Release Notes for Version 9.3.502 (Jul 2018)

Multiple

- Updated to new SecurEnvoy logo in web portals
- Improved multidomain user searching
- Added setting to force password expiry to be sent to email
- Added function to pre-warn for account lockout
- Added notification when user account disabled by admin
- Added new SMS Gateway templates
- Added licence revocation functionality
- Security patches
- Fixed Web Gateways not honouring proxy settings

Admin

- Latest version checking and alerting
- Reinstated legacy SaaS functionality as CSP
- VSA
    - Added ability to configure serve to allow login with a local account during initial setup wizard
    - Added ability to re-generate config.db during initial setup wizard
- Radius
    - Fixed delete trusted group functionality
    - Fixed "allow these domains" checkboxes when domain name is a substring of another domain
    - Fix for special characters in domain admin passwords
    - Fix for "Auth Group" nested checkbox
- Log
    - Fixed password appearing in log when invalid characters found
- Gateways
    - Fix for page constantly refreshing if login has expired
    - Added "Additional Auth Prompt" input for applicable voice gateways
- Users
    - Fixed for passcode resend button not working

Enrol

- Added "integration mode" for showing QR code in customer's environment in conjunction with REST API
- Soft token auto enrol when user in soft token enrol state fix

SecurMail

- Fixed display bug with html encoded characters
- Fix for CSRF cookie with nonstandard "secmail" URL

Release Notes for Version 9.1.501 (Oct 2017)

New functionality in this release
- Improved GUI
- New Dashboard status page in GUI
- Initial Setup Wizard in GUI replaces Advanced Config
- Added support for NFC in Mobile phone Apps
- Added support for YubiKey Hardware Tokens
- New REST API for automated remote administration from any OS
- Web SMS/Phone Gateway Setting moved to the Admin GUI
- LDAP Domain Management moved to the Admin GUI
- Support For Apple Push Notifications via https (port 443) on Windows Server 2016 Only
- Native Support for 64bit OS
- Added Support For TLS 1.1 and 1.2
- Added Support For Windows Server 2016

Bugs Fixed
- Pin enrol is requested incorrecly when primary domain is set to type ADAM and domain 2 is type AD
- When creating new user from helpdesk, now creates user as standard user not helpdesk
- LdapBase reporting within Security server Admin and Reporting wizard
- Passback Groups in Radius only passes one attribute if seperater is not set
- securectrl does not pass the AD group membership back to WLA when using UPN
- when selecting "Attachment" when replying to a SecurMail it sends the message rather than presenting the attachment upload page.
- users are allowed to re-use SMS sent OTP's when their mobile number is deleted

---

Previous Version 8.1.504 (Mar 2017)

Bugs Fixed
- If Apple Push Gateway is inactive for 2 or more hours, it does not automatically reconnect leading to one failed push attempt
- When enabling migration to a third party radius server, radius packets are incorrectly formed
- SecurPassword portal fails to reset password if the admin password contains certain control characters
- Windows logon agent offline is not case insensitive
- Windows logon agent fails if used without push
- Manage My Token, QRCode does not enlarge

SecurEnvoy
A Shearwater Group plc Company

Previous Version 8.1.503 (Aug 2016) OEM Only Release

New functionality in this release
- Added OEM installer for embedding SecurEnvoy Server into third party products

Bugs Fixed
- Changing to a black GUI ends up corrupting graphics, black graphics are no longer supported
- Fixed an issue where public mobile numbers are not cleaned up when sent as a Simple SMS Text

---

Previous Version 8.1.502 (Jun 2016)

New functionality in this release
- Advanced Config now includes tabs for different gateway types and test buttons for push connectors
- WebTemplates extended to include TextEncoding=URL20
- Radius migration extended to pass all received attributes
- Added support for 2 UserID attributes to allow for users that have different samaccountname to first part of userPrincipalName
- OEM white labelling added

Bugs Fixed
- If a Radius client with a password of 16 long is received incorrectly with two blocks of 16 data the second block is ignored
- Enroling secret answers that are longer than 13 error and reflect back the entered answer without encoding special characters
- SecurPassword secret question answers are checked to make sure they are longer than 3 characters and not blank

---

Previous Version 8.1.501 (Apr 2016)

New functionality in this release
- One Swipe Online Push added
- Option to protect Soft Token Phone App with Touch ID or Pin
- OneSwipe Offline QRCode Touch ID or PIN unlock to restore the last entered password
- SecurMail Sender Portal with mobile app support added
- Customisable rules for cleaning up mobile numbers
- Tmp Passcode, new “Device Not Lost” mode to restore the old token
- Group Deploy includes support for nested groups on Microsoft AD systems
- Custom install for Edge servers in the DMZ
- Automated server.ini sync between servers
- SAAS helpdesk admins can now see config tab for their domain
- Simplifed Radius GUI admin with names and copy button for easy reference
- Trusted LDAP groups bypass authentication for Radius clients setup with passcode only
- Improved performance when using large numbers of multi-domains
- Added command line option /import to import CSV file containing users, Example deploy.exe /auto /import=c:\test.csv
- Option to disable defaulting unknown domains to the default domain

- End user email notification if account disabled
- SecurPassword extended to notify users set to must change password on next login

Bugs Fixed
- When enabling an existing user the enable date is not updated which will affect reporting and automatic account disable
- Radius passwords encoded with UTF-8 are now supported
- SecurPassword web portal, UserID now checks UserIDMustNotInclude in server.ini
- LDAP failover now remembers the working server by updating LdapActiveServer in server.ini
- At enrol, If Group Deploy "Don't send initial enrol request is checked passcode is not resent to mobile even through mobile number is known to LDAP.

Previous Version 7.3.501 (Mar 2015)

New functionality in this minor release
- New admin type Log for only allowing access to Log viewer
- New Report for Log Admin
- GUI Report includes all domains
- SecurICE now supports multi domain
- SecurPassword option to prompt for a SecurEnvoy pin in a seperate input box
- SecurPassword now supports multi domain

Bugs Fixed
- Updated Clickatel template to refect changes in their API
- SecurMail Outlook Client 2007/10/13 fails to run plugin
- Trusted users that have authenticated with 2FA can access admin, this is now restricted to admin level users only

---

Previous Version 7.3.500 (Dec 2014)

New functionality in this minor release
- New Microsoft Server Agent (replaces IIS Agent) with support for RDGateway and ADFS on Windows Server 2012R2
- SMS Gateway speed improved with multi-threading
- SAAS Multi-domain reporting
- Max Tmp Days Added To Admin GUI (Default is 14)
- Real time and voice call now add one failure at the first step to stop multiple sms message
- Report Day Code users now include code every day count
- Report Department and Location added to file exports
- New Report Users That Have Not Enroled for Secret Questions
- New Report Custom to allow any ldap filter to be set
- New Report SecurAccess / SecurPassword User Count
- OneSwipe now supports IE10 and IE11 browsers via flash
- Oneswipe updated to use a single easy to add smart button object
- Oneswipe scan video now moves in the same direction as the phone
- If disable account if no authentication activity in xxx days is set server also checks last enabled date before disabling
- Option to allow create and delete users with openldap servers
- Group Deploy now sets Offline laptop if this it displayed in the GUI

Bugs Fixed

- Changing mobile numbers from public to private may result in lost secret answers.
- Webgateway under extreem load sometimes sends sms messages twice
- QRCode not being dynamically recreated when page is refreshed or new tab created
- SecurMail Improved error checking for mobile numbers longer than 18 digits
- IIS Plugin - Logoff cookie not deleted on some setups

Previous Version 7.2.504 (May 2014)

New functionality in this minor release
- Year added to all logs for improved SAAS billing.
- Reporting of users not authenticated in xxx days now also checks enabled date if user hasn't authenticated
- Windows Login Agent can be configured to only use 2fa on selected remote connections or the console

Bugs Fixed
- License count sometimes shows the incorrect number of users
- Web SMS Gateway service sometimes loops if DNS fails to return a valid ip address
- SecurMail expiry date fixed for store mode

Previous Version 7.2.503 functionality (Feb 2014)

New functionality in this minor release
- Automatic backup of unmanaged AD users
- Option to increase secret question enrol to three
- Radius Return attributes via LDAP Mapping extended to include types LDAP IP Address and LDAP Number.
- Improved qrcode image security in Manage My Token portal

Bugs Fixed
- DN and domain number are now taken from the controlled SecurEnvoy Cookie to prevent trusted users crossing to other DN's
- SecurMail Agent failed to get mobile number when sending in stored mode if contact contains upper case in the email address

---

Previous Version 7.2.502 functionality (Feb 2014)

- Improved admin browsing with license usage caching

Bugs Fixed
- Intermittent slow browsing as a result of CLI checking code cert

---

Previous Version 7.2.501 functionality (Jan 2014)

- OneSwipe
- Admin GUI Black or White background option
- IIS Agent enhanced security with mal formed URL detection (SecurEnvoy recommend all existing IIS agents should upgrade to this version)

- Option to allow email tokens at enrol
- SecurMail Outlook 2013 Agent
- Improved performance
- debug trace improved thread safety
- Added support for admin scripting via PowerShell V3
- Added support for Mac Server Open Directory
- Add nested checkbox to Radius group to allow easy disabling of nesting
- Pin Enrol option to force digits only
- New setting for Batch failure checking to allow for LDAP servers that takes longer that 5 minutes
- SecurPassword integrated with SecurAccess when Windows password is the PIN and the Windows password requires changing
- Trusted networks now return group data via Radius in the same way as authenticated users
- New GUI button under config - license to force a recount of all users

Bugs Fixed
- Install fails if license entry is skipped
- New users are disabled after xxx days even though "Disable account if no authentication activity after xxx days" is not checked
- users set to token type email fail to authenticate if no SMS gateways are available
- New user enrols with a mobile number shorter than a set minimum length incorrectly displays the option "Use existing Token"
- Enrol resends preloaded passcodes before they are entered if GroupDeploySentAtEnrol=True
- Group Deploy with real time SMS codes for users with a known mobile number fails to send enrol SMS if helpdesk is enabled
- IIS Agent fails authentication if german characters are using in the password

---

Previous Version 7.1.503 functionality (26th July 2013

New functionality in this minor release
- Windows Login Agent now supports off-line one time passcode authentication for users of token type soft token
- Additional SMS gateway templates for Dynmark and Paratel added

Bugs Fixed
- CM VOIP Password encryption fixed for older 128 bit systems
- New installs with no SMS gateway configured now automaticlly create email config
- Windows Login Agent server error messages fixed
- Remote reporting userid hyperlinks fixed

Previous Version 7.1.502 functionality (3rd July 2013)

New functionality in this minor release
- Radius LDAP group checking only apply to SecurEnvoy managed users to allow for better migration from third party 2FA servers
- Mobile numbers that contain - or / now have these characters removed
- Guest Enrol now includes a "Days" entry box
- SMS Gateways via email now include mobile number substitution in the body and Subject template
- Support Server Side for upcoming Windows Login Agent with off-line authentication via soft token

apps
- IIS Agent has even better Cross Site Scripting Defence

Bugs Fixed
- Windows Login Agent always authenticates users that are not in the authentication group, this is fixed to skip them
- Web SMS Gateways that connect via proxies are fixed

Previous Version 7.1.501 functionality (3rd June 2013)

Key new functionality in this release:
- Multi SMS Gateway with smart routing
- New SMS Gateway Option for email based gateways
- New token type Voice Call
- Per User Three Codes
- New “Token Type” section in Config to control which token types to use
- More end user choice, secenrol allows Preload, Three Codes, Real Time, DayCode, Soft Token and Voice Call
- Improved SAAS – Multi-domain with per-domain settings for most GUI config settings
- Mac Soft Token
- Improved URL Settings in Advanced Config
- Per-User Radius String Settings mapped from Ldap string attributes
- SecurPassword extended to multi-domains with better support for real time codes
- Enrol and remote admin authenticates all users via 2 step auth
- Support for Windows 2012 server
- New temp user valid for xx days
- Automatically disable inactive users after xx days (default 90 days) SOX’s compliance
- Automatically disable pending enrol requests after xx days (default 30)
- New option in group deploy to only send enrol message after user starts to login to secenrol
- New Alerting tab
- New ICE disable message
- ICE Enabled per domain
- Manage My Token (secenrol) now shows extra setting “Use Existing Token”
- SecurPassword Complexity and min length set via admin GUI
- Radius Trusted & Blocked Networks via Calling-Station-Id (RADIUS attribute 31)
- License Quote per domain for SAAS
- Increased performance of migration and IIS Agent
- Reporting added to the main GUI
- Admin gui includes mobile number self enrol
- Soft token display name can be set to a fixed string such as “office”

Previous Version 6.2.502 functionality

Key new functionality in this release:
- Option to disable resending a new passcode via email after enrol
- Option for soft token enrol via QRCode to passback the userid only or the userid@domain

Bugs Fixed

- user enrol fails if switching to soft token enrol without entering a phone number
- Group Deploy fails if default setting is Email and a mobile number exists
- iis agent fails is next token code is requested
- If the GUI config "Allow Passcode via Email" is unchecked soft token admin may fail

---

Previous Version 6.2.501 functionality

- Added Sophos Safeguard Integration
- Reporting Wizard userid links no longer require two factor authentication
- Automatic proxy detection added to PC soft token and SecurMail agent
- SecurMail recipient pickup and reply improved

Bugs Fixed
- IIS handler maps sometime cause adminAPI.dll errors
- IIS Agent MMC fails to show SecurEnvoy icon
- Admin GUI errors when changing a real time user from sending via mobile to email.
- localadmin may require 2fa on systems with more than one network card.
- Helpdesk authentication fails after secret question is answered incorrectly until browser is closed

---

Previous Version 6.2.500 functionality

- New Soft Token For PC's
- New Automatic Group Deployment with multi-server failover added for easy administration
- Smtp authentication and TLS encryption to mail servers is now supported
- Increased cookie security with host locking on all web based interfaces
- Increased cross site scripting defence and input length controls on all web based interfaces
- Helpdesk admin's can't change other helpdesk administrators

Report Wizard now includes 3 new reports, Private Mobile Numbers, Public Mobile Numbers, Passcodes via Email
- IIS Agent Enhanced Security with cookie host locking, Cross Site Scripting Defence and Input Length Controls

******** All earlier IIS agents should be upgraded to this version ********

Bugs Fixed
- QRCode image doesn't show on some browsers when enroling soft tokens
- Realtime users can be re-enabled from disable without needing to change to preload
- IIS Agent inactivity time out was timing out too early

Previous Version 6.1.503 functionality

- IIS Agent 6.2 included in this release as its required for ADFS (Office 365)
- IIS Agent Enhanced Security with cookie host locking, Cross Site Scripting Defence and Input Length Controls. All earlier IIS agents should be upgraded to this version
- IIS Agent support for all previous SecurEnvoy versions via RADIUS

Bugs Fixed

- After running "Users that have NOT authenticated in xx days" in the reporting wizard, Pressing Unmanage these users may unmanage more users than selected.
- Config ldap test button incorrectly shows OK

Previous Version 6.1.502 functionality

- Copy protection of soft token enrolment codes added
- Radius received packets extended to 4096 to allow for Microsoft NPS sending extra large numbers of attributes
- Administrator Resend for soft token enrol is now supported
- Soft token enrol now has clear highlighted warning to complete step 4
- Multidomains setup with trusts that incorrectly use the same admin account will now run the batch server on all domains
- New SMS Gateway called Stream SMS, Russian provider added
- Soft token enrol option added to deployment wizard

Bugs Fixed

- QRCode browser cache issues fixed when enrolling twice with the same user
- Soft token enrol logged incorrectly if update pressed by administrator
- User enrol with CN that contains : or ;, fixed
- Improved error handing with user enrol
- Helpdesk Admins with group filters fail to update users

Previous Version 6.1.501 functionality

- New Option For "Soft Tokens" that run on iPhone, Android, Blackberry
- Soft Tokens to be released via phones App store, iPhone submitted to Apple June 2011, Blackberry and Android to follow within next 2 months.
- Support for Google Authenticate Client which is available on iPhone, Android, Blackberry
- Added support for Migration from Vasco 2FA
- Option to strip domain name from userid when migrating
- Removed the need to create groups in non English operating systems prior to install

Bugs Fixed

- Fixed license count issues if creating a new user errors

Previous Version 5.4.503 functionality

- New Radius setting to handle all passcode types in the same way as Real Time Codes
- New sms template smspasscodeviaemail added
- Web SMS Templates now support basic authentication
- IIS Agent, remote browser is finger printed so that only the location that was authenticated is trusted
- SecurPassword Windows Login Agent automatically signs on after password is changed
- Added send mode mobile or email to deployment wizard
- Added support for import lists via email deployment in deployment wizard

- Added configuration option for Helpdesk Admins to view all log
- Radius Group passback optimised to use Microsoft LDAP Chaining
- Added support for IIS Agent version 5.1
- Added support for flow control settings in phone gateway
- Password only authentication added for unmanaged users that use search to locate there domain.

Bugs Fixed
- Fixed Replica install with 256bit config.db files
- Fixed RealTime Passcodes fail if Debug is set to False (the default)
- Fixed Migration to RSA SecurID fixed next token and new pin modes
- Fixed IIS Agent, Domain and Custom1/2 data in auth.htm templates fail to pass to passcodeok.htm
- Fixed Non primary groups now passback radius group info
- Fixed issue with send simple SMS selected, Radius fails to locate private mobile number.

Previous Version 5.4.502 functionality

- 2008 R2 servers now automaticlly adds .net 3.5 feature if missing
- New installs use 64bit IIS Application Pool (better compatibility with other 64 bit IIS applications)
- New Installs use AES 256, upgrade use existing AES 128 (no changes to existing ldap users)
- Ldap Base added to reporting wizard

Bugs Fixed
- Fixed MMC Crash on IIS7 if trusted networks and logoutURLs are set
- Fixed SecurMail read receipts
- Extended IIS restart timeout
- Batch Server constraint violation in admin user fixed
- Debug trace fully blanked when set to false

Previous Version 5.4.501 functionality

- Reporting Wizard Added
- Improved GUI Graphics
- Multi-day day codes restricted to one day of overlap
- Radius servrer now supports login's with userPrincipalName (userid can include @)
- Radius can be configured to only use 1 network card
- Security server can be upgraded without uninstalling first
- Email now sends HELO with FQDN host name
- Deployment Wizard can now export a list of uncompleted enrols
- SecurPassword now supports password reset directly in the login GUI with the Windows Login Agent
- Added server side support for SecurPassword via the Windows Login Agent
- SecurPassword re-enables and unlocks disabled users in AD after password is reset
- SecurPassword sends alert email to end user after password is reset (better security)
- SecurPassword can be configured to alert via email any number of administrators after a password is reset
- SecurAccess automatically re-enables and unlocks disabled users in AD after a user is enabled
- Self Helpdesk extended to allow PIN reset
- Added support for O2 sms gateway
- Support per-user “simple messages” (no flash or message overwrite)

• Encryption enhanced to FIPS 140 AES 256 bit
• Radius client in IIS Agent for better security on SAAS servers with customer based IIS agents
• Display when a specific user last logged in
• Separate local.ini and server.ini to allow easy replica update
• Sms templates moved to data\smstemplate
• helpdesk admin filter lines to only show local domain – better cloud security
• Helpdesk admin are restricted from allowing static user administration – improved security
• Deploy Wizard now supports Real Time and Number of Days for day codes within setup
• Reporting Wizard now includes an email option in the command line for sending report outputs
• Improved logging when windows account is disabled or locked or requires password changing
• ICE message can be edited via the GUI
• SecurMail now includes a “New SecurMail” button that always sends the created email via SecurMail even if send is pressed.
• SecurMail now supports sending from users set in Outlooks from field
• SecurMail easier to send Securmail with new “Send Secure” button directly in the Outlook Message ribbon.
• SecurMail Improved pickup graphics.
• SecurMail Received mails can be easily moved to recipients email program.
• SecurMail support for Outlook 2010
• SecurMail Recipient reply’s increased to 5Mb attachments

Previous Version 5.3.502 functionality

• Daycode locking of old code if new one used
• Radius group passback skips nested group checking on Novell as this isn't required.
• Support for userPrincipalName in AD
• Radius migration option to strip @domain from userid
• Add cut left of defined character in userid
• Added IIS agent timeout on inactivity
• Added IIS agent logout URL
• Added IIS agent sso for NTLM (Windows 2003 only)
• Enrol and helpdesk and SeurPassword web graphics improved
• Enrol bookmarking now support IE, Firefox and Opera browsers

Bugs Fixed

• Fixed Batch server runonstartup to run even if already run in last 23 hours
• Fixes radius single group passback
• Disabled batch server trace file

Previous Version 5.3.501 functionality

• SMS Gateways routing - local country sent to Modem and International to Web
• Migration - password only authentication for unmanaged users in AD group sepasswordonly have been added
• Migration – third party token servers (RSA etc)
• Support for Terminal Services 2003 32 bit and 64 bit version with a new Windows Logon Agent

• Support for Terminal Services Web Authentication 2008
• External logging via syslog
• Add support for multi-language user name encoding via UTF8 (Hebrew etc)
• Radius LDAP group authentication

Previous Version 5.2 functionality

• Support for Windows Server 2008 32bit, 64bit and Windows Server 20008 R2
• SecurAccess - Radius option to return member of AD groups (this allows for better access control with VPN's)
• SecurPassword - History list checking added when entering a new password
• SecurAccess - Only resend day code failures if passcode is incorrect and not if password is incorrect.
• SecurICE - Reset ICE Count if new (different) license is installed
• SecurAccess - IIS agent now supports multiple web sites from the GUI
• SecurMail - SMS messages are now configurable
• SecurMail - SMS Failed auth count is now configurable
• Additional Web SMS Gateways Added
• Added support for SMPP based SMS gateways (Ideal for Telco's)
• Mobile numbers starting with 00 are now recognized as international dialing
• All known issues in v5.1 fixed

Previous Version 5.1 functionality

• Support for internal managed users via Microsoft ADAM (B2B and B2C users)
• Support for AD, e-Directory, Sun Directory, OpenLdap and ADAM concurrently on the same server
• Helpdesk administration granularity via groups
• SecurPassword now includes SMS notification of passwords that will expire in xx days
• Improved administration graphics and online manuals
• Disabled user notification via SMS
• Improved logging with filtering and support for Microsoft Event log
• Support for multiple SMS third party gateways (10 included)
• Proxy server account authentication (Web SMS Gateway)
• Support for optional Real Time passcodes on a per user bases with flash SMS messages and session locking
• Improved performance
• Enhanced user deployment with tools for redeploying self enrolling users and support for user lists
• Improved SSO for IIS agent (no javascript required)
• SecurMail supports an option to re-use the recipients passcode for additional secure mails
• SecurMail has an option to store email for xx days
• New section in the admin GUI for SecurMail management of both senders and recipients
• SecurMail file upload performance improved
• All known issues in v4 fixed

Previous Version 4 functionality

SecurEnvoy
A Shearwater Group plc Company

• Added support for Multiple Domains
• In Case of Emergency (ICE) Support
• Helpdesk self administration for TMP CODES
• End User mobile number self enrol
• Web based install and administration guide linked to GUI and on-line web resources
• Remote Administration Now supports Helpdesk or Full Admin
• Added support for any https SMS web gateway via customisable templates
• email mass deployment for mobile number self registration
• Option To Send 3 One Time Passcodes with each one time SMS Message
• Added support for Firefox on remote admin
• Added support for e-Directory
• Admin search now ignores COMPUTER account
• config automatically fills in domain name with current systems domain
• IIS Agent authentication form now uses separate PIN (Windows Password) and Passcode fields
• End User secret questions enrol for Helpdesk authentication
• Enable / Disable For SecurPassword
• Add Support for Secret Questions in SecurPassword
• Add SecurPassword config to web admin
• Added support for SSL connections to LDAP
• Added support for blank LDAP search base
• Added support for t-Mobile SMS Gateway
• New Enterprise License for Multi Domain Support
• Day codes now resend if the incorrect daycode is entered
• Day Codes can be configured to only send if used (this is the default)
• Logging has been extended to include calling Client IP Address
• SMS Gateway logs now include the userID
• SMS Phone Gateway Now checks the SIM is OK and logs and errors or PIN/PUK locks
• Allows 10% over user license limit on SecurAccess or SecurPassword users (not ICE)
• No longer require LDAP Attribute PagerOther as it is now part of TelexNumber
• Hidden Mobile Numbers are cleaned up at point of entry
• admin GUI now gives an error message if both SMS Gateways are down
• Global Radius Secret for improved administration of Citrix GoToMyPC
• Radius to include default domain for each client with "only allow this domain" option MET managed service