Voice Transport added
- Reports by Email
- Appliance Synchronisation shared secret fix
- Synchronisation Administration shared secret added
- Inbound Servlet issues fixed
- User Attributes index fix
- PINpad display issues fixed
- Log Viewer screen sizing issue fixed
- HTML embedding displays security strings correctly
- Token Migration from MySQL fixed
- RADIUS proxy for alternative usernames using User Exists fixed
- TokenIndexImage and TokenIndex now accessible through the appliance proxy
- LDAP path names may now include '#'
- Session replication errors fixed
- Agent-XML bug fix

Patched release (build 1947 - Sep 25, 2014):

- Fix for non-sending of security strings

**Helpdesk Rights Update Patch for Version 3.10 (build 1747)**

This patch updates version 3.10 with enhanced helpdesk rights management. See the notes on the helpdesk rights patch for version 3.9.6 below for more information.

## Swivel 3.9.7 (1300)

released: 12 March 2014 Release Bulletin

- Configuration Replication, see Administration Synchronisation
- Admin API support for multiple user Attributes
- RADIUS debug log writes to standard log
- RADIUS LEAP new security string fix
- RADIUS calling station ID returns the client IP address where supported
- RADIUS challenge may optionally return username:
- RADIUS 2-stage automated subsequent authentication for correct password and internal IP
- Provision URL
- New User security string bug fix
- Copy strings to alert fix
- LDAP Browser now detects correct Base DN for AD Global Catalog
- Helpdesk Group Rights retained on upgrade
- Repository ID fix for User Sync job
- Error checking on Token seed entry added
- iOS Client Policy fix
- Base DN Global Catalog browser fix
- Improved handling of invalid OATH seeds
- Fix for RADIUS with LDAP passwords containing special characters

## Swivel 3.9.6 (1046)

released: 1st October 2013 Release Bulletin

- Transport changes take immediate effect without need for User Sync
- Support for OATH HOTP Tokens
- Management for OATH Token in Administration console
- Redirect filter for Admin login when not allowed
- Configurable Site ID (SSD) For mobile client settings
- Ability to send Site ID by transport
- Users marked with a * have been edited but not had a user sync
- New SMS Transports
- RADIUS Two stage Authentication, optionally do not send string after first stage
- RADIUS Two stage Authentication, allow unknown users to authenticate using only repository password
- RADIUS Two stage Authentication, allow different challenges to be sent after the first stage based on group membership
- LDAP Sync enhancement
- Resend credentials if destination changes, option removed
- Transport Attribute support using %{attr_name} Where attr_name is the name of the attribute, see Transport Configuration

NOTE: this build fixes the following issues found in the original release of 3.9.6 (build 896)

- Some User Administration functions would not work for usernames containing underscores and other special characters (fixed in build 927)
- Swivel would attempt to send messages even if no transport destination had been set (fixed in build 927)
- A slow memory leak was discovered if user syncs were scheduled too close together (fixed in build 927)
- Initial dual channel security strings were not sent out upon user creation (fixed in build 1046)

**Helpdesk Rights Patch for Version 3.9.6 (build 1777)**

Recent changes have given more control over which helpdesk users can manage which other users. However, in doing this, we removed the ability for helpdesk users to manage other helpdesk accounts. A number of customers have objected to this restriction, so version 3.10.1 made it possible to re-enable this feature. This patch is provided for 3.9.6, for customers who prefer not to upgrade. Note that this patch should only be applied to an appliance that already has version 3.9.6 installed. As it is an appliance patch, it must be applied using the method described in Patch Management.

Note that this update does not immediately re-enable the ability for helpdesk users to manage other helpdesk users. Rather, it allows administrators to decide whether or not this feature should be permitted. To change helpdesk rights in the Administration Console, go to *Repository* -> *Groups* and click the **Group Rights** button. See the documentation on that page for more information.

## Swivel 3.9.5 (550)

released: 20 May 2013 Release Bulletin

- Change PIN and Change Password independent
- Admin logout check for PINless user
- Appliance Session Replication (virtual or hardware)
- LDAP Based DN fix
- Helpdesk groups fix
- Group Membership display fix
- Policy PIN and OTC User Help updated
- DBRepository default attributes corrected

## Swivel 3.9.4 (415)

released 15 March 2013 Release Bulletin

- SSD Server for simple deployment of mobile client settings though a site-id
- Smart Phone site-id code entry to retrieve settings from SSD server
- Automatic or Manual Extraction from PIN, defineable as an option for mobile clients

- Helpdesk users report
- New repository enhancements for helpdesk actions
- SMS Spam STOP option
- LDAP writeable bug fix
- User Attributes database Migration bug fix
- Reporting display bug fixes
- Administration console user administration attributes now visible for SQL databases

### Swivel 3.9.3 (250)

released 14 Jan 2013

Maintenance Release

- Resolved issue with Groups and attributes causing error when editing them in Agents, RADIUS NAS and Transports
- Browsing LDAP group members with non-ASCII characters resolved.
- Resolved issue using a password for editable repositories which caused user sync to fail.
- Logging error due to context never set in AdminConsoleFilter resolved.
- Missing language strings for SMPP transport added
- Added Additional parameters required for SMPP transport
- Destination Attribute appearing twice on transports screen now only shows once
- Transports from Transport -> General can now be deleted
- Default user attributes email, phone, expanded to include username, alt-name (i.e. alternative username), family-name and given-name
- Additional transports
- PaloAlto RADIUS support. If a NAS has been configured to support PaloAlto vendor attributes when a VPN submits the correct credentials, the Swivel core now returns the name of the first group the user is a member of that contains the RADIUS group keyword. Now returns this data as the 5th value off a vendor specific attribute, vendor number 25461.

### Swivel 3.9.2 (5052)

released 15 Oct 2012 Release Bulletin

War file only for stand-alone installation.

- Monochrome or orange Single Channel images and backgrounds
- HTML preview for SMTP transports
- HTML case issues with SMTP resolved
- User search by different attributes such as surname
- Swivel natively supports PINpad for numerical security strings
- Insert personal names within any transport message using %{attrname}
- Admin API reports license entitlement
- Helpdesk API includes read functionality and allows requests from Agents that are not repository names
- Specify different transitory data locations for multiple instances
- Transitory data files missing from the 3.9.1 release now moved to external location
- Allow multiple authentication attempts supports security string index and standard security string delivery
- Multiple instances of Swivel with the *SwivelHome* environment variable
- MIGRATE allows users to be Appended to an existing data store

### Swivel 3.9.1 (4908)

released 30 July 2012 Release Bulletin

- Easier upgrades. Configuration files, data, xml repository, logs and reports are now stored externally to the Swivel application
- Importing of additional attributes from repository, such as multiple usernames For example, with Outlook Web Access, users can potentially log in using their usual username (sAMAccountName), their userPrincipalName (e.g. user@domain.local) or their email address.
- Status page shows number of queued messages

For more details on the additional attributes feature, see here.

### Swivel 3.9 (4900)

Swivel 3.9 (4900) released 20 July 2012

Swivel 3.9 (4854) released 14 June 2012

Documentation

- Telephony based authentication
- Report Scheduling
- Multiple writable repositories for OpenLDAP, ADAM and XML.
- Granular Helpdesk rights
- Improved LEAP support
- SSL support for SMTP
- Improved transports model
- Improved Federation (SAML 2.0) support
- Swivel logs changed to save logs by date rather than number of files
- Compressed log files
- Improved scheduler for sync jobs
- User can change repository
- Show next Mobile Token Index
- Import users from a CSV file

## Swivel 3.8.2 (4691)

released 19 March 2012

Documentation

- Several new transports
- Option to hide password field and auto-display TURing on admin login
- Fixes for SMTP transport: better HTML support, security strings working
- Domain suffix no longer added twice
- Bug fix: could not authenticate to Swivel for 10 minutes after mobile client provision.
- Bug fix for account unlocked message
- Bug fix: timed lockout didn't work with self-reset
- Bug fixes: various PositiveID issues
- New user details reports for admin API
- Bug fix: helpdesk users were unable to reset PINs in certain circumstances

## Swivel 3.8.1 (4256)

released 23 August 2011

Documentation

- Banned Credentials fixed
- VoiceSage Transport timeout added
- Two Stage authentication through RADIUS proxy fixed
- Reprovision for Mobile Phone Client users and not dual channel users
- ChangePIN policy enforcement
- Invalid LDAP FQDN on usernames caused by repository switches
- Case sensitivity fixes for various issues
- Corrected formatting of delimited transport strings

## Swivel 3.8 (3958)

released 18 February 2011

Documentation

- Two Way Authentication, to send a message to the SMS gateway
- Resend user credentials when their transport details change is now an option
- Copy Security string to Alert allows two destinations for security strings
- Transport group now defined as strings repository group
- Option to use vertical security strings
- Optional time based lockout for accounts
- Mobile Phone App Provisioning Security restrictions
- Optional Self Provision of Mobile Client
- Banned PIN numbers
- Custom Phone Number formatting by repository
- AD Domain suffix/prefix for a repository
- Check Password with Repository by XML-Agent or RADIUS NAS
- Reporting within the Administration console and exportable to CSV or XML
- GUI can now expand/collapse configuration options for simplification
- Manual Lock, to lock an account from the Administration Console
- RADIUS Proxy Option No User session to RADIUS proxy against another Swivel instance when no session is started

## Swivel 3.7.3727

released 2010

Minor fixes and extended logging for debugging

**Known Issues With 3.7.3727**

There is a known issue with this version only: every time a user sync is run, it generates a file in the logs folder (/usr/local/tomcat/webapps/pinsafe/WEB-INF/logs on an appliance) with a name beginning with "profile". These files can safely be deleted, as they are for diagnostic purposes only, and were not intended for production.

## Swivel 3.7.3474

released 3 December 2009 Swivel 3.7 software

Documentation

- RADIUS challenge and response
- RADIUS proxy
- RADIUS passing of group membership using specific vendor attributes
- Use of security strings to be valid for more than one authentication
- Helpdesk users can be allowed/disallowed from setting PIN's to a known value
- Helpdesk users can be allowed/disallowed from adding/deleting users to the XML repository
- SMS Transports "replace previous message" option is replaced by the Normal/Replace/Flash options
- View a users Security Strings

## Swivel 3.6.3369

released 19 October 2009

Documentation

- supports IPv6
- Animated Turing, PATtern, BUTton (requires Java 1.6 or later for animation)
- Additional Single Channel parameters
- Security String Index number can be requested when sending multiple security strings
- LDAP browser in Swivel Administration console
- RADIUS NAS Agents can be configured to allow only certain authentication modes
- XML Agents can be configured to allow only certain authentication modes
- Auto PIN reset, a new PIN can be sent on account expiry
- Account expiry, dates can be set when an account will expire
- Idle account status, allows idle accounts to be visually identified
- On Demand delivery, allows a new dual channel security string to be sent to user

Java Class paths are different to previous versions

Swivel 3.6.3275 users should upgrade to 3.6.3369

## Swivel 3.5.2989

released December 2008

Documentation

- Single Channel request sessions can be shared across a Swivel HA pair
- Mark as deleted option so deleted accounts can be recovered, keeping the users PIN
- Search in User Admin and usability features
- Job schedules changed from cron to user friendly format
- Helpdesk users can be restricted to their own repository or global
- All configuration passwords are now encrypted
- More than one syslog server can be defined
- Stack traces are written to the log files

## Swivel 3.4.2503

released 27 May 2008

Documentation

- Transport Attributes setting allows transport attribute to be defined for repository
- Admin/Helpdesk API to allow external applications make Create, Read, Update and Delete operations
- Reporting API
- Repository password checking
- Audit emails for account creation and deletion
- Repository Sync Jobs refinement for speed and reliability
- RADIUS Vendor Group Class attribute support
- OWA Integration option 'Allow non-PINsafe Users' requires Swivel 3.4 or higher.

## Swivel 3.3.2304

released November 2007

Documentation

- Multiple Data Sources, such as multiple AD and LDAP data sources
- Repository Groups, allowing mutiple data sources for each group
- Repository Group Management user views
- Repository deletion

## Swivel 3.2.1811

released 16 February 2007

- External Databases can be defined, such as MySQL, MSSQL, Oracle
- LDAP data source support
- IP Filter lockdown for Swivel Administration Console
- Ignore AD infrastructure change option
- Resend tab in user administration to send user a new PIN without knowing what the PIN is
- User has no security strings bug fix

**NOTE: config.xml cannot be copied from Swivel versions earlier than 3.2. Information must be entered manually**

## Swivel 3.1.4.716

released October 2006

- Agent Groups can be defined based on IP
- PINless option where an OTC is sent without PIN protection for SMS or as a CAPTCHA for Single Channel
- PIN Policy to prevent user choice of sequential or repeated digits
- Customisable security string text
- Address ranges may be specified for agents
- Improved XML sync times

### Swivel 3.1.3, 3.1.3a, 3.1.3b, 3.1.3c

released May 2006

Documentation

- Peer and Proxy against other Swivel servers
- Authentication Policies including PIN expiry, Change PIN on first login
- SMTP Alerting
- Syslog for Swivel logging
- Improved User Administration including user locking, searching and view by status

### Swivel 3.1.2

- Rotating characters for Single Channel
- Security string may now also include upper case and lower case or mixed case letters
- On Demand Authentication where the security string is not automatically sent
- Self Reset utility so a user can request a new PIN and unlock an account
- Usernames can be case sensitive on insensitive
- User Administration supports pages and includes a search facility
- RADIUS support for MS-CHAP and MS-CHAPV2

### Swivel 3.1.1

- User Repository API to support repositories in addition to AD and LDAP
- AD integration
- MySQL database replaced by an XML repository
- RADIUS supports CHAP
- Administration Console redesigned
- Windows GINA integration

## Swivel 2.x

### Swivel 2.2.6

- Agent API, AgentXML has been developed to exchange data between the Agent and the Swivel server.
- Administration Roles added
- Logging and reporting
- Static Password support
- Swivel MIDlet re-engineered for mobile phones updated and New Administration Pages
- Updated Administration Console

### Swivel 2.1.5

- Multiple Language Support
- GSM MODEM support
- SMTP Support for security strings
- Updated and New Administration Pages

### Swivel 2.1

- Variable PIN lengths (4-10 digits)
- PINsafe PIN Admin System
- Authentication by username supported in addition to Session ID
- Licensing Added
- SLIDEbar interface has been removed

## Swivel 1.4 and 2.0

- RADIUS Proxy Support
- PATTern and KEYpad user interfaces
- Database support
- Windows installer has been updated to support the use of MS SQL and Oracle.
- LINUX installer has been updated to support PostgreSQL