
RELEASE NOTES

AUTHCONTROL 4.2.4 Release Notes

SEPTEMBER 2025

CURRENT PRODUCTION VERSIONS

	Version	Build Number
AuthControl Sentry	4.2.4	(7269)
AuthControl User Portal	4.2.3	(7158)
AuthControl Single sign-on	4.2.3	(7156)

RECOMMENDED UPGRADE SPECIFICATIONS

Version 4.2.4 recommendations

4 cores and 8 GB 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 update.

AuthControl Sentry® 4.2.4 introduces enhancements to security, performance, and usability. This release includes security updates, improved email and notification reliability, enhanced user management capabilities, and various bug fixes to ensure system stability and performance.

1.0 UPDATE GUIDANCE

This section provides basic guidance on updating your AuthControl Sentry® appliance using our YUM update service. If you require additional assistance, please contact your Swivel Secure Partner, or if you have a maintenance agreement in place, contact the support team.

- Only direct upgrades from AuthControl Sentry® V4.x are supported. If you have a previous version of AuthControl Sentry®, please contact your Swivel Secure Partner or Support team.
- Upgrades require a V4.x license

- Internet Access is required
- Working external DNS is required

1.1 SPECIFICATION REQUIREMENTS

Before commencing the update, please ensure your appliance or appliances meet the required specifications below.

The required specifications for AuthControl Sentry® V4 virtual appliances:

- OS Version: 5.15.x or higher (migration to new VM version may be required)
- Single appliance: 2 GB RAM (minimum), 8 GB RAM Recommended
- For HA appliances or SSO: 4 GB RAM (minimum), 8 GB RAM Recommended
- 2 cores Minimum, 4 cores recommended
- 150GB HDD (Thick Provisioned)
- VMware ESX/ESXi 7 or above / Hyper-V Server 2019 or above
- 1 vNIC (minimum)
- Hardware only: Please ensure your hardware appliance has sufficient memory to perform the upgrade before starting

For high-load virtual environments, more resources (Memory & CPU) can be added. Please contact support for more information as additional settings may be required.

For virtual appliances - **ensure you take a snapshot before you start.**

For hardware appliances - **ensure you take a full backup through the CMI before you start.**

1.2 PERFORMING THE UPDATE

Before you begin, please connect to the Console/CMI and navigate to *Main Menu > Version Information*. Verify that your *OS Version* is 5.15.x or higher. If not, migration to new VM version will be required. Contact us at supportdesk@swivelsecure.com for further information and to obtain the latest VM version.

To perform the update, please connect to the Console/CMI and navigate to *Menu > Administration > Update Appliance*.

The order in which you perform a system update is important. Please follow the order below:

1. CMI - Please ensure you log out and then back in again after the CMI Update.
2. System (Linux OS, services, drivers, etc). There may be a requirement to perform multiple system updates depending on your current version. Please re-run the system update until no further updates are required. After each system update, a reboot should be performed.
3. AuthControl Sentry®

If you have an External database (e.g. MSSQL) be sure to back that up prior to commencing.

If you have a high availability (HA) environment, update the standby appliance first. Once successful, update the primary appliance.

2.0 AUTHCONTROL SENTRY® (ACS 4.2.4)

This section lists all the changes to AuthControl Sentry® version 4.2.4.

2.1 SECURITY AND COMPLIANCE

Push Messaging Credentials Added

New Firebase configuration is required for the latest mobile app published (push notifications). This is a critical update for environments using push-based authentication.

Impact: Environments must update android settings and deploy the new credentials file. Additionally, a new APN transport must be configured for the updated app. If legacy and new apps are to coexist, users must be segmented into distinct user groups and mapped to the appropriate APN transport. This only affects push-based provisioning — other authentication and enrolment flows remain unaffected.

RADIUS Vulnerability Fix - CVE-2024-3596

This update mitigates a critical vulnerability by improving protection against man-in-the-middle attacks in RADIUS communications.

Impact: Addresses CVE-2024-3596 by enforcing message authentication in RADIUS responses. This ensures integrity validation and protects against spoofed Access-Accept/Reject messages. Environments relying on unauthenticated RADIUS traffic may require configuration changes or updates to the client to remain compatible. This is a security-critical update and must be applied in all exposed environments.

License Reader Fix

Fixes failure to read legacy license keys caused by an internal format change. The system now works with previously valid licenses.

Impact: Prevents license activation failures in production and test environments using previously issued keys — avoiding downtime or blocked upgrades due to license rejection. Also resolves issues for systems without online access to the license key server (LKS).

2.2 EMAIL AND NOTIFICATION RELIABILITY

SMTP Logging Loop Fixed

Prevents error cascades when SMTP logging is enabled without a valid destination.

Impact: Ensures system stability by automatically suppressing email logging when recipient fields are left empty, avoiding recursive error logging and potential log flooding.

Modern Authentication Support for SMTP

Enables compatibility with SMTP providers' new security requirements by supporting non-basic SMTP authentication methods.

Impact: Customers using Gmail SMTP must switch to OAuth2 to continue sending emails due to the deprecation of basic authentication.

Non-Blocking Audit Emails

Improves reliability and responsiveness by preventing audit email failures from slowing down the system.

Impact: This resolves performance issues observed during peak hours when audit email delivery previously caused server bottlenecks.

2.3 BUG FIXES AND STABILITY IMPROVEMENTS

Policy Checker Thread Safety

Eliminates risk of shared errors/warnings in concurrent policy checks by isolating instance state.

Impact: This change enhances the integrity of authentication policy evaluations, especially in environments with parallel user activity or integrations.

Invalid Characters in Log Viewer Resolved

Sanitizes legacy exceptions to avoid breaking the log viewer.

Impact: This fix improves diagnostic reliability and prevents operational blind spots caused by log corruption.

PINpad No Longer Breaks on Unknown User

Provides a dummy session when a non-existent user is queried in the admin panel.

Impact: This ensures a stable and user-friendly experience for administrators, especially during support or diagnostic tasks.

Agent Matching Fixed for Auth via Source

Fixes incorrect agent selection when login sources are passed through by proxies.

Impact: This ensures that the correct agent is identified in environments with overlapping IP ranges or proxies — restoring support for secure multi-agent deployments.

Token Assigned to Wrong User

Corrects an issue where tokens could be mistakenly assigned to the wrong account.

Impact: Prevents incorrect token assignments due to UI/user resolution bugs, especially in cases involving usernames with special characters.

Startup Failure Due to Empty Database

Fixes a critical startup issue caused by an exception when an empty database was incorrectly loaded instead of a valid user store.



Impact: Prevented the appliance from starting correctly in misconfigured or edge-case environments.

Exception in DCMessage Fixed

Fixes a crash when a null session is passed to DCMessage.

Impact: Prevents server errors and potential service disruption by enhanced validations. This resolves issues observed when invalid session parameters are passed to DCMessage.

2.4 USER MANAGEMENT IMPROVEMENTS

Provisioning Honors Rights

Aligns API and UI behavior when provisioning users without mobile app rights.

Impact: This eliminates confusion, avoids partial or invalid provisioning attempts, and ensures provisioning logic respects intended security configurations.

Reprovisioning Support Added

Allows existing users to be reprovisioned without first deleting credentials.

Impact: Enables administrators to reassign mobile apps or reissue credentials without removing the user's existing identity — especially useful when users switch devices or encounter corrupted provisioning.

Session-Level PINless Control

Prevents unintended behavior by checking PINless status per session.

Impact: Resolves authentication failures where PINless users were incorrectly shown a limited TURing frame (4-digit) in sessions requiring a PIN.

2. CONFIGURATION AND USABILITY

Reports Respect Time Format Settings

Reports now follow appliance time format (12/24-hour) instead of being hardcoded.

Impact: Ensures that generated reports align with regional or organizational preferences, improving clarity and consistency in audit logs and scheduled report output for global teams.

Push Mode Added to Authentication Settings

Removes confusion by treating Push as a valid mode without needing the “Enable Push” toggle.

Impact: Simplifies the configuration process and avoids agent errors when Push is selected as the sole authentication method, improving reliability for integrations using Dual Channel mode.

Configurable App Links in Email Templates

Mobile app download URLs are now driven by appliance settings.

Impact: Prevents outdated links from appearing in user provisioning emails.

Scheduled Jobs Show Appliance Time Notice

Clarifies that job timing is based on the server clock, not local user time.

Impact: Prevents confusion when scheduling maintenance or auditing tasks, especially in geographically distributed teams, by clearly communicating that all times are interpreted using the appliance's system time, not the user's local time zone.

Improved Password Generator

Randomly generated passwords now exclude symbols known to cause issues in HTTP requests and XML parsing.

Impact: The password generator now restricts output to a safe set of symbols to avoid compatibility problems, especially when provisioning credentials via links or API requests.

2. PERFORMANCE ENHANCEMENTS

Improved User Sync

Improves user sync performance by batching reads and reducing DB operations.

Impact: In large-scale environments (e.g., syncing 10,000+ users from Active Directory), the new approach in this version significantly reduces sync duration by processing users in bulk instead of incrementally.

JDBC Connection Pooling Parameters Set

Prevents connection pool exhaustion by explicitly configuring max connections.

Impact: Ensures JDBC logging does not exhaust the database connection pool under high load by introducing explicit limits. This prevents cascading failures due to logging errors consuming all available connections, particularly important in environments with sustained or burst traffic.

Legacy Syslog Format Option Added

Supports customers still relying on pre-4.2.0 log formatting.

Impact: Restores support for legacy log parsing tools and monitoring systems by reintroducing the classic log layout. This prevents disruption for environments where Syslog consumers depend on fixed message formats.

Multiple Syslog Entries Supported

Fixes limitation that prevented using more than one syslog config.

Impact: Allows administrators to define and manage multiple syslog targets without conflicts — enabling more flexible log routing and improved observability across environments.

Optionally Cache Repository Password

Where an integration uses the repository password, for example Active Directory, or AD Agent for cloud instances, it is now possible to request that the password is cached locally. This means that after the first successful authentication, the password is cached securely (using a one-way hash). Subsequent authentication attempts will use this cached password. Optionally, it is possible to specify that the password is checked remotely after a specified number of local checks, or after a specific time.

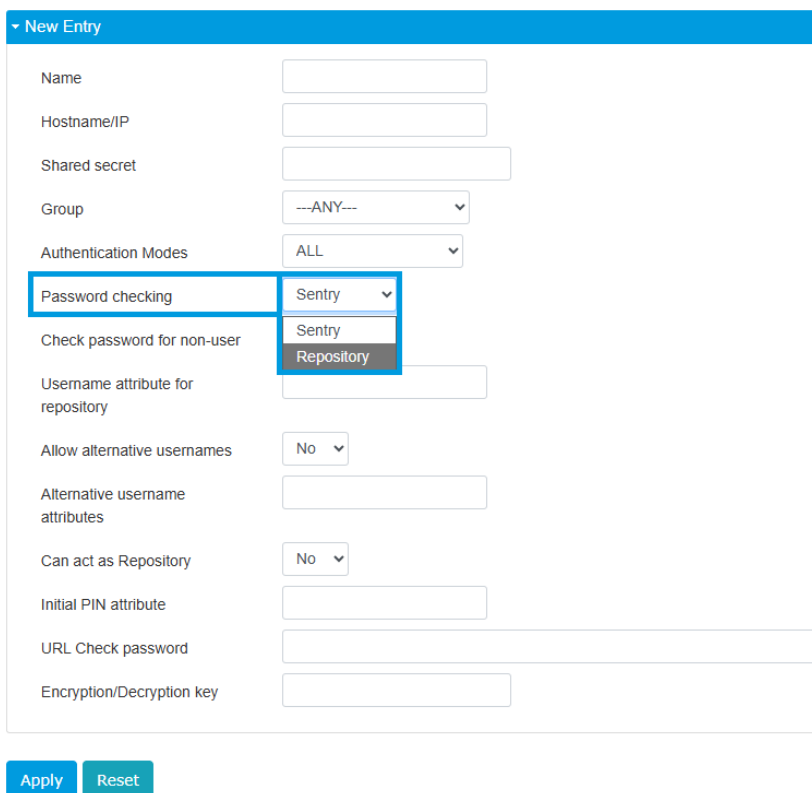
This option is configured under Policy -> Password.

2.7 MISCELLANEOUS UPDATES

Changes to Agent Password Checking

Previously for Server > Agent entries, there was the boolean option to 'Check Password with Repository' Yes or No. This has now been rephrased and replaced by a new setting 'Password checking' with 'Sentry' or 'Repository' as the selectable option. If 'Sentry' is selected it will check the user password set on the Administration console under User Administration (if the user has one set). If 'Repository' is selected it will check the user password against the user's source repository (e.g. XML, Active Directory etc). The old settings translate to the new settings as follows:

- "Check Password with Repository: Yes" is now "Password Checking: Repository"
- "Check Password with Repository: No" is now "Password Checking: Sentry"



The screenshot shows the 'New Entry' configuration form. The 'Password checking' dropdown menu is open, showing two options: 'Sentry' and 'Repository'. The 'Repository' option is highlighted. The form includes fields for Name, Hostname/IP, Shared secret, Group, Authentication Modes, Check password for non-user, Username attribute for repository, Allow alternative usernames, Alternative username attributes, Can act as Repository, Initial PIN attribute, URL Check password, and Encryption/Decryption key. There are 'Apply' and 'Reset' buttons at the bottom.

New Entry	
Name	<input type="text"/>
Hostname/IP	<input type="text"/>
Shared secret	<input type="text"/>
Group	---ANY---
Authentication Modes	ALL
Password checking	Sentry
Check password for non-user	<input type="checkbox"/>
Username attribute for repository	<input type="text"/>
Allow alternative usernames	No
Alternative username attributes	<input type="text"/>
Can act as Repository	No
Initial PIN attribute	<input type="text"/>
URL Check password	<input type="text"/>
Encryption/Decryption key	<input type="text"/>

Apply Reset

License Count Enhancement

Supports a specific use case for user existence during SSO logins.

Impact: Supports the ability to add licences for users who need to participate in SSO logins, but who do not use Sentry authentication.

Path Simplification in Configuration

Removes full class paths in admin UI, enabling cleaner and more maintainable setups.

Option to Disable Full-Text Indexing for Database Logs

We have observed that full-text indexing of logs in the database can take up a lot of disk space. The workaround is to disable full-text indexing. This results in slower search times in the log viewer, but saves a lot of disk space.

This feature cannot be enabled in the normal administration settings: if required, you need to contact Swivel Secure Ltd to make the necessary changes.

3.0 FURTHER ASSISTANCE

If you are an existing customer and have purchased through a Swivel Secure Partner, please contact them for further assistance.

If you are an Accredited Partner and you wish to raise a ticket, please use our support portal.

As a customer with a Premium Maintenance Agreement, our team of security experts are here to help you 24/7. The service agreement you received categorises issues in priority order P1 through P4.

COPYRIGHT

All contents copyright © 2025 Swivel Secure Ltd. All rights reserved.

PRIVACY POLICY

Swivel Secure Limited is a private limited company registered in England and Wales, whose registered address is Regus City West, Building 3, Gelderd Road, Leeds, LS12 6LN, with registered company number 04068905. Swivel Secure Limited is committed to respecting the privacy rights of visitors to the Swivel Secure website at www.swivelsecure.com and our associated customer support portal at supportdesk.swivelsecure.com.

For more information on the Swivel Secure Privacy Policy please visit our website.