SecurEnvoy Security Server Administration Guide

SecurEnvoy Global HQ
The Square | Basing View | Basingstoke | Hampshire | RG21 4EB
Tel: 0845 2600010 Fax: 0845 260014 www.SecurEnvoy.com

SecurEnvoy Security Server

Administration and Configuration Guide v8.1

The SecurEnvoy Security server is the main central component of the SecurEnvoy suite of products. It has direct integration into a LDAP directory server (Microsoft Active Directory, Novell e-Dir, Sun One Directory Server and Linux Open LDAP Directory Server) for user information, controls and manages the authentication of SMS passcodes and the subsequent sending of them.
This must be installed for SecurAccess, SecurPassword SecurICE and SecurMail

SecurEnvoy Administration and Configuration Guide v8.1

© 2016 SecurEnvoy

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Publisher
SecurEnvoy Publishing

Managing Editor
SecurEnvoy Training Dept

Technical Editors
A Kemshall Technical Director
P Underwood WW Pre – Sales

Cover Designer
SecurEnvoy Marketing

Revision	
V1.0 AK PU	10/05/2008
V1.1 AK PU	21/12/2008
V1.2 PU	07/07/2009
V1.3 PU	03/11/2009
V1.4 PU	18/01/2010
V1.5 PU	16/06/2010
V1.6 AS	12/01/2010
V1.7 PU	11/05/2011
V1.8 PU	29/06/2011
V1.81 PU	30/11/2011
V1.9 PU	20/04/2012
V1.9.1 PU	28/06/2012
V2.0 PU	10/05/2013
V2.1 TD	09/01/2014
V2.2 PU	23/05/2014
V2.3 TD	11/12/2014
V2.4 PU	14/12/2014
V8.1 RDS	02/02/2016
V8.1 RDS	13/03/2017

Printed: Mar 2017 in United Kingdom

Foreword

SecurEnvoy is the trusted global leader of tokenless two-factor authentication. As the pioneers of mobile phone based tokenless authentication; SecurEnvoy leads the way with ground breaking solutions that others aspire too.
Our innovative approach to the tokenless market now sees thousands of users benefitting from our solutions all over the world. With users deployed across five continents, our customers benefit from a significant reduced time to deploy and a zero footprint approach means there is no remote software deployment and administrators enjoy the management tools allowing them to rapidly deploy up to 100,000 users per hour.

Our design philosophy is based on re-using existing customer technology investments such as Microsoft Active Directory, simplifying the end user authentication experience while enhancing the overall security.
With no token manufacturing costs the return on investment (ROI) is so much more acceptable to businesses and organizations, and environmentally the green benefits of a zero carbon footprint also attract environmentally responsible purchasers. We are truly now providing solutions that have zero impact on our environment.
SecurEnvoy distribute through the channel, providing customers the value added benefits of working with local partners. We have now built up a technical and sales infrastructure that supports most languages and cultures around the world.

The business was officially incorporated in 2003 after preliminary, coding and testing in our labs. Years on we now have happy customers across the five continents and regional support. Business levels have more than doubled year on year due to our subscription sales model that is an acceptable route that allows our clients to budget more effectively. This model includes local support and annual subscriptions.
Founded by Andrew Kemshall and Stephen Watts, the two founders work relentlessly to achieve business growth worldwide. This massive growth has been possible through the quality of people and the experience within the company both from sales and technical expansion.
SecurEnvoy continues to shape the way millions of people plan their authentication requirements and purchasing decisions.

Contents

SecurAccess, SecurPassword, SecurICE and SecurMail

1 Overview 6
1.1 Server Topology 7
1.2 Passcode Delivery Options 9
2 Domain model for LDAP 15
3 Support for multi LDAP environments 19
4 Configuration 22
5 Advanced Configuration Wizard 32
5.1 Multi Domain configuration 35
5.2 eMail Gateway Configuration 40
5.3 IIS URL's 41
5.4 SMS / Voice Gateway 42
5.5 Radius Server configuration 46
6 User management settings 47
6.1 Scripting With Microsoft PowerShell V3 52
6.2 Soft Token Support 53
6.3 One Swipe 56
7 Automated User Provisioning 58
7.1 Deployment Wizard GUI 59
7.2 Deployment Wizard command line options 63
7.3 Automatic Group Deployment 65
8 Configuring RADIUS clients 66
9 Migration 73
10 Resilience 76
10.1 Resilience (Batch Server Logic) 79
10.2 Resilience (RADIUS) 79
10.3 Resilience (Server.ini) 80
10.4 Resilience (Gateway.ini) 81
11 Web SMS Templates 82
12 SecurMail Administration 86
12.1 SecurMail Virus Checking Integration 88
12.2 SecurMail Server Security Considerations 90
13 Frequently Asked Questions 91
14 Help 96
15 Recommended Backup procedure 99
16 Troubleshooting 101
17 SecurEnvoy Additional Tools 104
17.1 Reporting Wizard (GUI) 105
17.2 Reporting Wizard (Cmd Line) 110
17.3 Reporting Wizard (Admin GUI) 111
18 Alerting 112
19 Appendix 114

1 Overview

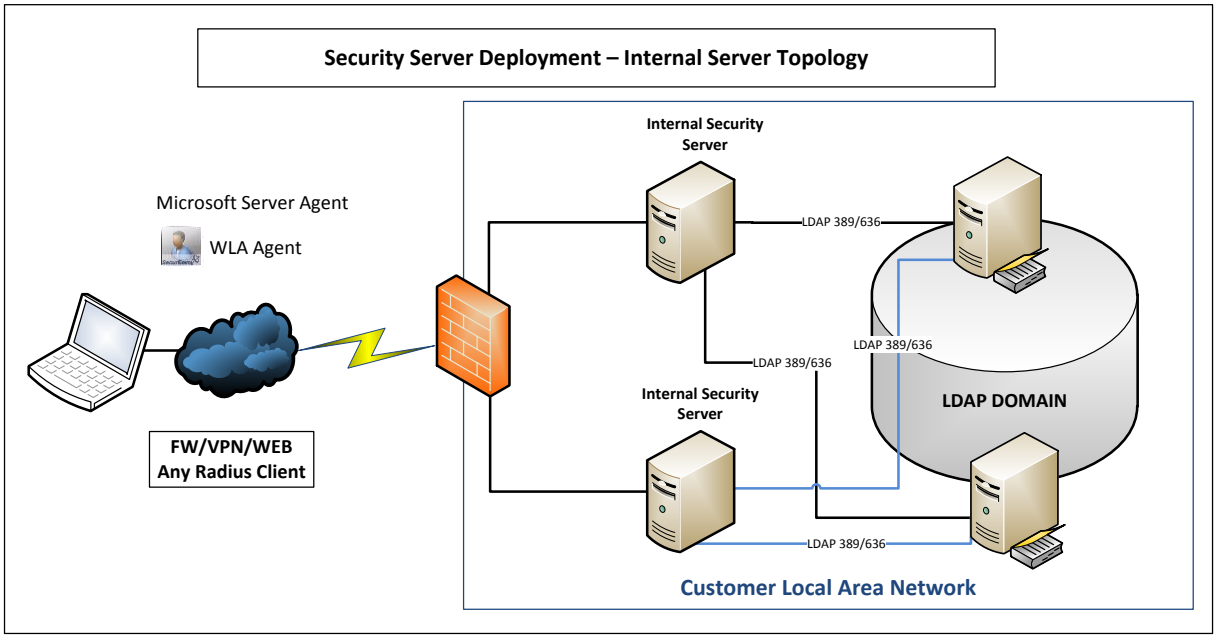
Chapter 1

1.1 Server Topology

Version 8.1 of SecurEnvoy Security Server introduces some exciting new features into the two-factor authentication (2FA) arena, including push notification technology and Near Field Communication (NFC). Push notifications work by sending a message to the notification centre or status bar of a users' smartphone. NFC allows a customer to authenticate contactlessly using their smartphone. These new features are dependent on the architectural topology of the SecurEnvoy Server implementation. This section of the guide has been created to provide some guidelines for selecting the correct topology to deliver all required features of each organization's SecurEnvoy Security Server solution.

> **Note**
>
> *It is important that this decision is made in advance of installing the product.*

Internal Server (no external facing web portal)



Advantages of this topology

No external Internet facing portals. Therefore no hardening of servers is required and the risk of attack to these portals is limited to internal users only.
Note: SecurEnvoy's Manage My Token portal requires two-factor authentication.

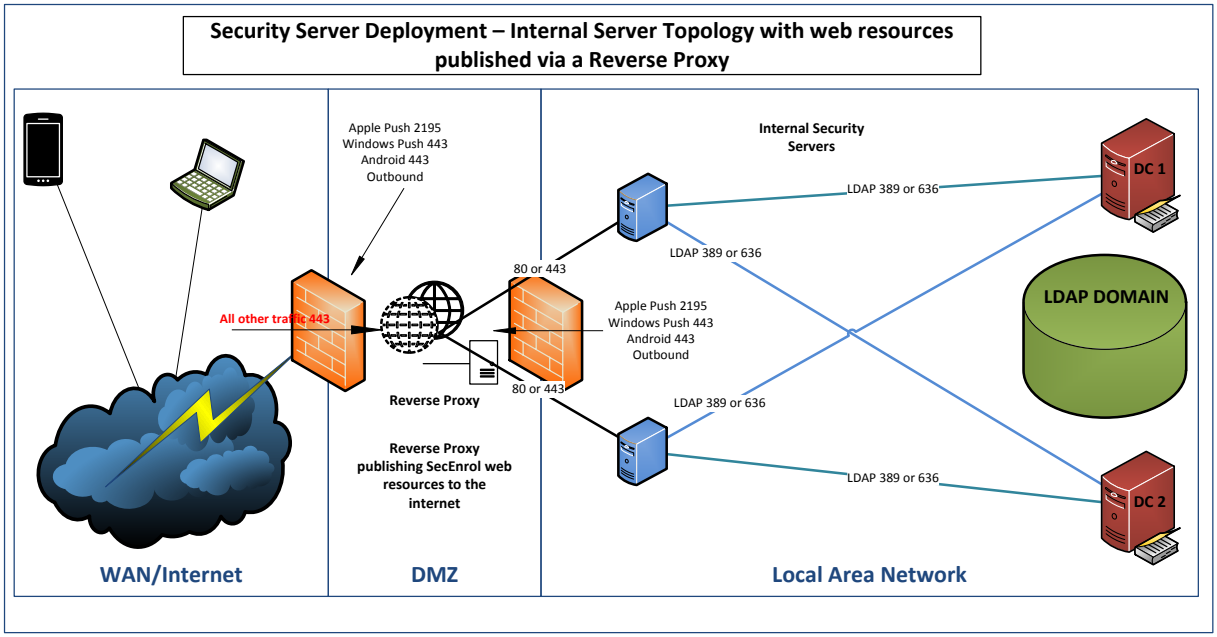
Disadvantages of this topology

The following token types are not supported:

- Oneswipe online push
- Oneswipe offline NFC

In addition, a user will need to be on the internal local area network (LAN), or connected over VPN, to manage changes to their token types on the Manage My Token portal.

Internal Server with web resources published via a Reverse Proxy (SSL VPN etc.)



The Manage My Token portal located in IIS default website (SecEnrol) must be published to the Internet via a reverse proxy or load balancer appliance.

Advantages of this topology

All token types are supported including oneswipe push and NFC.
Users are able to manage their tokens externally from any Internet location.

Disadvantages of this topology

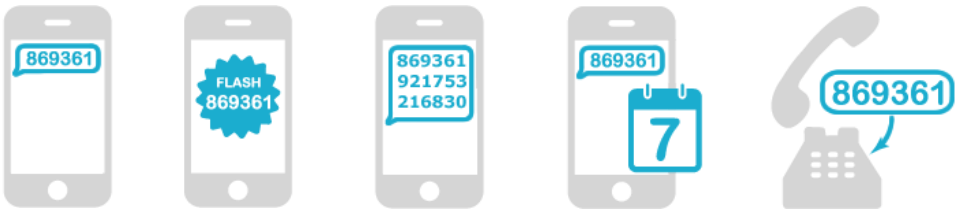
Manage My Token portal must be published to the Internet.
The risk of attack to this and other portals is exposed to external users.

1.2 Passcode Delivery Options

SecurEnvoy utilises a self-management interface known as "Manage My Token", this web portal allows the user to not only enrol themselves initially, but thereafter can manage the life cycle of their device. For instance upgrading soft token from one phone type to another, they simply visit manage my token portal, where they can re-provision their new phone and automatically their previous one.

Consideration should be given as to whether this web portal is published directly upon the Internet or only allowed for internal use. SecurEnvoy recommends that this is published externally as the portal is protected with Two-Factor authentication and will lead to significantly less support calls, if users are allowed to manage their own device.

The users' mobile phone can receive a one time passcode (OTP) via SMS, voice call, or be generated upon the phone with the SecurEnvoy Soft Token. Furthermore, SecurEnvoy's patented approach provides a far greater range of tokenless types, including the following methods, the passcode sent via SMS can be delivered in real time, pre-loaded as an OTP, pre-loaded with 3 OTP or a reusable Daycode.



In addition SecurEnvoy has the ability to support VOICE tokens, by sending a voice call directly to a physical landline, DDI extension. The user first enters their pin or passcode, after which a six digit passcode is displayed. At the same time a phone call is automatically made. The user answers the phone and enters this passcode on the phone's keypad. This is recommended for users that only have access to a land line or don't have a smart phone and can't receive SMS reliably. This allows the user to keep working, even if the user may not be in an area of good GSM coverage for when they require their passcode.



SecurEnvoy soft tokens for your phone or desktop can be used to generate one time passcode (OTP) for two factor authentication that can be checked by your companies SecurEnvoy server or Google's cloud login. Quick Response codes are an excellent method to display a bar code matrix for the deployment of the "seed record" for the end users Soft Token. The user only has to scan the QR code with their phones camera to ensure a fully automatic enrolment process to a SecurEnvoy Soft Token.

The eighth version of SecurAccess takes our industry-leading mobile, two-factor authentication platform and adds even easier authentication with soft token Push based notifications. It supports Support for 'push' notification within the app and support for push on 'Wearables' and all phones & tablets

SecurEnvoy One Swipe provides a simple user experience, easier than a password with the added strength of 2FA. SecurEnvoy extends its phone app to provide One Swipe single sign on, via a One Time QR code.

Soft Token's are available for all Smart phone applications as well as a P.C. and MAC OS soft token. Understanding the various methods that SecurEnvoy support for delivering and managing Passcodes.

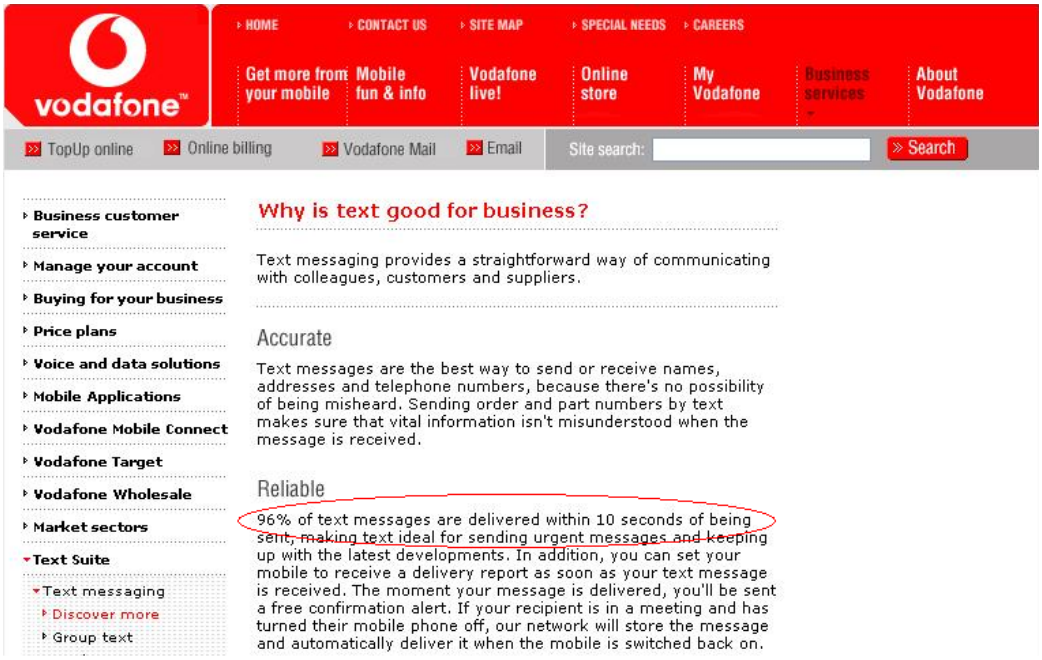
Email delivery is not user selectable as SecurEnvoy recommends that this method of passcode delivery is configured by Administrators who understand the implications of email. SMTP traffic is not an encrypted protocol, Administrators must be able to make decisions regarding email delivery, as it may be that a Blackberry system is in place with end to end secure email delivery.



With the advent of smart phones, SecurEnvoy leverages all leading brands and provides an elegant solution to provision a phone Soft Token. Users engaging in this approach do not require any GSM or data connection as the OTP is generate directly upon the smart phone.

SMS delivery is delayed

Although most SMS text messages are transmitted in seconds, it's common to find them delayed when networks become congested. SMS traffic is not sent point to point, it is 'queued', and then sent on to the required network cell, where it is again queued and finally sent to the end users phone. This queuing gives rise to delays at peak operator periods. Vodafone's own sales literature claims that 96% of all SMS messages are delivered within 20 seconds. This means that 4% of users trying to authenticate will fail and will need to raise a help desk call to gain emergency access. Thus for a deployment of 5000 users authenticating each day, 200 help desk calls would be raised per day!



Signal dead spots

Mobile phone signals are not always available, particularly in buildings with wide outer walls, in underground basements or in computer rooms that give off high RF noise. Consider a user trying to authenticate in one of these locations. They would first enter their UserID and PIN and would then fail to receive their authentication code. They would next need to move to a location that has a signal, receive their authentication code, then move back to the original location to enter their passcode, all within a timeout period of 2 minutes!
Users located within these locations would have no alternative but to raise help desk calls to gain emergency access.

Mobile phone is used to connect to the Internet

In most cases when a mobile phone creates a data connection, it can't receive SMS messages. Users trying to utilize their mobile phone as a way of connecting to the Internet would not receive their passcode until they hang-up the data connection. End-users would need to start authenticating the UserID and PIN, hanging up the connection, waits for the SMS message, reconnects and re-enter their UserID, Pin and Passcode, all within 2 minutes.

Why Pre Load Passcodes

The key strategy for successful use of SMS for delivering passcodes is resolving intermittent network coverage and SMS delivery delays. SecurAccess is fundamentally designed to resolve these issues by utilising:

- Pre-loaded one time passcodes (each authentication attempt sends the next required passcode)
- Three pre-loaded one time passcodes with each message (3 authentications before requiring the next message)
- Reusable session passcodes that change each day or multiple days
- Optional self-help web interface to allow users to request temporary passcodes
- Passcodes can be sent via email

Real Time SMS Delivery

There are times when a Pre Load SMS passcode is not acceptable for certain deployments; these tend to be ecommerce type environments where a user logs on infrequently to the network or web resource.

In these scenarios SecurEnvoy has the ability to allow a "Real Time passcode" delivery option. The user typically would log onto a resource with their UserID and password, at this point a SMS passcode is sent to their registered mobile phone. The SMS passcode can be set with a time to live in minutes to provide additional security around the logon.

- Real Time Delivery can be enabled upon a per user basis
- Passcode "time to live" is configurable from 1-99 minutes
- Works with existing SecurEnvoy IIS web agent and Radius clients that support "Challenge-Response"

Soft Tokens

SecurEnvoy's approach to soft tokens is based on zero management time for the IT or admin staff as the end-user downloads and provisions the apps themselves without any interaction with the corporate helpdesk or IT staff. Multiple token seeds can be stored in each soft token.

More flexibility for the User
The latest SecurEnvoy server V6 allows user far greater choice of security - either tokenless SMS two factor authentication or a soft token downloaded as an app such as this. Available free of charge to current customers from either SecurEnvoy or Google Authentication, soft tokens are suitable for most types of mobile devices i.e. iPhones, iPad's, Blackberry's, Android phones, Mac and Windows operating systems including Vista and Windows 7.

A simple process

For the organisation there is nothing they need to do. It is all down to personal preference of the end-user to choose whether they want their two factor authentication passcode sent via SMS or via their app.

The user simply:

1. Visits the app store – either SecurEnvoy or Google, and downloads the app

2. Logs into the SecurEnvoy enrolment page – cleverly they can authenticate themselves with their current user name and passcode

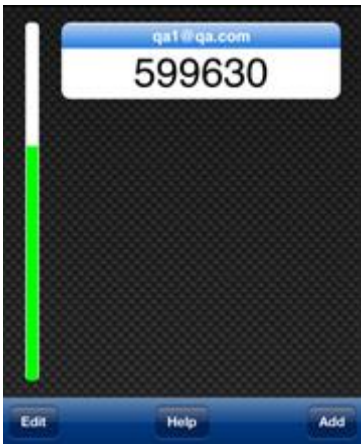
3. A barcode appears on the screen which the user scans with the camera button on their phone

4. Within 60 seconds the user can be authenticated and start using their phone as a soft token.

5. In the case of the P.C. Soft Token, the user only has to authenticate with the built in interface from the client. The SEED is automatically deployed with no user intervention. (Please see P.C. Soft Token manual for more information)



Mobile Phone "Soft Token"



P.C. "Soft Token"



iOS Soft Tokens - Push Notifications

The latest SecurEnvoy iOS soft token application ships with Push Notification functionality. When a user authenticates with SecurEnvoy 2FA a push notification message is sent to the notification centre or status bar of a users' iPhone. The user can simply choose to accept or deny the authentication request from within their soft token application.

There is a way to disable push per authentication attempt using the –nopush switch.

-nopush this disabled push and its associated delay

Example

Userid = qa1
Password = Password123-nopush

- This should disable push and reply with a passcode prompt without a delay

Soft Tokens - Near Field Communication

The current Soft Token One Swipe method works as follows: the user generates, in the soft token app for smartphones, a one-time QR code that contains important login and user information and then simply holds this code in front of a webcam on a laptop or tablet in order to prove his/her identity and thus gain access to the network. Near Field Communication technology provides the user with the option to transmit via NFC chip instead of scanning this QR code.

VOICE Tokens

SecurEnvoy's approach to VOICE tokens is based on complete "ease of use" to the end user. Unlike other industry methods where the user has to remember the passcode content of the prerecorded voice message, then entering this into the logon screen. SecurEnvoy session locks the Internet and Phone session together, whilst providing a seamless logon experience, the user doesn't have to remember the passcode, but only has to read the passcode from the logon screen and enter this upon the phones keypad.

This simple logon scenario can be accomplished via Web and also VPN type connections. The user accesses the point of logon and enters their UserID and PIN (typically a domain password) they are then confronted with the logon challenge. The user then receives a real time voice call, at which point they then input the displayed passcode (OTP) via the phones keypad. Once complete the voice call automatically hangs up, the user then selects the "Login" button to complete the process.

2 Domain model for LDAP

Chapter 2

SecurEnvoy has the ability to fully support direct integration with the following LDAP servers:

Microsoft Active Directory
Microsoft ADAM (Active Directory Application Management)
Novell eDir
Sun Directory server
OpenLDAP

In addition, SecurEnvoy can support a fully heterogeneous environment, allowing various vendor's LDAP servers to coexist and be managed by a single SecurEnvoy server. This allows companies exceptional scope to manage a truly heterogeneous LDAP environment.

Security Server scenarios

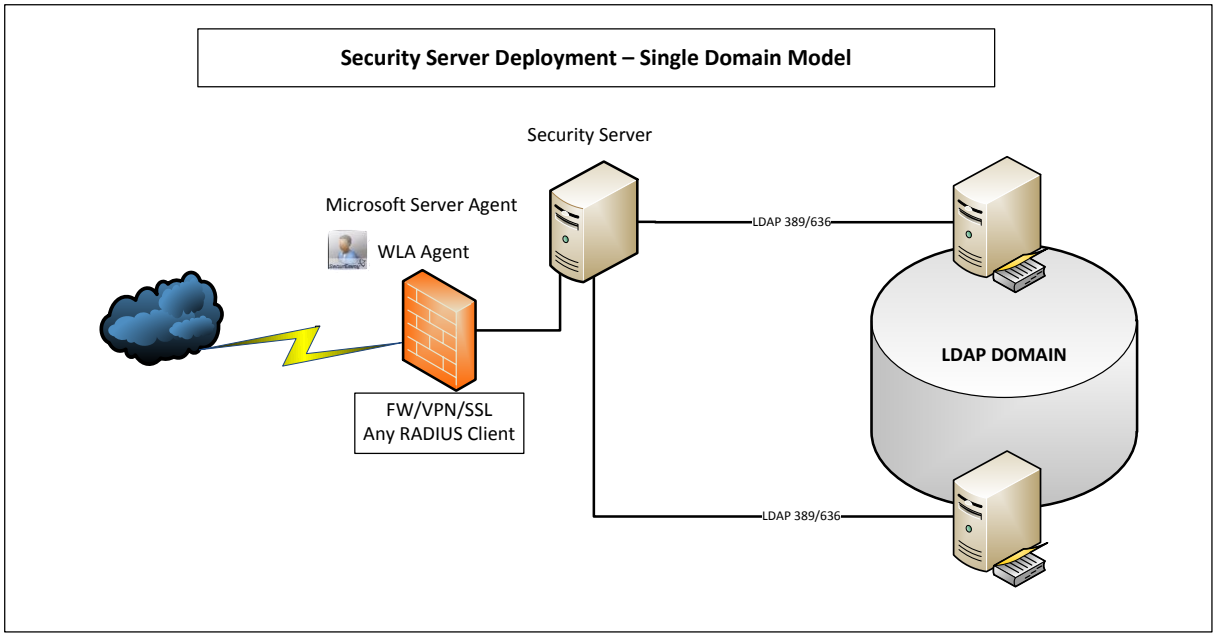
SecurEnvoy can be deployed many ways into a network environment; these are discussed in the topics below.

There are three deployments to consider:

- Single security server
- Multiple security servers
- Multiple domain model

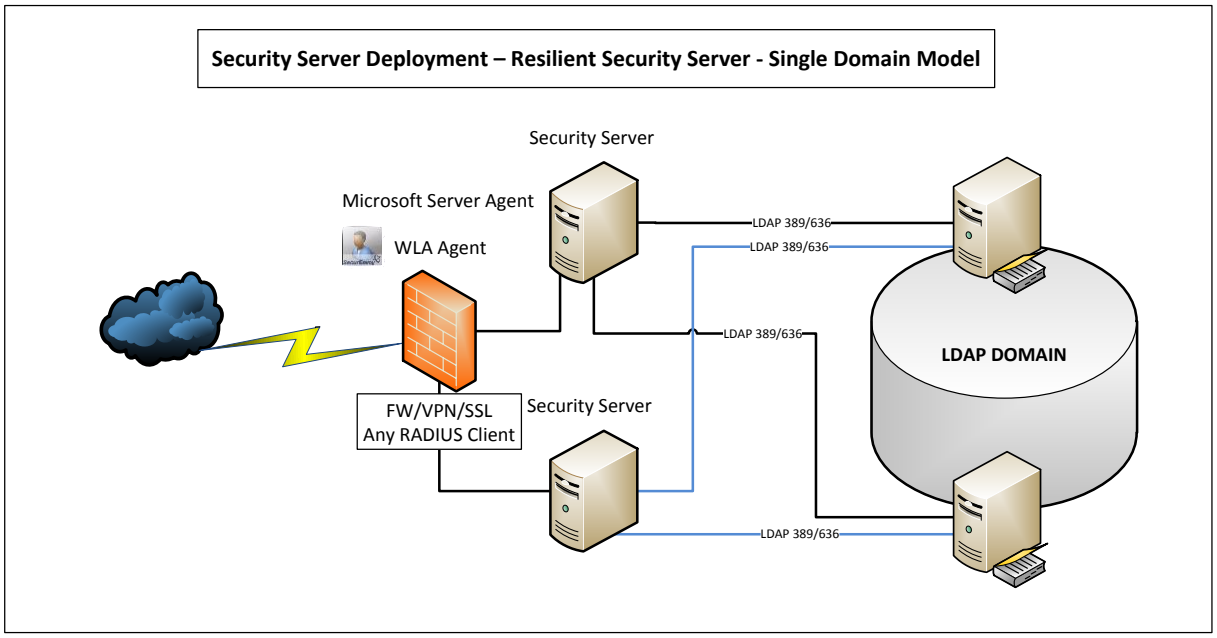
It should be noted that version 5 onwards of SecurEnvoy can support any multi LDAP server environment within a network and is not limited to all LDAP servers of being the same type.

Single Security server



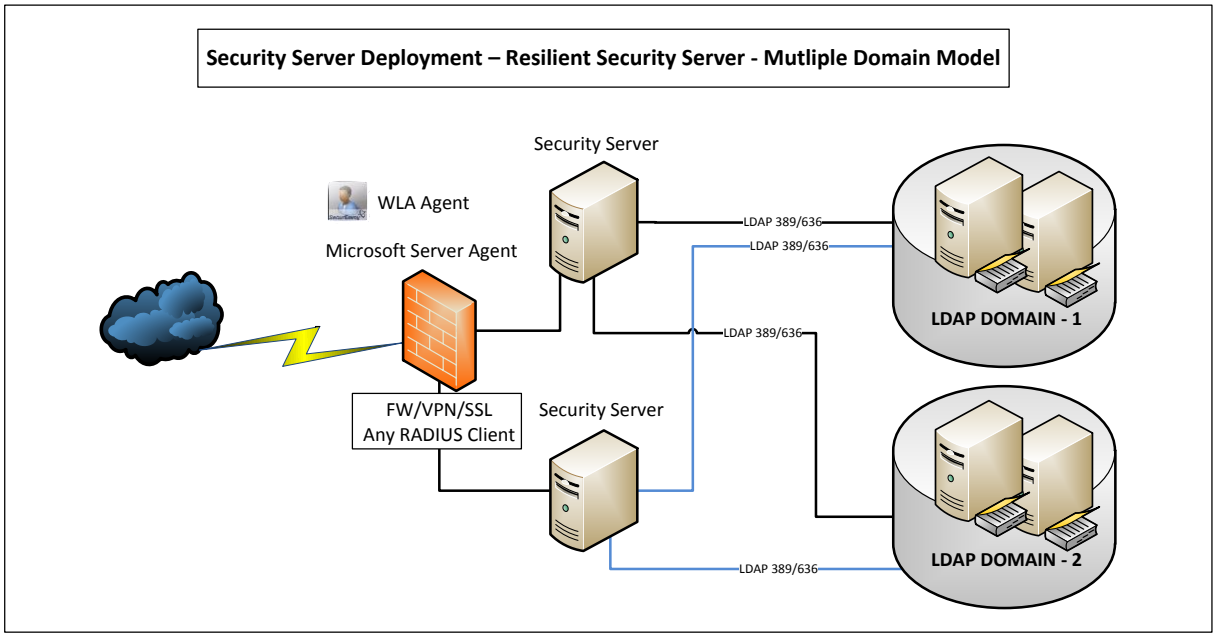
A single SecurEnvoy security server instance is installed, although in a very simple deployment there is no redundancy for the authentication, as only one SecurEnvoy security server is installed and configured.

Multiple Security servers



In a multiple SecurEnvoy security server example, each site's RADIUS or Web device will be configured to send authentication requests to one of two SecurEnvoy security servers. Each SecurEnvoy security server will share the same config.db key across all installations. Each SecurEnvoy security server will be paired to two LDAP servers. This provides a highly redundant authentication topology. Alternatively one SecurEnvoy server can be located at each site with each VPN using the other sites SecurEnvoy server as its second server

Multiple Domain model



Each SecurEnvoy security server can be configured with up to two LDAP servers for each domain your company uses, with no limit on the number of domains. Each domain can be configured for any of the supported LDAP server types. The domain component of the UserID is used to dynamically switch the security server to the relevant domain. If no domain component is given in the UserID then a default domain or search for first match can be used.

3 Support for multi LDAP environments

Chapter 3

To have the ability to deal with various customer networks and associated user LDAP repositories, SecurEnvoy can facilitate and manage disparate environments via a single administration console. This reduces the burden on existing IT staff for ongoing management of users.

Some of the most common deployment scenarios are discussed below:

- Company with Internal users requiring 2FA

A company who already has users stored within a LDAP server (Microsoft AD, Novell eDir, Sun One or OpenLDAP) requires very little configuration. All that is needed is a service account upon the SecurEnvoy servers that has read and writes privileges to the "telex number" attribute.

SecurEnvoy then reads in all user information without having to recreate a separate user database to allow 2FA to be deployed into the network. As users are already configured, administration is reduced, as well as allowing a high level of end user acceptance. This is achieved since the end user is not required to remember any more authentication information. They can reuse their existing UserID and password, complimented with a 6 digit OTP sent via SMS to their mobile phone.

- Company requiring a Business to Business 2FA

A company, who has to allow external users to connect to their internal network, but does not want to place these users into their own LDAP server, can use the "SecurEnvoy managed users" configuration. This utilises Microsoft ADAM, which is a cut down version of the Active Directory, but all user management is conducted by the SecurEnvoy admin GUI.

All user information is stored within Microsoft ADAM, to allow a greater control of external users, separate MS ADAM instances can be configured to bring physical separation to how the external users are managed. E.g. multiple support companies who require network access.

- Company requiring a Business to Consumer 2FA

A company who wants to conduct business with consumers, but does not want to place these users into their own LDAP server can use the "SecurEnvoy managed users" configuration. This utilises Microsoft ADAM, which is a cut down version of the Active Directory, but all user management is conducted by the SecurEnvoy admin GUI.

All user information is stored within Microsoft ADAM, to allow a greater control of external users, separate MS ADAM instances can be configured to bring physical separation they want to manage various consumers. E.g. Banking and Finance may have different requirements for retail banking consumers when compared to private clients banking.

- Company requiring 2FA for a ASP/ISP type model

Option 1

Managed customers allow connectivity to their own LDAP servers for user management (2FA, this requires read and write access to the telexnumber attribute).

The advantage of this option is that user's information already exists and is maintained in real time by the customer's own IT staff. In addition, deployment is rapid, as all user data is reused and users can be deployed on mass via the SecurEnvoy deployment wizard. (See 7.0 Automated User Provisioning).

All 2FA user information is effectively stored within the customer's own LDAP environment and thus replication and backup is managed within the customer's own network.

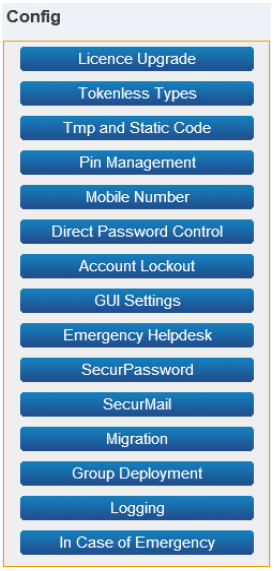
Option 2

A managed customer who does not allow access to their internal LDAP servers or will not allow write access to the telexnumber attribute. This approach utilises Microsoft ADAM, which is a cut down version of the Active Directory, but all user management is conducted by the SecurEnvoy admin GUI.

All user information is stored within Microsoft ADAM to allow greater control of external users. Separate MS ADAM instances can be configured to bring physical separation, in which the external users are managed. E.g. multiple companies who require network access to hosted applications.

4 Configuration

Chapter 4



Start the SecurEnvoy Admin GUI and select the "Config" menu.

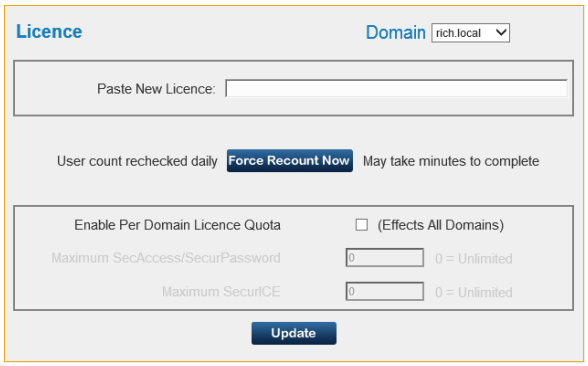
The Config page has fourteen sections that can be configured:

These allow parameter changes to be made to the SecurEnvoy Security Server, all of these settings can be applied on a per Domain basis. All except "Logging" as this is a global setting for the whole Security Server.

Start the SecurEnvoy Admin GUI and select the "Config" menu.

The Config page has 15 sections that can be configured:

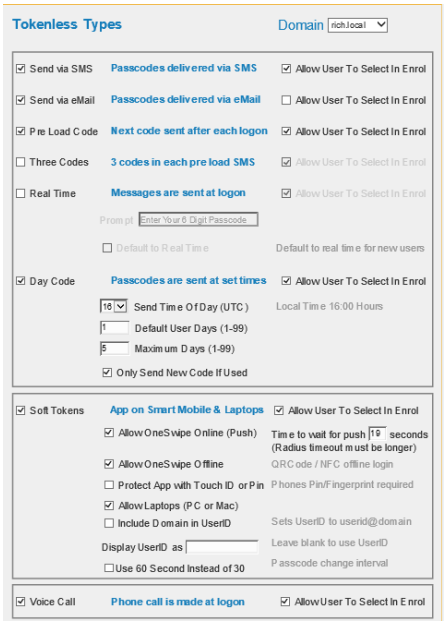
License Upgrade



The current existing license can be upgraded easily by copying and pasting the new license string into the "upgrade license" window within the Config page. Confirm replacement by clicking "update". The User count is rechecked daily but can be forced by selecting "Force Recount Now"

Thereafter "Enable Per Domain License Quota" can be enabled, this allows a quota to be applied per domain. The LDAP domain can be selected from the drop down menu bar, once selected a quota of licensed users can then be applied to this domain.

The quotas can be applied for SecurAccess/SecurPassword products as well as SecurICE



Tokenless Types

There are two enable boxes for the Token types, and each of these can be assigned upon a per domain basis. The first dictates what Token types are available for the relevant domain. The second is for enabling the user to switch between different Token types via the "Manage My Token" page (*https://machine.domain.com/secenrol*).

Passcodes can be **delivered via SMS**.

Passcodes can be **delivered via email**, email setup is via the Advanced config wizard. User is then setup for "Passcodes via Email" under the "User" tab of the admin GUI. SecurEnvoy does not believe that the user should be given the option to select email, a SMTP is not an encrypted protocol and may not be using TLS. SecurEnvoy believes that administrators should be in control as to whether email is used for passcode delivery. An example; Blackberry systems encrypt email delivery to the end device.

The default is to **"pre-load"** the SMS delivery, the passcode is sent when a user is first enabled and refreshed at time of logon.

The system can be enabled so that either a **single or three One Time Passcodes** are sent within each SMS message. This caters for users who are in an area that has weak or erratic mobile phone signal.

SecurEnvoy have the ability to send the **passcode in "real time"**. Once enabled the system has the ability to deliver a "real time" passcode that the user requests. The passcode then has a certain amount of time to live before expiry (configured in minutes 1-99). To enable this function tick the checkbox and set the prompt that user should see (default = Enter your 6 digit passcode). The real time SMS delivery can be enabled upon a user basis or can be set globally for new users by enabling the "New User have real time by default" checkbox.

The **Day Code mode** automates the process of changing passcodes every set number of days, this can be in the range of 1-99 days. Day codes are reusable passcodes that are automatically changed every xx days (Global Default User Days) at a pre-defined day and time (Day Code Send Time). Global Default User Days is used on all new users as the default and can be changed for each user. Additional logic can be applied where a new Day code is only sent if the previous one has been authenticated.

To enable the use of **Soft Tokens** upon the SecurEnvoy server check the "Enable" box, this must be completed for all SecurEnvoy servers that are to be used for "Soft Token" support.
This will allow Soft Token to be used on a Mobile phone. To support a PC or Mac based Soft Tokens, enable the checkbox "Allow Laptops". The soft token refresh rate can be set to 60 seconds if preferred but the default is 30.

SE Administrators can allow users to use Oneswipe Online (push) and Oneswipe Offline (QR Code /NFC Offline Logon) per domain. Access to soft tokens can be protected by either a biometric Touch ID or the phones security access PIN code. You can only use Protect App with Touch ID or PIN if you have not enabled push, as push requires your pin to be entered at the login to initiate a push request.

Voice Call, brings the ability for a real time interactive voice call for users who cannot receive a SMS.

NOTES: Day Code usage

Note

All servers in all domains must have the same Day Code Send Time set (allowing for any time zone differences) such that they all run at the same time

The next required passcode will be sent to this user's mobile phone at 16:00 by default (Day Code Send Time).
If "Only Send New Day Code If Used" is selected then the next required Day Code is only sent if the current or previous day codes have been used.

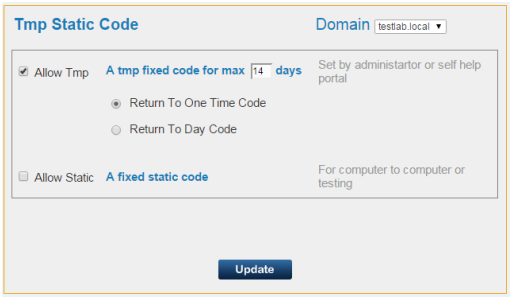
Note

A valid passcode is the current or the previously sent code; this eliminates any SMS delays or intermittent signal loss within a 24 hour period.

Note

Configuration changes that affect the batch server will only be seen when the batch server next runs. If you change the Day Code Send Time it may take up to 24 hours for this change to be set. If you re-start the SecurEnvoy Batch Service, these changes will take place immediately.

TMP and Static Code

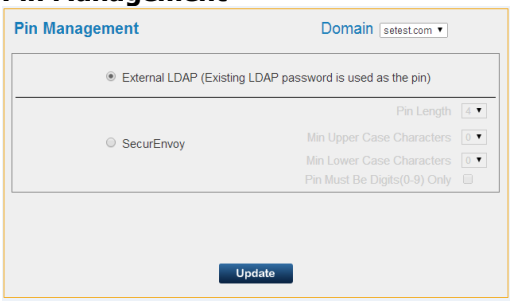


This setting allows what should happen to a user when they have exhausted their temporary static code status; the global setting allows either reverting to a One Time Passcode or a Day code.

When testing is beneficial to have the ability to allow a "Static code", as SMS or Voice gateways may not be ready or available. This feature allows end to end testing prior to the gateways going live.

All of these settings can be assigned upon a per domain basis

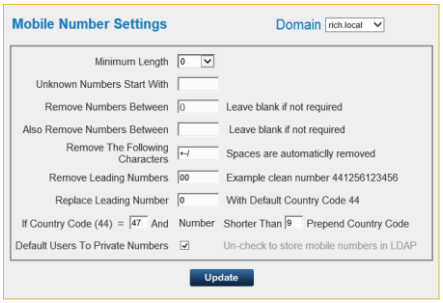
Pin Management



Pin Management will setup the Security server to either use Microsoft Windows password as the Pin for each respective user enabled upon the system, or will use SecurEnvoy to separately manage it. If set to SecurEnvoy, the Pin can be between 4-8 numeric or alphanumeric. The Pin can be set by the administrator or the user via the enrolment process.

All of these settings can be assigned upon a per domain basis

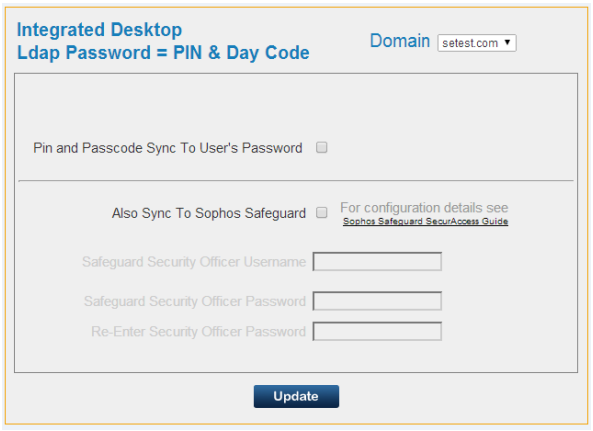
Mobile Number Settings



The system can be setup to validate the mobile number that is entered into the system. The first check is to make sure the mobile number is of a certain length (length 5-18), in addition any number that is entered that is not recognised can be automatically preceded with a set number. Numbers can be removed between specified characters, as can specified characters, leading numbers can be removed or replaced and country codes manipulated as required.

All of these settings can be assigned upon a per domain basis.

Direct Password Control



Integrated Desktop is achieved by generating a new day code (or week code) for enabled users and sending it to the users registered mobile phone. This is used in combination with the user's secret PIN. The PIN can be alphanumeric to surpass any Windows security policy that requires an amount of upper and lower case characters. The day code is written in real time to the Active Directory at time of generation.

Sophos SafeGuard Support allows SecurEnvoy to provide 2FA support for Sophos Safeguard, to enable, tick the "sync to Sophos SafeGuard" box, then enter Sophos Security Officer credentials, click "update" when complete. For more details on Sophos SafeGuard integration, please see the following integration guide:
http://www.securenvoy.com/integrationguides/sophossafeguardsecuraccess.pdf

All of these settings can be assigned upon a per domain basis

Understanding Direct Password Control

Password Automation will change and send out the new Domain password via SMS to all enabled users. This is the dynamic component of the Domain login; a separate static Pin is required to make up and complete the Domain authentication, which is managed by SecurEnvoy. Setting the correct level of upper and lower case characters as well as numeric, allows the passcode to meet Domain Security policy requirements. Enabling Password Automation is on per user basis.

Note

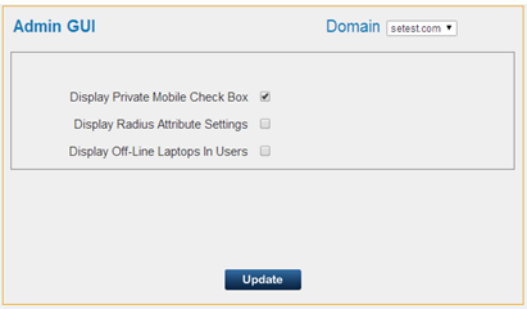
SecurEnvoy recommends that Integrated desktop mode uses SSL over LDAP (SDLAP 636) to fully meet all of the above stated requirements of a password reset.

To meet a domain password policy, it is recommended that the PIN is a combination of both upper and lower case. Example PIN = Se12, Passcode =234765, Domain password = Se12234765

Integrated Desktop Management is only supported when using a Daycode, one time passcodes are not supported.

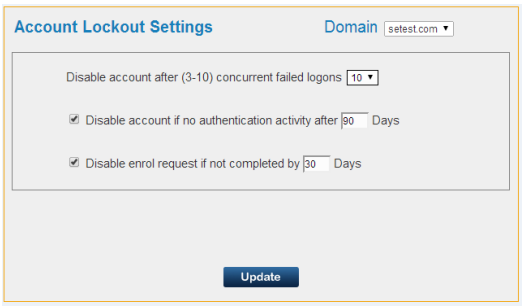
To enable the integrated desktop mode of SecurEnvoy, we first need to understand the password reset process.

LDAP Password Modification
The first technique that is always attempted is an LDAP-based password modification. The core of this technique involves modifying the unicodePwd attribute directly. SetPassword does one modification with the "Replace" modification type specified, and "ChangePassword" does two modifications with a Delete and an Add specified, in that order. Active Directory enforces a restriction that any modification to the unicodePwd attribute must be made over an encrypted channel with a cipher strength of 128 bits. Otherwise, the server will reject the attempted modification. This helps ensure that the plaintext password is not intercepted on the network.



Therefore, with this in mind, there are only two ways to accomplish an encrypted tunnel for password modification:
Active Directory supports two mechanisms for channel encryption: SSL and Kerberos. However, only SSL supports the minimum 128-bit cipher strength on all Active Directory platforms. Kerberos-based encryption has been strengthened to meet this requirement on Windows Server 2003 and above. Because the function attempts to work with either version of Active Directory, it always selects only SSL for the channel encryption technique.
This is unfortunate, because Kerberos-based encryption works out of the box with Active Directory, but SSL requires additional configuration steps including the acquisition of proper SSL certificates for each participating domain controller.

Account Lockout Settings



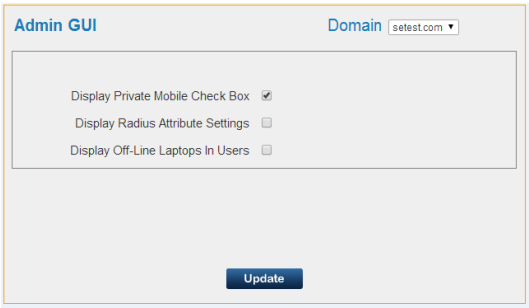
This can be set between 3-10 concurrent bad authentications since the last good authentication, before the user is disabled. Once disabled, no more passcodes are sent and the user is denied access. If using SMS, the user is sent an alert SMS explaining that their account is now locked.

User accounts can be automatically disabled if there is no authentication activity for (xx) number of days (configurable, default is 90).

User accounts that do not complete an enrolment request are disabled, (configurable, default is 30 days).

All of these settings can be assigned upon a per domain basis

GUI Settings



The administration interface is configurable, so that only certain elements are displayed. Use the checkboxes to configure the Admin interface.

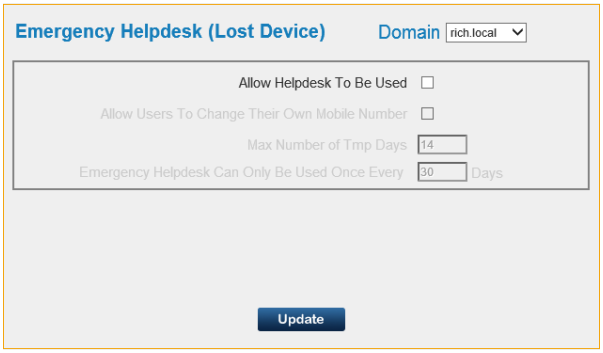
These are as follows:

Display private mobile checkbox. Private mobile Checkbox is displayed or hidden in admin GUI
Radius attribute settings configure and control Radius settings

Offline laptops settings Enable/disable offline passcodes for Integrated Desktop Logon

All of these settings can be assigned upon a per domain basis

Emergency Helpdesk



Self Helpdesk allows users to assign themselves a temporary code or change their mobile number in the event that they have no phone signal or no access to their mobile phone. This section controls whether this is enabled, and whether the user can set their own mobile number, the maximum number of days a temporary code can be assigned and how often the helpdesk can be used within a period of time.

All of these settings can be assigned upon a per domain basis

To use the Self Helpdesk, a user must first enrol and provide answers to two security questions. The enrolment request is sent automatically when a user is first enabled. (This will only occur if the "Allow Helpdesk To Be Used" checkbox has been enabled).

The security questions are read from a template file to allow for customisation. The file path is Security Server\Data\ENROLMENTTEMPLATE\questions.txt within the SecurEnvoy installation directory (e.g. for 32 bit installations
C:\Program Files\SecurEnvoy\Security server\Data\ENROLMENTTEMPLATE\questions.txt).
For 64 bit installations
C:\Program Files (x86)\SecurEnvoy\Security server\Data\ENROLMENTTEMPLATE\questions.txt).

Note

Enable helpdesk by ticking the checkbox and then set parameters of what the user can do, example change own mobile number. When a user is deployed they are sent a URL link to "Enroll". This can either be sent via email or SMS.

SecurPassword



SecurPassword allows a user to reset their Microsoft Domain or other LDAP password using Two Factor Authentication. In addition to the passcode, up to three attributes of data can be used to help validate the authentication request for a password reset. Also, the user can use security questions that were answered within the enrolment process. Any data that is held within the Directory Server can provide further checks to the user's credentials. Attributes like employee number, department etc. can provide additional authentications parameters.

User can be automatically alerted by SMS a set number of (xx) days (configurable) prior to their password expiring.

Password parameters can be assigned such as age, minimum length and complexity.
All of these settings can be assigned upon a per domain basis

User can be automatically sent a "Password expiry warning" via SMS, this feature will send out a SMS warning message at x days before their user password expires. (Default is 7 days)

The prompt for each attribute is a text string that is presented in the password logon web page.
To enable SecurPassword a valid license must be installed. Enable the Allow SecurPassword checkbox must be ticked. The only decision is to either use existing attributes to check for authentication, or use the security questions a user has enrolled with. (See Self Helpdesk above)

Note

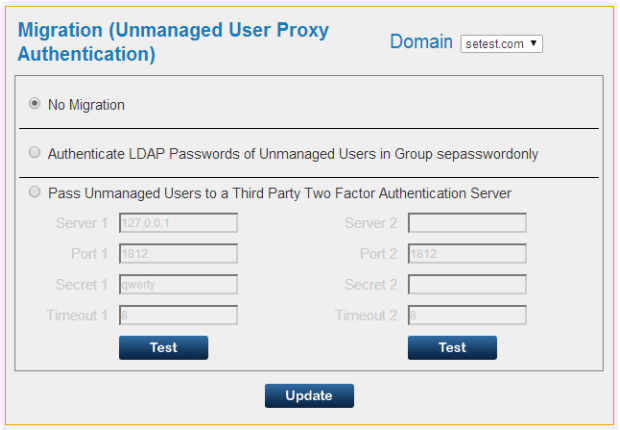
If the "secret questions" box is left un-ticked and no attributes are populated, a user will be able to reset their password with just the passcode.

Note

SecurEnvoy recommends that SecurPassword uses SSL over LDAP (LDAPS 636) to fully meet all of the above stated requirements of a password reset.

Enable the SSL option using the Advanced Configuration Wizard

Migration (Unmanaged User Proxy Authentication)



The Migration feature allows users to be migrated to a SecurEnvoy solution from an existing password-only or token solution. Once configured, users can be migrated in stages as required, allowing a smoother transition.

All of these settings can be assigned upon a per domain basis

Migration from Password-Only

Users that have not been enabled within SecurEnvoy will need to be members of a group named "sepasswordonly". This group must be configured within the directory server prior to deployment. These users will then be allowed to authenticate using only their username and password. Once migrated to SecurEnvoy, they can be removed from this group and have a full 2FA experience.

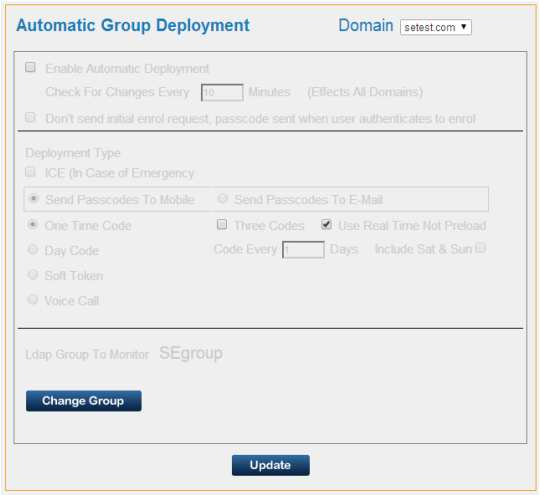
Migration from Third-party Two Factor Token Server

RADIUS authentication is configured to use the SecurEnvoy server. If the user is not enabled within SecurEnvoy, the SecurEnvoy server will act as a proxy, and forward the RADIUS request to the configured third party token server.

Up to two configured third party token servers are supported. IP address, port, shared secret, and timeout information is required. Once configured, the test button will initiate an interactive logon.

Automatic Group Deployment

SecurEnvoy Security Server has the ability to provision users. This can be completed with the Deployment wizard (recommended for first time user deployments) as it allows an extremely granular approach to how users are deployed. Or with the Automatic Group Deployment within the admin GUI. This caters for ongoing deployments of users.
The Deployment Wizard is a tool that allows enterprises to carry out an initial deployment to a high number of users easily. It is customisable so that passcodes can be sent via SMS or Emailed to users in one seamless mechanism. This tool can be used in one of two ways, via a graphical user interface for manually deployments or in command line mode for scripts or batch jobs to use. This is a separate SecurEnvoy tool, that is accessed from "Start" - "Programs" - "SecurEnvoy" - "Deployment Wizard"
The Automatic Group Deployment is an embedded feature that allows simple ongoing provisioning of users, a dedicated group of users (only one group per domain is supported) is monitored, any user added to this group is automatically deployed with the options set in the GUI. If a user is removed from the group, they are automatically unmanaged.



SecurEnvoy has the ability to automatically provision users with its Automatic Group Deployment option. All of these settings can be assigned upon a per domain basis

The following options are able to be set:

Enable Automatic Deployment
Enables or disables the automatic deployment option, an additional setting allows a time in minutes to be set. This is how often the Automatic Deployment should check for users being added or removed from a group.
Deployment Type
ICE (In Case of Emergency) for emergency users, business continuity, disaster recovery.
Send Passcodes to Mobile / Email
Example - User will stay explicit to the mode of deployment, if deployed with a passcode to mobile, they will always receive a passcode via SMS. As long as the mobile attribute is populated. If not, the system will check and then deploy the user by email, the user will then follow the enrolment instructions in the email to update their own mobile number into SecurEnvoy. If user deployed via email, they will always stay in this mode.

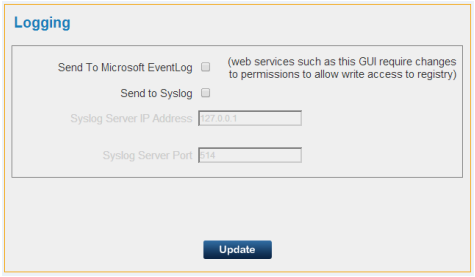
NOTE: Mobile or email attribute must be populated.

One Time Code / Real time
Select users to have a One time passcode in "Pre-Load" mode or use "Real time delivery".
Soft Token
Users are deployed with an enrolment message to setup their soft token.
Day Code
Users are deployed with a Day Code, the code refresh in (n) days can be set, this is global setting for all deployed users

Note

If a group is declared in the Automatic Group deployment option, the user will be enabled and provisioned or unmanaged depending on whether they are a member of the declared group.
If "Allow any group" is selected, all users in the domain will only be provisioned. Caution, this could cause a high number of user to be provisioned.

Logging



SecurEnvoy has three supported options for logging information. They are –

- SecurEnvoy log file. This resides locally upon the machine
- Microsoft Event Log. SecurEnvoy writes log information to the Application Log
- Syslog server. Enter the details of your Syslog server.

In Case of Emergency



ICE (In Case Of Emergency) allows the ability to turn on strong, two-factor authentication, for all users in the event of an emergency. The user's existing Microsoft password is the first factor, and a passcode sent to the user's mobile phone is the second. There is no need for the user to enrol and remember an additional PIN, and no need for extra tokens or smart cards.

The ICE message content can be directly edited in the admin GUI.

Thereafter a "return to work" message can be configured, once the emergency is over, this is sent when ICE is turned off.

All of these settings can be assigned upon a per domain basis

5 Advanced Configuration Wizard

Chapter 5

The SecurEnvoy "Advanced Configuration Wizard" controls all configuration data of the SecurEnvoy Security server. To launch this tool go to:

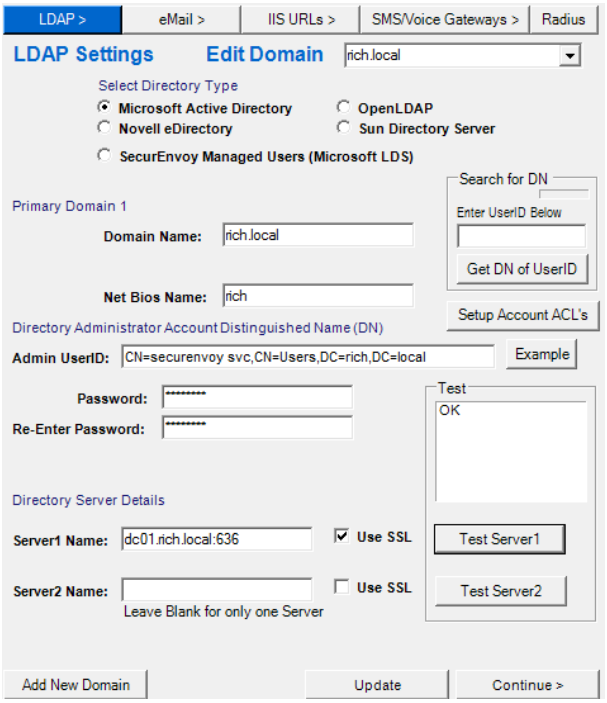
Start/Programs/SecurEnvoy/Advanced Configuration Wizard

By default, the wizard will always launch to the IIS and LDAP tab, you can step through each tab automatically after making changes to each relevant section. Or you can go directly to the section of your choice by selecting the correct tab required.

LDAP tab

Enter details for the Web server (machine that will run the SecurEnvoy admin GUI) and select the Directory server type, either "MS Active Directory, Novell E-dir, Sun One Directory server, LINUX OpenLdap or MS ADAM".

Select Directory Type - First step is to select the Directory Type either "MS Active Directory, Novell e-Directory, SecurEnvoy Managed Users – MS ADAM, OpenLDAP – Linux, Sun Directory server".



Primary Domain 1 - The *Domain Name* is the domain where the active directory resides and user information is stored and retrieved.

Directory Administrator Account Distinguished Name - Use the Tab key to step into the *Search for DN* section and into the field *Enter UserID*. Type the name of the account that will run the SecurEnvoy server. Click *Get DN of UserID,* this will automatically populate the DN account details providing you are currently logged on as a domain administrator of this domain. If correct, enter the password for the User ID account.

Using the button *Example* will provide a real example of the administrator DN directly from Active Directory.

Directory Server Details - Finally enter the names of your Directory servers. If certificates have been deployed upon your directory servers, LDAPS (port 636) can be utilised by enabling the "Use SSL" check box, note that LDAPS generally requires the server name to be fully qualified.

Test – after completing the required details, the connection can be tested by clicking Test Server 1 or Test Server 2. If OK is returned then click Continue. If OK is not returned, errors should be rectified before proceeding.

Note

LDAPS generally requires the server name to be fully qualified.

If "Use SSL" is selected, the server name MUST be the same name as set in the common name of the Directory's server certificate

If you wish to add an additional domain, click the "Add New Domain" button and enter the LDAP Settings for each new domain. The web server is the machine that the security server software was installed upon, this does not require changing.

The domain name is the additional domain where user information will be stored and retrieved. The Net Bios Name is optional and only needs setting if UserID logons use Net Bios Domain names for example "SECURENVOY\john smith".

Once the above information has been entered and a successful test established, click Continue. A warning will be displayed in the Wizard that confirms that the batch services are being installed

Click Save and Continue.

Note

Any combination of Vendor LDAP server is supported in any order, each domain can be configured with its own SecurEnvoy administration account for read and write permissions.

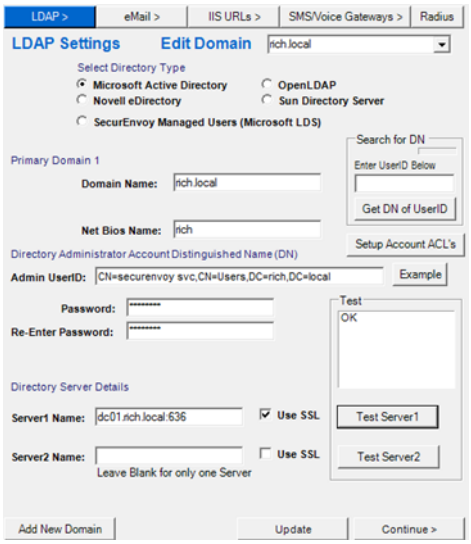
*Each Domain **MUST** share the same SecurEnvoy administration account, or secondary servers in the same domain will elevate to batch master, causing the batch server to affectively run many times &result in multiply day codes being sent.*

5.1 Multi Domain configuration

Start/Programs/SecurEnvoy/Advanced Configuration Wizard, select LDAP tab.

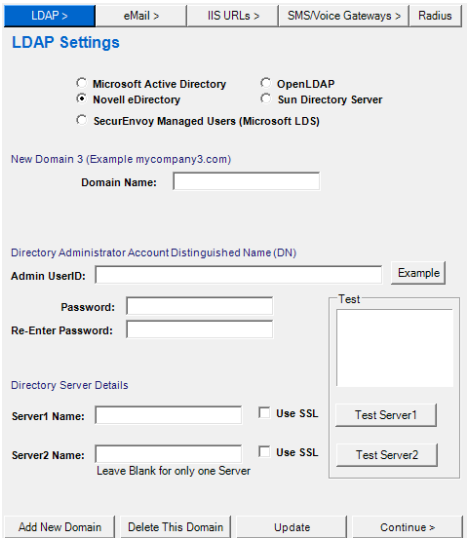
Additional Microsoft AD, click "Add New Domain" and then select domain type and populate with required information.

Adding additional Microsoft AD domain, click "Add New Domain", then select domain type and populate with required information.



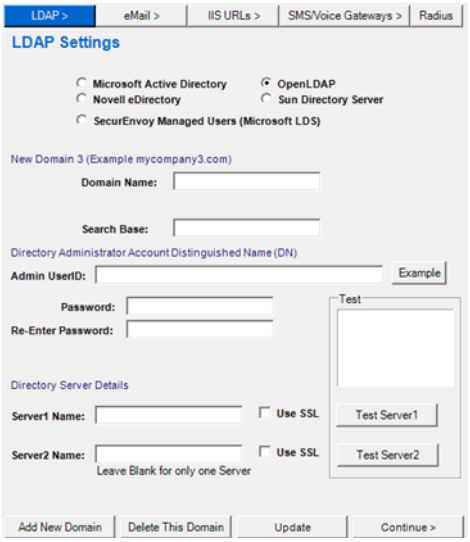
Click Update or continue when complete

Adding Novell e-Dir domain, click "Add New Domain", then select domain type and populate with required information.



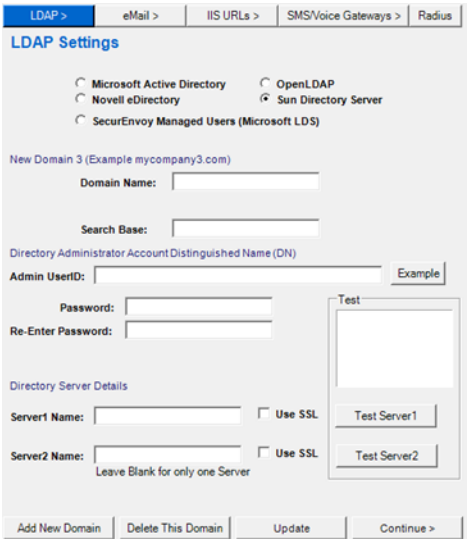
Click Update or continue when complete

Adding OpenLDAP domain, click "Add New Domain", then select domain type and populate with required information.



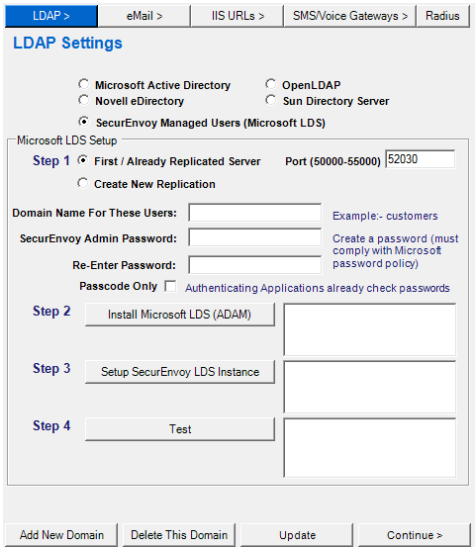
Click Update or continue when complete

Adding Sun Directory server domain, click "Add New Domain", then select domain type and populate with required information.



Click Update or continue when complete

Adding Microsoft ADAM / AD/LDS (SecurEnvoy Managed Users)



Selecting "SecurEnvoy Managed Users" allows the creation of a user database when no corporate directory server exists or can be used. This utilizes Microsoft ADAM (Windows Server 2003) / AD/LDS (Windows Server 2008), and allows user creation and management to be completed via the SecurEnvoy Admin GUI.

To create a Microsoft ADAM / AD/LDS instance, select "SecurEnvoy Managed Users", then select whether this is the first or subsequent replica ADAM instance (for redundancy) and populate the domain name required for these users e.g. "Sales".

The "passcode only" checkbox controls whether SecurEnvoy will authenticate both the PIN and passcode of the authentication request or just the passcode.

Follow steps 1-4, which will install Microsoft ADAM / AD/LDS, configure the instance and test that it is operational.

Note

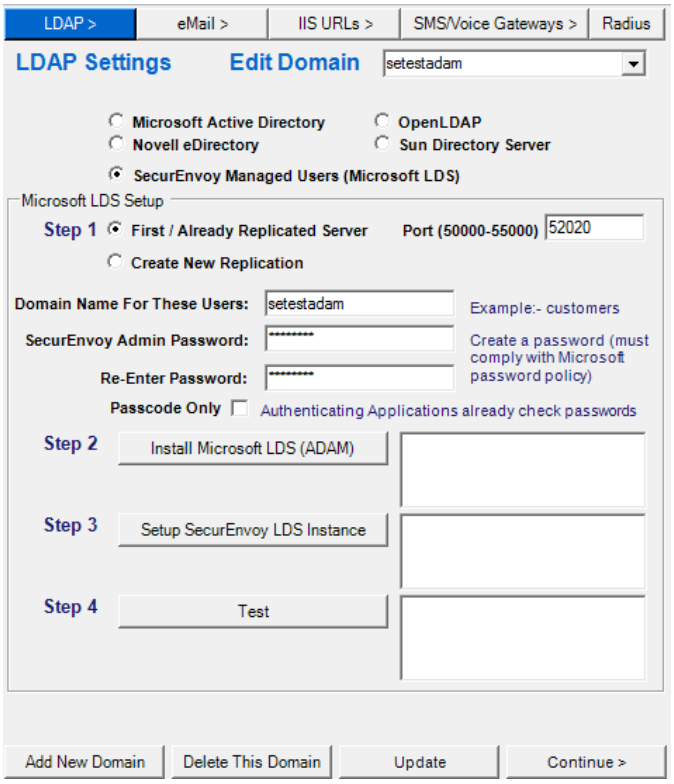
The port number for MS ADAM is automatically configured and incremented for each individual instance. This can be manually changed to suit the requirements of each environment that it is installed upon.

Adding Microsoft ADAM Replica (SecurEnvoy Managed Users)

To install an ADAM replica, run the SecurEnvoy "Advanced Config Wizard", select:

Note

To facilitate ADAM replicas, the machine that is to have ADAM replica installed, must be a member of the same domain as the ADAM master. Also you must be logged in with "Domain Admin" rights for the ADAM replica install to succeed.



LDAP tab, select SecurEnvoy Managed Users (Microsoft ADAM) and select Create New Replication on Microsoft ADAM Setup window. Enter details for the port in TCP Port, enter details for "Server To Replicate From" This must be in a FQDN format.

Note

The port number should be the same for each Microsoft ADAM Master and Replica instance.

Note

The Server To Replicate From must be in a FQDN format. IP addresses are not supported.

Note

The ADAM domain name can only support characters 0-9 and A-Z

Enter the domain name information for the ADAM instance.

Enter the password details for the SecurEnvoy admin Password. These should be the same as the ADAM master.

Then follow steps 2-4 to complete the install.

When complete click "Update or Continue"

Points to note regarding ADAM or AD LDS replication

1. Windows Firewall seems to block update notifications to replicas so you need to create a custom rule on both servers to trust all inbound communications from the other servers IP address.

2. If these servers are not in the same domain, change the windows service SecurEnvoyADAM*** to run under a user account that is a member of administrators group (not the default system account).

3. On the second server, create the replica via SecurEnvoy Advanced Config and change the windows service SecurEnvoyADAM*** to run under a user account that is a member of administrators group (not the default system account).

Note

The ADAM replica instance will take up to 10 minutes before it is fully replicated and published.

Adding and editing SecurEnvoy Managed Users (Microsoft ADAM / AD/LDS)

Example

Within the SecurEnvoy Admin GUI, select the ADAM domain created "Demo".

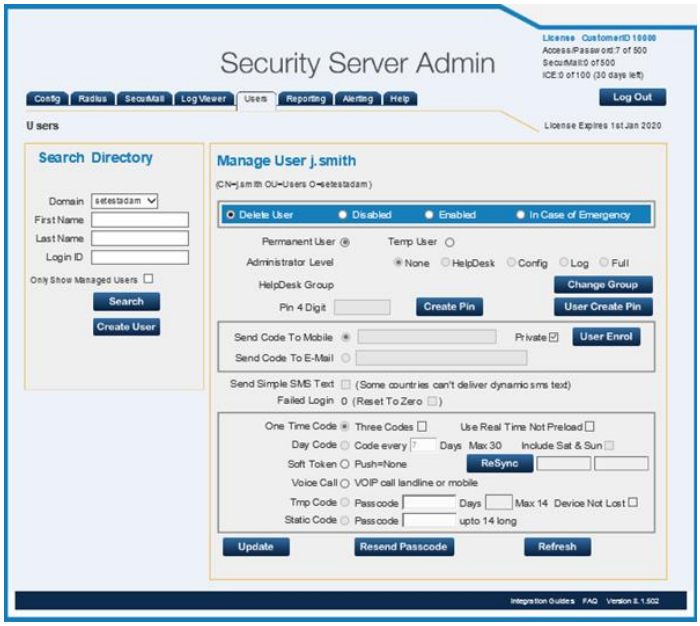
To add a new user:



Populate Naming information and then select the "Create User" button

Note

An additional button is created within the SecurEnvoy admin Gui, this allows user creation. User information is typed into the "search Directory window"



The user screen for the created user will now be displayed. Additional information regarding the account can now be populated.

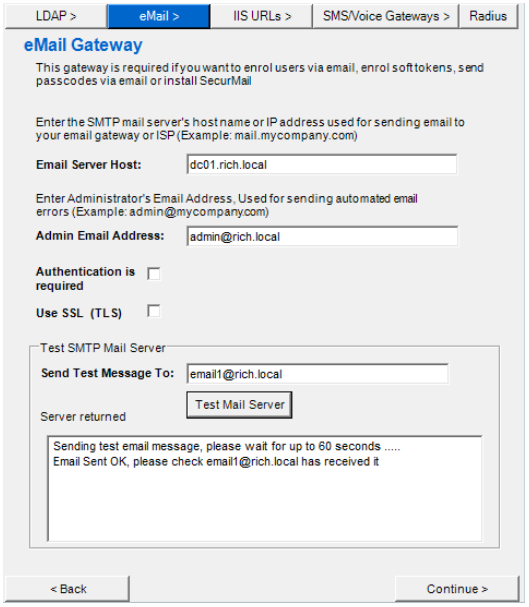
Note

SecurEnvoy recommends that if a PIN is required, it is managed by SecurEnvoy as it is stored encrypted (Default action for all SecurEnvoy data). "ADAM passwords are not supported as they are not as secure as SecurEnvoy PIN's"

5.2 eMail Gateway Configuration

Start/Programs/SecurEnvoy/Advanced Configuration Wizard, select eMail Gateway tab.

The eMail gateway settings are displayed below:



For the eMail Gateway configuration, enter details of the SMTP server that should be used for the sending of emails and the associated email account you wish to use.
There are two further options, for SMTP servers that require authentication, enable the checkbox and enter account details.
To support SMTP server that utilises TLS, enable the checkbox.

Once setup a test email can be sent to a recipient to test if the configuration is correct.

Note

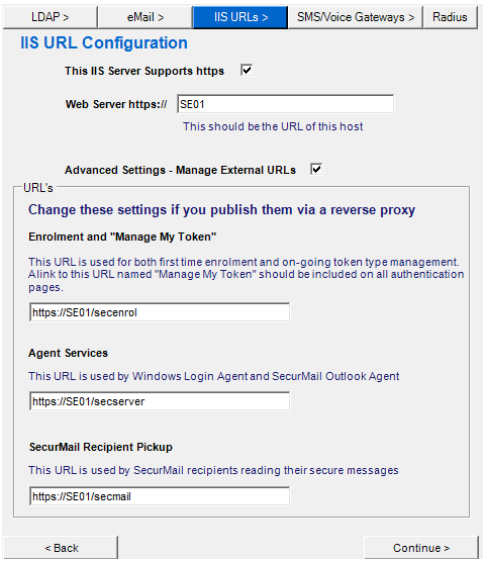
Please ensure that your SMTP server has been setup to allow relaying from the SecurEnvoy server.

Note

The SecurEnvoy Advanced Configuration Wizard can be exited at any time after configurations have been made.

5.3 IIS URL's

Start/Programs/SecurEnvoy/Advanced Configuration Wizard, IIS URL's tab.



The URL configuration can be viewed and maintained from this tab. If the server supports HTTPS, then this can be selected. This setting will be inherited in the URL values that are displayed when selecting Manage My URLs. These URL values are included in system generated Emails sent to users. For example user enrolment Email.

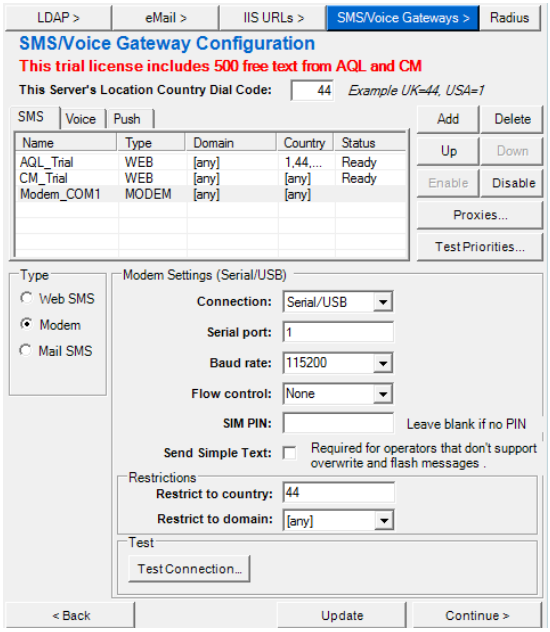
Click Save and Continue.

Note

The SecurEnvoy Advanced Configuration Wizard can be exited at any time after configurations have been made.

5.4 SMS / Voice Gateway

Start/Programs/SecurEnvoy/Advanced Configuration Wizard, select SMS / Voice Gateway tab.



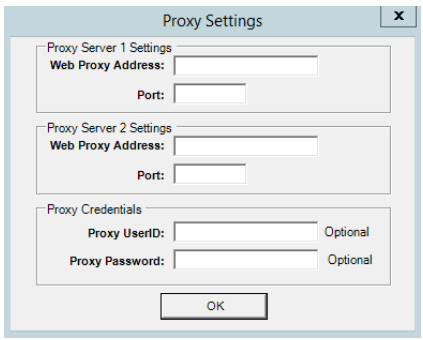
Multiple gateways can now be setup and maintained via this Tab. It is possible to setup as many gateways as required to meet the operational requirements of the organisation. SecurEnvoy can support various gateway types from Web SMS, SMPP, Voice through to Serial or TCP/IP Modems.

The gateways can also be setup in priority order and can also be disabled as required very easily from with this wizard. The priority ordering of the gateways in controlled using the "Up" and "Down" buttons.

The gateways can be restricted to per country and per LDAP domain, to allow the administrator more control as to which service is used in certain countries. This is used to overcome difficulties sending SMS into countries that might not support advanced SMS features such as flash message and SMS overwrite.
Once complete priority can then be assigned for multiple gateways that will support the same countries/ domains.

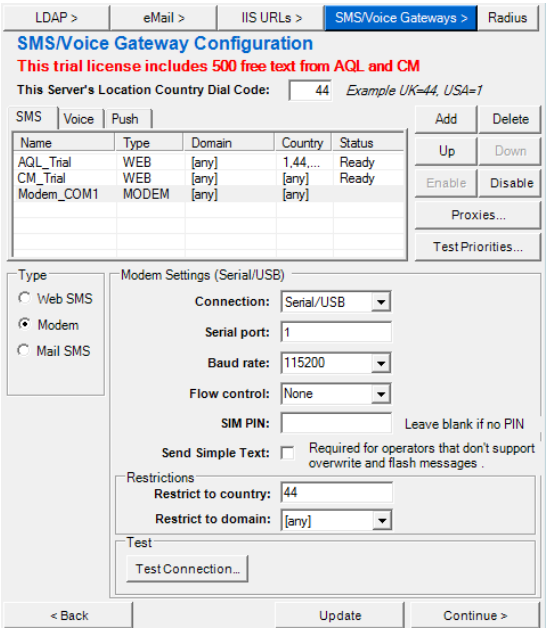
For **Web SMS gateway** option a suitable provider account MUST already be setup and account details MUST be entered.
Restrict to Country / Domain allows the administrator to define what SMS gateways are used, this can be assigned per domain or by country code. Enter dialling codes for countries or domain that should be served by this SMS gateway, this can be selected from the radio button drop down menu. When dealing with country codes, for a particular SMS gateway, multiple country codes can be assigned, by comma separating.

Finally a test connection button allows the SMS gateway to be tested that it is operational and any user account information is correct.



If a proxy server is being utilised upon the network, then proxy information can be entered
Click Update if any changes have been made or Continue when complete, this will then save all SMS Gateway information.

SecurEnvoy can connect to many Web based SMS providers. A new template may be required – See Security Server Administration Guide *for more details*



To "Add" a **GSM Modem**, select Add then check the Modem radial button

Then select the connection type Either Serial/USB or TCP/IP
If USB/Serial enter Comm port and baud rate settings for the connected GSM modem.
If TCP/IP select the IP address and port number.

The above two options allow a corporation to use its own SIM chip from their Telco and take advantage of any free or group SMS call rates.

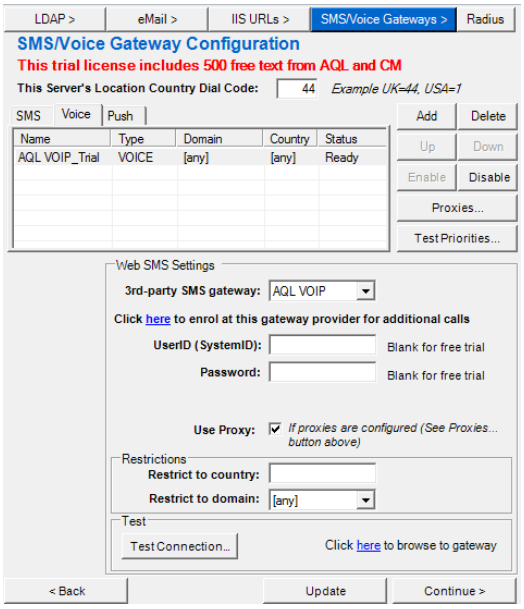
The following are configurable options:

Send Simple text
When enabled allows a SMS to be sent in simple mode. Use this if the Telco operator does not support message overwrite (PDU mode).

Enter dialling codes for countries or domain that should be served by this SMS gateway, this can be selected from the radio button drop down menu. When dealing with country codes, for a particular SMS gateway, multiple country codes can be assigned, by comma separating.

When complete click the OK button to test. The test will carry out an ATI and signal strength test. Version information will be shown as well as signal strength information. Signal strength is measured from 0-31. An acceptable figure is 16 or above.

Click Update if any changes have been made or Continue when complete, this will then save all Gateway information.



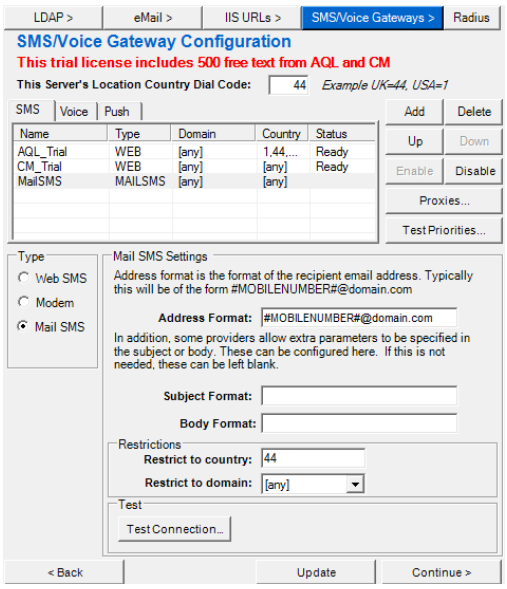
To "Add" a **Voice Gateway**, select Add then check the Voice radial button.
Select the appropriate voice provider from the drop down menu list.

For **Voice gateway** option a suitable provider account MUST already be setup and account details MUST be entered.

Restrict to Country / Domain allows the administrator to define what SMS gateways are used, this can be assigned per domain or by country code.

Enter dialling codes for countries or domain that should be served by this Voice gateway, this can be selected from the radio button drop down menu. When dealing with country codes, for a particular SMS gateway, multiple country codes can be assigned, by comma separating.

Click Update if any changes have been made or Continue when complete, this will then save all SMS Gateway information.



To "Add" a **Mail SMS Gateway**, select Add then check the Mail SMS radial button.

This approach provides a facility to send a SMS via a SMTP server, a gateway can be setup and included in the prioritised list of gateways.

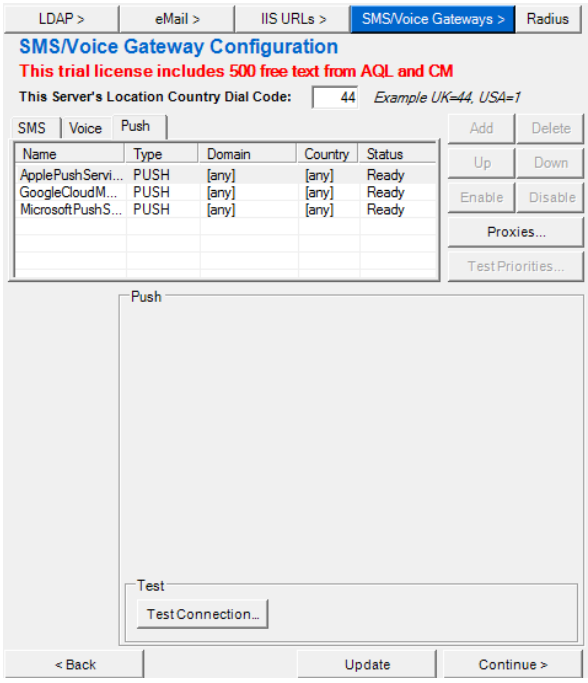
The Address format which should be #MOBILENUMBER#@atyourprovider.com

If the Telco provider allows user modifications to Subject and Body formats, please set these.

Enter dialling codes for countries or domain that should be served by this Voice gateway, this can be selected from the radio button drop down menu. When dealing with country codes, for a particular SMS gateway, multiple country codes can be assigned, by coma separating.

Click Update if any changes have been made or Continue when complete, this will then save all SMS Gateway information.

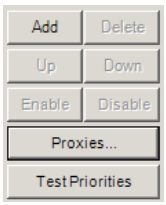
To test and diagnose a **Push Gateway**, select the Push tab in SMS/Voice Gateways.



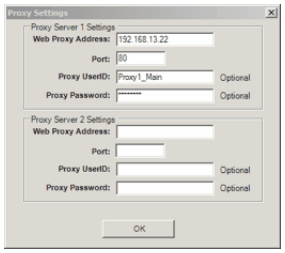
The below three push notification gateway services connections can be tested from the "Push" Tab by selecting "Test Connection"

- ApplePushService
- GoogleCloudMessaging
- MicrosoftPushService

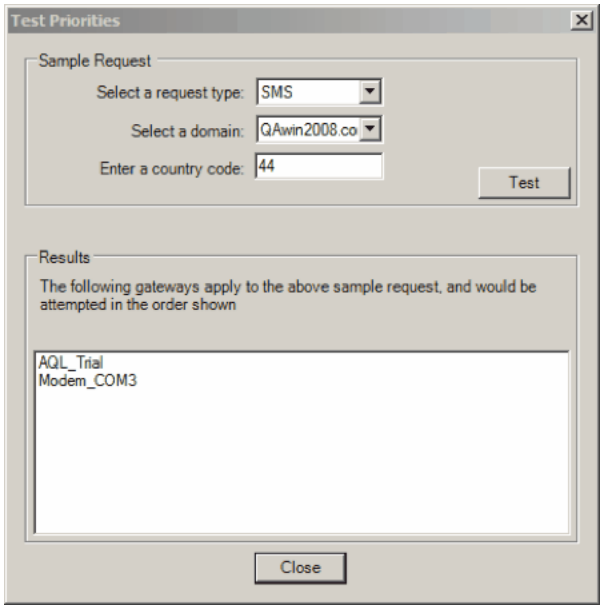
The test connection will return a status and a Trace can be displayed if required.



Proxy for Web Services
If the organisation requires the use of a Proxy Server, this must be setup using the Proxies button:



Once the properties for the proxy server have been saved, the user can select to use the Proxy when setting up the individual gateways for web services such as Web SMS or Voice.



Priorities can be tested to check that the correct priority has been applied for each gateway method.

Select "Test Priorities" button.

Select "Request type", options are SMS, VOICE

Select the Domain and finally select the country code.

Once "Test" is invoked, an output will show the priority order for the selected gateway method.

Click close when complete.

Note

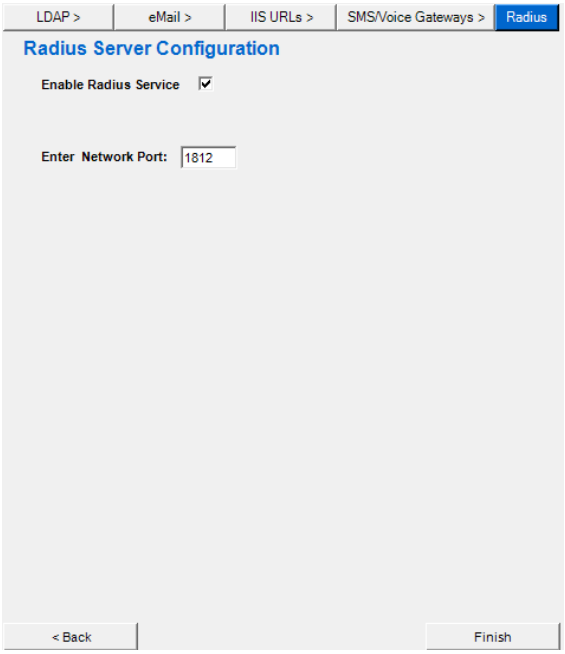
SecurEnvoy supports proxy servers - enable the checkbox and populate proxy settings

Note

The SecurEnvoy Advanced Configuration Wizard can be exited at any time after configurations have been made.

5.5 Radius Server configuration

Start/Programs/SecurEnvoy/Advanced Configuration Wizard, select Radius tab.



Radius server (if the check box is enabled) will install the Radius component to allow integration with any network access devices that can utilise the Radius protocol i.e. SSL appliance, Firewall or VPN.

To setup the Radius Service, enter port information to reflect the network environment the SecurEnvoy Security server is to operate within.

Click Save and Finish.

Note

If the SecurEnvoy Security server has multiple IP Addresses and or Network Interface Card's a RADIUS listener will be started on each individual IP address.

6 User management settings

Chapter 6

To start the adminGUI locally:
Start/Programs/SecurEnvoy/Local Security Server Administration.

Or click the desktop shortcut

To start the GUI remotely open a Microsoft web browser and enter the following **http(s):///(security_server_host_name)/secadmin**

By default the page will always open at the Local Users page.

This menu allows you to search and administer your LDAP (Directory Server) based users. You can enable users for two factor authentication; manage PIN's, manage mobile numbers and email addresses, resend passcodes and set static passcodes



In the left side window, select the domain you wish to interrogate (Only required if you have multiple domains configured). If you leave the fields blank, all of your LDAP users will be displayed.

To restrict this list enter one or more characters in First Name, Last Name or Login ID.
For example if you want to manage the user QA, enter **"Q"** in the Login ID field and press search.

A list of all users with a Login ID starting with **"Q"** will be displayed.
Select the user you want to manage and you will see the following screen options

Unmanaged / Disabled / Enabled / In Case of Emergency
The first option is to set the user's relationship with SecurEnvoy. Unmanaged means that the SecurEnvoy server has no data for this user, and the user is not consuming a license. Disabled means there is data for this user, and the user is consuming a license, but cannot authenticate. Enabled means there is data for this user, the user is consuming a license and can authenticate. ICE is only displayed if you are license for ICE users. Selecting ICE means that the user will consume an ICE license and will be able to authenticate if Emergency access mode is set.

Permanent or Temporary User
When enabling a user, the account can be setup as a permanent account or a temporary account.



If set to a temp user, then start and end dates with specific hours can be set. At the end of this time the user is automatically unmanaged.

*When a user is enabled and **Self Helpdesk or SecurPassword** is active, users are sent an enrolment message. Enable the "Enrol Secret questions checkbox" if you wish users to be able to use the Self Helpdesk or SecurPassword secret questions. (See 4 Config)*

Administrator
Select either None, Helpdesk, Config or Full administration rights for this user. This controls what remote management capabilities the user has. Full allows full access to all areas. Config allows a user to change Config, Radius settings and access the Log Viewer, but cannot see or change users. Helpdesk allows access to the Users and Log Viewer sections only. (The users they can see and change will be restricted by their domain and Helpdesk group if configured).

Pin
The PIN component can either be the existing Domain password or a traditional static numeric PIN that the user will use when authenticating. This traditional PIN can be up to 8 digits. (See 4 Config)

Mobile Number
If this user already has a mobile phone number defined in LDAP, this field will be populated. If not you MUST enter one if you want to send passcodes via SMS.

Email
This option is displayed if passcodes are allowed via email (See 4 Config)

Send Simple SMS
This option allows a RAW (simple) SMS to be sent, this caters for some countries or carriers that do not support the PDU mode of SMS.

Failed Login
Displays the number of failed logins since the last good authentication. This can be set to have between 3-10 bad authentications before the user is disabled. Once disabled no more passcodes are sent. You can reset this count back to 0 by checking Reset

One Time Code
If this mode is selected, passcodes can only be used once. This mode is the most secure as any attempt to re-use passcodes will fail. Further options include the ability to have 3 passcodes in each SMS message. Or the ability to use a "real time" delivery of the SMS message.

Day Code
This mode automates the process of changing passwords every xxx days. Day codes are reusable passcodes that are automatically changed every (x) days (Configurable see Chapter 4.0) . At a pre-defined day and time (Configurable see Chapter 4.0) the next required passcode is sent to this user's mobile phone. A valid passcode is the current or the previously sent code.

Select this option if your security requirements only need passwords to change every xx days.

Note

Day codes can be set up so that they are not sent over a weekend. Also new Day code's will only be sent if the old one has been used (Configurable see Chapter 4.0)

Pin & day codes can be used to automatically update user Microsoft Active Directory passwords (Configurable see Chapter 4.0)

Soft Token
This mode supports the use of a "Soft Token", this will be available for main stream smart phones such as Apple's iPhone, Blackberry, Android and Windows 7 phone, Windows 7, 8.1 and 10 desktop will also be supported. Please see Apple App Store, OVI, Blackberry Shop or SecurEnvoy web site for more details.
When a user is deployed, they can select to use a soft token, the phone will then scan a QR code upon the enrolment page to configure the "seed" record and activate the user for "Soft token" mode.



The GUI User tab will then show if the soft token has Push enabled, for example Push=IOS.

No additional user overhead is required. The "Soft Token" can also be re-synched by entering two following passcodes. Please see section 6.1 for more information

VOICE Token
For users who wish to use a Voice token, select this option, when the user logs on with UserID and PIN (password) they will receive a real time voice call and will then follow instructions in the voice message. At the same time their logon screen will present a OTP. To use this feature requires a version 7 IIS agent or RADIUS with challenge-response supported.

Tmp Static Code
Passcodes of up to 14 characters can be entered. The user can use this agreed static passcode multiple times for up to the number of days entered. After this time has passed, this user is automatically switched back to One Time Code's and sent their next required passcode. This mode is intended for users that have lost their mobile phone or will be out of contact from a mobile signal for a number of days.

Static Passcode
This is a reusable static passcode; it must be 6 characters long. Should only be used for testing.

Update User
Press this button to update this user with any entered/amended setting

Resend Passcode
Press this button to resend a passcode and update any changes to this user.

Note

Users being enabled will automatically be sent a passcode. When using default of "Pre Load for SMS delivery

Refresh
Press the button to cause a manual refresh of the displayed user information.

Example

Deploying Users via Admin GUI



1. Launch the SecurEnvoy admin GUI via the desktop shortcut or program link
2. Click upon search to find any user within the domain, select your user by clicking upon appropriate link 
3. Enable user, assign a mobile number (if required) and select One Time passcode, click "update" when complete
4. System will return an OK message, user will receive a passcode (default pre-load) if user set to receive a real time, no code will be sent.
5. Test logon with either Radius based connection or with IIS web Agent.

6.1 Scripting With Microsoft PowerShell V3

> **Note**
>
> **AdminAPI.dll is a 32bit assembly so you MUST start the 32bit version of PowerShell V3**

Start PowerShell V3 - Start – Accessories – Windows PowerShell - Windows PowerShell (x86)
Enter the following commands in PowerShell V3 to load the adminAPI (assumes SecurEnvoy is installed in the default location on a 64bit OS):-

```
Add-Type -Path "“C:\Program Files (x86)\SecurEnvoy\Security Server\ADMIN\adminAPI.dll")" $admin = new-object  securenvoy.admin
```

Example: list all methods and properties of AdminDll.dll

```
$admin | Get-Member
```

Example: list the existing user (DN of CN=aaa1,CN=Users,DC=dev,DC=com)

```
$admin.listuser("CN=aaa1,CN=Users,DC=dev,DC=com")
 $admin
```

Example: change an existing user (DN of CN=aaa1,CN=Users,DC=dev,DC=com) mobile number to 123456

```
$admin.listuser("CN=aaa1,CN=Users,DC=dev,DC=com")
$admin.sMobile="123456"
$admin.edituser()
```

Example: list the existing user with a UserID of aaa1 (Note required version 7.1.504 or higher)

```
$admin.listuser($admin.getdn("aaa1"))
$admin
```

Example: change an existing user (DN of CN=aaa1,CN=Users,DC=dev,DC=com) Admin to FULL

```
$admin.listuser("CN=aaa1,CN=Users,DC=dev,DC=com")
$admin.Admin = ([securenvoy.admin+eAdmin]::FULL)
$admin.edituser()
```

Example: change an existing UserID aaa1 to Disabled (Note required version 7.1.504 or higher as getdn is used)

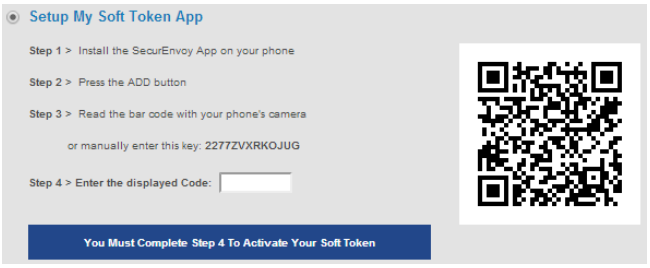
```
$admin.listuser($admin.getdn("aaa1"))
$admin.Enabled = ([securenvoy.admin+eEnabled]::DISABLED)
$admin.edituser()
```

> **Note**
>
> SecurEnvoy PowerShell sample scripts can be found in “C:\Program Files (x86)\SecurEnvoy\Security Server\SDK\admin\power shell samples”

6.2 Soft Token Support

SecurEnvoy now provides soft tokens for your phone to generate one time passcodes (OTP) for two factor authentication that can be checked by your company's SecurEnvoy server. End-users have total flexibility with zero admin or overhead costs providing a mobile security solution to suit the user.

Multiple soft tokens can be enrolled and used within the same app for multiple SecurEnvoy servers eliminating the need to carry multiple hardware tokens or install multiple soft token apps. The latest SecurEnvoy server v6 allows user far greater choice of security - either tokenless SMS two factor authentication or now with this soft token.



Users can simply log on to your company's SecurEnvoy server enrolment portal and can switch themselves to use the soft token. Then they simple scan the presented QRCode to transfer their unique seed record to the app. SecurEnvoy Soft Tokens provide an innovative and simple solution to end users requiring a flexible method of two factor tokenless authentication without fuss or administration overhead.

Support for Google Authenticator
SecurEnvoy soft tokens for your phone or desktop can be used to generate one time passcode (OTP) for two factor authentication that can be checked by your companies SecurEnvoy server or Google's cloud login.
Please note that there is decreased security upon the "Google" Soft token, as it has no copy protection at enrolment. SecurEnvoy recommend that the SecurEnvoy soft token be used where possible.

More flexibility for the User
The latest SecurEnvoy server V6 allows user far greater choice of security - either tokenless SMS two factor authentication or a soft token downloaded as an app such as this. Available free of charge to current customers from either SecurEnvoy or Google Authentication, soft tokens are suitable for most types of mobile devices i.e. iPhones, iPads, Blackberry's, Android phones, Mac and Windows operating systems including Vista and Windows 7.

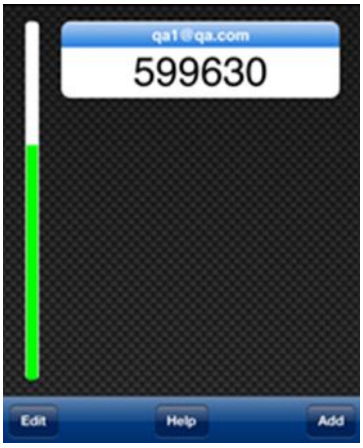


A simple process
For the organisation there is nothing they need to do. It is all down to personal preference of the end-user to choose whether they want their two factor authentication passcode sent via SMS or via their app.

The user simply:
1. Logs into their companies SecurEnvoy server's enrolment page (/secenrol) – cleverly they can authenticate themselves with their current user name and passcode
2. A barcode appears in the screen which the user scans with the camera button on their phone
3. Within seconds the user is authenticated and can start using their phone as a soft token.

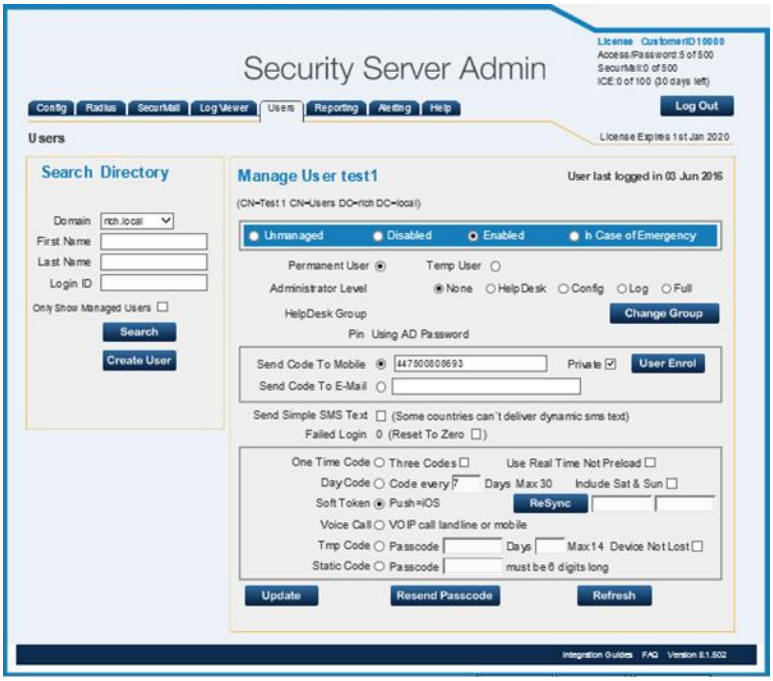
4. In the case of the P.C. Soft Token, the user only has to authenticate with the built in interface in the client. The SEED is automatically deployed with no user intervention. (Please see P.C. Soft Token manual for more information)

Mobile Phone Soft Token



P.C. Soft Token





To provide support for a "Soft Token" the selected user can be deployed via SMS or email and then at the enrolment stage, the user can opt to use a "Soft Token".

If the user is selected to only use a "Soft Token", an email address must be used to provide the enrolment details.

The "Soft Token" can also be re-synched by entering two following passcodes.

Soft Token Security

SecurEnvoy Soft token, is OATH TOTP compliant, but with additional security enhancements to the OATH specification. These are:

Secure Copy protection locks the Seed record for generating passcodes to the phone. The innovative approach allows the SecurEnvoy security server to generate the first part of the seed, the second part of the seed is generated from a "Fingerprint" on the phone when the Soft Token application is run for enrolment and each time the Soft Token application is run to generate a passcode.

Protection of the Seed records. The Seed records are dynamically generated by the Server/phone and are stored with a FIPS 140 approved encryption algorithm, this encrypted data is generated and stored at the customer premise. SecurEnvoy do not store or keep any sensitive customer seed records.

Stored DATA. All stored authentication data is generated and encrypted with AES 256-bit encryption and is kept within the customer LDAP server. SecurEnvoy supports all LDAP v2 and v3 compliant directory servers, including:

Microsoft Active Directory, Microsoft ADLDS. Novell e-Dir, Sun/Oracle One Directory server IBM and Linux Open LDAP

Security Watermarking

The SecurEnvoy Security Server deletes the used passcode and any previous passcodes from the system, thereby alleviating any replay attacks from any used or any previous unused passcodes. This process is known as "Watermarking".

Automatic Time Re-sync

When a user travels overseas, typically their phone will sync to the new country time once they have arrived at destination. The OATH compliant algorithm then derives passcodes based upon this new time, which could be many hours forward or backwards in time. SecurEnvoy has a unique approach that will handle users in this conundrum, where it allows complete unhindered World Wide travel for the user

6.3 One Swipe

One Swipe can be integrated into any existing HTML forms based logon page.

On the first login web form do the following:

Step 1 Add oneswipe.js and oneswipe.swf

- Copy oneswipe.js and oneswipe.swf from the SecurEnvoy server's install directory\ADMIN\js to the root location on your Website.
- Browse to /oneswipe.js to confirm it's URL location
- Copy oneswipe.png from the SecurEnvoy server's install directory\ADMIN\images\buttons to the root location on your Website.

Step 2 Add One-Swipe Smart Button Object

- Locate the area you want the One-Swipe button / QRCode Scan panel to go and copy and paste the following:

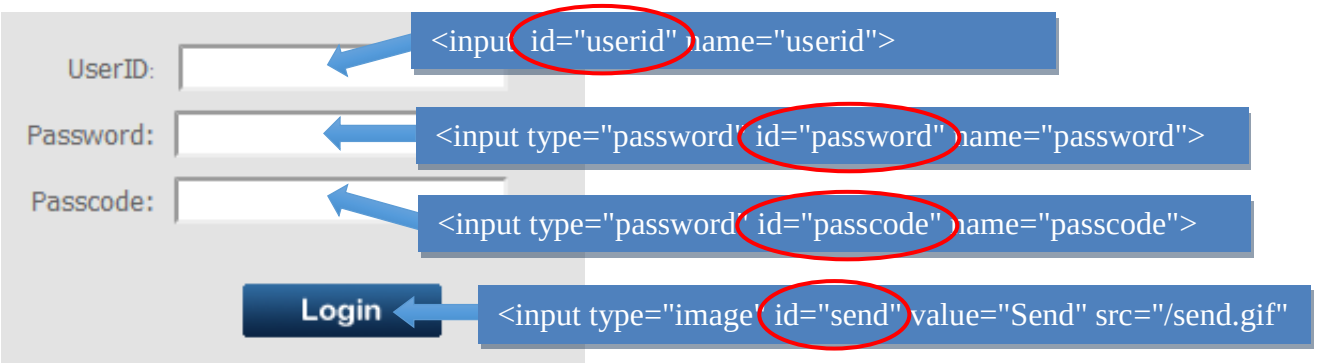
```
<img src="/oneswipe.png"
onclick="se_oneswipe_username='USER';se_oneswipe_pin='PASSWORD';se_oneswipe_passco
de='PASSCODE';se_oneswipe_submit='SEND'; (typeof se_oneswipe_click ==
'function')?se_oneswipe_click():alert('OneSwipe script not found, please verify the location of
oneswipe.js.');"/>
<div id='se_oneswipe_status'></div>
<canvas id='se_oneswipe_canvas' style='display:none'></canvas>
<div id='outdiv' style='display:none; width: 300px;'></div>
<script type='text/javascript' src='/oneswipe.js'></script>
```

Step 3 Change the blue text to the id of your input boxes

- USER, PASSWORD, PASSCODE should be changed to the ID of your input boxes (or deleted, set to '' two single quotes if not used) and SEND the id of the send/login button (add id= to your <input> tags if it's not present).

  Note you can change width: 300px in the second to last line to suit your required qrcode scan video width.

Example



If you have passcode entry on a separate login form do the following:

Step 1 Add One-Swipe Script

Locate the close body tag </body> in the passcode entry form page and add the following just before this:

```
<script type='text/javascript' src='/oneswipe.js'></script>
<script type='text/javascript'>(typeof se_oneswipe_challenge ==
'function')?se_oneswipe_challenge('', 'PASSCODE', 'SEND') :alert('OneSwipe script not found, please verify the location of oneswipe.js.')</script>
```

Step 2 Change the blue text to the id of your input boxes

- PASSCODE should be changed to the ID of your passcode input box and SEND the id of the send/login button (add id= to your <input> tags if it's not present).

Cleanup

If it's possible to change the application page presented after login, do the following:

Locate the main <body> tag and add the following after this:

```
<script type='text/javascript' src='/oneswipe.js'></script>
<script type='text/javascript'>(typeof se_oneswipe_cleanup ==
'function')?se_oneswipe_cleanup(''):alert('OneSwipe script not found, please verify the location of oneswipe.js.')</script>
```

7 Automated User Provisioning

Chapter 7

Automated User Provisioning

SecurEnvoy Security Server has the ability to provision users. This can be completed with the Deployment wizard (recommended for first time user deployments) as it allows an extremely granular approach to how users are deployed. Or with the Automatic Group Deployment within the admin GUI. This caters for ongoing deployments of users.

The Automatic Group Deployment is a new feature that allows simple ongoing provisioning of users, a dedicated group of users (only one group per domain is supported) is monitored, any user added to this group is automatically deployed with the options set in the GUI. If a user is removed from the group, they are automatically unmanaged.

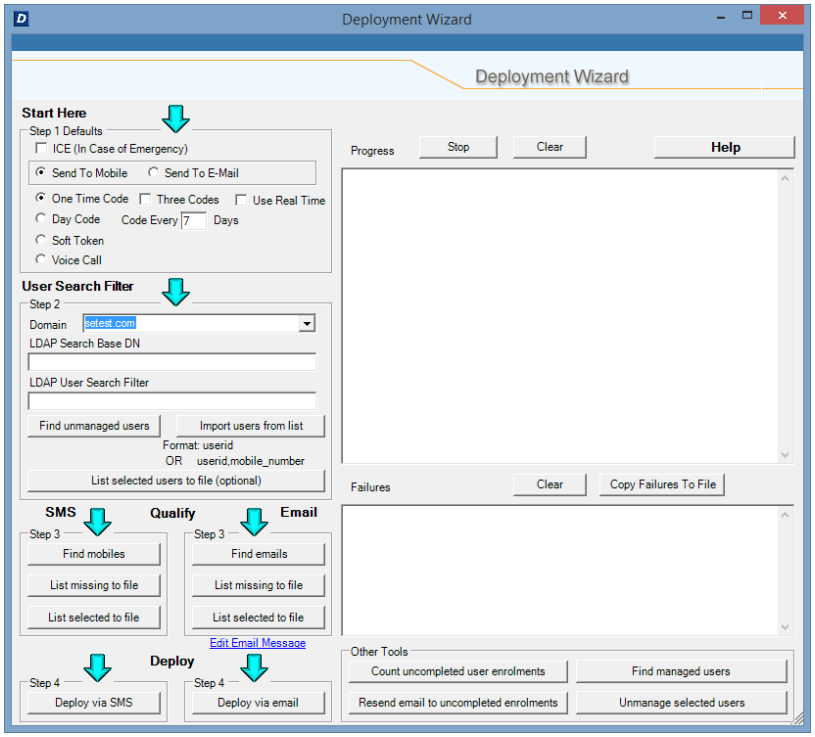
Mass deployment of users can be automated with the use of a tool called the Deployment Wizard.

The Deployment Wizard is an embedded tool that allows enterprises to deploy Passcodes to a high number of users easily. It is customisable so that passcodes can be sent via SMS to users in one seamless mechanism. The deployment wizard has the ability to allow users to Two Factor authenticate and enroll their mobile telephone number which is then stored encrypted within the Directory server (only SecurEnvoy Software or administrators will have access to these mobile numbers).

This tool can be used in one of two ways, via a graphical user interface for manually deployments or in command line mode for scripts or batch jobs to use.

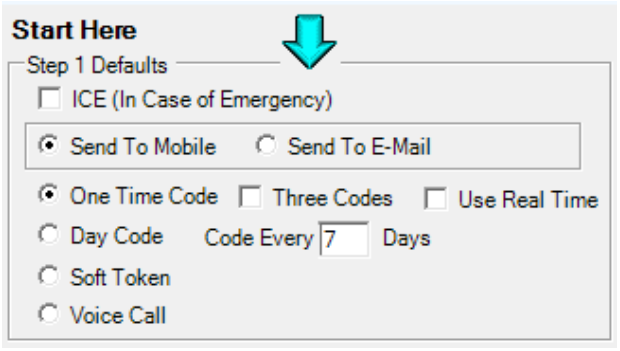
7.1 Deployment Wizard GUI

To launch this tool go to Start → Programs → SecurEnvoy → Deployment Wizard

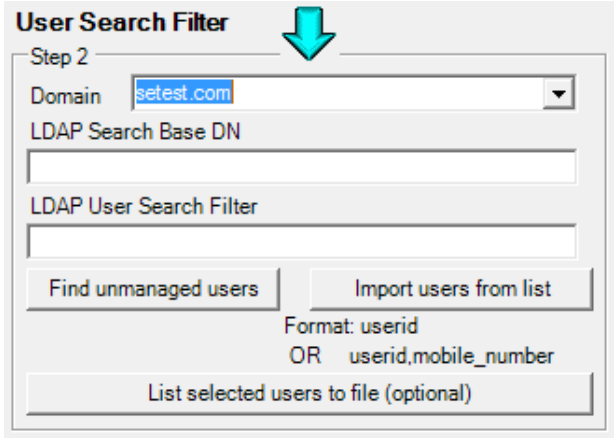


The Deployment wizard has a simple flow chart operation of usage.

The user account that runs this wizard MUST be a member of Administrators group.



Step 1
Set up the End User Deployment Defaults; select a One Time Code (default with Pre load) or Use Real Time delivery, a Day Code or an ICE user (In Case of Emergency).



Step 2
Select the Domain you wish to administer, then enter the LDAP search base or leave blank.

Common examples are:
DC=SecurEnvoy, DC=com
CN=Users, DC=SecurEnvoy, DC=com
OU=IT, OU=HQ, SecurEnvoy, DC=com

Note

If the LDAP Search Base is blank, searching with include all objects (the top of the tree)

Enter the LDAP User Search Filter information, by default the search filter will only look for user accounts that have not already been activated with SecurEnvoy.

The filter uses the following guidelines:
Expressions can use the relational operators: <, <=, =, >=, and >

Example 1	cn=a* Locate all users with "a" at the start on their common name
Example 2	lastName>=Davis Locate all users with surnames between "Davis" and "zzzzz" Compound expressions are formed with the prefix operators & and !.
Example 3	(&(lastName=Davis)) Locate Users that have the surname Davis If both operators are required then & expressions must precede ! expressions.
Example 4	(&(lastname=a*)(!(building=42)(building=43))) Locate all users with lastname starting with "a" that are not in building 42 or 43.
Example 5	memberof=CN=RAS,CN=Users,DC=dev,DC=com Locate all users that are a member of group CN=RAS,CN=Users,DC=dev,DC=com

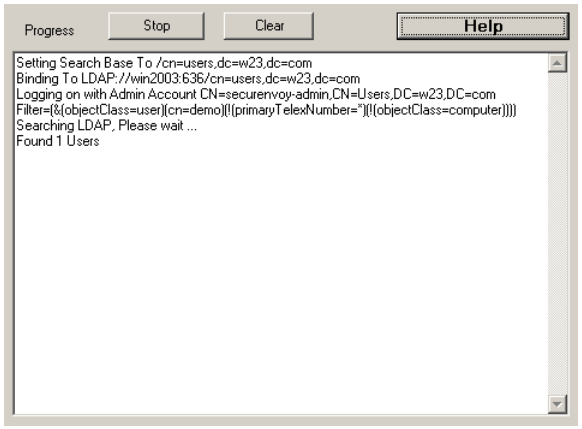
Nested Group Support
To support searching of Nested Groups an OID value is used in the filter statement. Searching for Nested Groups is only supported upon Microsoft Windows 2003 server with SP2 installed and Microsoft Windows 2008 server.
By adding the value: 1.2.840.113556.1.4.1941: to the filter statement all users who are members of selected group will be returned. Whether they are a direct member of the selected group or are members of a nested group.

Example memberof:1.2.840.113556.1.4.1941:=CN=RAS,CN=Users,DC=dev,DC=com
Locate all users that are a member of group CN=RAS,CN=Users,DC=dev,DC=com

Note

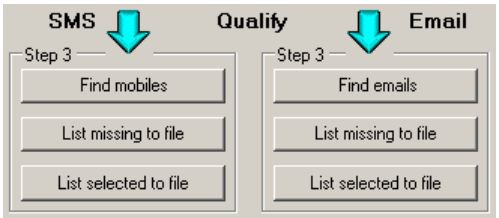
Computer accounts are ignored

Click on the "Find Unmanaged Users" button. The following screen is displayed.

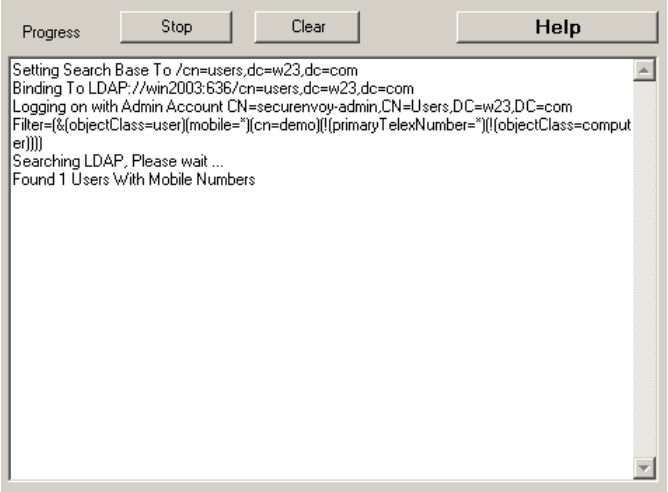


These users can then be listed to a file to allow additional checks before progressing. Click the "List selected users to a file" button shown in step 2.

Step 3



The next operation is to select which medium is to be used for the deployment, either SMS or Email. If email is chosen the SecurEnvoy server must be configured appropriately (see Section "4 Configuration"). In addition, your company SMTP server must be setup to relay from the SecurEnvoy server.



Click either "Find mobiles" or "Find emails" button. The following "progress" screen is displayed,

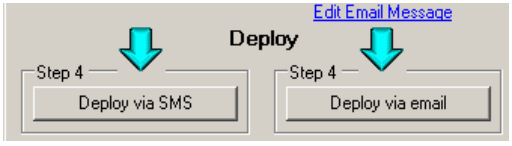
There are numerous examples of different outcomes, the following are some examples:

Example 1
100 users are listed in step2, however only 60 users have a mobile from step3.
Therefore users with missing mobile numbers can be listed by clicking "List missing to file" and then checked and updated accordingly.
The deployment can continue with only 60 users or can be restarted to allow for all 100 users to be deployed.

Example 2
100 users are listed in step2, however only 0 users have a mobile from step3.
Therefore users with missing mobile numbers can be listed by clicking "List missing to file" and then checked and updated accordingly.
Or the users with missing mobile can be deployed via email if they have a valid email address. The user will receive an email with a URL and one time passcode.

Step 4

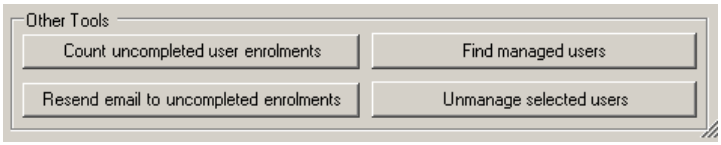
Select either "Deploy via SMS" or "Deploy via email"



If deploying via email, you have the ability to change the default message that is emailed to selected users. Click upon the "Edit email message"



The Deployment Wizard will now run. Any errors will be displayed within the "Failures" screen.



The "Other Tools" brings additional functionality to the "Deployment wizard".
It is made up of four parts, these are:

Count uncompleted user enrollments	Find and display the number of users who have part enrolled or who have not enrolled.
Resend email to uncompleted enrollments	Resend the email enrollment request to the users who have not enrolled or have part enrolled.
Find managed users	Find and display the number of users who are managed upon the system for 2FA
Unmanage selected users	Unmanage selected user

Note

When un-managing users, if you do not specify a search base or search filter than all SecurEnvoy managed users will be unmanaged!

Note

Warning: Caution should be used with this tool as hundreds of users can be unmanaged within one minute!

7.2 Deployment Wizard command line options

The following command line options are available

/auto	Must be set to use command line options
/default=one, realtime, day or ice	Optional, step 1 settings, default is one time code
/day=(number of days)	Required if /default=day, number of days between each code
/domain=(Domain name)	Optional, defaults to primary domain
/base=(DN)	Optional, location in tree to search, default top
/filter=(filter text)	Optional, the search filter, default is no filter
/deploy=sms, email	Optional, step 3&4 deployment method, default is sms
/unmanage	Optional, if set will un-manage all selected users
/hidegui	Optional, if set will hide the graphical interface
/listtofile=(file name)	Optional, if set will list selected users to this file
/findmanaged	Optional. finds managed users
/debug	Optional, if set will enable debug

It is strongly recommended that you check the setting and filter are correct with the deployment gui before using the command line.

Example 1
Deploy to all users that are a member of the Windows group RAS in the domain dev.com
deploy.exe /auto /filter=memberof=CN=RAS,CN=Users,DC=dev,DC=com /deploy=email

Example 2
Remove all managed users that leave the Windows group RAS
deploy.exe /auto /filter=!memberof=CN=RAS,CN=Users,DC=dev,DC=com /unmanage

Note: "!" means not a member of the group

Nested Group Support
To support searching of Nested Groups an OID value is used in the filter statement. Searching for Nested Groups is only supported upon Microsoft Windows 2003 server with SP2 installed and Microsoft Windows 2008 server.
By adding the value: 1.2.840.113556.1.4.1941: to the filter statement all users who are members of selected group will be returned. Whether they are a direct member of the selected group or are members of a nested group.
It is strongly recommended that you check the setting and filter are correct with the deployment gui before using the command line.

Example 3
Deploy to all users that are a member of the Windows group RAS in the domain dev.com

deploy.exe /auto /filter=memberof:1.2.840.113556.1.4.1941:=CN=RAS,CN=Users,DC=dev,DC=com /deploy=email

Example 4
Remove all managed users that leave the Windows group RAS

deploy.exe /auto /filter=!memberof:1.2.840.113556.1.4.1941:=CN=RAS,CN=Users,DC=dev,DC=com /unmanage

Note: "!" means not a member of the group

Group Deployment Multi Domain Templates

Version 8.1 has the ability to customize the Group Deployment enrolment email template per domain. This allows for one custom message to be sent to new users of an internal customers and another to external customers or third party vendors.

If a new user in a secondary domain is deployed via Group Deploy, the mail or sms templates can be read from DATA\MAILTEMPLATE_name_of_domain or DATA\SMSTEMPLATE_name_of_domain.

- Copy the directory DATA\MAILTEMPLATE and all files to DATA\MAILTEMPLATE_name_of_your_domain and customize templates as required.

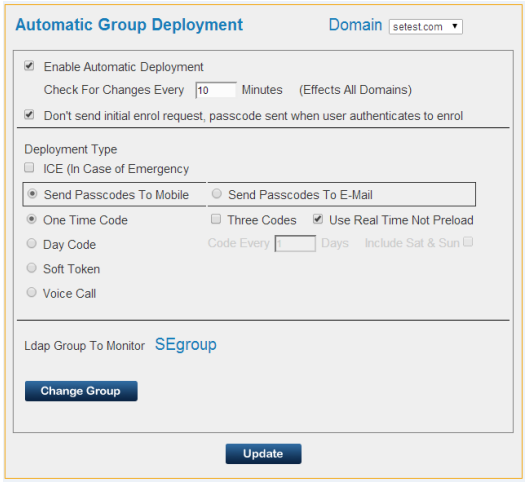
- Copy the directory DATA\SMSTEMPLATE and all files to DATA\SMSTEMPLATE_name_of_your_domain and customize templates as required. This is optional.

7.3 Automatic Group Deployment

The Automatic Group Deployment is an embedded feature that allows simple ongoing provisioning of users, a dedicated group of users (only one group per domain is supported) is monitored, any user added to this group is automatically deployed with the options set in the GUI. If a user is removed from the group, they are automatically unmanaged.

The following options are able to be set:

Enable Automatic Deployment



Enables or disables the automatic deployment option, an additional setting allows a time in (n) minutes to be set. This is how often the Automatic Deployment should check for users being added or removed from a group.

Deployment Type

ICE (In Case of Emergency) for emergency users, business continuity, disaster recovery.

Send Passcodes to Mobile / Email

Example - User will stay explicit to the mode of deployment, if deployed with a passcode to mobile, they will always receive a passcode via SMS. As long as the mobile attribute is populated. If not the system will check and then deploy the user by email, the user will then follow the enrolment instructions in the email to update their own mobile number into SecurEnvoy. If user deployed via email, they will always stay in this mode.

One Time Code / Three Codes / Real time - Select users to have a Onetime passcode in "Pre-Load", "Three Codes" mode or use "Real time delivery".

Soft Token - Users are deployed with an enrolment message to setup their soft token.

VOICE Token - Users are deployed with an enrolment message to setup their VOICE token.

Day Code - Users are deployed with a Day Code, the code refresh in (n) days can be set, this is global setting for all deployed users

NOTE: Mobile or email attribute must be populated.

Note

If a group is declared in the Automatic Group deployment option, the user will be enabled and provisioned or unmanaged depending on whether they are a member of the declared group.
If "Allow any group" is selected, all users in the domain will only be provisioned. Caution this could cause a high number of user to be provisioned.

8 Configuring RADIUS clients

Chapter 8

Use this window to define your RADIUS client's IP Address, shared secret, default domain and any dictionary profile setting

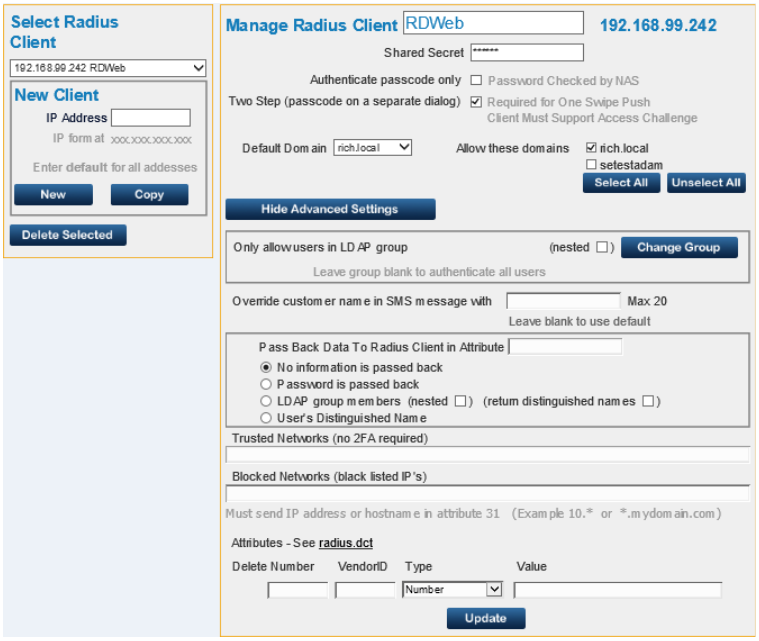
Supported RADIUS functions:
Basic Password Authentication via the attribute "User-Password"
Profiles that apply to all users

Unsupported RADIUS functions:
Accounting
Profiles that map to one or more users but not all of them
MSChapV2 authentication

Note

If user profiles or accounting are required it is recommended that an additional third party Radius server such as funk's Steel Belt RADIUS or Cisco's ACS RADIUS server is used. See http://www.funk.com/ or http://www.cisco.com . To authenticate users via Steel Belt or Cisco's Proxy Radius, this will pass RADIUS authentication requests to SecurEnvoys RADIUS Server and allow you to manage accounting and user profiles within Steel Belt or Cisco ACS.

To Configure Radius Clients select the Radius Tab



NAS IP Address
This is the IP address of the RADIUS client that will be sending RADIUS authentication requests. It must be entered in the format xxx.xxx.xxx.xxx or default

If "default" is used as the IP Address, all unknown Radius client IP Addresses will use these settings.

To create a new Radius client configuration select New and enter the required details. To copy an existing Radius Client, select the configuration to copy and click on Copy. To delete a Radius Client, select the Client to delete and click on Delete.

Note

*If the security server has more than one network interface card, **SecurEnvoys** Radius service will start a listener on each of them*

Managed Shared Secret
This is a secret (password) that must be entered exactly the same at both the RADIUS client end and in this entry box.
If this secret is not entered the same at both ends the **SecurEnvoy** Radius server will ignore incoming network packet.

Note

SecurEnvoy supports the use of ASCII 127 for the shared secret, extended characters (ASCII 128) like £ signs are not supported. Also note that some RADIUS clients have limitations on the length of the shared secret.

Authenticate Passcode Only
If this check box is selected then only the 6 digit passcode will be authenticated. This option should only be used if the Radius client has already authenticated a password or PIN and only requires the second factor to be checked by this server.

Passcode prompt is on a separate dialogue box
This setting will instruct the SecurEnvoy Radius server to challenge response all authentications. The user will then login with UserID and PIN/Password, after which they will then be challenged for the passcode, irrelevant of mode in operation – Pre Load OTP, Daycode, TMP code.

Note

This option will only work if "Real time passcodes" are enabled within the section 4 Configuration

Default Domain
If the UserID does not include a domain name then the selected domain name will be used. Alternatively you can select "search" SecurEnvoy will then process each valid configured domain until a match is found upon the UserID. This works well in environments that have network equipment that removes the domain portion of the UPN or domain NetBIOS logon

Note

Selecting "Search" as the default domain MUST only be used for up to 5 domains as each domain may take up to 2 seconds to reply. The UserID must be unique across all domains being searched

Allow These Domains
If this is set then users can only authenticate to the selected domain name(s). This is ideal for managed service providers that do not wish customers from one domain to cross over to other customer domains.



Only Allow Users that are in the LDAP group
SecurEnvoy can only authenticate users if they are a member of a specific LDAP group.

Click the "Change Group" button to select the desired group from the available LDAP domain groups.

Settings allow for a single selected LDAP group or any LDAP group membership.

Override Customer name in SMS message
Enter the text that you wish to supply within the passcode message. Leave blank for default message.

Passback data to Radius client in Attribute
Configure Single sign and group membership via RADIUS attribute 25 (Default port); please see your network vendor documentation for use of this RADIUS attribute.

Settings are:
No information passed back
Password is passed back
LDAP group members are passed back, this can be the FQDN or the short NetBIOS naming convention.
User UPN can be passed back, this allows user to application mapping.

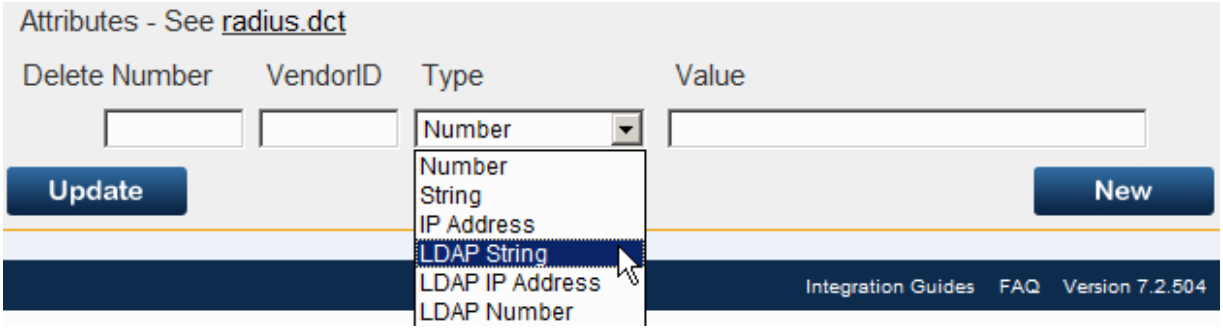
Trusted networks
Declare trusted networks that do not require a 2FA logon experience, Space separated IP's (Example 10.* 192.168.1.1) NAS must send IP address in attribute 31.

Blocked networks
Declare blocked networks, that are not allowed to authenticate against the SecurEnvoy RADIUS server, this could be due to a brute force attack or DOS attack against RADIUS. Any request from these networks is dropped and not processed. Space separated IP's (Example 10.* 192.168.1.1) NAS must send IP address in attribute 31.

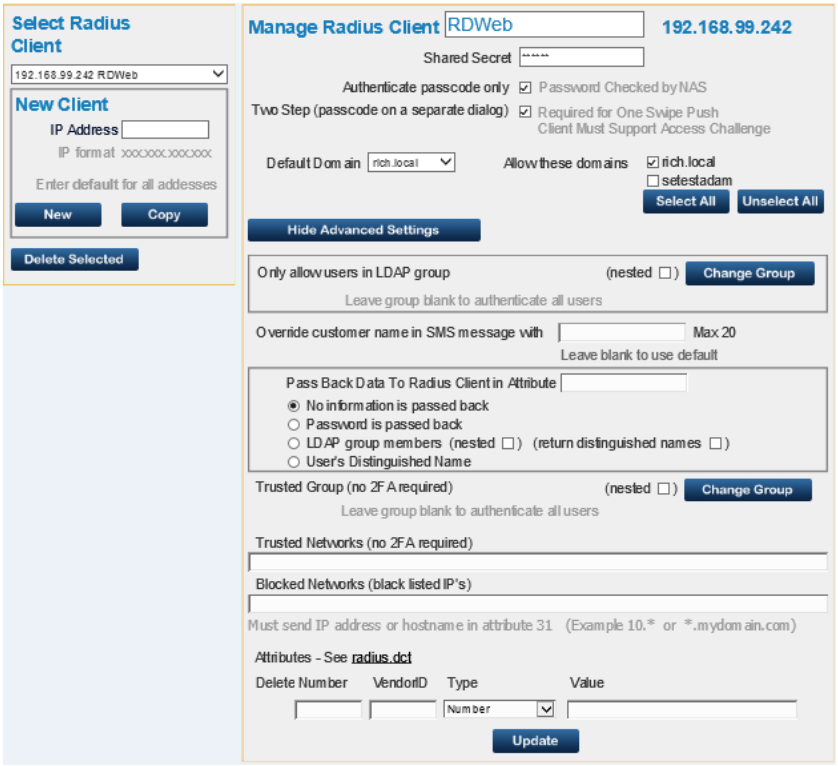
Attributes (Not displayed by default)
To Display Attribute setting, select Config from the menu and Check "Radius Attributes" in the Admin GUI section.
The RADIUS standard uses lists of agreed settings called Dictionary's; SecurEnvoy is installed with a list of the main dictionaries. This can be viewed by selecting the link **radius.dct.**
The main file is RADIUS.dct. Also included are most manufacturers published extensions.
See the following examples for details of how to enter Attributes.

There are a number of options that can be used. From the traditional response of a:
Number
String
Or IP Address

To a completely dynamic read of DATA in any LDAP attribute. Support is included for:
LDAP String
LDAP IP Address
And LDAP Number



Trusted Group (no 2FA required)



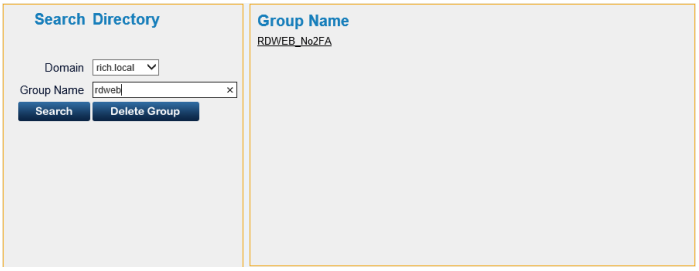
Version 8.1 now has the ability to trust AD groups per Radius Client. This means that members of the selected AD group will not require 2FA when authenticating to a Radius Client with trusted groups enabled.

Trusted Groups also supports nested groups but selecting nested groups may reduce performance. The Trusted Groups option is not available in the Radius tab by default. To enable this option, ensure that "Authenticate passcode only" is ticked and click on Update

If Oneswipe Push is enabled, then the Radius Client timeout should be set to 29 seconds.

To add a Trusted Group click on Change Group, search for the required group by entering the first few characters of the AD group's name and then select it.

If required, AD groups can also be deleted from Trusted Groups by selecting them and clicking on the Delete Group button.



Example 1

You wish to add the standard Attribute "Framed-Protocol" and set it to "PPP"
For 32 bit installations:
Open the file Program Files\SecurEnvoy\Security Server\Data\RADIUS\DICT\RADIUS.dct
For 64 bit installations:
Open the file Program Files(x86)\SecurEnvoy\Security Server\Data\RADIUS\DICT\RADIUS.dct

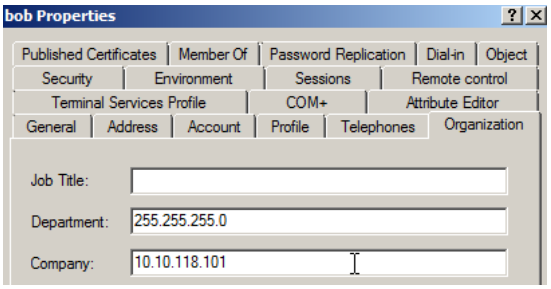
Locate the line that contains Framed-Protocol - This line defines the Number (7) and Type (number)
Below this line are the values that can be set, PPP has a VALUE of 1
In the GUI admin window enter the following:

At the column Number enter 7 Ignore the Column VendorID
At the column Type select Number
At the column Value enter 1

Example 2

You wish to add a Cisco vendor Attribute "3076-26" to define an IP address and Netmask per user, in addition you also require to provide a string for additional authorisation parameters.

Select the RADIUS profile you wish to edit.
At the column Number enter 8 (IP Address), enter 3076-26 in Column VendorID.



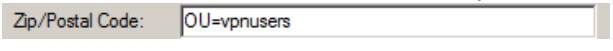
At the column Type select LDAP IP Address.

At the column Value enter the LDAP attribute that contains this information. In this example LDAP attribute "company" was used.

Complete this task for the netmask setting

At the column Number enter 9 (IP Address), enter 3076-26 in Column VendorID.
At the column Type select LDAP IP Address.
At the column Value enter the LDAP attribute that contains this information. In this example LDAP attribute "department" was used.

Finally add settings for the "string" settings
At the column Number enter 25 (string), leave Column VendorID blank.
At the column Type select LDAP string.
At the column Value enter the LDAP attribute that contains this information. In this example LDAP attribute "PostalCode" was used.



The RADIUS response is shown as to what is returned to the Cisco device. These settings are all user specific.

[8] Framed-IP-Address	6	IETF	ip addr	10.10.118.101
[9] Framed-IP-Netmask	6	IETF	ip addr	255.255.255.0
[25] Class	13	IETF	string	OU=vpnusers

Example 3 Configuration of Routing and Remote Access - RRAS

Windows 2003 server SP1 - IPSec VPN

1. Install Routing and remote access service if not already installed
2. Launch Routing and remote access MMC, select server and click "configure and enable Routing and remote access"
3. Follow wizard and setup for VPN access, set up for IPSec VPN. Start RRAS service
4. Select the server within RRAS MMC, go to properties
5. Select Security, select Radius for Authentication provider, select configure. Populate with Radius information. Timeout should at least be 10 seconds.
6. Select Authentication methods, deselect all, and only enable PAP protocol.
7. Restart RRAS service.

Client Windows XP SP2

1. Create new network connection wizard, select VPN
2. Go to properties, select Security tab, select Advanced, and go to settings.
3. Change Data encryption to "Optional encryption", and only select PAP for protocols.
4. Enter Pre shared key for IPSec settings.

Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can utilise the existing Microsoft password as the PIN. This allows the users to only remember their Domain password. SecurEnvoy supplies the second factor of authentication, a dynamic one time passcode (OTP) which is sent to the user's mobile phone.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click "Config" Select Windows – Microsoft Password is the PIN under PIN Management

This will now use the users existing password as the PIN. Click "Update" to confirm the changes

Click the "Radius" Button

Enter IP address and Shared secret for each Server that has Routing and Remote Access installed and wishes to use SecurEnvoy Two-Factor authentication.

Click "Update" to confirm settings.

Click "Logout" when finished. This will log out of the Administrative session.



Test Logon

Enter the UserID in the Username field

Enter password and passcode in the password field.

E.g. P4ssw0rd678123

9 Migration

Chapter 9

SecurEnvoy has the ability to provde a "Migration" path from exitsing authenication methods.

Two types of "Migration" are supported, existing passwords and existing third party tokens.

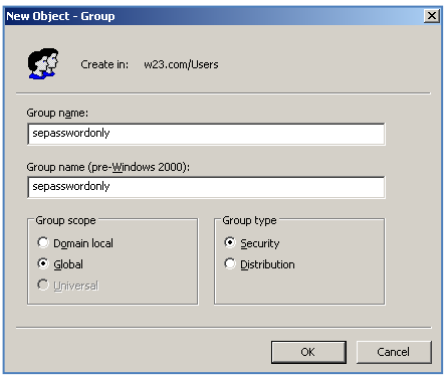
Migration of Passwords

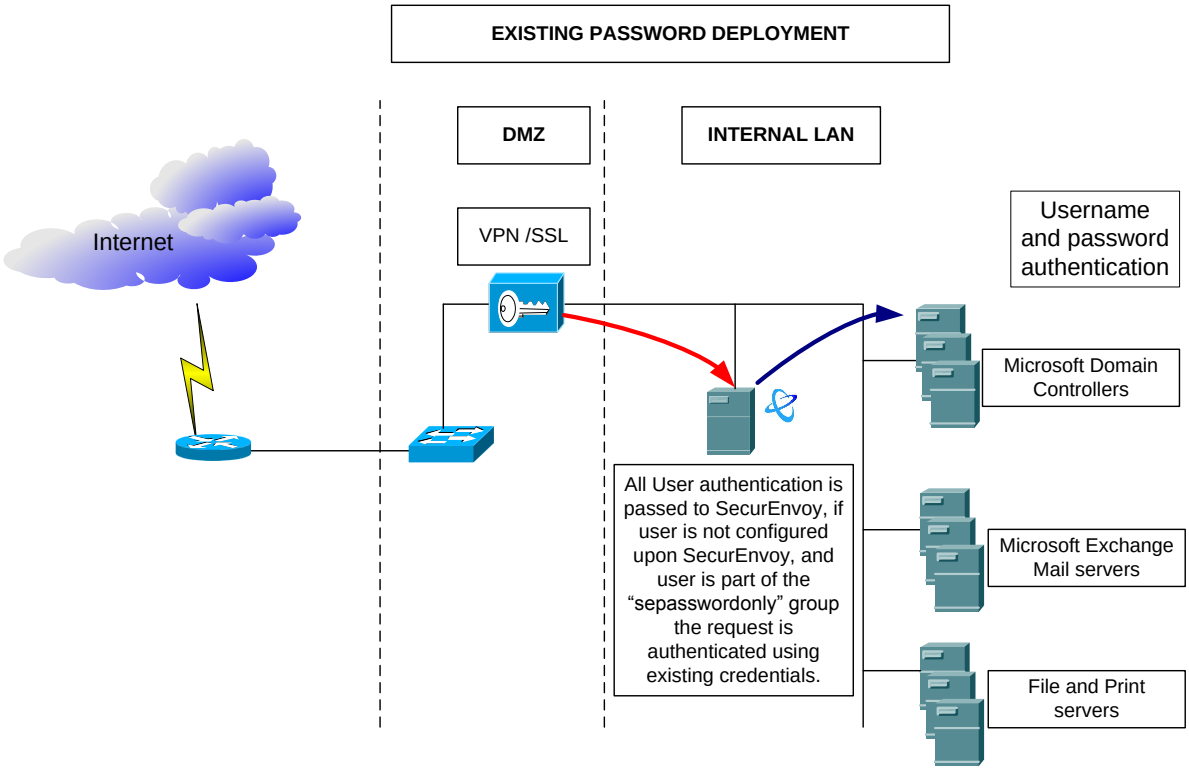
To support user's with existing passwords, the VPN/SSL device is reconfigured to pass all authentication requests to SecurEnvoy server. If the user is not configured upon SecurEnvoy and is a member of the "sepasswordonly" group, the user credentials are checked against the existing LDAP account.
Supported LDAP types are (Microsoft Active Directory, Novell e-Dir, Sun Directory server, Linux Open LDAP)

A group called sepasswordonly must be created upon the directory server.

Users who are required to authenticate with a username and password must be added to the sepasswordonly group.

See section 4 forconfiguration settings

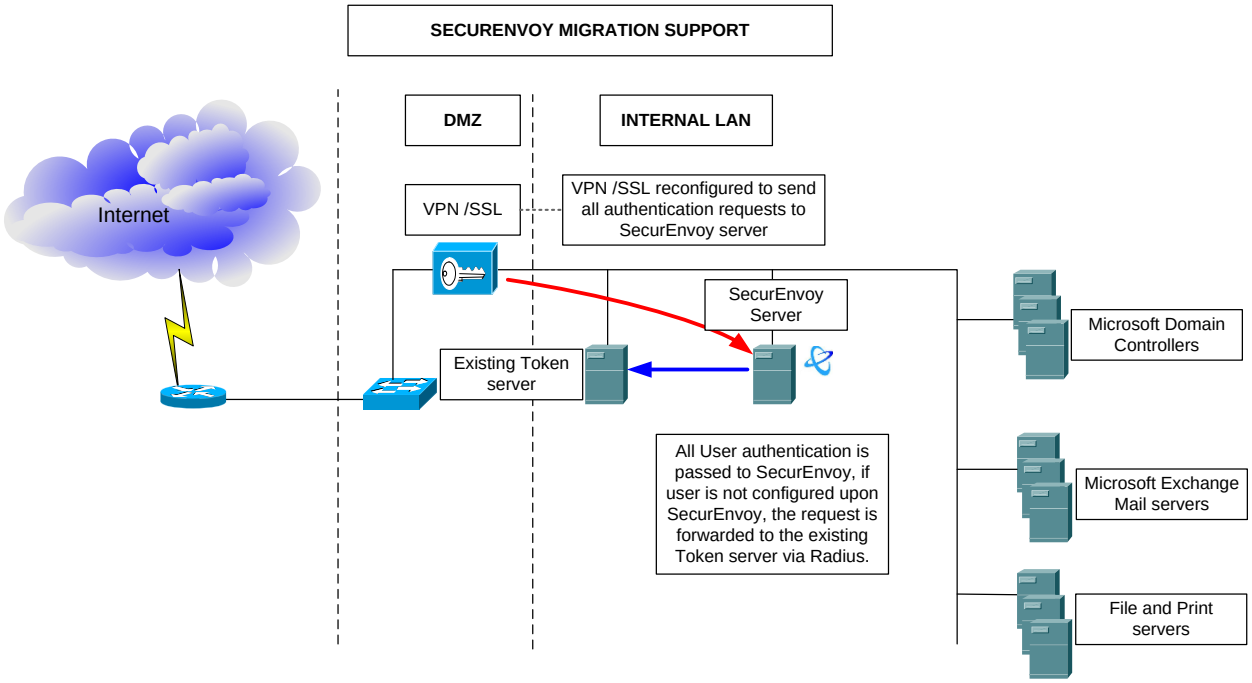




Migration of existing third party Token Server

To support user's with existing third party Token server, the VPN/SSL device is reconfigured to pass all authentication requests to SecurEnvoy server. If the user is not configured upon SecurEnvoy, the request will then be forwarded to the configured "Token server". Only the Radius protocol is supported for existing third party token server.

Supported Token servers: any Token server that uses the Radius protocol for authentication.



See section 4 for configuration settings

10 Resilience

Chapter 10

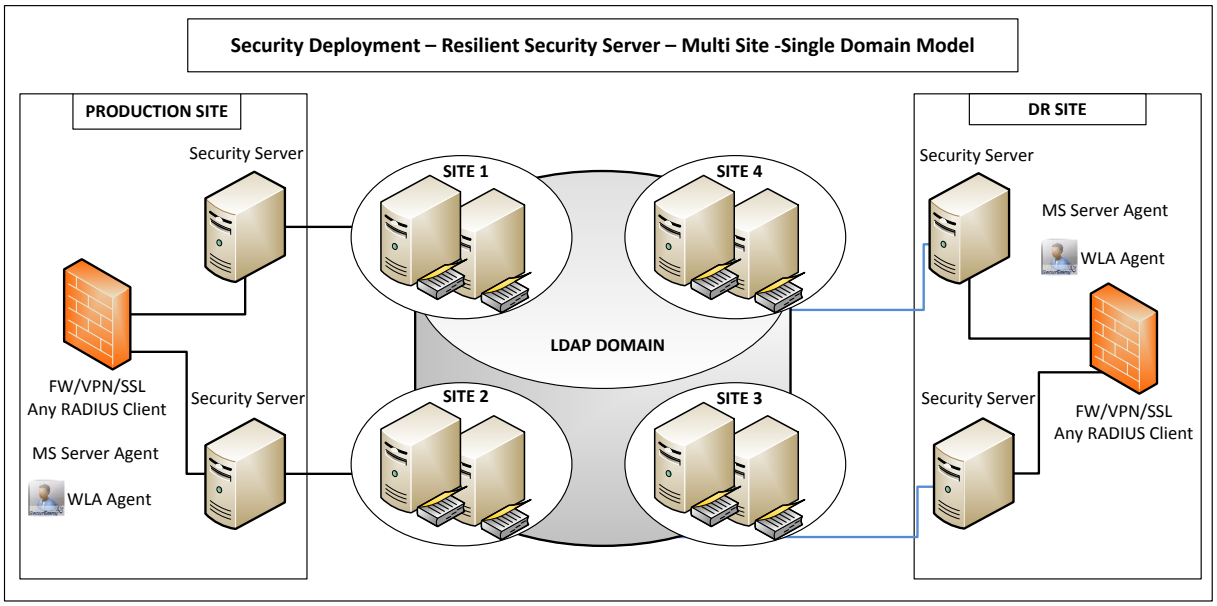
SecurAccess

Each SecurAccess Agent or Radius Client can be configured for up to 2 Security Servers

Each Security Server can be configured for up to two LDAP servers

The following diagram illustrates a typical resilient design with two VPN Servers (Radius Clients)

For most large user deployments, only 2 servers are required. Additional servers are only required where limited network connectivity exists to the Radius Client.



SMS Gateway Resilience

When two security servers are installed with one SMS phone gateway modem or one SMS Web Gateway on each server, the following failover logic occurs:

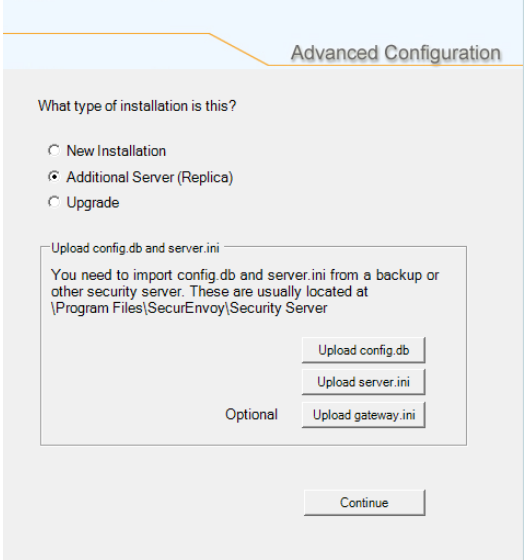
If one of the web gateways or phone modem fails to connect, this server will failover incoming authentication requests to the next configured security server and it's working SMS gateway. The failed SMS gateway will be polled every 60 seconds to see if the fault has cleared. Once the fault has been resolved, the gateway will automatically detect that the web or modem is now working and allow authentication requests.

If the Phone SMS gateway and Web SMS gateway are both installed on the same security server then priority can be given to the phone or web gateways and if one of them fails the other gateway service will automatically become enabled.

Setting up Multiple Security Servers

Multiple security servers must share the same security encryption key (config.db)

To Install additional security servers do the following:-



1 Run the Security Servers setup.exe install program on the next required server,

1.1 Select "Additional server"

2 Press the "Upload config.db" button and browse to the config.db file on the first security server you installed, default location for this file is for

32 bit installations:
C:\Program Files\SecurEnvoy\SecurityServer\
And 64 bit installations
C:\Program Files(x86)\SecurEnvoy\SecurityServer\

Carry out the same task for the "server.ini" file.

Note

Each SecurEnvoy security server will use a local.ini file and a server.ini file, this has been created to assist deployments, where multiple SecurEnvoy servers exist.

The local.ini file stores data regarding local configuration details
The server.ini file stores data that are global configuration details

3 Start the Admin GUI on this new server and select the menu "config".

Match any changes made so that all servers have the same configuration settings.

Additional servers MUST share the same SecurEnvoy administration account for each domain they manage

The Batch server start times must be set to start at the same time allowing for any local time zone changes.
Multiple batch server processes must run within 10 minutes of each other or multiple day codes may be sent to end users.

Note

Additional servers MUST share the same SecurEnvoy administration account for each domain they manage

10.1 Resilience (Batch Server Logic)

SecurEnvoy Batch Server

This Windows service is only required for SecurAccess, SecurMail Product and SecurPassword.
It handles users set to TMP MODE and DAY MODE and carries out an absolute license count check.

Every 24 hours at a defined time, it checks all users in LDAP and if required sends them the next required passcode. In the case of TMP MODE, it counts down the number of days this user is allowed to be in TMP MODE. When zero is reached, the user is automatically switched back to ONE TIME CODE and sent a new passcode.

The Batch Server can also delete any Emails that have resided upon the SecurMail server. If the email message is older than defined limit, it will be deleted. (Controlled in x days)

Multiple Batch Server Logic

Multiple security servers that have more than one batch server running has additional logic built into the operation. It works in the following description. Each server first checks the last run date from the LDAP attribute PrimaryTelexNumber for the Admin user's account.

If a server has not run in the last **15 minutes** it then requests a lock by generating a unique 8 digit lock code and writing it to the above LDAP attribute for the Admin user. It then waits a 30 second period to allow Active Directory (LDAP) to replicate completely. If the same lock code is read back then the batch server runs, if it reads a different lock code than one of the other servers has also requested a lock and will run instead.

Multiple Batch Server Pre-requisites

All Batch Server's that manage the same domain and search base of users **MUST** have the same run time and period set.
The clock's time of these servers should not be more that 10 minutes adrift between them.

10.2 Resilience (RADIUS)

SecurEnvoy Radius Server

To provide resilience for RADIUS clients, the NAS folder can be copied from the first SecurEnvoy server to each subsequent SecurEnvoy server that is deployed. Make sure that each RADIUS client is updated with the correct IP address of each SecurEnvoy replica server.

The NAS folder can be located at the following location:

For 32 bit installations:
Open the file Program Files\SecurEnvoy\Security Server\Data\RADIUS\DICT\RADIUS\NAS
For 64 bit installations:
Open the file Program Files(x86)\SecurEnvoy\Security Server\Data\RADIUS\DICT\RADIUS\NAS

10.3 Resilience (Server.ini)

Server.ini - Global settings

If any configuration changes are made upon one of the SecurEnvoy servers, it may be necessary that these changes are replicated around each of the SecurEnvoy servers that are deployed.

One example is if a new domain was added into the configuration.

As the server.ini file only holds global information, this allows the file to be copied to each SecurEnvoy server.

> **Note**
>
> *All SecurEnvoy servers should be at the same software revision level*

The server.ini file is located at:

For 32 bit installations:
Open the file Program Files\SecurEnvoy\Security Server\
For 64 bit installations:
Open the file Program Files(x86)\SecurEnvoy\Security Server\

The configuration changes are automatically detected and used.

Automated server.ini sync between SecurEnvoy servers

The software now has the functionality to dynamically update the server.ini file to all SecurEnvoy Security servers if any changes are made to it. To enable this functionality the below line needs to be set to true in the server.ini (C:\Program Files (x86)\SecurEnvoy\Security Server) file. By default this setting is configured to False.

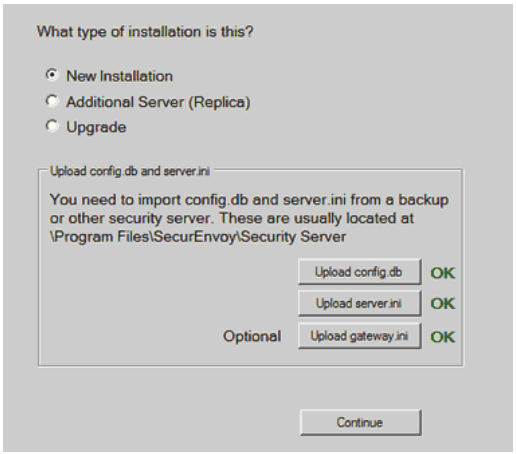
```
# Automaticlly copy server.ini to all replica servers, Version above MUST
be the same on all servers (True or False)
# Make sure this server can browser all replicas
(http://my_replica_host_name/secrep should download server.ini)
SyncServerINI=True
```

Once this setting has been updated on the master server, the server.ini needs to be manually copied to each SecurEnvoy server one last time so that each server has this setting configured to True. All servers must have the same version of the software installed.

Once configured, the server.ini will update across all servers regardless of whether the changes are made on the master or a replica.

10.4 Resilience (Gateway.ini)

SecurEnvoy SMS/Voice Gateway



To provide resilience for SMS/Voice Gateway providers.

This can be easily added by copying the gateway.ini file from one SecurEnvoy server to another.

The gateway.ini file exists in the following paths:
For 32 bit installations:
Open the file Program Files\SecurEnvoy\Security Server\gateway.ini

For 64 bit installations:
Open the file Program Files(x86)\SecurEnvoy\Security Server\gateway.ini

Recommend that the SecurEnvoy Web SMS Gateways service is restarted
If a replica server or upgrade is carried out, the gateway.ini file can be added at time of installation, see diagram.

11 Web SMS Templates

Chapter 11

A web template allows configuration to any third party web SMS provider, all that is required is the web SMS provider accepts an http(s) POST or GET statement or an XML POST.

Requirements

The selected third party gateway MUST support https as encrypted passcode SMS messages sent across the internet is mandatory.
In addition for an enhanced end user experience, message overwrite (Protocol ID 61-67) should also be supported. Message overwrite allows new passcode messages to overwrite old SMS messages from the same senders address. This feature removes the burden of deleting used SMS passcode messages from the end users phone.

File Location

Main control file MUST end in _control.txt and should be located in Data\WEBSMSTEMPLATE

Control File Selection

The registry key "HKLM\Software\SecurEnvoy\WebSMS Gateway\TemplateFile" should be set to the file name of the control file

Control File Settings

Init File (POST Data)
The following dynamic strings will be replaced:

#USERID#	UserID for Authenticating With Gateway
#PASSWORD#	Password for Authenticating With Gateway

Send File (POST Data)
The following dynamic strings will be replaced:

#USERID#	UserID for Authenticating With Gateway
#PASSWORD#	Password for Authenticating With Gateway
#MOBILENUMBER#	Mobile Number
#SOURCEADDRESS#	Source Address
#MESSAGE#	SMS Message to Send
#10DIGITID#	Unique 10 Digit Code
#OVERWRITE#	Overwrite String For Setting Overwrite Last Message
#FLASH#	Flash String to flash message on screen (Real Time Passcodes Only)

InitURI
The following dynamic strings will be replaced:

#USERID#	UserID for Authenticating With Gateway
#PASSWORD#	Password for Authenticating With Gateway

SendURI
The following dynamic strings will be replaced:

#USERID#	UserID for Authenticating With Gateway
#PASSWORD#	Password for Authenticating With Gateway
#MOBILENUMBER#	Mobile Number
#SOURCEADDRESS#	Source Address
#MESSAGE#	SMS Message to Send
#10DIGITID#	Unique 10 Digit Code
#OVERWRITE#	Overwrite String For Setting Overwrite Last Message

Certificate Enrolment

1. create a policy request file caller c:\certpol.txt and add the following:-
   [NewRequest]
   Subject="cn=SecurEnvoy,o=SecurEnvoy,ou=SecurEnvoy"
   RequestType=pkcs10
   Exportable=TRUE

2. Create the pkcs#10 certificate request in a cmd window
   certreq –v –New c:\certpol.txt c:\certreq.txt

3. After third party SMS Gateway CA have signed this request import the user certificate and root certificate

4. Move the cert and private key to the local machine store as follows:-

   a. With ie6 export cert and private key to cert.pfx
   b. Start mmc with certificate plug-in for local machine
   c. Right click "personal/certificates" "All Tasks/Imports"
   d. Import cert.pfx

5. With mmc certificate plug-in, select this cert and export the cert without the private key:
   For 32 bit installations:
   c:\program files\SecurEnvoy\Security Server\DATA\WEBSMSTEMPLATE\clientcert.cer
   For 64 bit installations:
   c:\program files(x86)\SecurEnvoy\Security Server\DATA\WEBSMSTEMPLATE\clientcert.cer

Message Text Encoding

SMS messages can be encoded before they are replaced in the #MESSAGE# string
Leave blank for no encoding

URL
Characters are URL encoded with UTF8

HexIA5
Characters are converted to a 2 digit hex Ascii code and the follows are converted to IA5
@ = 00
$ = 02
LineFeed = 0A
CR = 0D

XMLGSM
The following characters are converted then the message is url encoded

` = '
" = "
& = &
> = >
< = <
LineFeed =

CR =

XMLONLY
The following characters are converted (not url encoded)

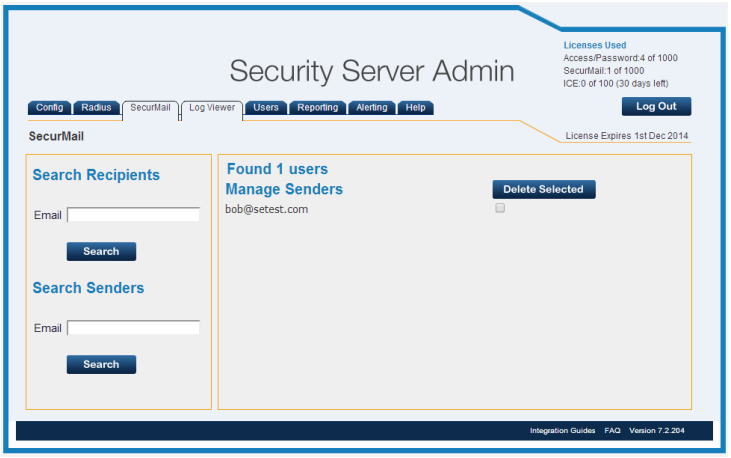
` = '
" = "
& = &
> = >
< = <
LineFeed =

Document Encoding
Post document data can be encoded, valid options (URL)

URL
Characters are URL encoded with ISO-8859-1

12 SecurMail Administration

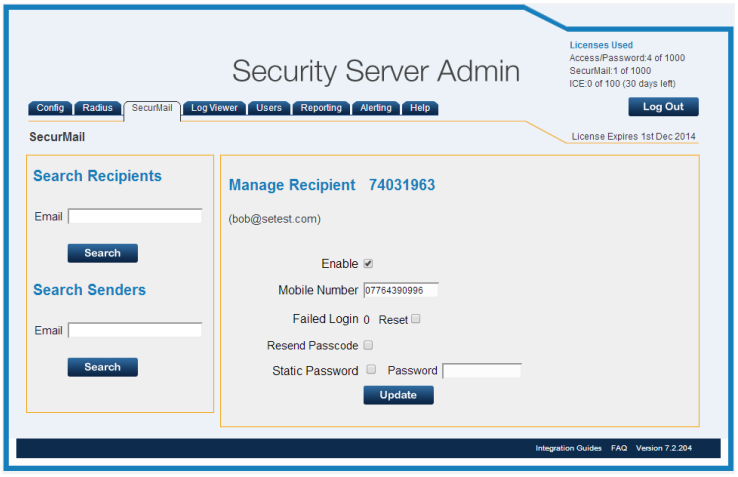
Chapter 12



Launch the SecurEnvoy Admin GUI and select the SecurMail tab. The following screen is displayed.

Searching for "Senders" will display all users who are configured and have sent a SecurMail. Users that are displayed after searching can be deleted and removed from the system.

Searching for "Recipients" will display users who have been sent a SecurMail in "Auto Enrol and Store" mode.



Clicking a Recipient search result will display their associated mailbox and provide additional management options –

- The Mailbox can be enabled and disabled
- The mobile number can be updated
- The Failed login can be reset, as after 10 consecutive bad authentications the mailbox is locked.
- The passcode can be resent via SMS
- A static password can be applied to the mailbox

12.1 SecurMail Virus Checking Integration

Email send via the "Send Secure" button in Outlook are uploaded to the Security Server and stored in an encrypted state. Virus software deployed on the security server would not be able to check these messages as there are encrypted so any virus checking must be integrated into the security server.

If virus checking is enabled, the message subject, body and any attachments are submitted to a third party virus scanning engine after they are uploaded and before they are encrypted.

If a virus is found a warning message is displayed at the Outlook agent and sending this email is aborted.

SecurMail can integrate with any third party virus software that supports a command line interface and will delete infected files.

The following products have been tested:

Symantec Scan Engine V4.30
Trend Micro Office Scan Corporate Edition 6.5

Integration procedure

Step 1 Install the third party Virus checker on the Security Server

Step 2 Start a command window (cmd)

Step 3 Test the third party's recommend commend line program with a test document and note the response for a clean file.

Step 4 Test the third party program with a test infected file. Note non-harmful test viruses can be downloaded from www.rexswain.com/eicar.html
Check that file is deleted

Step 5 Update setting in server.ini file as detailed below:

Step 6 If disk virus checking is preformed; change the virus checker's configuration to ignore the DATA directory located by default:

For 32 bit installations:
c:\program files\SecurEnvoy\Security Server\DATA
For 64 bit installations:
c:\program files(x86)\SecurEnvoy\Security Server\DATA

Step 7 Recipient reply emails. Reply emails are forwarded as is with no checking.
Make sure the MailHost configured in is set such that emails still pass through any email virus checking gateway that you have installed.

The virus settings of SecurMail are location in the server.ini file in:

For 32 bit installations:
c:\program files\SecurEnvoy\Security Server\
For 64 bit installations:
c:\program files(x86)\SecurEnvoy\Security Server\

SecurMail settings are located in the SecurMail Section

Virus_Checking	Can be set to True or False If set to True will run the program Virus_Command with arguments Virus_Command_Args after the Outlook agent has uploaded the message body or attachments. Default: False
Virus_Command	The full path to the third party virus checking program
Virus_Command_Args	The arguments required to pass to the checking program defended in Virus_Command. Note that $FILENAME$ must be used in place of the test document you checked
Virus_Return	The return message displayed if execution worked and no viruses are found

Example 1

Integration with Symantec's Scan Engine V4.30
Virus_Command= For 32 bit installations:
c:\program files\Symantec\Scan Engine\savsecls\savsecls.exe
For 64 bit installations:
c:\program files(x86)\Symantec\Scan Engine\savsecls\savsecls.exe

Virus_Command_Args=-verbose $FILENAME$
Virus_Return= 0

Example 2

Integration with Trend Micro's Office Scan Corporate Edition 6.5 with the virus definition file lpt$vpn.335
Virus_Command= For 32 bit installations:
c:\program files\Trend Micro\OfficeScan\PCCSRV\Engine\vscanwin32.com
For 64 bit installations:
c:\program files(x86)\TrendMicro\OfficeScan\PCCSRV\Engine\vscanwin32.com

Virus_Command_Args=/D /NM /NB /C /P

For 32 bit installations:
c:\program files\Trend Micro\OfficeScan\PCCSRV\lpt$vpn.335" $FILENAME$
For 64 bit installations:
c:\program files(x86)\Trend Micro\OfficeScan\PCCSRV\lpt$vpn.335" $FILENAME$

Virus_Return=1 files have been checked

12.2 SecurMail Server Security Considerations

Virtual Directory Security

IIS Virtual Directory Secmail

The server should be hardened according to Microsoft's recommendations. Once installed only one virtual directory requires being published externally, this is Secmail. This can be controlled via IIS properties, a firewall or reverse proxy server.

It is recommended that any other SecurEnvoy virtual directory is not exposed to the Internet, unless especially required.

Microsoft IIS Server

It is recommended that a dedicated instance of SecurEnvoy SecMail security server be installed for being public facing on the Internet, ideally within the DMZ environment. A reverse proxy such as Microsoft ISA 2010 or various vendor SSL VPN are capable of providing this functionality.

For SecurMail access, it is strongly recommended that a trusted public web server certificate is installed in the IIS server.

The only Virtual directory that should be accessible from the internet is the "secmail" as this is the only one needed by the recipients. All other virtual directories should be set to be accessible from the internal network.

Recipients must access the secmail directory over https. Therefore the server (or the reverse proxy in that case) must use a public trusted certificate.

It is considered more secure to use the reverse proxy method, because there is only a single point of access and you share the certificate with other content using the reverse proxy.

Microsoft Windows 2003 Security resource
http://technet.microsoft.com/en-us/library/cc163140.aspx

Microsoft Windows 2008 Security resource
http://technet.microsoft.com/en-us/library/cc514539.aspx

Microsoft Windows 2012 Security resource
http://technet.microsoft.com/en-us/library/jj898542.aspx

Load Balancing and Redundancy
It is recommended that two SecurMail servers should be installed for redundancy. These servers can either be software or hardware clustered, alternatively the data directory can be installed upon NAS or a SAN device. The data directory path will be the same upon both SecurEnvoy SecurMail servers.
The IIS server needs to be configured so that they are active-active or active-passive to each other. Layer 7 switches are one way to load balance across multiple IIS server running SecurMail.
Alternatively install Microsoft network load balancing (NLB) on both servers. Using NLB, the same data is stored on multiple servers, so if one becomes unavailable, the client is redirected to another server with the same information. Please see http://technet.microsoft.com/en-us/library/cc770558.aspx

13 Frequently Asked Questions

Chapter 13

Q: Which SMS gateways do you support?
You can send SMS messages via a connected Wavecom or Siemens modem or via an Internet SMS gateway provider see **SMS Gateways** for more information.

Q: Should the onetime passcode be sent in real time as I am authenticating?
This approach is fundamentally flawed because of the following problems:

1. SMS delivery is delayed

Although most SMS text messages are transmitted in seconds, it's common to find them delayed when networks become congested. SMS traffic is not sent point to point, it is 'queued', and then sent on to the required network cell where it is again queued and finally sent to the end users phone. This queuing gives rise to delays at peak operator periods, Vodafone's own sales literature claims that 96% of all SMS messages are delivered within 20 seconds. This means that 4% of users trying to authenticate will fail and will need to raise a help desk call to gain emergency access. Thus for a deployment of 5000 users authenticating each day, 200 help desk calls would be raised per day!

2. Signal dead spots

Mobile phone signals are not always available, particularly in buildings with wide outer walls, in underground basements or in computer rooms that give off high RF noise. Consider a user trying to authenticate in one of these locations. They would first enter their UserID and PIN and would then fail to receive their authentication code. They would next need to move to a location that has a signal, receive their authentication code, move back to the original location to enter their passcode, ALL within a timeout period of 2 minutes.
Users located within these locations would have no alternative but to raise help desk calls to gain emergency access.

3. Mobile phone is used to connect to the internet

In most cases when a mobile phone creates a data connection it can't receive SMS messages. Users trying to utilize their mobile phone as a way of connecting to the Internet would not receive their passcode until they hang-up the data connection. End-users would need to start authenticating the UserID and PIN, hanging up the connection, wait for the SMS message, reconnect and re-enter their UserID, Pin and Passcode all within 2 minutes.
The SecurAccess product does not require on-demand SMS messages. The end user first enters their UserID, then enters their windows password and appends their 6 digit passcode that is already stored on their mobile phone as it was sent to them when they last authenticated. An approach that pre-loads the next required passcode each time a user authenticates resolves all the issues relating to SMS delays or short term signal loss and data connectivity.
This technique eliminates any problems with SMS delivery delays, as typically an end user does not require their next passcode until the next working day. This length of time is more than adequate to allow for any SMS delays and gives plenty of time for the end users to move to a location that has a signal, for example when they commute to or from their place of work. SecurEnvoy also supports sending 3 valid passcodes within each SMS passcode. This technique allows for up to 3 valid authentications before requiring the next SMS message to be received.

Q: What is the difference between a One Time Code and a Day Code?
In "One Time" mode, the entered passcode can only be used once in exactly the same way as token companies such as RSA. A new one time code is sent to the user after every authentication attempt, good or bad. Any attempt to replay the entered code will fail, as the authenticated passcode is locked and can only be entered once. This mode of operation is ideal for remote users on "malicious" systems, home PC or in view of the public when authenticating. These users are only authenticating to a VPN which uses a session key so would typically only authenticate once or twice a day at the most. On average remote access users authenticate twice per week, as some users may only authenticate once per month or less.

Note

These users would not be authenticating their local PC's screen lock as it maybe a third party system or home PC.

In "Day Code" Mode, a reusable passcode is sent each day (or any number of days for example every week), this code can be reused for that day or the following day, so the risk of replay attack is limited to two days which is significantly stronger that a 30 day password (weekends can be skipped). If the user does not use a day code it isn't known publicly and therefore cannot have been intercepted, so a replacement day code is only send if previously used. This mode of operation is ideal for in-house desktop users that authenticate many times a day as it only requires one SMS passcode per day or less if the user is on holiday and not using their day code. So basically you can tailor the risk, ease of use and cost of SMS to suite each user's requirement depending on their environment.

Q: Some of my users do not have mobile phones how can I use this solution?
These users may not have a company supplied phones, but they almost certainly have their own mobile phones, as statistics say that there are nearly twice as many live handsets as people in the UK. Even if they don't have a personal mobile phone, SecurAccess can still send a passcode to a landline telephone or even a DDI number behind a PBX.

Q: What if end users do not want to use their personal mobile phone?
The question is why don't they want to use their own phones? You will not be putting any software on their phone. You will simply be sending them an SMS message which will not cost the end user anything. In some cases it's simply that they don't want to receive phone calls from other employees. Personal mobile numbers are stored encrypted so that only the SecurEnvoy administrators can read it, which prevents other staff trying to call it. What is more inconvenient to the user, using up pocket space for a token or using virtual space on their mobile phone?

Q: How good is the GSM phone coverage?
GSM network consists of over 860 networks in 220 countries/areas of the world. Coverage Maps can be found at: http://www.gsmworld.com/roaming/gsminfo/index.shtml

Q: I live in a bad or no GSM coverage how do you manage this?
If you frequent a place that has intermittent coverage, it is possible to utilise the day code option within the software. This means that a passcode can be reused for between 1 and 99 days. As SecurEnvoy works on pre-loaded methodology the user will always have a working code on their phone. Alternatively the security server can be configured to send 3 one time codes with-in each SMS message. Finally it is possible for SecurAccess to send a passcode to a landline telephone or DDI number behind a PBX.

Q: How does the server send the SMS messages?
There are two options on how to send the SMS messages. First option is to use a Wavecom outbound only commercial strength GSM modem. This option allows the client to utilise their existing contract with their mobile telecom carrier. The telecom carrier may offer either a package where inter-calls (and SMS) between the companies phone are free, or they have a significant number of minutes and SMS per month included in the contract. Using this method the client can almost run the service for nothing. Alternatively they can pick up a single user contract. Most leading providers have packages that typically include 3000 SMS for around £20 per month. The second option is to sign up with one of the Web SMS gateways. This is basically a HTTPS connection to the Web SMS gateway, and the provider then sends the messages for you. This option is faster and more scalable than the GSM modem option, but can be more expensive.

Q: How well can the SecurEnvoy server scale?
The answer is very well. SecurEnvoy scales directly with LDAP, as this is its database, therefore the question should be "how well can your existing LDAP scale?". Microsoft has spent much time and money perfecting the replication between domain controller servers. SecurEnvoy benefit from this replication as it directly integrates with AD or other LDAP servers such as eDirectory.

Q: What happens if the user deletes the SMS?
Simply enter your username and complete the logon process without the passcode, the system will see this as a bad logon and send a new passcode. This will work as long as you have not gone passed the set number of concurrent failed logons, otherwise the account will be disabled.

Q: How do I know what passcode to use?
When you are enabled on the system, your first passcode will be automatically sent, pre-loading the codes caters for any delay with the SMS delivery. After authentication a new passcode will be sent, this new code on most mobile phones will overwrite the old one. Therefore only one code will be seen on the mobile phone.

Q: How do I know if a hacker is trying to guess my login details?
If a hacker tries a guessed login with your correct UserID then you will receive the next required passcode. Receiving this SMS message will act as an alert to you that someone is trying to break into your account.

Q: What Integration does SecurEnvoy have with RAS and NAS type network devices?
SecurEnvoy has implemented a Radius server, therefore we can support any application that supports basic password RADIUS authentication. In addition, SecurEnvoy has integration guides for the majority of common SSL/VPN, IPsec VPN and dial up vendors. Web based applications hosted on Microsoft IIS web server, for example OWA and Citrix can be authenticated via the SecurEnvoy IIS Agent.

Q: Do you have any reference sites or case studies?
There are multiple case studies on our web site, these cover various market verticals.

Q: I've deleted my passcode from my phone, what do I do?
Simply enter your username and complete the logon process without the passcode, the system will see this as a bad logon and send a new passcode. This will work as long as you have not gone passed the set number of bad logons, otherwise the account will be locked.

Q: I have no signal in some areas of the office, how do I receive a passcode?
By pre-loading the passcodes before you require them, allows plenty of time to receive your passcode when there is a signal. Alternatively you can use day codes, which allows a single code to be used for a set number of days or the security server can be configured to send 3 one time codes with-in each SMS message.

Q: How do I upgrade from a trial license to live license?
This is very simple, Start the Admin GUI and select the menu "Config" then paste the new live license key into the field marked License. If you plan to use a Web SMS Gateway then run "Advanced Config" skip to Web SMS Gateway and enter a valid UserID and Password that was allocated to you from your chosen Web SMS Gateway Company.

Q: How do I setup multiple SecurEnvoy Security Servers for redundancy?
Multiple security servers must share the same security encryption key (config.db) each time you install a new copy of the security server you will be prompted with the question "Is this the first server or any additional server?" If you select additional, you will then be prompted to upload the config.db file from the first server.

Q: My SecurEnvoy Radius Server fails with "Error Opening Local Port", How do I fix this?
Check that no other program is using the Radius port (1812).Stop the SecurEnvoy Radius Service and wait 60 seconds. In a CMD window run "netstat –a –p UDP" You should NOT see the line "UDP xxxx:radius *:*" where xxxx is the system name. If you do it may be that Microsoft's Internet Authentication Manager (IAM) is Installed, if so on some window versions there is a Microsoft bug that causes IAM to still use the Radius port even when stopped or uninstalled! It is recommended that the default ports in IAM are changed thus releasing the Radius port.

Q: If I use IE7 for local administration, start help and then exit the help window, why am I prompted to re-authenticate?
This is a known bug with Microsoft IE7. The session cookies are getting deleted when you close a 2nd window. At the moment no Microsoft fix exists. However the following workaround generally resolves this problem. Change your IE7 settings in Tools/Internet Options/General/Browser History Settings to "Every time I visit the web page".

Q: Why does local administration re-authenticate every page?
Both IE6 and IE7 browsers fail to return the authentication cookie if there is a '_' in the host name. Rename the host or use Firefox as the default browser.

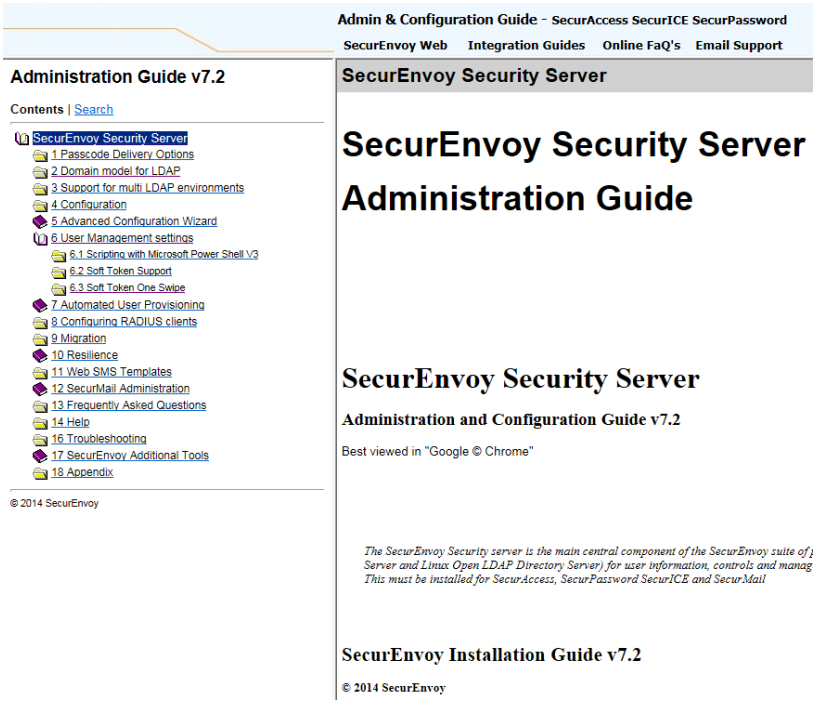
Q: Do you support 64bit OS servers
Yes, both the server and IIS agent support 64bit operating systems.

14 Help

Chapter 14

To view the help files, click upon the Help button within the Admin GUI.

This will launch the Help, which will open in a separate browser window.

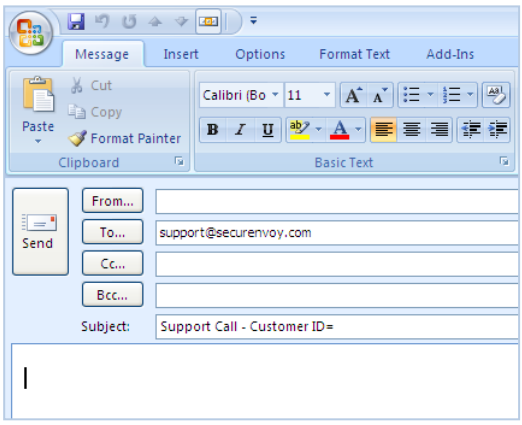


The Help page is made up of a navigation pane on the left hand side, where you can locate information on administration based tasks. The right hand side will display selected information. By default the help page displayed is linked to the Admin GUI menu, i.e. if in "Config" menu will display "Config" Help page.

The top bar within the Help window has four quick links, three of these are links to the SecurEnvoy



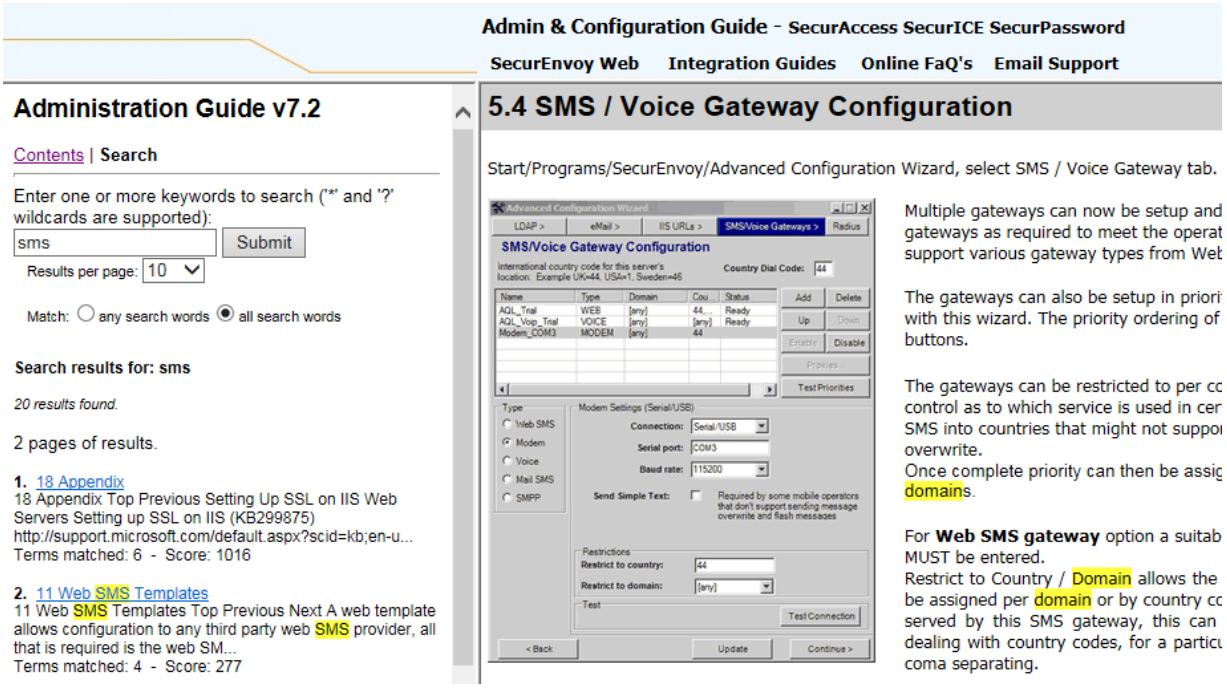
Web site to provide up to date information regarding SecurEnvoy, product integration guides and online FaQ's. The last link will launch your email client so that a "support email" can be sent.



When sending a "support email" please include the Customer ID (this is listed on your license certificate) with all correspondence.

Search Capability

Included with the Help Manual is the "Search Capability", click upon the "search" link within the left-hand navigation pane. Enter search criteria and click "submit"



All results are then displayed, they are shown in order with complete matches and a score associated with the search. You can then select and click upon the relevant link to display the information.

15 Recommended Backup procedure

Chapter 15

After the initial installation is complete or after re-installation of the security server software.
The Master Encryption key and configuration files are located by default for 32bit installations:

in C:\Program Files\SecurEnvoy\Security Server\

for 64 bit installations:

in C:\Program Files(x86)\SecurEnvoy\Security Server\

The following files should be backed up
config.db, configpre54.db, local.ini and server.ini should all be backed up.
It is also recommended that you backup the following regularly –

The DATA subfolder located in the SecurEnvoy installation folder. This contains the following information –

- LOG files
- RADIUS configuration Data
- SMS Message Queue and Controls
- SecurMail messages
- SecurMail mailbox authentication data
- Web Templates (Local SecurEnvoy server)
- SMS Message Templates

The SecurEnvoy server data stored in LDAP (in the telexnumber attribute on Novell eDir, Sun Directory, OpenLDAP; In the PrimaryTelexNumber and TelexNumberOther attributes on Active Directory).

For Microsoft ADAM / AD/LDS please see Microsoft article number 737702 on Tech Net for the recommended procedure. All SecurEnvoy ADAM / AD/LDS files are stored in the DATA\Adam subfolder of the SecurEnvoy installation folder.

Automated Unmanaged users backup

SecurEnvoy makes a backup of all unmanaged users & stores these within date stamped ldf files:

For 32 bit installations:
C:\Program Files\SecurEnvoy\Security Server\Data\BACKUP
For 64 bit installations:
C:\Program Files (x86)\SecurEnvoy\Security Server\Data\BACKUP

To restore all unmanaged users from a given day, run the following:

1. Run cmd with an administrator account
2. ldifde -i -f (file name to restore)

Example, restore all users unmanaged on the 26th March 2014 run the command
ldifde -i -f 26_Mar_2014.ldf

16 Troubleshooting

Chapter 16

Modem Fails to Initialise
1.Check that the Wavecom Modem has a flashing red LED
If the LED isn't flashing, check the power and SIM.

2. Check SIM type, if Vodafone PDU, mode must be set to False in the HKLM\software\SecurEnvoy\PhoneGateway1
Try setting to false even if it's not a Vodafone SIM

3.Stop the SecurEnvoy WebSMS Gateway service
Open Microsoft's Hyperterm (Start/Programs/Accessories/Communications)
Open the Com port that the modem is connected to
Change com port, baudrate, as required to get a connection.

Note

Wavecom defaults to 9600 8 No Stop Bits 1

Enter **ATI** you should get "**WAVECOM MODEM**" or "**SIEMENS TC35i**"

4. Check signal strength, start Hyperterm.
Enter **AT+CSQ** you should get **+CSQ: 22,0** where 22 is a number between 0 and 31 that defines the signal strength.

5. Check for a GSM connection
Enter **AT+CREG?** you should get OK

6. Try sending an SMS message manually
Enter **AT+CMGF=1**
Enter **AT+CMGS="4479xxxx"** where 4479xxxx is your mobile number in international format without a +
Enter **HELLO** then press Ctrl Z

7. Remove the SIM from the Wavecom and place in a normal GSM phone. Check the SIM can send SMS messages to International Numbers.

8. Check the Setting in the Registry
HKLM\SOFTWARE**SecurEnvoy**\WebSMS Gateway
Restart SecurEnvoy WebSMS Gateway after changes

9. Check that no other program is using the serial COM port before starting the SecurEnvoy WebSMS Gateway Service

SecurEnvoy Radius Server Fails with "Error Opening Local Port"

Check that no other program is using the Radius port (1812)
Stop the **SecurEnvoy** Radius Service and wait 60 seconds.
In a CMD window run "netstat –a –p UDP"

You should **NOT** see the line "UPD xxxx:radius *:*" where xxxx is the system name.

If you do it may be that Microsoft's Internet Authentication Service (IAS) is installed. On some window versions there is a Microsoft bug that causes IAS to still use the Radius port even when stopped or uninstalled!

It is recommended that the default ports in IAS are changed thus releasing the Radius port.

Log file displays Windows password incorrect when using Radius and Windows Password as the PIN

If the Windows password is correct, fault lies with an incorrect Radius "Pre shared key". SecurEnvoy support ASCII 127 characters.

Admin GUI does not run or SecurPassword does not run

This can occur for the following reasons:
1. There is another web instance using ports 80 and or 443
2. There aren't enough privileges to allow the ADMIN GUI to run, on IIS 6.0 go to IIS Manager, Application pools, default app pool, properties and change the identity to use a "Network Service" or use a pre defined account, usually the SecurEnvoy Admin account. On IIS 5.0 go to IIS Manager, default Web site, secadmin, select properties, Directory Security, Anonymous Access click edit. Under anonymous access click edit and enter details of the SecurEnvoy Admin account.

When executing the Set Pin program, error if unable to set the user PIN

Check within IIS manager that the anonymous web account has enough privileges to run the set pin program.

How do I setup multiple SecurEnvoy Security Servers for redundancy?

Multiple security servers must share the same security encryption key (config.db)
Each time you install a new copy of the security server you will be prompted with the question "Is this the first server or any additional server?" If you select additional, you will then be prompted to upload the config.db file from the first server.

How do I upgrade from a trial license to live license?

This is very simple, Start the Admin GUI and select the menu "Config" then paste the new live license key into the field marked License.
If you plan to use a Web SMS Gateway then run "Advanced Config" skip to Web SMS Gateway and enter a valid UserID and Password that was allocated to you from your chosen Web SMS Gateway Company

17 SecurEnvoy Additional Tools

Chapter 17

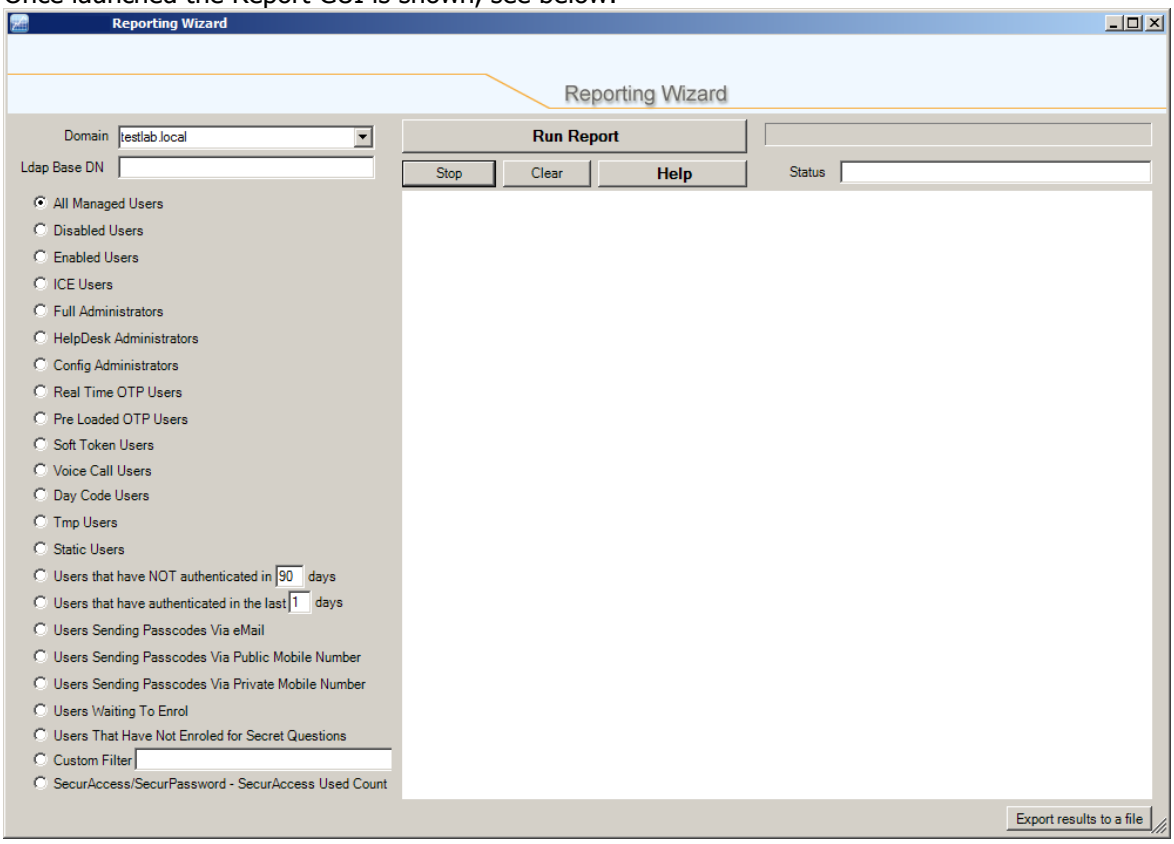
17.1 Reporting Wizard (GUI)

SecurEnvoy now has an additional tool called "Reporting Wizard" which allows further detailed investigation of user set up and overall system usage.
The Report tool is included in version 5.4 and above; all customers who are currently using any version 5 can download this additional Report tool from www.securenvoy.com/ftp/report.zip. Customers who are on version 4 or below are required to upgrade to allow this additional functionality.

This tool can be used in one of two ways, via a graphical user interface for manually creating reports or in command line mode for scripts or batch jobs to use.

The SecurEnvoy Report tool can be launched from the "Start" "Programs" "SecurEnvoy" Report Wizard link, alternatively run:
32 bit installations \Program Files\SecurEnvoy\Security Server\Report\report.exe
And 64 bit installations \Program Files(x86)\SecurEnvoy\Security Server\Report\report.exe

Once launched the Report GUI is shown, see below:

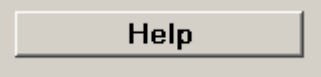




To run the selected report click "Run Report" The status field will show activity and a progress bar may be shown upon heavily used systems, this will be displayed to the right of the status field.



When a report is running the Stop button may be clicked to halt the current report. The Clear button will clear any previous report that has been outputted to the GUI screen.



The Help button will provide detailed information of how to use the report wizard in HTML format

SecurEnvoy administrators have a number of pre configured reports to run against selected configured domains. Once complete, report information can be managed from the GUI or can be exported to CSV file.

Domain Selection
All domain information is obtained from the server.ini file. All that is required is to select the domain that a report is required for.

LDAP Base DN
The LDAP base DN can be set to only interrogate a certain part of your directory server. Example OU=HQ,DC=W23,DC=com, so only users in HQ are reported upon.

Once the Domain has been selected, it is a case of choosing one of the reports.

All Managed Users
This will output to the screen all users who are currently managed (This will include users who are in ICE mode or a user who is disabled but still having a license assigned to them). Upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition a CSV report can be generated by clicking the "Export results to a file" button.

Report: All_Managed_Users Found 44

Domain	First Name	Last Name	Login ID
w23.com	adam		adam
w23.com	ahold		ahold
w23.com	amber		amber
w23.com	andrew		andrew
w23.com	arne		arne
w23.com	bank		bank
w23.com	bcx		bcx
w23.com	bm		bm
w23.com	Bob	Bob	Bob
w23.com	bull		bull
w23.com	CMC		cmc
w23.com	conrad		conrad
w23.com	cyber		cyber
w23.com	Demo		Demo
w23.com	ed		ed
w23.com	fibi		fibi
w23.com	Hans		Hans

When the report has run, information will be outputted to the report GUI console.

Clicking upon any of the Login ID user links will allow direct management via the SecurEnvoy local Admin GUI.

Disabled Users
This will output to the screen all users who are in a disabled state upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Enabled Users
This will output to the screen all users who are in an Enabled state upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

ICE Users
This will output to the screen all users who are in ICE Mode state upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Full Administrators
This will output to the screen all users who have Administrative role based permissions upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

HelpDesk Administrators
This will output to the screen all users who have HelpDesk role based permissions upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Config Administrators
This will output to the screen all users who have Config role based permissions upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Real Time OTP Users
This will output to the screen all users who are setup for "Real Time OTP" mode upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Pre Loaded OTP Users
This will output to the screen all users who are setup for "Pre Loaded OTP" mode upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Soft Token Users
This will output to the screen all users who are setup for "Soft Token" mode upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Daycode Users
This will output to the screen all users who are setup for "Daycode" mode upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Tmp Users
This will output to the screen all users who are setup for "Tmp code" mode upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Static Users
This will output to the screen all users who are setup for "Static code" mode upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Users who have NOT authenticated in (x) days
This will output to the screen all users who have not authenticated in (selectable) days upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Users who have authenticated in the last (x) days
This will output to the screen all users who have authenticated in the last (selectable) days upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button.

Users Sending Passcodes Via eMail
This will output to the screen all users who are setup to receive "Passcodes via eMail" mode upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button

Users sending Passcodes Via Public Mobile Number
This will output to the screen all users who are setup that have a "Public Mobile Number" i.e. Mobile is populated in LDAP within the "Mobile" attribute. The Mobile number will be displayed in the output. The SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button

Users sending Passcodes Via Private Mobile Number
This will output to the screen all users who are setup that have a "Private Mobile Number" i.e. Mobile is encrypted by the SecurEnvoy server. The Mobile number will be displayed in the output. The SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button

Users Waiting To Enrol
This will output to the screen all users who still haven't completed the enrolment process upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button

Custom Filter
This will output to the screen any custom filter that is inputted to this window. A custom filter can be generated by any LDAP tool or by an AD query string.
In addition, a CSV report can be generated by clicking the "Export results to a file" button

SecurAccess SecurPassword _ SecurAccess Used count
This will output to the screen all users who are using both SecurAccess and also SecurPassword upon the SecurEnvoy server; the SecurEnvoy administrator will then be able to directly manage any selected users via the Report GUI.
In addition, a CSV report can be generated by clicking the "Export results to a file" button

17.2 Reporting Wizard (Cmd Line)

The following command line options are available

Usage: report.exe /auto /report=(number) /file=(file name and path) /days=(number of days) /domain=(domain name) /hidegui /debug
The report number is a logical number assigned to each report, therefore please see table below for number to report mappings

Report Number

1	All Managed Users
2	Disabled Users
3	Enabled Users
4	ICE Users
5	Full Administrators
6	HelpDesk Administrators
7	Config Administrators
8	Real Time OTP Users
9	Pre Loaded OTP Users
10	Soft Token Users
11	Voice Token Users
12	Daycode Users
13	Tmp Users
14	Static Users
15	Users who have NOT authenticated in (x) days
16	Users who have authenticated in the last (x) days
17	Users Sending Passcodes Via eMail
18	Users Sending Passcodes Via Public Mobile Number
19	Users Sending Passcodes Via Private Mobile Number
20	Users Waiting to Enrol
21	Users that have not enrolled secret questions
22	Custom report
23	SecurAccess used count

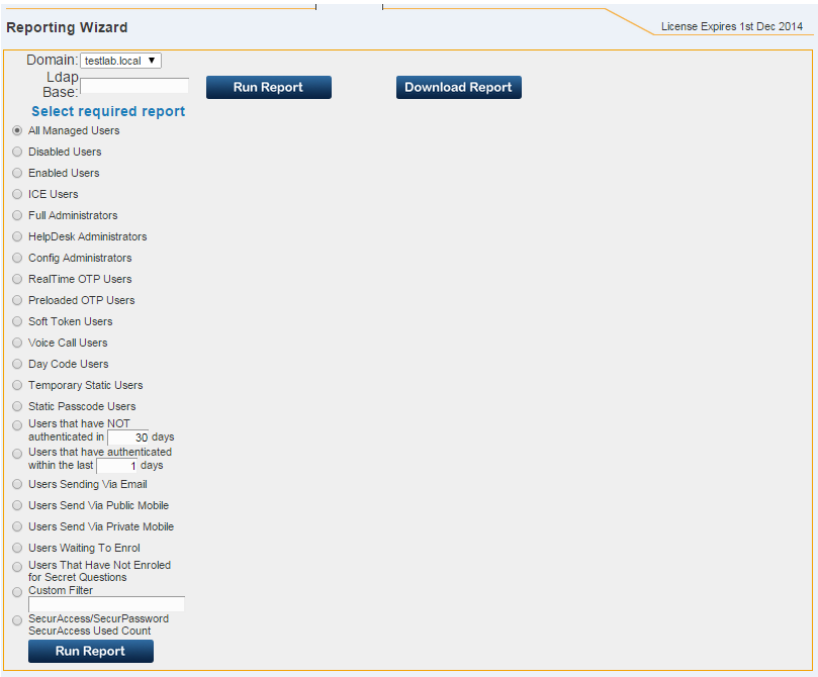
/auto	Must be set to use command line options
/report=(number)	Must be set to the number of the radio button to select. 1=All Manager Users, 2=Disabled users etc
/file=(file name)	Must be set to the file name and path the report is created in. Example c:\report.csv
/days=(number of days)	Only required for reports the need the number of days entering
/domain=(domain name)	Optional, defaults to primary domain
/ldapbase=(LDAP Base DN)	Optional, defaults to primary domain
/hidegui	Optional, if set will hide the graphical interface
/email=(recipient)	Optional, sends report to the email address (recipient), multiple recipients must be separated with a semicolon
/debug	Optional, if set will enable debug

Example1:
Report /auto /report=1 /file="c:\reportout.csv"
Example2:
Report /auto /report=13 /file="c:\tmp\not_authenticated.csv" days=30 /domain="securevoy.com" /hidegui"

17.3 Reporting Wizard (Admin GUI)

Reports can now be generated directly within the SecurEnvoy Admin GUI.

There are 23 pre-configured reports that can be run against each LDAP Domain. In addition to selecting the LDAP Domain, the LDAP base can also be configured. This allows large Enterprises to designate reports against certain Business units with their own LDAP Domain (OU's)



The list of reports are displayed right of this screenshot.

Once the designated report has run the output is displayed in the right hand window of the Admin GUI, this allows the Admin or Helpdesk operator directly manage the listed user from within the Admin GUI.

1 All Managed Users

2 Disabled Users

3 Enabled Users

4 ICE Users

5 Full Administrators

6 HelpDesk Administrators

7 Config Administrators

8 Real Time OTP Users

9 Pre Loaded OTP Users

10 Soft Token Users

11 Voice Token Users

12 Daycode Users

13 Tmp Users

14 Static Users

15 Users who have NOT authenticated in (x) days

16 Users who have authenticated in the last (x) days

17 Users Sending Passcodes Via eMail

18 Users Sending Passcodes Via Public Mobile Number

19 Users Sending Passcodes Via Private Mobile Number

20 Users Waiting to Enrol

21 Users that have not enrolled secret questions

22 Custom Report

23 SecurAccess used count

18 Alerting

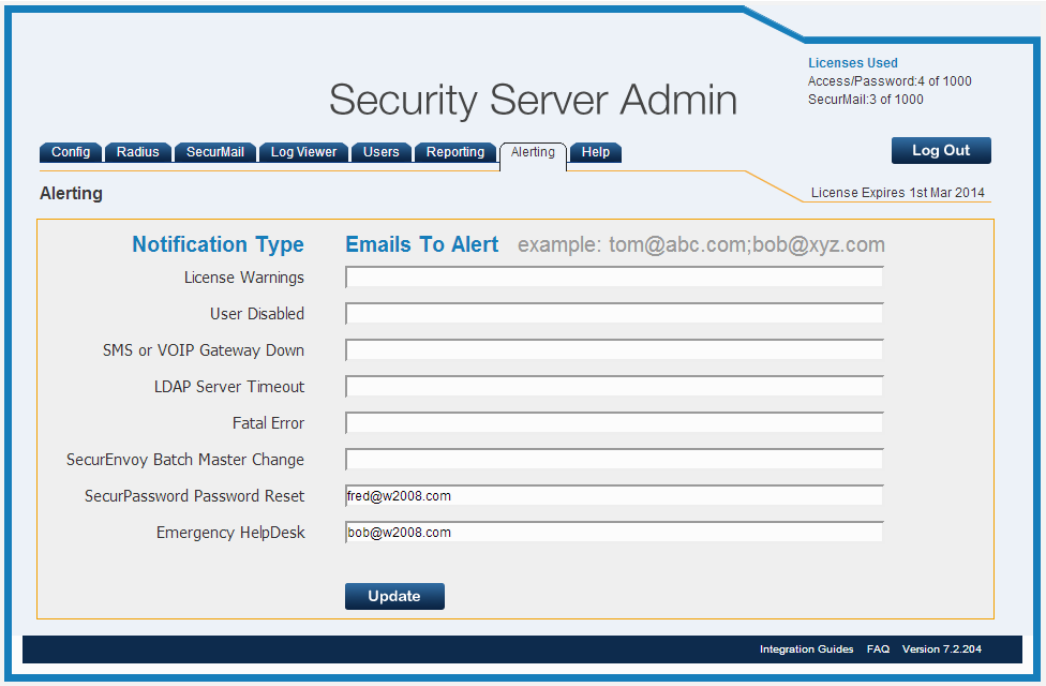
Chapter 18

Real Time email alerts can be setup via the Alerting tab.

Simply select the event that you wish to be alerted upon. There are eight available options that can be chosen.

Then add the email address, email group or multiple email addresses that should be notified.

Click "Update" when complete.



19 Appendix

Setting Up SSL on IIS Web Servers

Setting up SSL on IIS (KB299875)
http://support.microsoft.com/default.aspx?scid=kb;en-us;299875

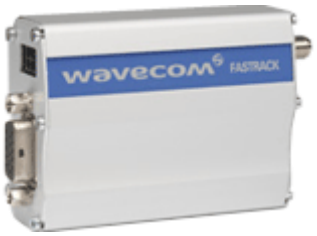
SMS Gateway Options

SecurEnvoy support two options for sending SMS messages:

Option1

A Directly connected Wavecom

This options uses a mobile phone SIM card and will send SMS messages in the same way as a mobile phone



Parts List For Wavecom (Serial Only) (SecurEnvoy preferred solution)
1. Wavecom Fasttrack
1. 12v Mains PSU
1. Serial Data Cable 15D to 9D (PC Serial Port)
1. Magnetic Mount Arial with SMA male 3M lead
Vendor information **here**
Note: can support USB via a serial adapter cable

or Siemens modem



Parts List For Siemens TC35i (Serial Only)
1. Siemens TC35it Pack B
Note that Pack B contains a TC35 Modem, Mains PSU, Serial Cable and a 2 meter magnetic mount aerial.

Or Mutlitech modem.



Parts List For Mutlitech (USB or Serial Modem)

1. Modem Model:MTCBA-G-U-F4 (USB Modem)
1. Magnetic Mount Arial with SMA male 3M lead Vendor information **here**

Option2

An Internet based SMS gateway provider. SMS messages are sent via the Internet to a company that hosts a gateway connection to worldwide mobile phone network providers.

SecurEnvoy currently support the following third partys:

AQL	(www.aql.com) (recommended for UK and Europe)
PSWinCom	(www.pswin.com)
V-First	(www.vfirst.com)
T-Mobile	(www.tmobile.co.uk)
O2	(www.infracast.com)
Silver Street	(www.silverstreet.com)
HSL SMS	(www.hslsms.com)
Clickatel	(www.clickatell.com)
m:science	(www.m-science.com)
2SMS	(www.2sms.com)
smsglobal	(www.smsglobal.com)
end2end	(www.promessaging.net)
Mollie	(www.mollie.nl)
SysorVest	(www.systorvest.no)

Note

Any other third party provider that supports https can be added for 2 days consultancy.

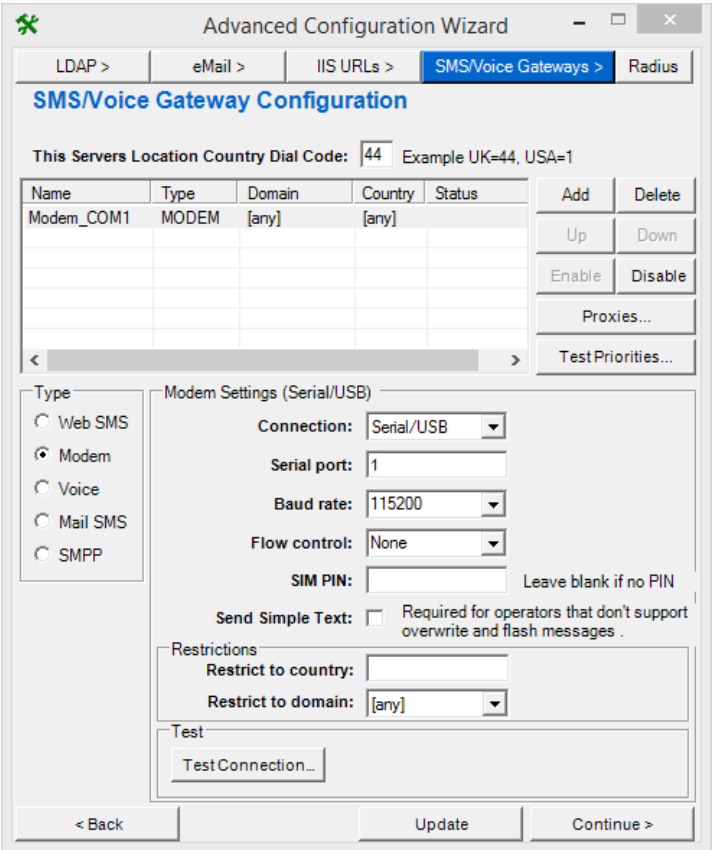
AQL Application Form

To apply for an AQL Web gateway account please go to the following URL

http://www.AQL.com/SE

Follow details onscreen

Vodafone SIM Considerations



Vodafone do not adhere to the SMS standard when using the PDU mode.

If using a Vodafone SIM, you are no longer able to use the PDU mode (dynamically overwriting of SMS texts); this is due to Vodafone having their own proprietary method of completing this.

Therefore enable the checkbox "Send Simple Text". Otherwise the sending of a SMS passcode will fail.

Supported ASCII Data Codes

Overview

SecurEnvoy supports ASCII 127 for use with "Radius Pre Shared Keys". ASCII stands for American Standard Code for Information Interchange. Below is the ASCII character table for ASCII 0 through ASCII 127.

Standard ASCII Code Table

Decimal	Octal	Hex	Binary	Value
000	000	000	00000000	NUL (Null char.)
001	001	001	00000001	SOH (Start of Header)
002	002	002	00000010	STX (Start of Text)
003	003	003	00000011	ETX (End of Text)
004	004	004	00000100	EOT (End of Transmission)
005	005	005	00000101	ENQ (Enquiry)
006	006	006	00000110	ACK (Acknowledgment)
007	007	007	00000111	BEL (Bell)
008	010	008	00001000	BS (Backspace)
009	011	009	00001001	HT (Horizontal Tab)
010	012	00A	00001010	LF (Line Feed)
011	013	00B	00001011	VT (Vertical Tab)
012	014	00C	00001100	FF (Form Feed)
013	015	00D	00001101	CR (Carriage Return)
014	016	00E	00001110	SO (Shift Out)
015	017	00F	00001111	SI (Shift In)
016	020	010	00010000	DLE (Data Link Escape)
017	021	011	00010001	DC1 (XON) (Device Control 1)
018	022	012	00010010	DC2 (Device Control 2)
019	023	013	00010011	DC3 (XOFF) (Device Control 3)
020	024	014	00010100	DC4 (Device Control 4)
021	025	015	00010101	NAK (Negative Acknowledgement)
022	026	016	00010110	SYN (Synchronous Idle)
023	027	017	00010111	ETB (End of Trans. Block)
024	030	018	00011000	CAN (Cancel)
025	031	019	00011001	EM (End of Medium)
026	032	01A	00011010	SUB (Substitute)
027	033	01B	00011011	ESC (Escape)
028	034	01C	00011100	FS (File Separator)
029	035	01D	00011101	GS (Group Separator)
030	036	01E	00011110	RS (Request to Send) (Record Separator)
031	037	01F	00011111	US (Unit Separator)
032	040	020	00100000	SP (Space)
033	041	021	00100001	! (exclamation mark)
034	042	022	00100010	" (double quote)
035	043	023	00100011	# (number sign)
036	044	024	00100100	$ (dollar sign)
037	045	025	00100101	% (percent)
038	046	026	00100110	& (ampersand)

039	047	027	00100111	' (single quote)
040	050	028	00101000	((left/opening parenthesis)
041	051	029	00101001	) (right/closing parenthesis)
042	052	02A	00101010	* (asterisk)
043	053	02B	00101011	+ (plus)
044	054	02C	00101100	, (comma)
045	055	02D	00101101	- (minus or dash)
046	056	02E	00101110	. (dot)
047	057	02F	00101111	/ (forward slash)
048	060	030	00110000	0
049	061	031	00110001	1
050	062	032	00110010	2
051	063	033	00110011	3
052	064	034	00110100	4
053	065	035	00110101	5
054	066	036	00110110	6
055	067	037	00110111	7
056	070	038	00111000	8
057	071	039	00111001	9
058	072	03A	00111010	: (colon)
059	073	03B	00111011	; (semi-colon)
060	074	03C	00111100	< (less than)
061	075	03D	00111101	= (equal sign)
062	076	03E	00111110	> (greater than)
063	077	03F	00111111	? (question mark)
064	100	040	01000000	@ (AT symbol)
065	101	041	01000001	A
066	102	042	01000010	B
067	103	043	01000011	C
068	104	044	01000100	D
069	105	045	01000101	E
070	106	046	01000110	F
071	107	047	01000111	G
072	110	048	01001000	H
073	111	049	01001001	I
074	112	04A	01001010	J
075	113	04B	01001011	K
076	114	04C	01001100	L
077	115	04D	01001101	M
078	116	04E	01001110	N
079	117	04F	01001111	O
080	120	050	01010000	P
081	121	051	01010001	Q
082	122	052	01010010	R
083	123	053	01010011	S
084	124	054	01010100	T
085	125	055	01010101	U
086	126	056	01010110	V
087	127	057	01010111	W
088	130	058	01011000	X
089	131	059	01011001	Y

090	132	05A	01011010	Z	
091	133	05B	01011011	[	(left/opening bracket)
092	134	05C	01011100	\	(back slash)
093	135	05D	01011101	]	(right/closing bracket)
094	136	05E	01011110	^	(caret/circumflex)
095	137	05F	01011111	_	(underscore)
096	140	060	01100000	`	
097	141	061	01100001	a	
098	142	062	01100010	b	
099	143	063	01100011	c	
100	144	064	01100100	d	
101	145	065	01100101	e	
102	146	066	01100110	f	
103	147	067	01100111	g	
104	150	068	01101000	h	
105	151	069	01101001	i	
106	152	06A	01101010	j	
107	153	06B	01101011	k	
108	154	06C	01101100	l	
109	155	06D	01101101	m	
110	156	06E	01101110	n	
111	157	06F	01101111	o	
112	160	070	01110000	p	
113	161	071	01110001	q	
114	162	072	01110010	r	
115	163	073	01110011	s	
116	164	074	01110100	t	
117	165	075	01110101	u	
118	166	076	01110110	v	
119	167	077	01110111	w	
120	170	078	01111000	x	
121	171	079	01111001	y	
122	172	07A	01111010	z	
123	173	07B	01111011	{	(left/opening brace)
124	174	07C	01111100	|	(vertical bar)
125	175	07D	01111101	}	(right/closing brace)
126	176	07E	01111110	~	(tilde)
127	177	07F	01111111	DEL	(delete)