SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

SecurAccess Release Notes Version 9.4.515

Mar 2025

Support for Windows Server 2025

- Ensured the SecurAccess Server and all associated Agents are compatible with Windows Server 2025.

Radius Message authenticator support (Blast Radius vulnerability)

- Fixes for the **Blast Radius vulnerability** have been applied and implemented across the SecurAccess server, the MS Server agent, and the Radius migration

New Windows Login Agent (WLA)

- The "API Key support" in the SecurAccess and WLA 10.0.522 Release has improved security.
- WLA 10.0.522 to provide Windows 2025 support

SecurCtrl security controls

- API key and IP address control

Others/Bug fixes

- Updated CM SMS web template
- Additional Radius configuration logging
- Fixed race condition and enumeration in SecurCtrl (Security fix)
- WLA 10.0.522 to handle of un-managed user accounts

Previous Releases

Release Notes for Version 9.4.514

Security fixes

- Security fixes associated with an enumeration of user accounts in the system
- Enhanced security control checks associated with LDAP injection attacks.

Real-time Voice Push Authentication

- Added a new voice gateway Authentication type to support the Real-Time voice Push.
- The Passcodes will be sent at logon and read out to the user via a phone call, and this authentication type requires the "AQL Voice Push" Voice Gateway to be configured.

Android Push

Added a new Android Push as the Previous Android service was deprecated.

Release Notes for Version 9.4.513

Debug/Logging

- Debug and Log messages generated by Windows will always be written in English
- Fix issue that can occur if a service's debug directory is deleted whilst the service is running.

Email Settings

- Add support for using Graph API to send emails via O365 when SMTP authentication has been disabled. Please refer to the Administrator Guide for information on how to configure this.

RADIUS

- Add support for Radius Trusted Network/Group when "Authenticate Passcode Only" is not checked. Previously the Radius trusted network/group settings were intended to be used with a Radius client that was already performing the first factor authentication itself.
- Improved handling of Radius listener lifetime..

Release Notes for Version 9.4.512

Emergency Helpdesk

- Fixed an issue where users could not log in to emergency helpdesk, and instead were shown a "UserID Required" error message.

Enrol

- Fixed an issue where a user that is configured to self-enrol to a Hardware Token would not be allowed to login to other applications after self-enrolling their token.

SecServer

- Fixed an issue where attempting a password reset through the Windows Login Agent would return an error: "SecurPassword is not enabled"

Release Notes for Version 9.4.511

General

- Added a per domain LDAP setting "UseKerberos" which forces LDAP Authentications to connect using Kerberos. This fixes an issue with authenticating users that are in the "Protected Users" group of Active Directory.

Hardware Tokens

- Fix an issue where the installer would overwrite the types.json file on upgrade

PC Soft Token

- Fix an issue with the SecurEnvoy Server not responding to PC Soft Token, resulting in a timeout error.

REST API

- Fix an issue where a POST request to create a user would return a 404 error.
- Errors will now be shown in the server log as well as the response body.

Web SMS Template Files

- Added Sveve template files.
- Added Augnet template files.

Release Notes for Version 9.4.510

General

- Fix an issue where the installer could remove a file necessary for decrypting data if the server has been upgraded from version 5.3 or earlier at any point
- Fix an issue caused by a user's UPN and SamAccountName usernames not matching

Admin

- Fix potential vulnerability in Admin GUI

Web SMS Template Files

- Added Swisscom V2 template files
- Fixed an issue with SMS template header files needing a specific line ending character

Release Notes for Version 9.4.509

General

- .NET Framework 4.8 or higher is now required

Admin

- Fixed a bug that could corrupt the domain list in server.ini when a domain was removed via the Admin GUI
- Fixed "This will deploy X users" count in Group Deployment configuration

Batch Server

- Fixed a potential race condition that could occur during Group Deployment un-management on a server with multiple domains
- Added extra safeguards for Group Deployment un-manage user feature

Enrol

- Added configurable session timeout (Enrol_inactive_timeout in server.ini)

Helpdesk

- Added configurable session timeout (Helpdesk_inactive_timeout in server.ini)

Password

- Added configurable session timeout (Helpdesk_inactive_timeout in server.ini)

Soft Token Push

- Updated the Google/Android push control file to support a change to the Google push notification API

Web SMS Template Files

- Updated AQL Voip control file with new API address
- Updated SMSGlobal control file with new API address

Release Notes for Version 9.4.507

General

- Support for using HTML email templates for any message sent via email. This can be enabled using the "MailHtmlBody" setting in server.ini

Admin Rest API

- Added support for enrolling, querying, and validating a user's secret questions via the Admin Rest API. This functionality replicates what is currently available via the Emergency Helpdesk Portal. Please see the Admin Rest API Guide for more detailed information

Enrol

- Fix for issue where a user could enrol a Yubikey without entering the generated code
- Fix for an issue where a user could not enrol a new Yubikey if they had already enrolled one before

Release Notes for Version 9.4.506 (Internal and Beta)

Enrol

- Fix for issue when enrolling a soft token when user's mobile number is set to "User Enrol"

PC Soft Token

- Fix for issue when enrolling a PC Soft Token with the latest versions of SecurEnvoy Server

Release Notes for Version 9.4.505 (Oct 2020)

General

- Fix for delays when communicating with external resources (e.g. LDAP servers) relating to inaccessible CRL servers due to locked down network access.

Release Notes for Version 9.4.504 (Sep 2020)

General

- Fix for decryption of data using AdminAPI when the system is configured for 128bit encryption

Release Notes for Version 9.4.503 (Aug 2020)

Push Authentication

- Fix for soft token seed storage migration issue when upgrading from a pre-9.4 version.

SecurICE

- Fix for ICE message being sent immediately to user when enabling them as an ICE user with Day Codes, even if ICE is not currently enabled.

SMS Modem Gateway

- Fix for gateway service hanging while starting up when a modem gateway has been added and HTTP/2 is being used for Apple push notifications.

Release Notes for Version 9.4.502 (Jul 2020)

New Feature – TOTP Hardware Token Support

TOTP Hardware Tokens are now supported as an authentication method.

Includes a new token management page to allow importing of token seeds.

Hardware tokens can be deployed in the following ways:

- Manual deployment – select a token from a list to assign to a user.
- Group deployment – 2 methods:
  - Auto choose an available token.
  - User self enrol token by entering token Id and a passcode from the token.
- Import assigned users along with seeds. User will be assigned the token and switched to the hardware token authentication type.

Admin – mobile numbers

- Fix for + character being removed from existing AD mobile number when updating a user.
- Fix for mobile formatting settings not being allowed to be blank.

Day Codes

- Fix recovery logic if SMS Request counter became corrupted.

Email Sending

- Add support for alternative email sending library. Fixes issues with SMTP servers using port 465.

ICE

- Fix for deploying extra ICE users once ICE has been enabled.

Password Authentication

- Remove 32 character password limit for two step authentications.

Rest API

- Trusted addresses can now be configured as IP address ranges using CIDR format.

SMS Web Gateways

- Added support for sending headers to gateway
- Added support for sending JWT authentication token to gateway
- Added templates for IMI Mobile
- Added templates for GOV.UK Notify

Yubikey

- Support newer Yubikeys with longer serial numbers.

Version 9.3.505 (Internal and Beta)

General

- Fix for push notifications when using OpenLDAP as the user repository.

Version 9.3.504 (Internal and Beta)

General

- Added an alternative LDAP connection method to solve authentication issues found with some LDAP directory servers

Admin

- Removed Google Cloud Messaging from list of Push gateways as it has now been turned off by Google

Version 9.3.503

Bugs

- A number of General Bugs have been resolved
- Fixed potential for mixed web content issues when protecting and offloading SSL for SecurAccess portals, through Load Balancer or WAF's (Web Application Firewall) - (please check & consider existing LB or WAF config in case they are performing rewrite of URL's to resolve mixed content in previous releases)
- Fixed secenrol login issues when enabling UPN authentication per domain.

TLS

- Outbound HTTPS connections will now use the highest TLS version supported by the server (up to 1.2)

Admin

- Fixed an issue where Replica LDS domains could not be created
- Fixed an issue with HTML appearing at the bottom of a downloaded report
- Fixed an issue where temp user dates were displaying incorrectly on a non-English language

Push Notifications

- Updated Apple certificate included in installer
- Updated Apple certificate update URLs in server.ini
- Introduced facility to enable Push notifications per user
- Support for FCM (Firebase Cloud Messaging) - GCM (Google Cloud Messaging) will be deprecated in April 2019.

Yubikey

- Fixed support for Yubikey authentication through a minimum of TLS 1.1 & TLS 1.2
- Fixed support for Yubikey authentication when utilising a Proxy Server

Batch Service

- Fixed an issue with account disablement pre-warnings being sent out at incorrect times

CSP Reporting

- Introduced automatic daily reporting of domains and user licence consumption to central SecurEnvoy licencing platform.
- Fixed support for CSP reporting when utilising a Proxy Server
- Fixed an issue where CSP user report would not report correctly when a single domain was configured.

Helpdesk

- Fixed an issue with helpdesk password length being restricted to 20 characters

Reporting

- Fixes an issue with subsequent ADAM/LDS domains not being reported on

SecurMail

- Fixed an issue where
 was appearing in some SecurMail messages
- Windows Login Agent
- Removed sensitive information from appearing in debug trace under specific scenarios

Windows Server Agent

- Fixes an issue where the user would be presented with a double logon prompt if they did not have a cached favicon
- Refreshed Server Agent Templates for OWA and RDP

SMS Gateways

- PSI Wincom template updated with a new textencoding "EscapedNewlines"
- Additional Web SMS Gateways added (Twilio, CM Platform, Link Mobility)

RESTapi

- Fixed an issue when updating a user via api, it required toAuth to be sent otherwise it defaulted back to SMS preload.

SecRep

- Removed support for SecRep in IIS