SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

Administrators Guide

v9.4.502

Authenticating Users Using SecurAccess Server by SecurEnvoy

SecurEnvoy SecurAccess Security Server Administration Guide

Contents

Disclaimer

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

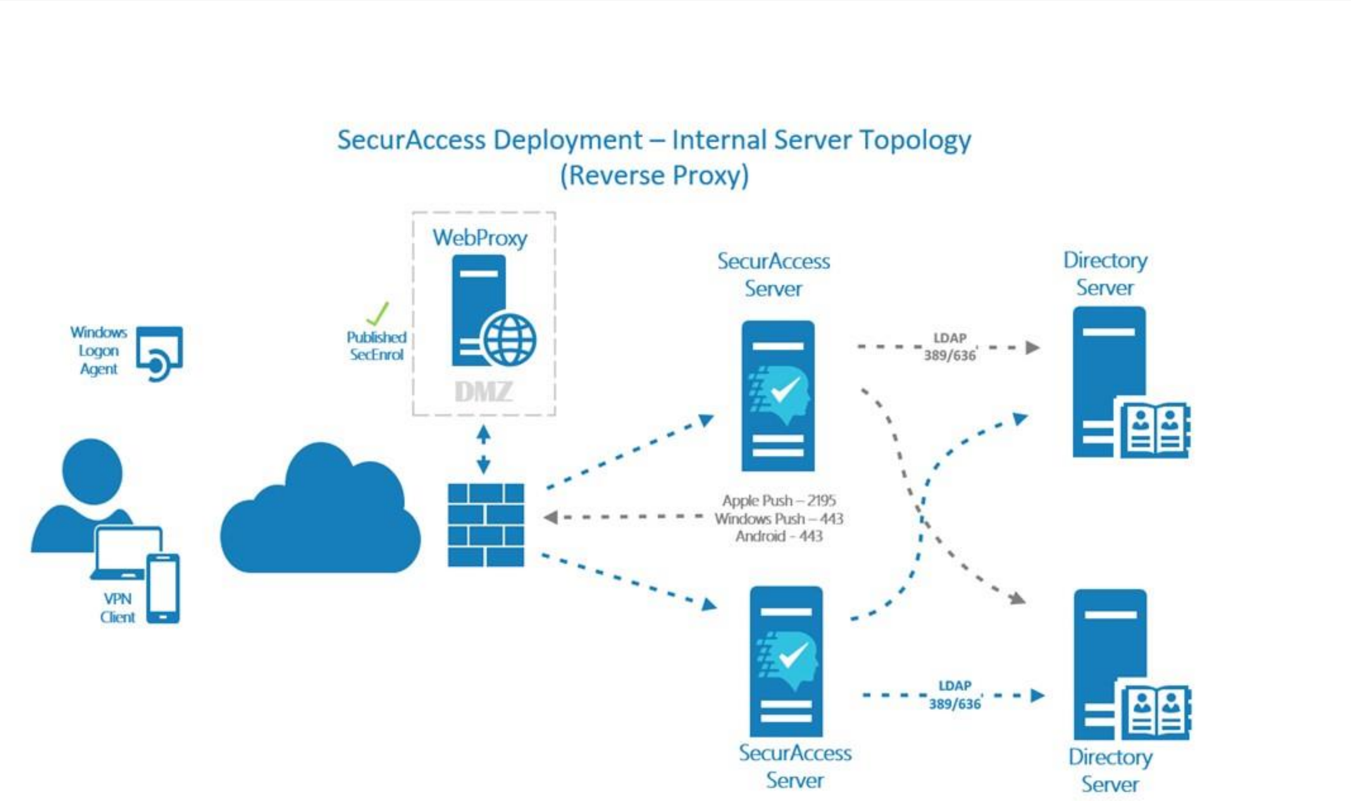
Legal

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.

Deployment Topology

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.

Deployment Using a Reverse Proxy



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.

Disadvantages of this topology
The following token types are not supported:

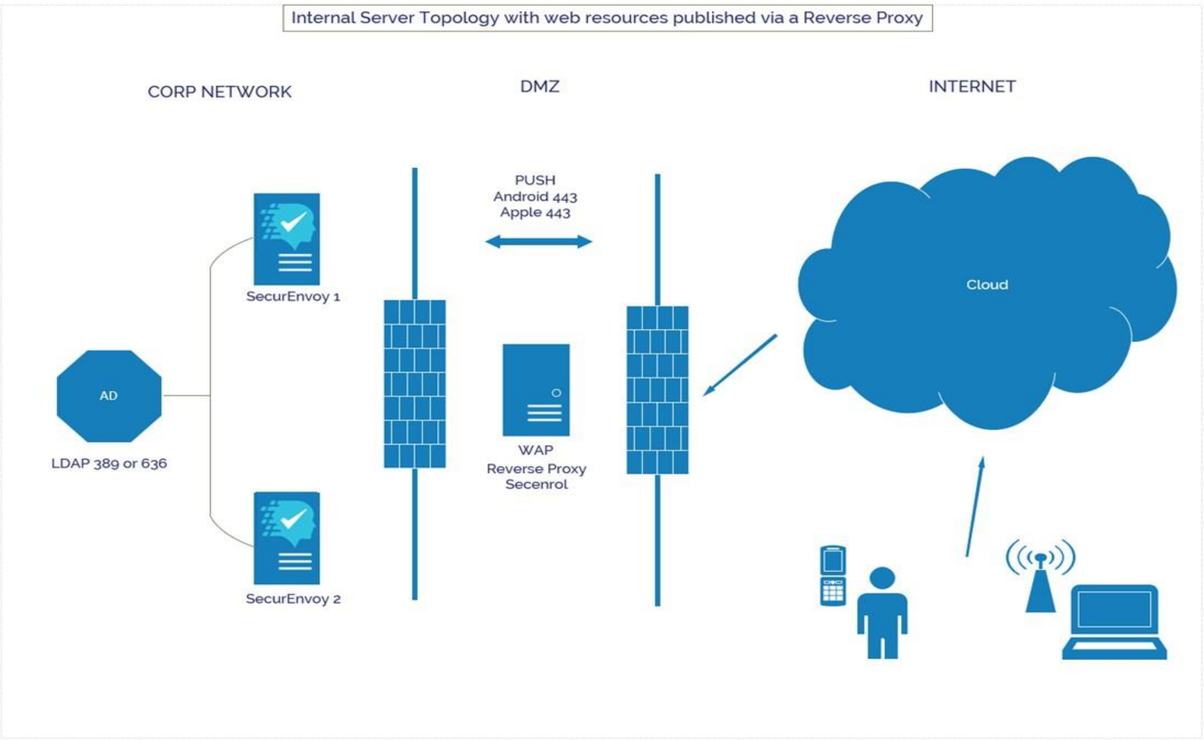
- Push Notifications

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.

Note: SecurEnvoy Manage My Token portal requires two-factor authentication.

Internal Server with web resources published via a Reverse Proxy

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



Advantages of this topology
All token types are supported including Push
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.

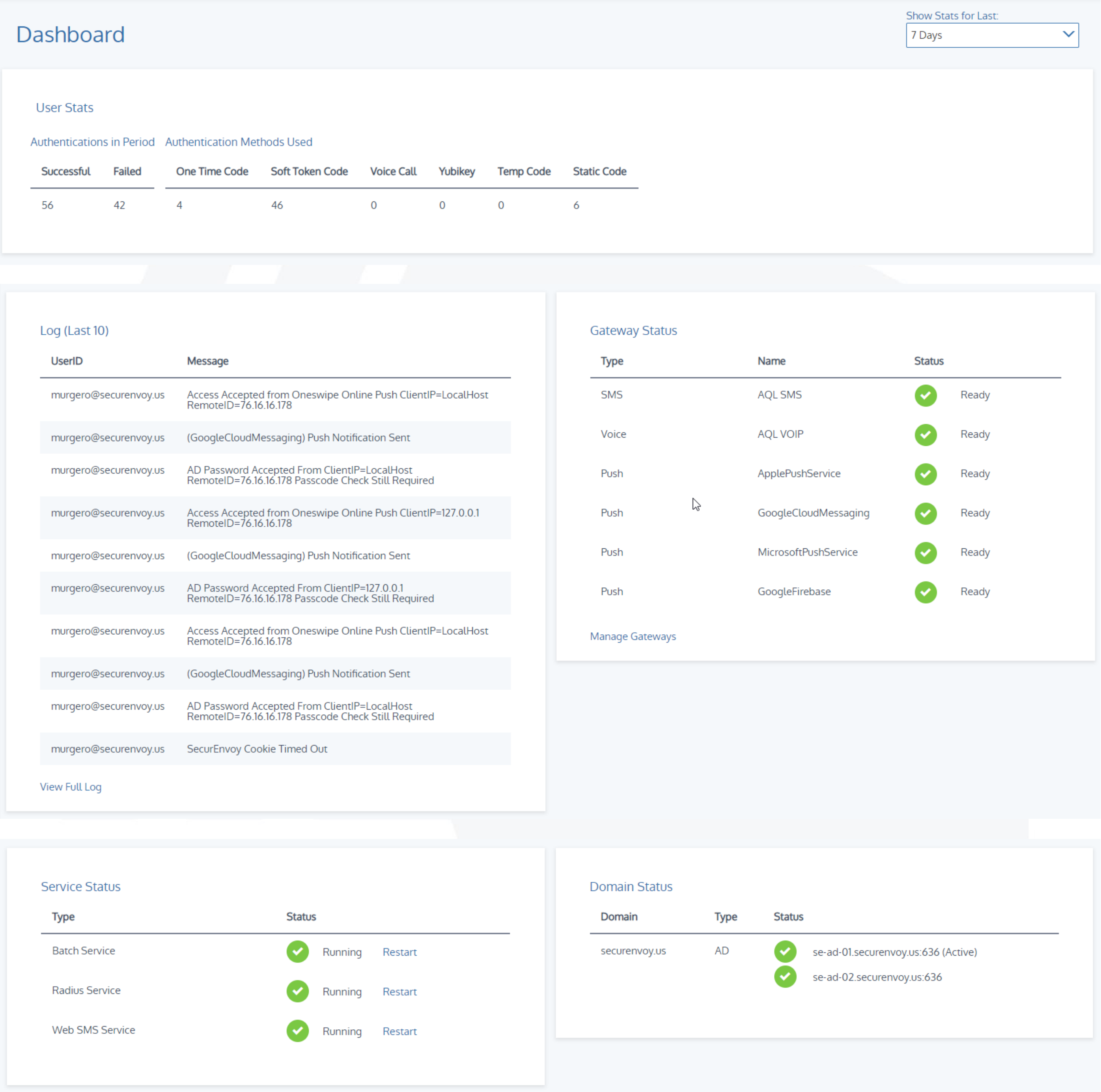
System Consoles

There are several consoles available for use by the system administrator and the user.

Management Console

http(s)://domainname.com/secadmin

This is the management interface for administrators and contains the dashboard and all configuration options for the solution. The primary Dashboard (show here) gives the administrator an immediate summary of the systems status, health and connections.



Dashboard

Show Stats for Last: 7 Days

User Stats

Authentications in Period		Authentication Methods Used					
Successful	Failed	One Time Code	Soft Token Code	Voice Call	Yubikey	Temp Code	Static Code
56	42	4	46	0	0	0	6

Log (Last 10)

UserID	Message
murgero@securenvoy.us	Access Accepted from Oneswipe Online Push ClientIP=LocalHost RemoteID=76.16.16.178
murgero@securenvoy.us	(GoogleCloudMessaging) Push Notification Sent
murgero@securenvoy.us	AD Password Accepted From ClientIP=LocalHost RemoteID=76.16.16.178 Passcode Check Still Required
murgero@securenvoy.us	Access Accepted from Oneswipe Online Push ClientIP=127.0.0.1 RemoteID=76.16.16.178
murgero@securenvoy.us	(GoogleCloudMessaging) Push Notification Sent
murgero@securenvoy.us	AD Password Accepted From ClientIP=127.0.0.1 RemoteID=76.16.16.178 Passcode Check Still Required
murgero@securenvoy.us	Access Accepted from Oneswipe Online Push ClientIP=LocalHost RemoteID=76.16.16.178
murgero@securenvoy.us	(GoogleCloudMessaging) Push Notification Sent
murgero@securenvoy.us	AD Password Accepted From ClientIP=LocalHost RemoteID=76.16.16.178 Passcode Check Still Required
murgero@securenvoy.us	SecurEnvoy Cookie Timed Out

View Full Log

Gateway Status

Type	Name	Status	
SMS	AQL SMS	✓	Ready
Voice	AQL VOIP	✓	Ready
Push	ApplePushService	✓	Ready
Push	GoogleCloudMessaging	✓	Ready
Push	MicrosoftPushService	✓	Ready
Push	GoogleFirebase	✓	Ready

Manage Gateways

Service Status

Type	Status		
Batch Service	✓	Running	Restart
Radius Service	✓	Running	Restart
Web SMS Service	✓	Running	Restart

Domain Status

Domain	Type	Status	
securenvoy.us	AD	✓ ✓	se-ad-01.securenvoy.us:636 (Active) se-ad-02.securenvoy.us:636

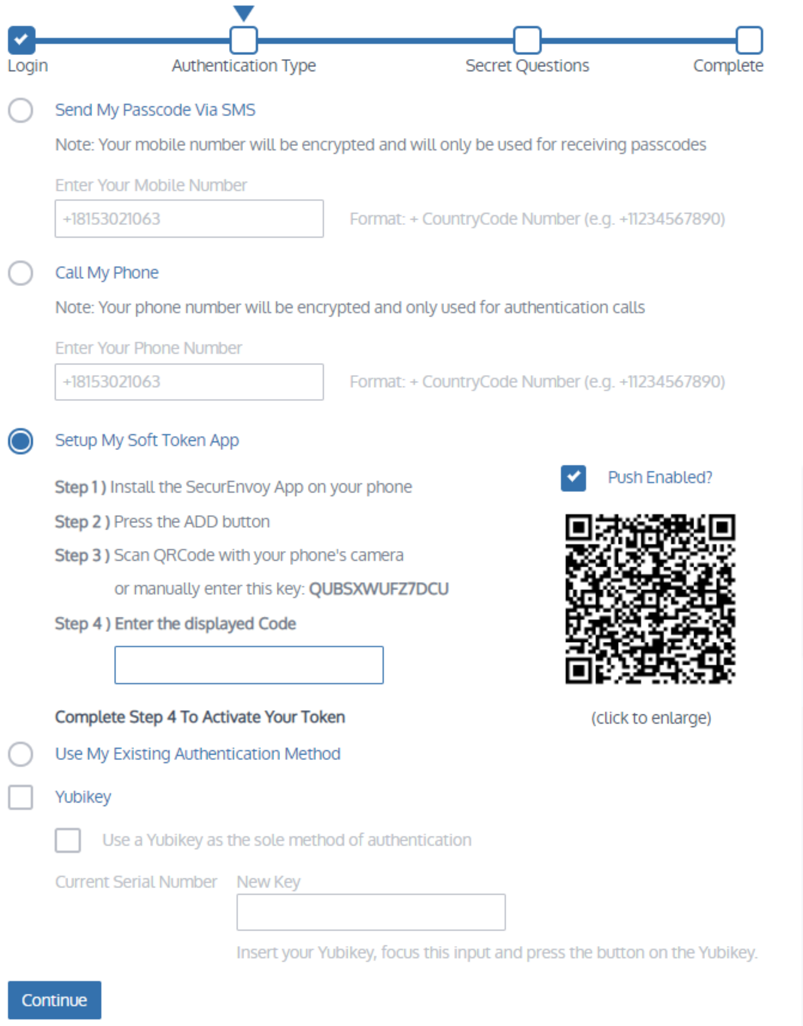
Note: Access to this console from the server directly authenticates the administrator's Windows credentials. Access remotely, requires that the user be defined as a system admin and have a registered token, covered later in this guide.

User Enrolment

http(s)://domainname.com/secenrol

User registration and token management is performed in this management console. Users will use this console for initial registration, preferred token selection and changes if they prefer.

Users can return to this page, authenticate using multi-factor and adjust as needed to best fit their requirements.



○ Send My Passcode Via SMS

Note: Your mobile number will be encrypted and will only be used for receiving passcodes

Enter Your Mobile Number

+18153021063 Format: + CountryCode Number (e.g. +11234567890)

○ Call My Phone

Note: Your phone number will be encrypted and only used for authentication calls

Enter Your Phone Number

+18153021063 Format: + CountryCode Number (e.g. +11234567890)

● Setup My Soft Token App

☑ Push Enabled?

Step 1) Install the SecurEnvoy App on your phone

Step 2) Press the ADD button

Step 3) Scan QRCode with your phone's camera

or manually enter this key: **QUBSXWUFZ7DCU**

Step 4) Enter the displayed Code

(click to enlarge)

Complete Step 4 To Activate Your Token

○ Use My Existing Authentication Method

□ Yubikey

□ Use a Yubikey as the sole method of authentication

Current Serial Number New Key

Insert your Yubikey, focus this input and press the button on the Yubikey.

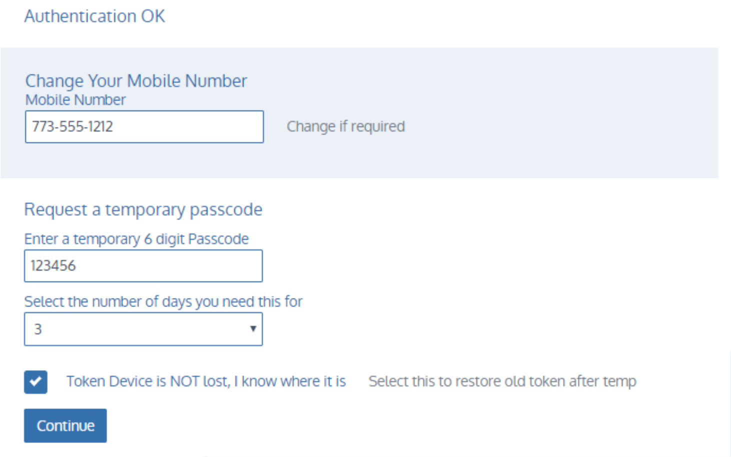
> *Note:* It's important to know that the options shown above are directly tied to selections you make in the management console's authentication type section.

Emergency HelpDesk

http(s)://domainname.com/sechelpdesk

With the understanding that we're all human, we know that there will be occasions that users drop, break and lose their mobile devices. This console, if configured for use, will allow the user to authenticate using their standard Microsoft Active Directory Credentials and answering Security Questions.

Once authenticated, they will have the ability, if allowed by the administrator to change phone numbers, give themselves and/or give themselves a temp token code.



Authentication OK

Change Your Mobile Number

Mobile Number: 773-555-1212 — Change if required

Request a temporary passcode

Enter a temporary 6 digit Passcode: 123456

Select the number of days you need this for: 3

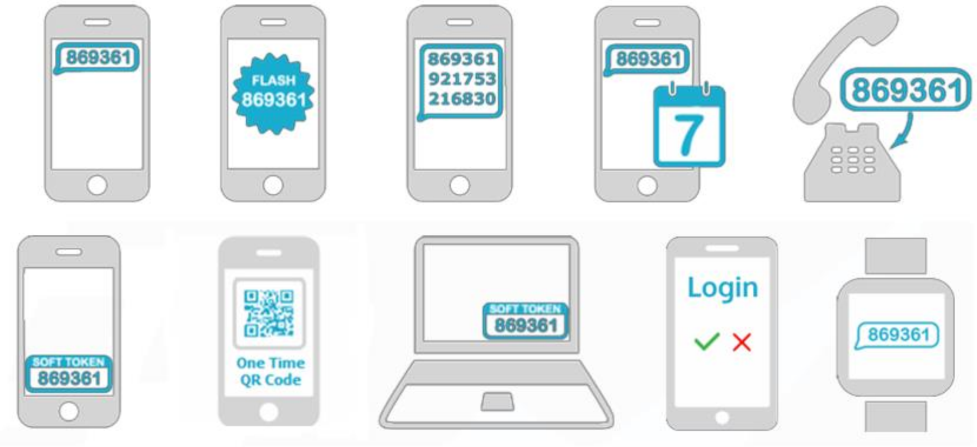
☑ Token Device is NOT lost, I know where it is — Select this to restore old token after temp

Pro Tip: In the administrative console, you can specify how often a user is allowed to use this emergency helpdesk. This provides an additional layer of security and prevents users from using this as a bypass method.

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 can 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 Day code.

In addition, SecurEnvoy can 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.

Soft Tokens are available for all Smart phone applications as well as a P.C. and MAC OS. 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.

Note: In most all cases, delivery of Push Notifications, SMS Messages and Push Notifications reach the user in a matter of seconds. However, there are rare occasions where network congestion can delay the delivery of authentication cores to the users’ mobile device.

Integration Options

Security Server Integration Options

Your initial LDAP Connections is created during the initial setup and configuration of the system.

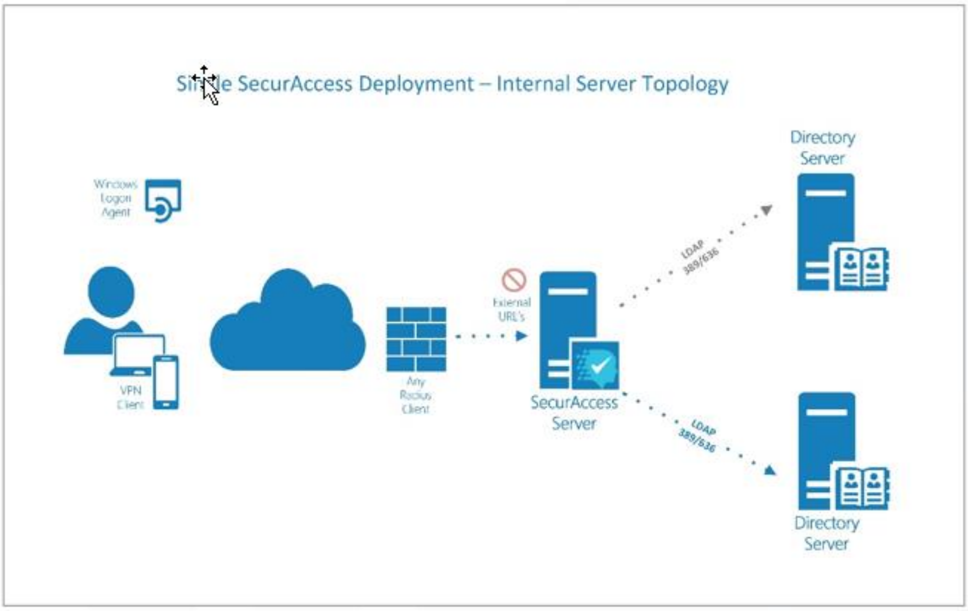
There are many ways to deploy, integrate and configure the SecurEnvoy Security Server within your environment. The following are all supported.

- Single Server Deployment
- Multiple Server Deployment
- Single Data Center
- Multiple Data Centers

Note: In all instances (single or multiple) you will require a service account on the directory that you are connecting to for users. Additional details are covered in the SecurEnvoy Security Server Installation Guide.

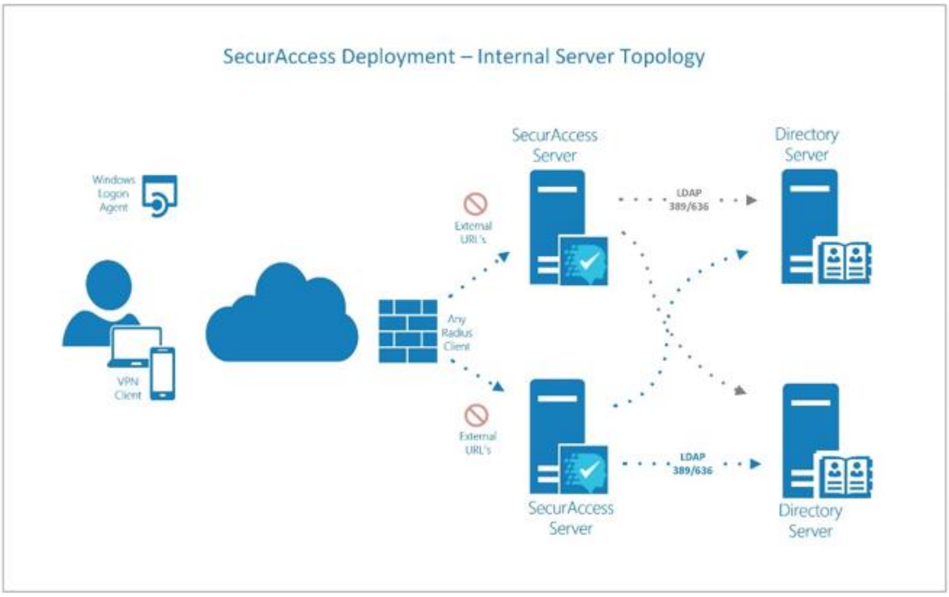
Single Server Deployment

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 Server Deployment

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. Alternately one SecurEnvoy server can be located at each site with each VPN using the other sites SecurEnvoy server as its second server



> *Note:* You can use a load balancer to provide high availability for authentication services in a multiple server deployment. You should treat this system the same as any other SSL based system by turning on SSL Persistency in your load balanced configuration.

LDAP Environment Integration

Integration with a LDAP Authentication Repository is an important part of the configuration for the SecurEnvoy Security Server. The SecurEnvoy Security Server does not make or require any changes to the directory schema itself.

SecurEnvoy can fully support direct integration with the following systems:

- Microsoft Active Directory
- Microsoft LDS (Lightweight Directory Services)
- OpenLDAP

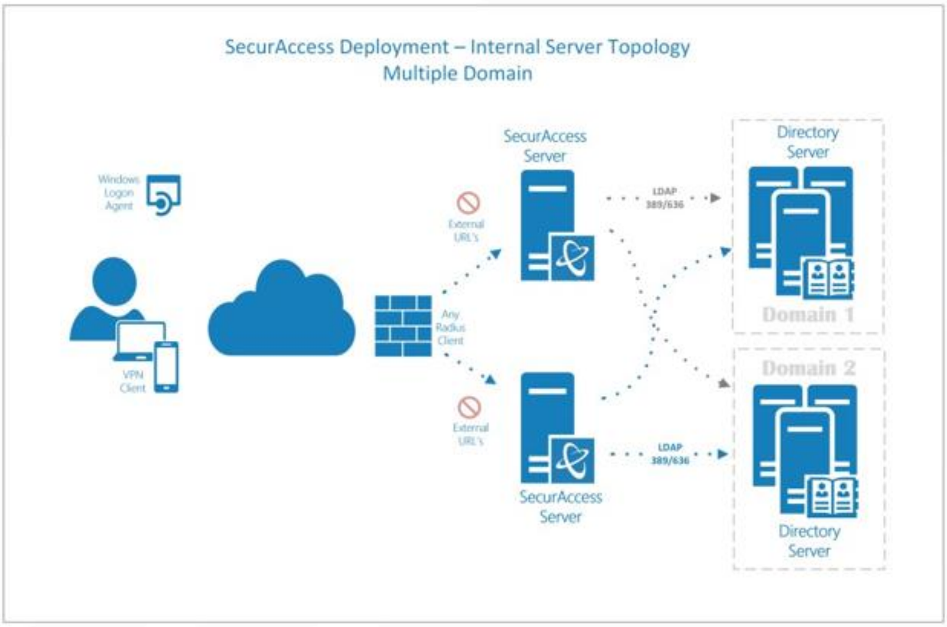
Legacy LDAP Support Options

- Sun Directory Server
- Novell eDirectory

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.

Multiple LDAP Environments

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.



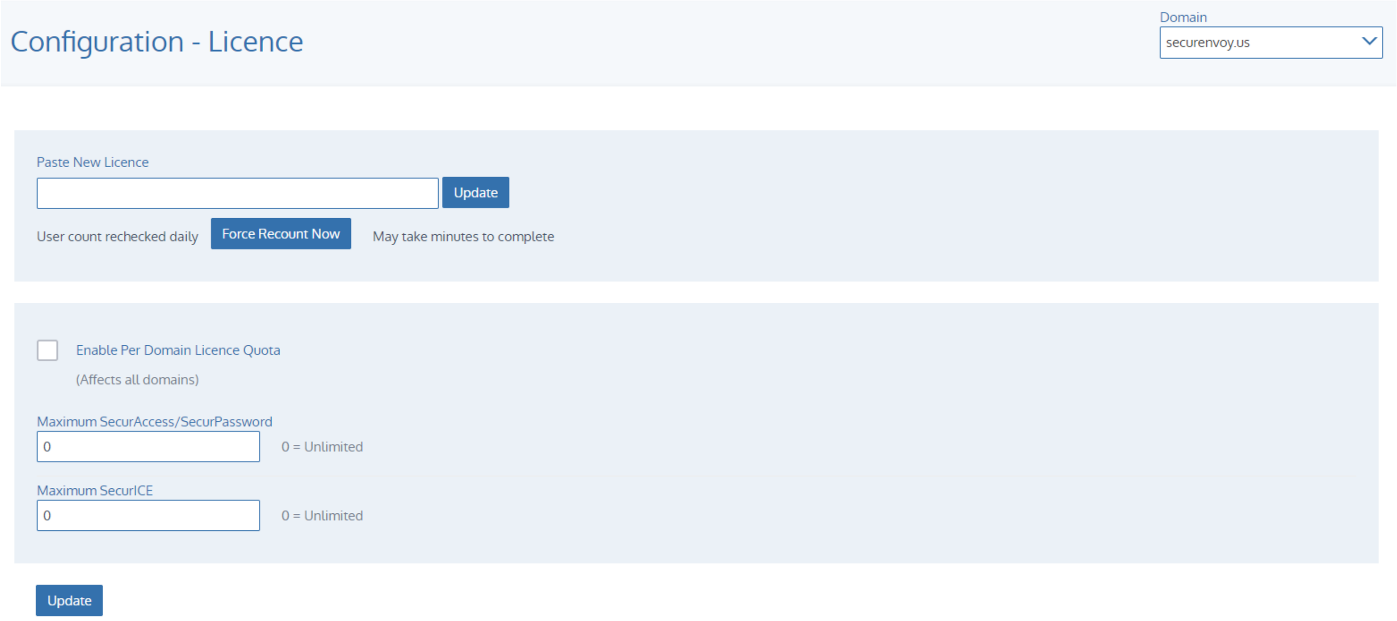
> *Note:* Assure that connectivity to the Directory Server is available before adding to the SecurEnvoy Security Server to prevent issues while configuring the new integration.

System Configuration

There are sixteen sections to the configuration of the system. Each section is highly customizable, which will help meet challenging business requirements.

License(s)

Your initial license (either trial or permanent) would most likely have been entered during the initial setup of the system. However, if you elected to skip that part to enter a license later – or alternatively if you are adding another domain and have specific licenses for that domain which you would like to use, you may enter them here.



Configuration - Licence

Domain: securenvoy.us

Paste New Licence

User count rechecked daily May take minutes to complete

☐ Enable Per Domain Licence Quota
(Affects all domains)

Maximum SecurAccess/SecurPassword: 0 — 0 = Unlimited

Maximum SecurICE: 0 — 0 = Unlimited

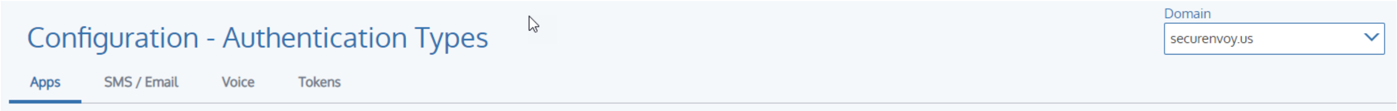
Additionally, you can enable Per Domain Quotas to further manage licensing distribution.

Note: If you are connecting to multiple different directories, assure that the correct directory is selected before adding your License.

Authentication Types

Options selected here change the options that users will receive during their initial enrolment and ongoing management of their token. When a user is enrolling for the first time, they will be selecting a default method based on the selections you make here.

We've separated this part into four sub-categories as shown here.



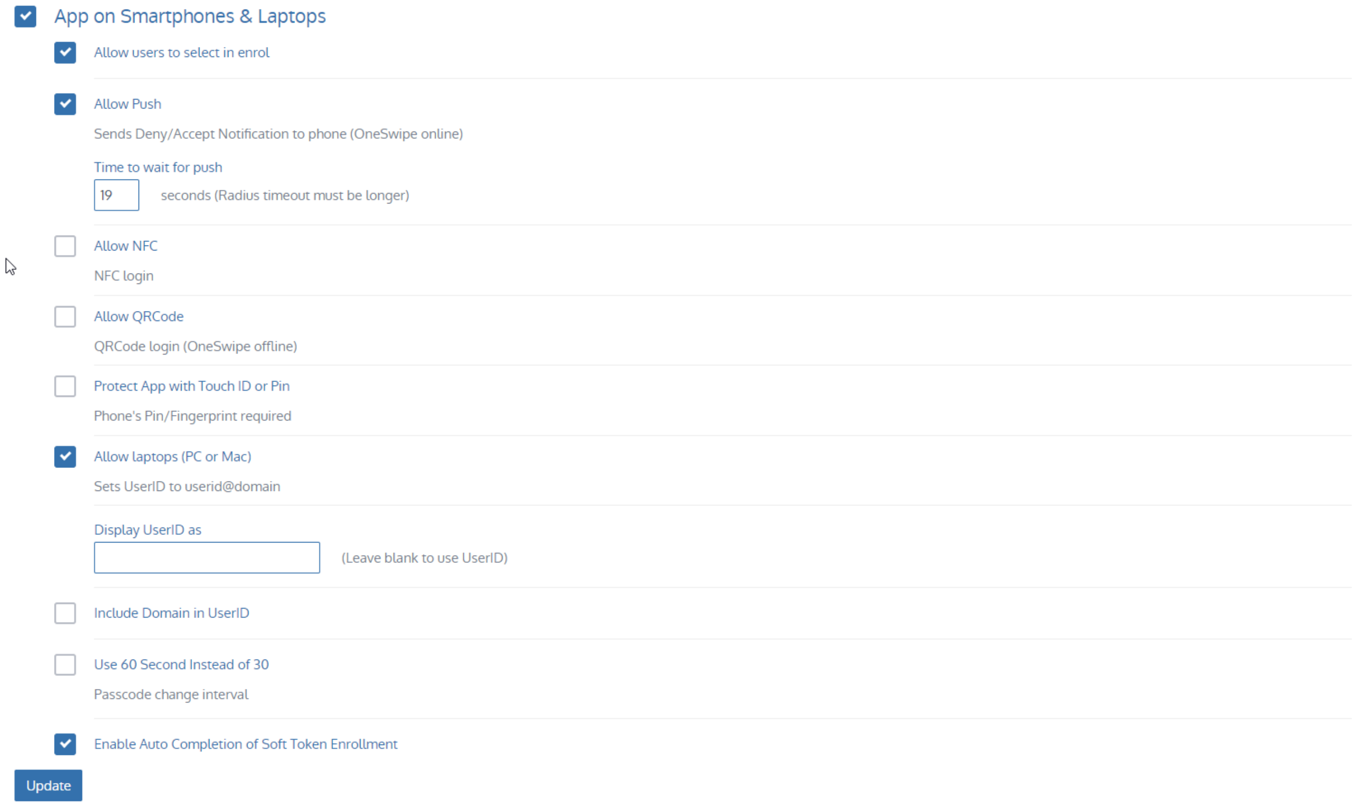
Configuration - Authentication Types

Domain: securenvoy.us

It's recommended that you review each section and select the options that are appropriate for your environment and user community.

Apps

The Apps section contains options specific to soft token apps for smart phones and laptops. These settings are domain specific and you can choose different options for each directory integration.



☑ App on Smartphones & Laptops

☑ Allow users to select in enrol

☑ Allow Push

Sends Deny/Accept Notification to phone (OneSwipe online)

Time to wait for push: 19 seconds (Radius timeout must be longer)

□ Allow NFC

NFC login

□ Allow QRCode

QRCode login (OneSwipe offline)

□ Protect App with Touch ID or Pin

Phone's Pin/Fingerprint required

☑ Allow laptops (PC or Mac)

Sets UserID to userid@domain

Display UserID as: (Leave blank to use UserID)

□ Include Domain in UserID

□ Use 60 Second Instead of 30

Passcode change interval

☑ Enable Auto Completion of Soft Token Enrollment

Note: If you have allowed Push, our Authenticator App is required for users that wish to use that option.

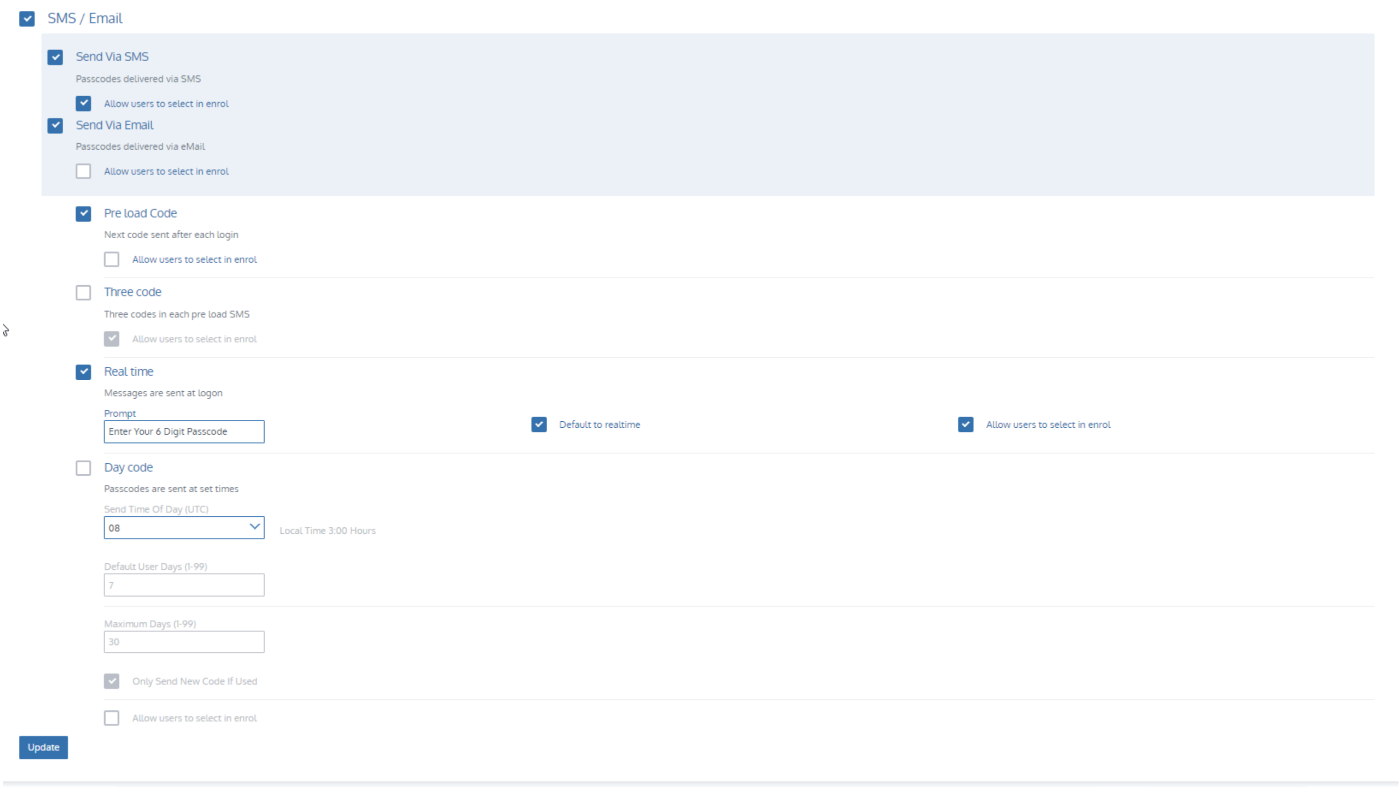
Pro Tip: Push Notifications are by far the most common authentication method. When using Push, the response from the user's smartphone will return to us where it is processed and approved. Then, we must send the approval to your Radius Server to continue with the authentication process for the user.

Make sure that your RADIUS timeout is greater than this value. Remember you can change both, so if you have a longer requirement – make sure to set both sides properly.

Example; Cisco ASA VPN RADIUS timeout set to 60 Seconds; SecurEnvoy Security Server Push timeout set to 50 Seconds.

SMS / Email

There are many options for text messages and email. Parts highlighted by the blue shaded background are mandatory. We require a default method of delivering initial email or text communication to the users for the purposes of enrolment. You should review these options and select ones that meet your requirements.



☑ SMS / Email

☑ Send Via SMS
Passcodes delivered via SMS
☑ Allow users to select in enrol

☑ Send Via Email
Passcodes delivered via eMail
☐ Allow users to select in enrol

☑ Pre load Code
Next code sent after each login
☐ Allow users to select in enrol

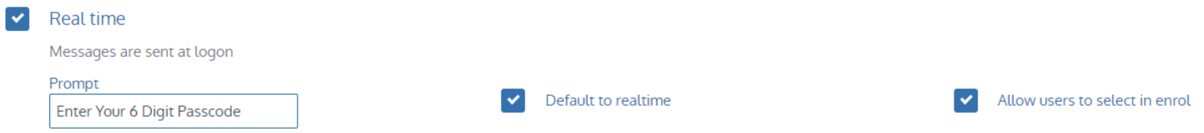
☐ Three code
Three codes in each pre load SMS
☑ Allow users to select in enrol

☑ Real time
Messages are sent at logon
Prompt: Enter Your 6 Digit Passcode
☑ Default to realtime
☑ Allow users to select in enrol

☐ Day code
Passcodes are sent at set times
Send Time Of Day (UTC): 08
Local Time 3:00 Hours
Default User Days (1-99): 7
Maximum Days (1-99): 30
☑ Only Send New Code If Used
☐ Allow users to select in enrol

Update

The selections you make here will either limit or expand the options that the user has when registering or managing their side of the authentication methods



☑ Real time
Messages are sent at logon
Prompt: Enter Your 6 Digit Passcode
☑ Default to realtime
☑ Allow users to select in enrol

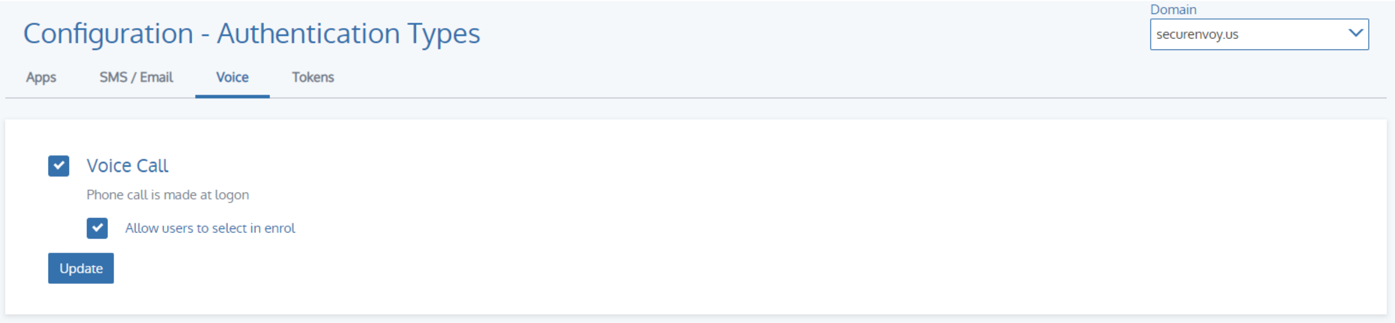
Pro Tip: Text Messages in real time is a popular choice.

The ‘Enter Your 6 Digit Passcode’ Prompt is presented when the user is required to enter a token code manually. This prompt can be customized.

You should also use caution when sending codes via email. Depending on your mail server configuration, emails may not be encrypted at times.

Voice Authentication

There are occasions where a user may not be able to use a smartphone or soft token. Voice authentication, when enabled will use the voice gateway to place a phone call to the users predetermined and defined phone number. During this time, a token code is presented on screen and the user will be prompted to enter this token code using the keypad on the phone.



Configuration - Authentication Types

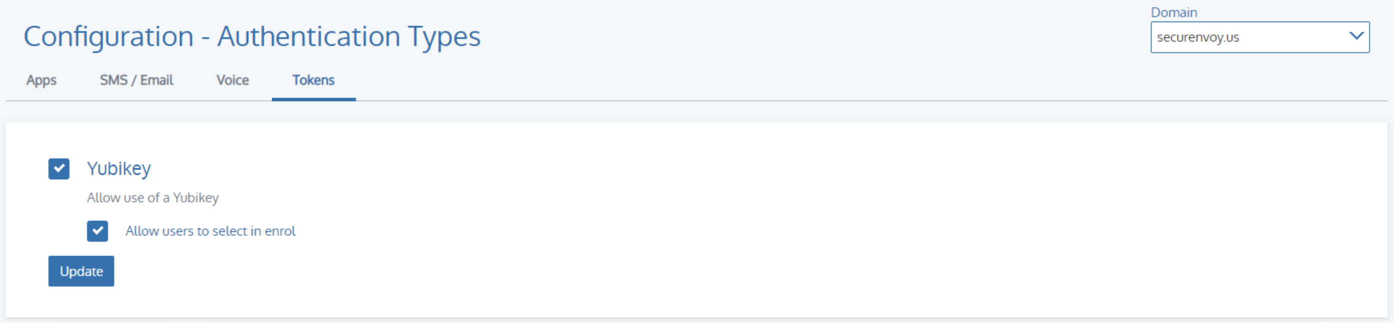
Domain: securenvoy.us

☑ Voice Call
Phone call is made at logon
☑ Allow users to select in enrol

Note: This uses the same phone number as defined in the user properties for the user in the Active Directory.

Yubikey

While the intent of the SecurEnvoy Security Server is to reduce (and in most cases eliminate) the requirements for physical tokens there are still occasions where these may be required.



Configuration - Authentication Types

Domain: securenvoy.us

☑ Yubikey
Allow use of a Yubikey
☑ Allow users to select in enrol

The Yubikey will automatically complete the carriage return eliminating any need to manually press the return/enter key.

How the process works

- The protected application prompts the user for their username and password and then asks for the OTP.
- The User physically taps the Yubikey's button to trigger input to generate the OTP string.
- The OTP string is sent from the SecurEnvoy server to the Yubico server for authentication checking.
- Once the token check has completed, the Yubikey servers we verify that the key matches.

Yubikey tokens are normally provided with a seed record pre-installed on them. These tokens are supported by SecurEnvoy by passing on the authentication request to Yubico’s cloud service.

Yubico’s cloud service URL’s:

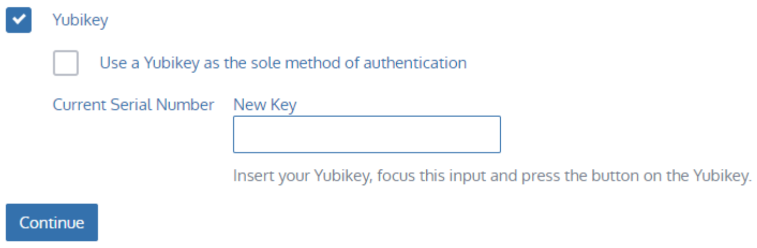
- https://api.yubico.com
- https://api2.yubico.com
- https://api3.yubico.com
- https://api4.yubico.com
- https://api5.yubico.com

All 5 URL’s are accessed at the same time with the first one to respond being utilised.

Note: Yubikey uses the generic, built-in keyboard drivers that are already installed and will operate as an automatic keyboard, cut and paste to insert tokens into required fields. You can test Yubikey function using a notepad document.

Yubikey Enrolment

Enrolling a Yubikey is different than enrolling the SecurEnvoy Authenticator. The process is simple and shown below. A user simply inserts the Yubikey into the computer, puts the cursor in the New Key field and clicks the button on the Yubikey to insert a code for registration.



☑ Yubikey

□ Use a Yubikey as the sole method of authentication

Current Serial Number New Key

Insert your Yubikey, focus this input and press the button on the Yubikey.

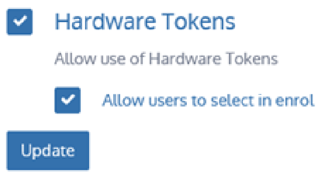
Continue

Hardware Tokens

Note: SecurEnvoy Hardware Tokens are only compatible with a Base 32 string value.

Enabling Hardware Tokens

Hardware Token Support can be enabled via Config > Authentication Types > Tokens > Hardware Token. Once enabled, there will be an option to allow users to select a Hardware Token in their Manage My Token Portal (SecEnrol).



☑ Hardware Tokens

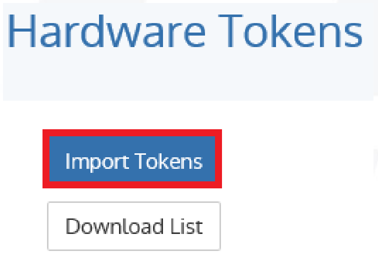
Allow use of Hardware Tokens

☑ Allow users to select in enrol

Update

Import Tokens via Hardware Token Management

Hardware Token Management allows the import of Hardware Tokens via a .txt file. There will be various options on how to map specific fields in the .txt file before importing to the GUI. These options include Hardware Token ID numbers, Seed Number Algorithms and the option to assign a Hardware Token to a specific user.



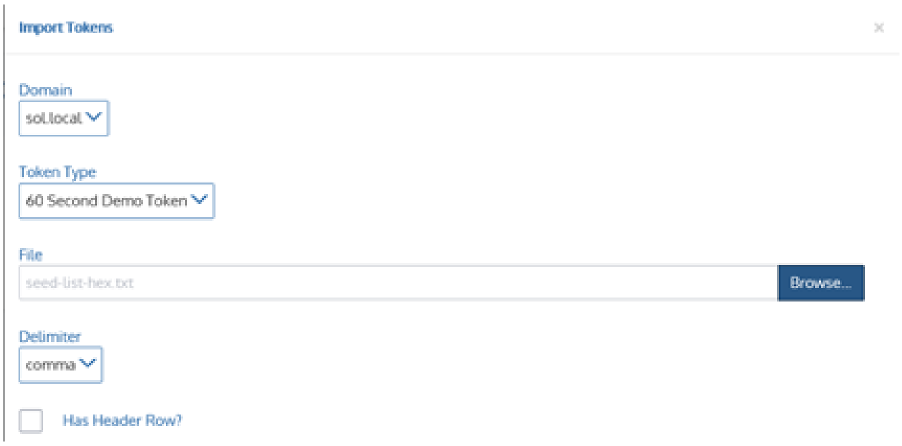
Hardware Tokens

Import Tokens

Download List

Import List – Manual Method (No User Assignment) via Hardware Token Management

There is the ability to import a list of Hardware Token ID's and Seed Numbers via a .txt file, in Hardware Token Management.



Import Tokens ×

Domain
sol.local

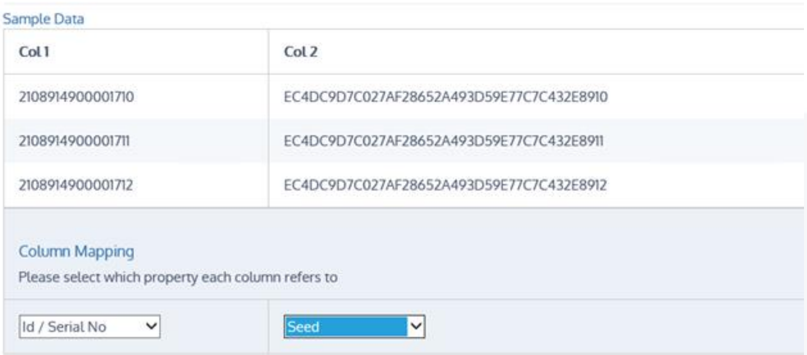
Token Type
60 Second Demo Token

File
seed-list-hex.txt
Browse...

Delimiter
comma

□ Has Header Row?

Once these have imported into the Admin GUI, the next step will be to configure the layout of the .txt file delimiter (comma, space, semicolon etc.). Once completed, proceed to the “Column Mapping” section, where this allows mapping of Hardware Token configuration data from the .txt file.



Sample Data

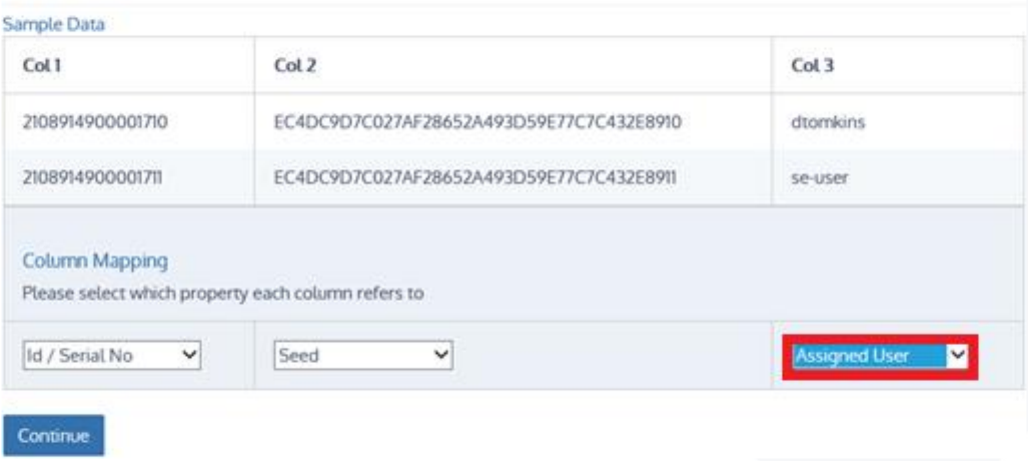
Col 1	Col 2
2108914900001710	EC4DC9D7C027AF28652A493D59E77C7C432E8910
2108914900001711	EC4DC9D7C027AF28652A493D59E77C7C432E8911
2108914900001712	EC4DC9D7C027AF28652A493D59E77C7C432E8912

Column Mapping
Please select which property each column refers to

Id / Serial No	Seed

Import List – Manual Method (User Assignment) via Hardware Token Management

Once these have imported into the Admin GUI, the next step will be to configure the layout of the .txt file delimiter (comma, space, semicolon etc.). Once completed, proceed to the “Column Mapping” section, where this allows mapping of Hardware Token configuration data from the .txt file. In addition to the option of mapping token ID and seed number, there is the ability to assign tokens to specific users. This is not a mandatory requirement, as this allows the assignment of Hardware Tokens via the User Tab. Finally, users can assign the tokens themselves via the Manage my Token Portal (SecEnrol).



Sample Data

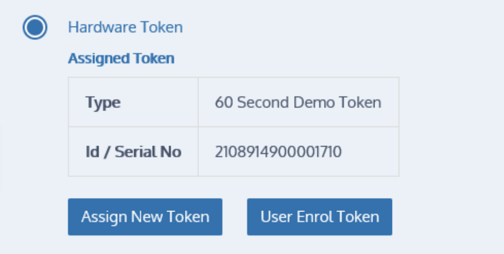
Col 1	Col 2	Col 3
2108914900001710	EC4DC9D7C027AF28652A493D59E77C7C432E8910	dtomkins
2108914900001711	EC4DC9D7C027AF28652A493D59E77C7C432E8911	se-user

Column Mapping
Please select which property each column refers to

Id / Serial No	Seed	Assigned User

Assigning Hardware Tokens via User Tab

Once imported, the Hardware Tokens ID and Seed numbers will be displayed in the Hardware Token Management. There will be an option to manually assign each Hardware Token to a User. This can be completed via Users > Specify User > Authentication Type > Hardware Token > Assign Token.



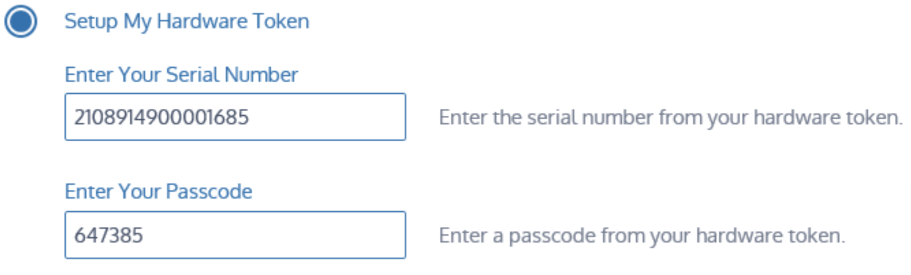
● Hardware Token

Assigned Token

Type	60 Second Demo Token
Id / Serial No	2108914900001710

Assigning Hardware Tokens via Manage my Token Portal

Users will be able to select and assign a specific hardware token via the Manage my Token Portal (SecEnrol). To allow this option, please ensure that the “Allow Users to select in enrol” option is enabled, from Config > Authentication Types > Tokens > Hardware Token.



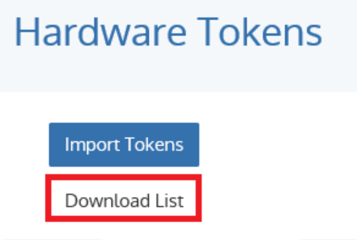
● Setup My Hardware Token

Enter Your Serial Number: 2108914900001685 — Enter the serial number from your hardware token.

Enter Your Passcode: 647385 — Enter a passcode from your hardware token.

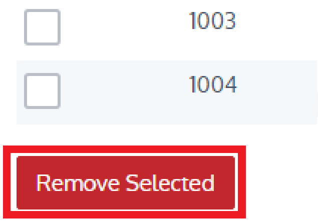
Download List via Hardware Token Management

Download List will generate a .txt file of the current Hardware Tokens that have been imported into Hardware Token Management. This is a useful tool if there are multiple imported .txt files, as this will provide an up-to-date list of Hardware Tokens, and their assigned deployment to users, this provides a very useful tool for system auditing of Hardware Tokens.



Remove a Hardware Token via Hardware Token Management

To remove a Hardware Token from an existing deployment, select the relevant Hardware Token(s) that require removing and click the “Remove Selected” button.

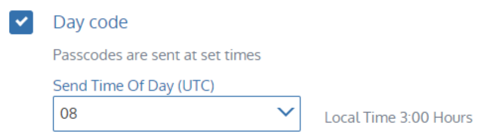


□ 1003

□ 1004

Day Codes

Using day codes may be preferred for temporary employees or other business requirements. Using this method means that a user will receive a six digit code that will be valid for the entire 24 hour period.



☑ Day code

Passcodes are sent at set times

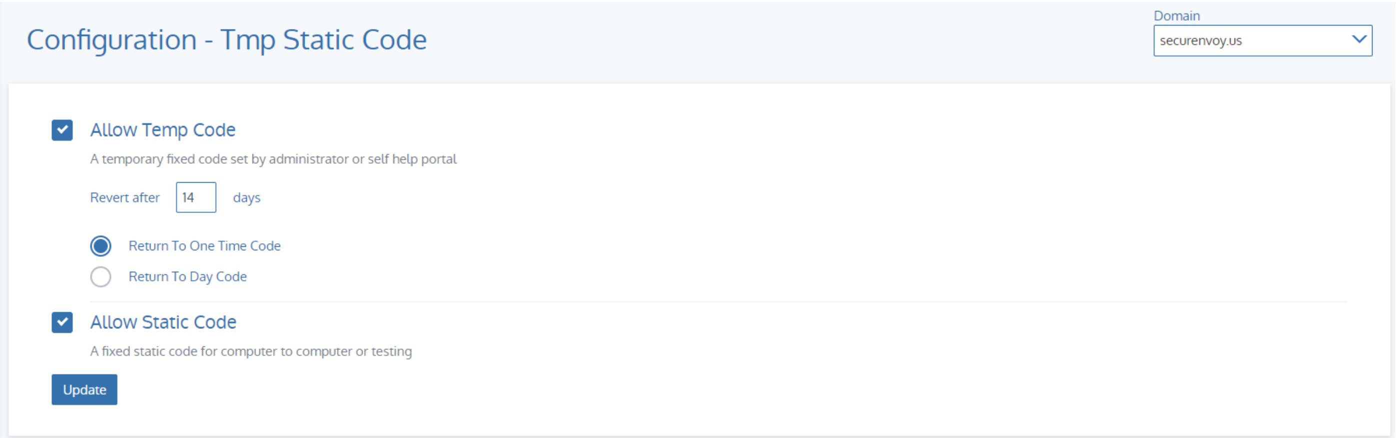
Send Time Of Day (UTC): 08

Local Time 3:00 Hours

> *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. 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.
>
> 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.

Temp and Static Codes

There may be occasions where support personnel need to use a temporary or static code to get a user authenticated. SecurEnvoy allows for this function as shown below. A user is assigned a temp code in only two ways; either by the support desk entering it directly to the user account on the system, or when the user accesses the Emergency Help Desk, if available.



Configuration - Tmp Static Code

Domain: securenvoy.us

☑ Allow Temp Code

A temporary fixed code set by administrator or self help portal

Revert after 14 days

● Return To One Time Code

○ Return To Day Code

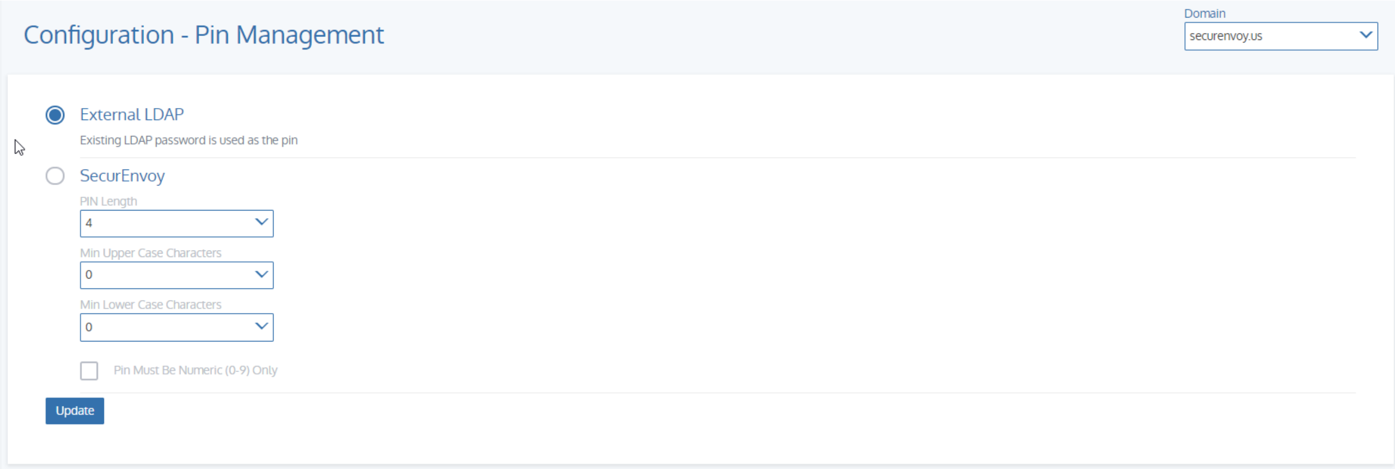
☑ Allow Static Code

A fixed static code for computer to computer or testing

> *Note:* When testing it is helpful to have the ability to assign a temp or static token, since other services, like SMS and Voice may not yet be configured or available.

Pin Management

This 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.



Configuration - Pin Management

Domain: securenvoy.us

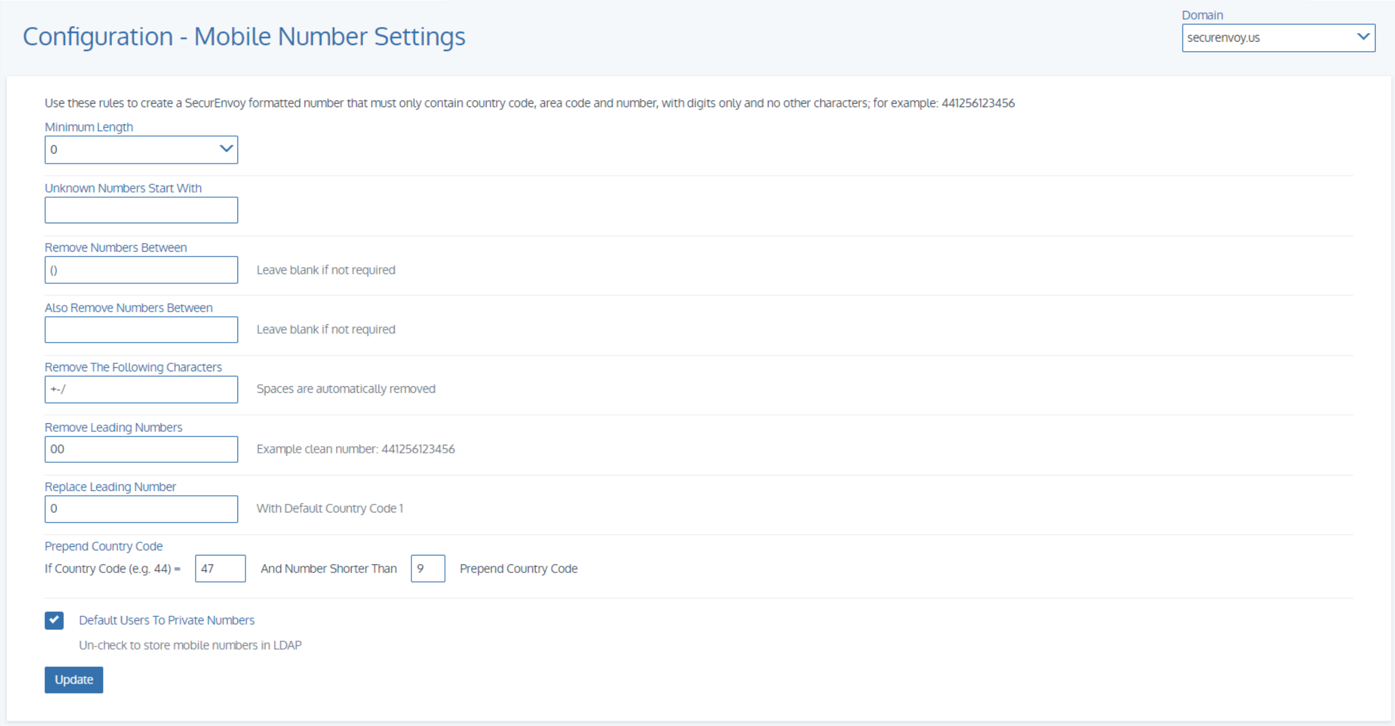
● External LDAP
Existing LDAP password is used as the pin

○ SecurEnvoy
PIN Length: 4
Min Upper Case Characters: 0
Min Lower Case Characters: 0
□ Pin Must Be Numeric (0-9) Only

It's generally recommended that you use the LDAP Password as the user's PIN.

Mobile 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.



Configuration - Mobile Number Settings

Domain: securenvoy.us

Use these rules to create a SecurEnvoy formatted number that must only contain country code, area code and number, with digits only and no other characters; for example: 441256123456

Minimum Length: 0

Unknown Numbers Start With:

Remove Numbers Between: () Leave blank if not required

Also Remove Numbers Between: Leave blank if not required

Remove The Following Characters: +-/ Spaces are automatically removed

Remove Leading Numbers: 00 Example clean number: 441256123456

Replace Leading Number: 0 With Default Country Code 1

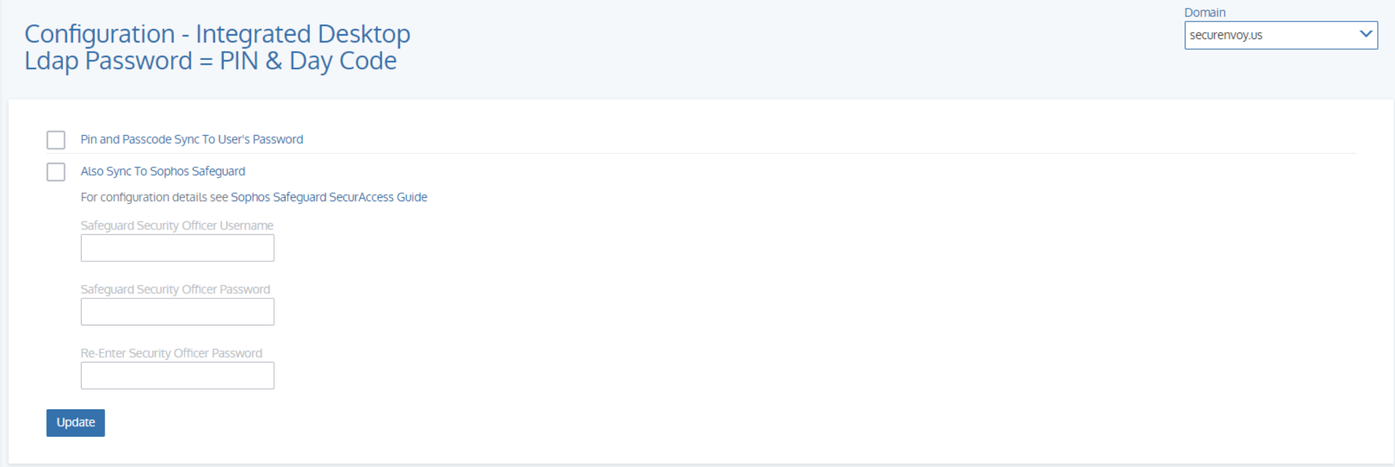
Prepend Country Code
If Country Code (e.g. 44) = 47 And Number Shorter Than 9 Prepend Country Code

☑ Default Users To Private Numbers
Un-check to store mobile numbers in LDAP

Pro Tip: Make sure to Default the mobile numbers as private (shown above) to keep them from populating the Global Address List(s).

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.



Configuration - Integrated Desktop
Ldap Password = PIN & Day Code

Domain: securenvoy.us

□ Pin and Passcode Sync To User's Password

□ Also Sync To Sophos Safeguard

For configuration details see Sophos Safeguard SecurAccess Guide

Safeguard Security Officer Username

Safeguard Security Officer Password

Re-Enter Security Officer Password

Understanding Direct Password Control

Password Automation will change and send out the new Domain password via SMS to all enabled users. Thisis 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 Day code. One-time passcodes are not supported.

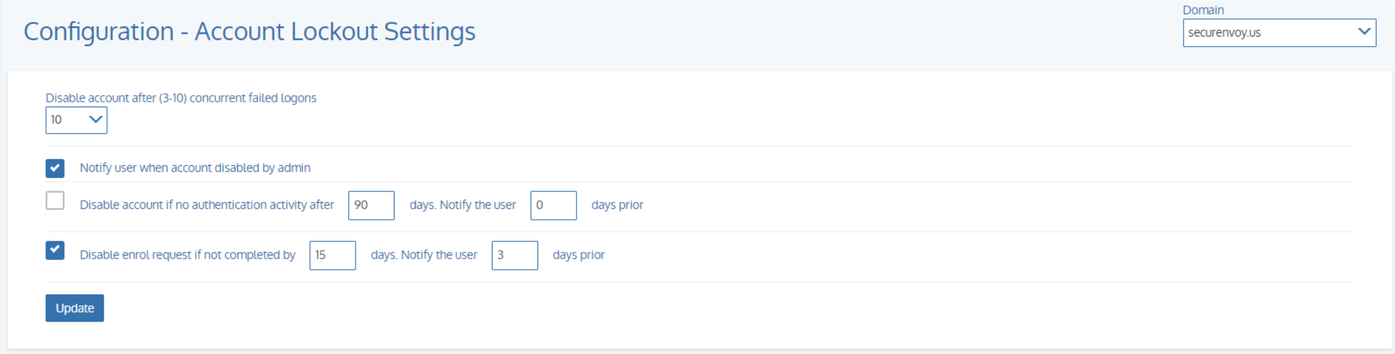
LDAP Password Modification

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 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.



Configuration - Account Lockout Settings

Domain: securenvoy.us

Disable account after (3-10) concurrent failed logons: 10

☑ Notify user when account disabled by admin

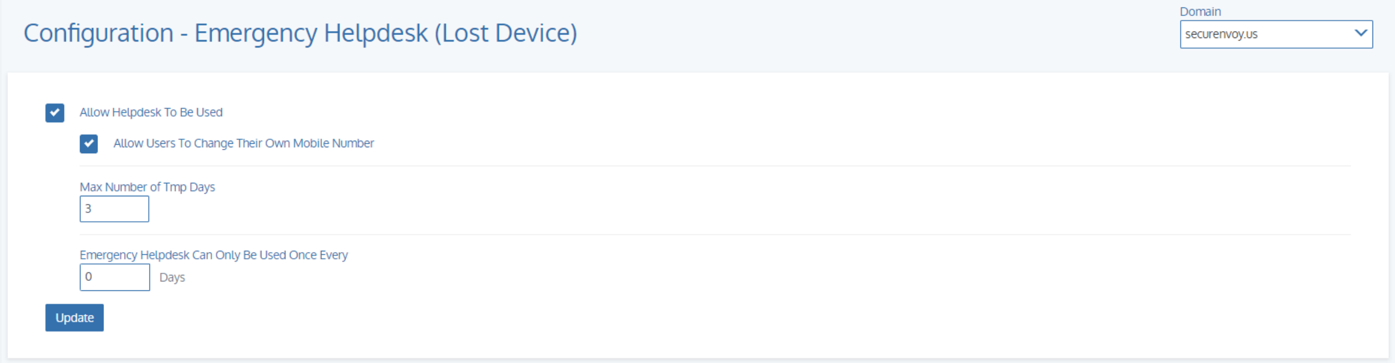
☐ Disable account if no authentication activity after 90 days. Notify the user 0 days prior

☑ Disable enrol request if not completed by 15 days. Notify the user 3 days prior

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).

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.



Configuration - Emergency Helpdesk (Lost Device)

Domain: securenvoy.us

☑ Allow Helpdesk To Be Used

☑ Allow Users To Change Their Own Mobile Number

Max Number of Tmp Days: 3

Emergency Helpdesk Can Only Be Used Once Every 0 Days

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).

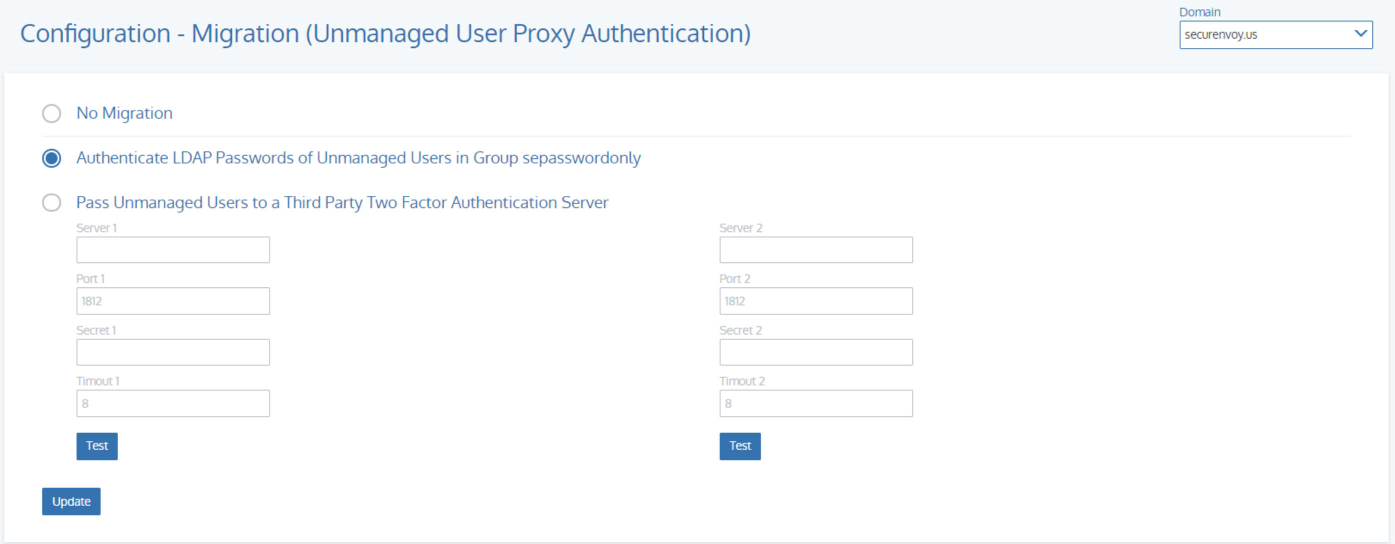
Pro Tip: The security questions are read from a template file to allow for customisation. Make sure you modify these default questions PRIOR to users registering their devices.

32-Bit Location C:\Program Files\SecurEnvoy\Security Server\Data\ENROLMENTTEMPLATE\questions.txt
64-Bit Location C:\Program Files (x86)\SecurEnvoy\Security server\Data\ENROLMENTTEMPLATE\questions.txt

We generally recommend that administrators develop questions that are more business and employee specific, removing the standard ‘Mothers Maiden Name’ questions that we’ve used as defaults.

Migration

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.


Configuration - Migration (Unmanaged User Proxy Authentication)

Domain: securenvoy.us

○ No Migration

● Authenticate LDAP Passwords of Unmanaged Users in Group sepasswordonly

○ Pass Unmanaged Users to a Third Party Two Factor Authentication Server

Server 1:	Server 2:
Port 1: 1812	Port 2: 1812
Secret 1:	Secret 2:
Timout 1: 8	Timout 2: 8

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.

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

The Automatic Deployment Wizard 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. 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 here. If a user is removed from the group, they are automatically unmanaged.

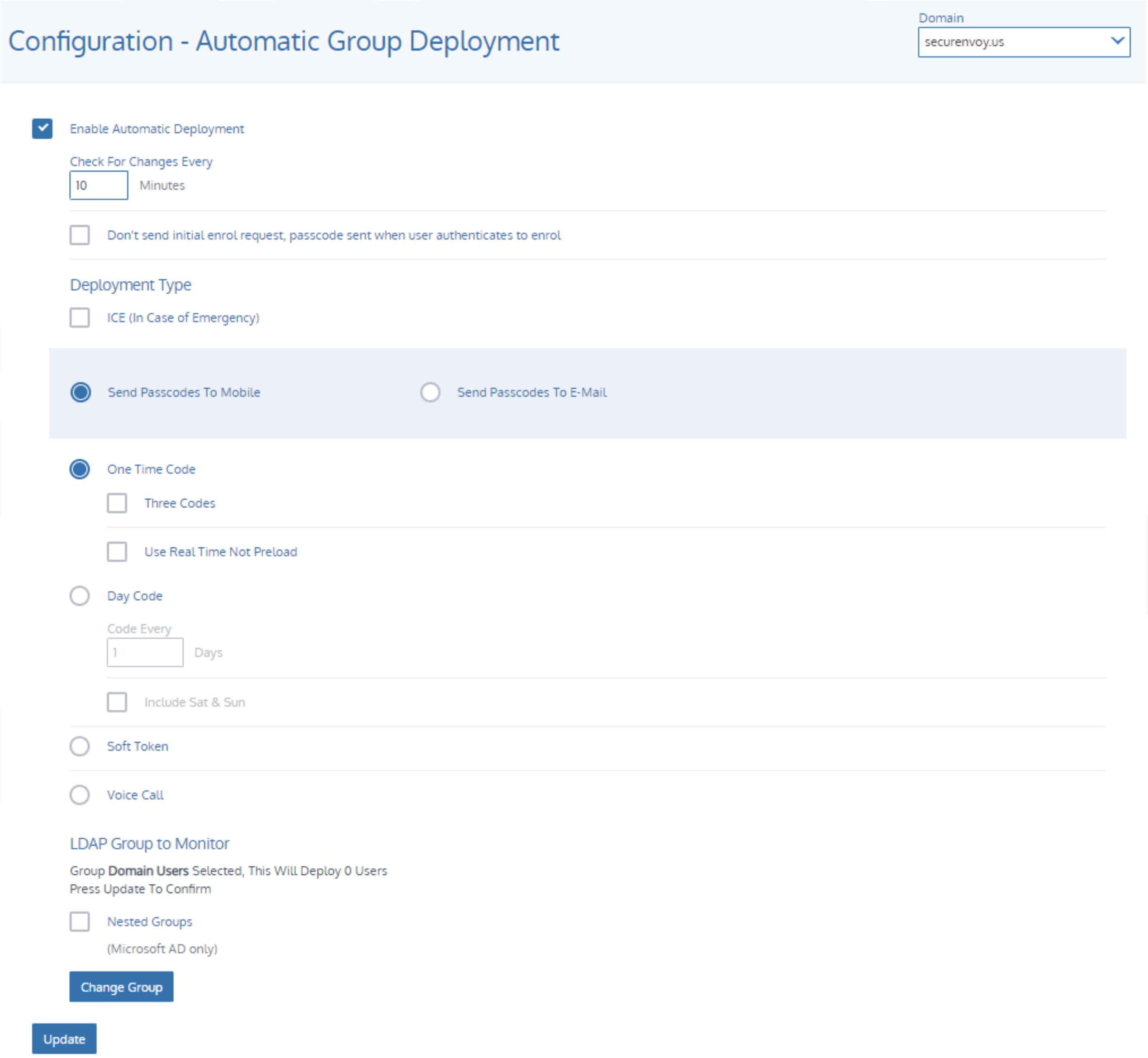
Deployment Type
ICE (In Case of Emergency) for emergency users, business continuity, disaster recovery.

Send Passcodes to Mobile / Email
Specifies the type of initial communication with the user for the purpose of delivering the Welcome Enrolment Email.

One Time Code / Three Codes / Real time
Select users to have a one time 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



Configuration - Automatic Group Deployment

Domain: securenvoy.us

☑ Enable Automatic Deployment

Check For Changes Every: 10 Minutes

□ Don't send initial enrol request, passcode sent when user authenticates to enrol

Deployment Type

□ ICE (In Case of Emergency)

● Send Passcodes To Mobile ○ Send Passcodes To E-Mail

● One Time Code

□ Three Codes

□ Use Real Time Not Preload

○ Day Code

Code Every: 1 Days

□ Include Sat & Sun

○ Soft Token

○ Voice Call

LDAP Group to Monitor

Group **Domain Users** Selected, This Will Deploy 0 Users
Press Update To Confirm

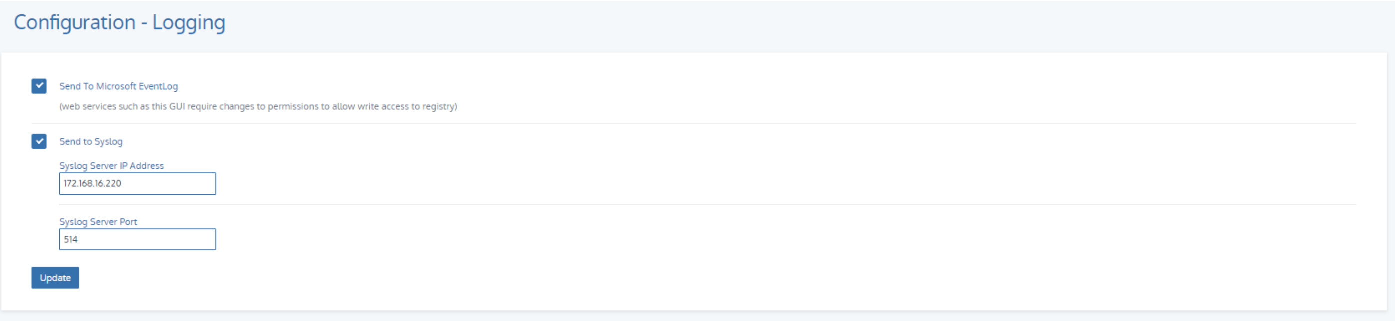
□ Nested Groups
(Microsoft AD only)

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 users to be provisioned.

Pro Tip: 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 the user is deployed via email, they will always stay in this mode.

Configuration Logging

SecurEnvoy log files reside locally on the server. Additionally, we can also send our log events to the Microsoft Logs and a Syslog server if you have one as shown below.



Configuration - Logging

☑ Send To Microsoft EventLog

(web services such as this GUI require changes to permissions to allow write access to registry)

☑ Send to Syslog

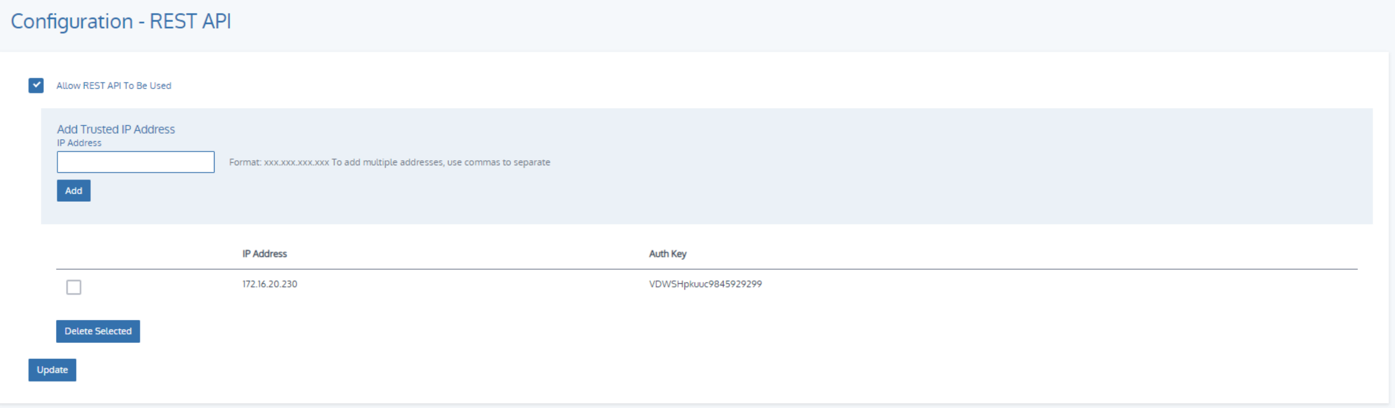
Syslog Server IP Address: 172.168.16.220

Syslog Server Port: 514

Rest API

We provide access to a Rest API for integration with specialized systems and custom developed solutions.

Start by adding your IP address to the admin config REST API section for each device you want to authorise. You will need to use the API, or 127.0.0.1 if you want to be able to use it from the server machine itself and tick the box to enable usage of the API.



Configuration - REST API

☑ Allow REST API To Be Used

Add Trusted IP Address

IP Address:

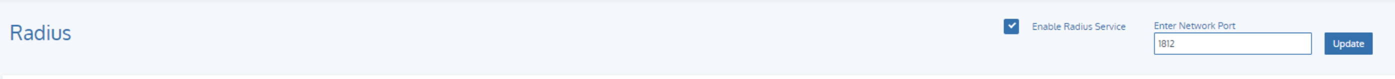
Format: xxx.xxx.xxx.xxx To add multiple addresses, use commas to separate

	IP Address	Auth Key
□	172.16.20.230	VDWSHpkuuc9845929299

Note: Navigate to here: "C:\Program Files (x86)\SecurEnvoy\Security Server\SDK\admin" for the full Rest-API guide.

RADIUS

This is a widely used standards-based authentication protocol. For integration with other vendor solutions, a Radius connection is required. Use this window to define your RADIUS client's IP Address, shared secret, default domain and any profile settings.

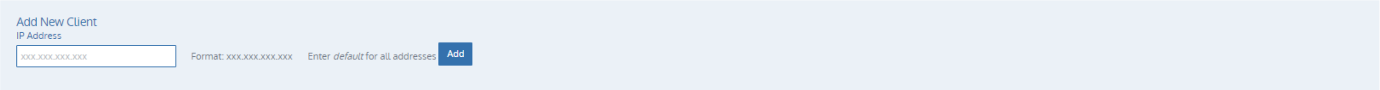


Radius

☑ Enable Radius Service

Enter Network Port: 1812

The Radius Service Port can be changed to a different port if your needs require it.



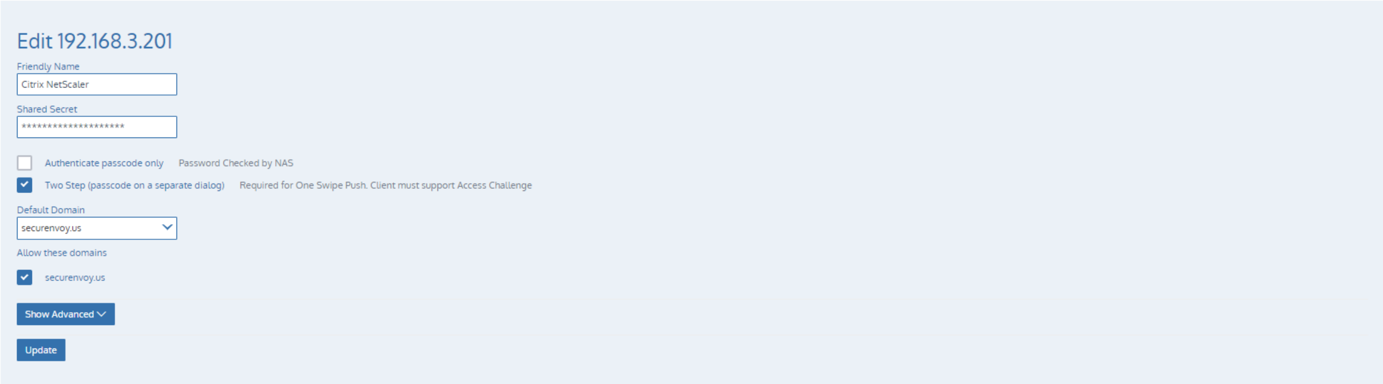
Add New Client

IP Address: xxx.xxx.xxx.xxx

Format: xxx.xxx.xxx.xxx Enter *default* for all addresses

The Radius Service Port can be changed to a different port if your needs require it.

Radius will use a Shared Secret to authenticate one device to another and establish secure communications. This 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.



Edit 192.168.3.201

Friendly Name: Citrix NetScaler

Shared Secret: ********************

☐ Authenticate passcode only Password Checked by NAS

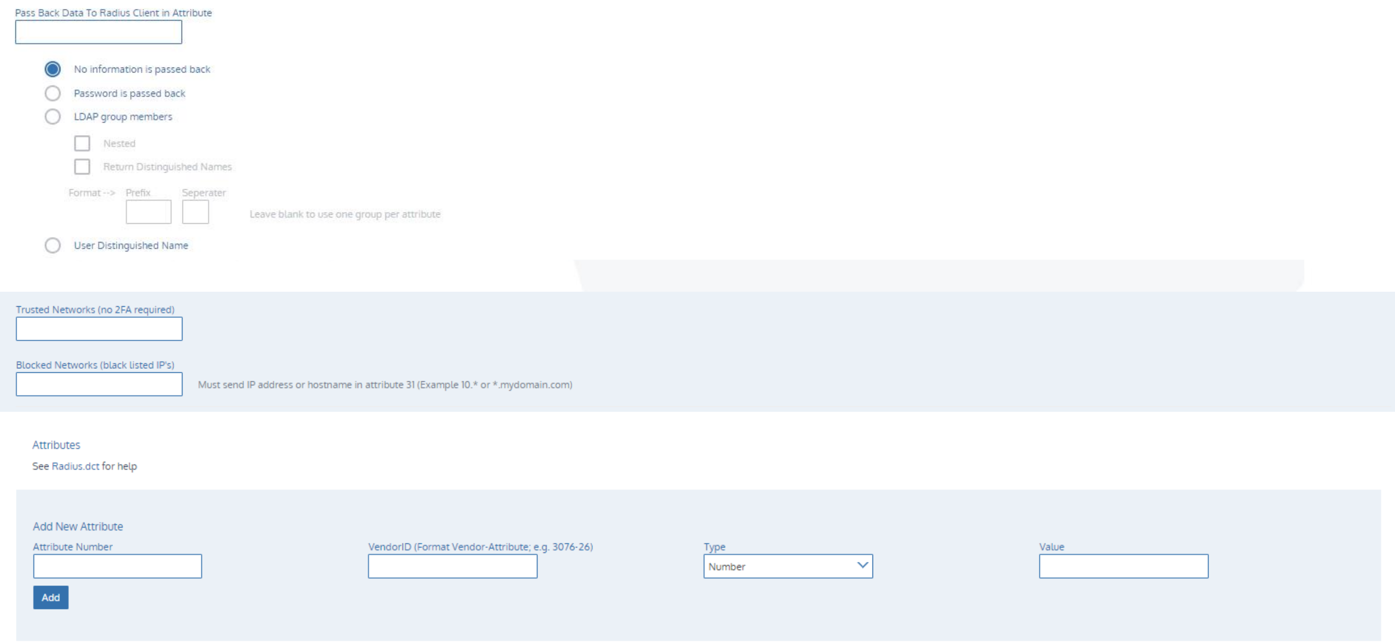
☑ Two Step (passcode on a separate dialog) Required for One Swipe Push. Client must support Access Challenge

Default Domain: securenvoy.us

Allow these domains

☑ securenvoy.us

Advanced Settings are available for connections that require specific data returned or LDAP Group Membership checked.



Pass Back Data To Radius Client in Attribute

● No information is passed back

○ Password is passed back

○ LDAP group members

☐ Nested

☐ Return Distinguished Names

Format --> Prefix Seperater Leave blank to use one group per attribute

○ User Distinguished Name

Trusted Networks (no 2FA required)

Blocked Networks (black listed IP's) Must send IP address or hostname in attribute 31 (Example 10.* or *.mydomain.com)

Attributes

See Radius.dct for help

Add New Attribute

Attribute Number	VendorID (Format Vendor-Attribute; e.g. 3076-26)	Type	Value
		Number	

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, SecurEnvoy's 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 Use rid and PIN/Password, after which they will then be challenged for the passcode, irrelevant of mode in operation – Pre-Load OTP, Day Code, TMP code.

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.

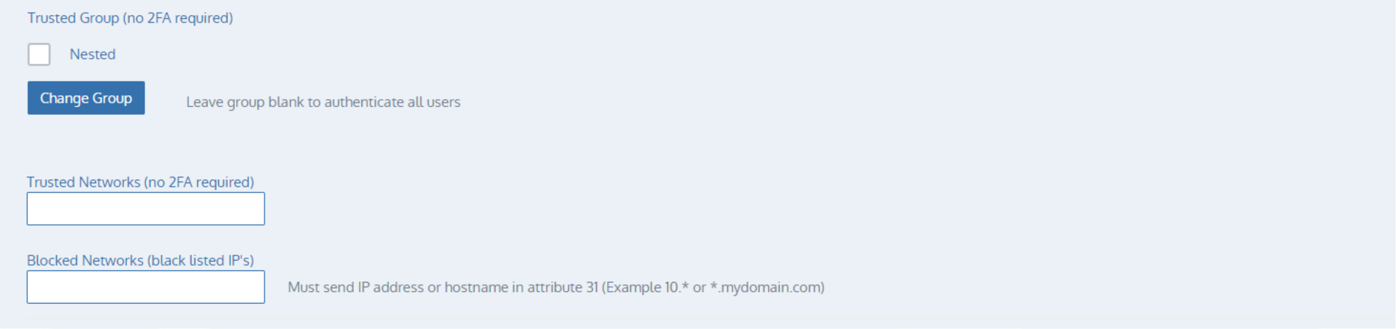
Trusted Group

SecurAccess can 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

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.



Trusted Group (no 2FA required)

□ Nested

Change Group   Leave group blank to authenticate all users

Trusted Networks (no 2FA required)

Blocked Networks (black listed IP's)

Must send IP address or hostname in attribute 31 (Example 10.* or *.mydomain.com)

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 Dictionaries; SecurEnvoy is installed with a list of the main dictionaries. This can be viewed by selecting the link radius.dct. Also included are most manufacturers published extensions.

User Management

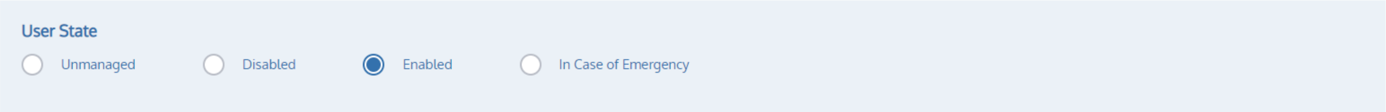
This section allows you to search and administer your LDAP (Directory Server) based users. You can enable users for two factor mobile numbers and email addresses, resend passcodes and set static passcodes

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.

Unmanaged / Disabled / Enabled / In Case of Emergency
The first option is to set the users 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.



User State
○ Unmanaged ○ Disabled ● Enabled ○ In Case of Emergency

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.

Administrator Level
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.
- Log allows access to Log Viewer only.

User Type: Permanent User
Administrator Level: Full

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.

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.

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 xx days. Day codes are reusable passcodes that are automatically changed every (xx) days. At a pre-defined day and time, the next required passcode is sent to this users' 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 Pin and day codes can be used to automatically update user Microsoft Active Directory passwords

Soft Token Authenticator
This mode supports the use of our Soft Token Authenticator, this will be available for mainstream smart phones such as Apple and Android. Please see Apple App Store or Google Play Store for Download or our 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 and activate the Soft Token Authenticator.

No additional user overhead is required. The "Soft Token" can also be re-synched by entering two following passcodes.

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 an 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
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.

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

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

SecurEnvoy Soft Token Authenticator

Overview

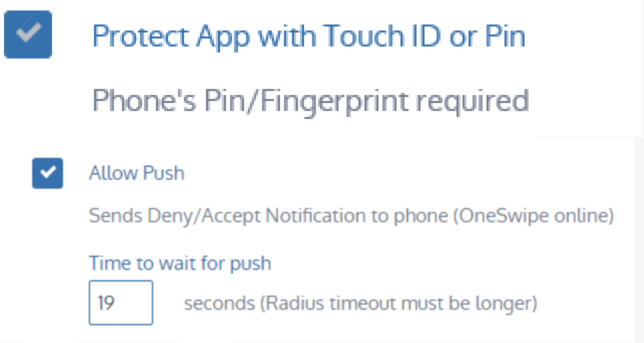
The SecurEnvoy Mobile Authenticator Application is available for iOS and Android OS. The latest SecurEnvoy Mobile Authenticator Application comes with a variety of the new features. These include the use of full biometrics on a per token basis, providing added security for the user. The updated UI provides an easy to understand and simple navigation of the application. The latest application will continue to accommodate all features from the previous SecurEnvoy Authenticator, including Push Authentication, a 60 second token option (or default 30 second token).

Biometrics

With the use of biometrics becoming increasingly more popular within company or personal use for users. The new Mobile Authenticator Application features full biometrics on a per token basis, to give users an additional layer of protection for their Tokens.

Enabling Biometrics

Biometrics integration for the Authenticator App can be configured via the SecurEnvoy Local Admin Console (SecAdmin) > Config > Authentication Types > Apps.



☑ Protect App with Touch ID or Pin

Phone's Pin/Fingerprint required

☑ Allow Push

Sends Deny/Accept Notification to phone (OneSwipe online)

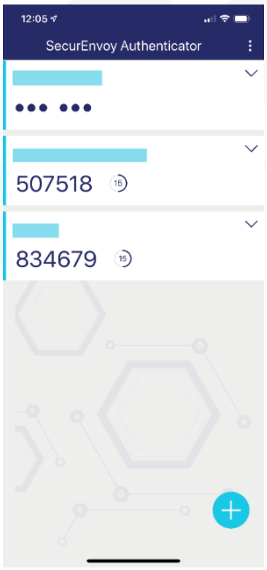
Time to wait for push

19 seconds (Radius timeout must be longer)

Using Biometrics in SecurEnvoy Authenticator App

Once biometrics have been enabled for the Authenticator Application, users will have the additional security on token codes not being displayed until a Push or interactive login has required the biometric unlock. In addition, for Android OS, screen capturing, and screen casting is disabled to prevent any malware capturing passcode data.

Authenticator App



12:05

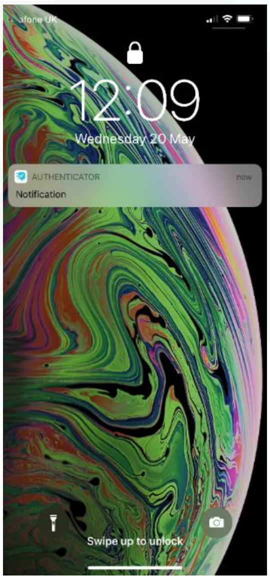
SecurEnvoy Authenticator

••• •••

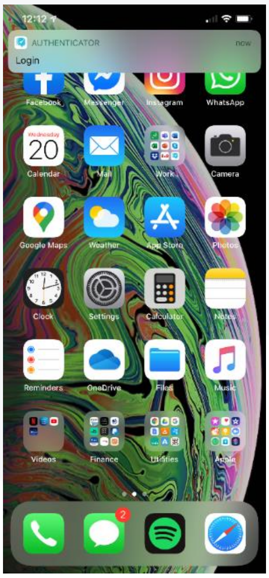
507518

834679

Lock Screen



Home Screen



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.

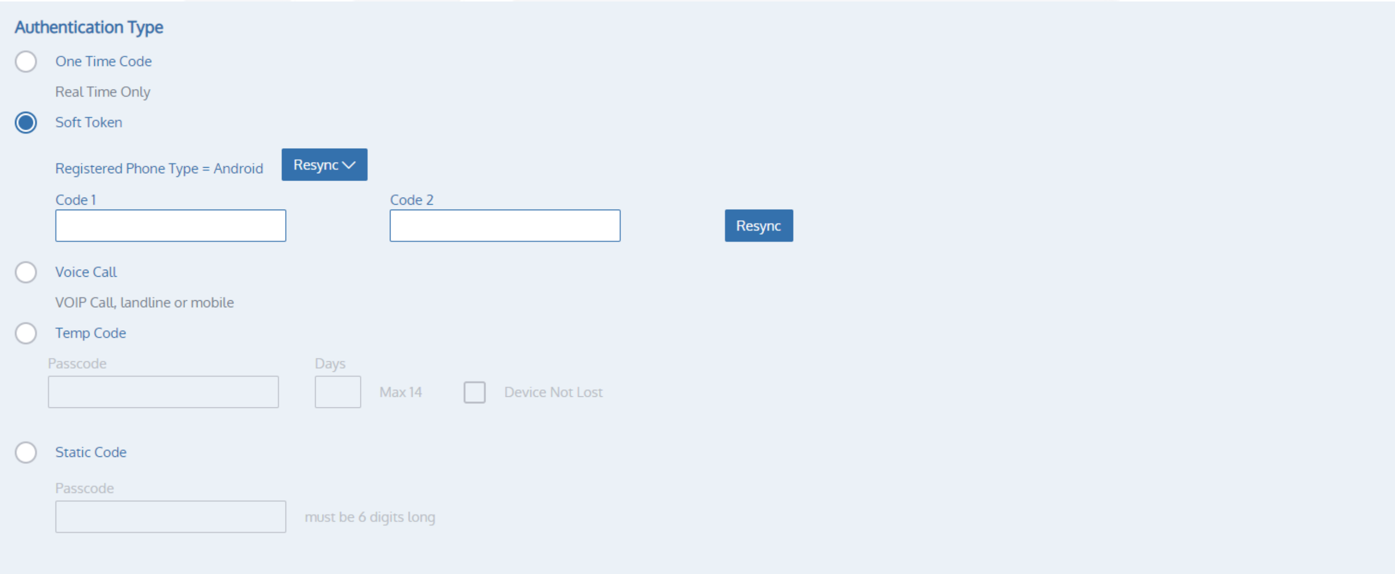
Multiple soft tokens can be enrolled and used within the same app for multiple SecurEnvoy servers eliminating the need to carry multiple hardware tokens or install multiple soft token apps. The latest SecurEnvoy server allows user far greater choice of security - either tokenless SMS two factor authentication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

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.

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

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



Authentication Type

○ One Time Code

Real Time Only

● Soft Token

Registered Phone Type = Android

Code 1

Code 2

○ Voice Call

VOIP Call, landline or mobile

○ Temp Code

Passcode

Days

Max 14

□ Device Not Lost

○ Static Code

Passcode

must be 6 digits long

Soft Token Security

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

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”.

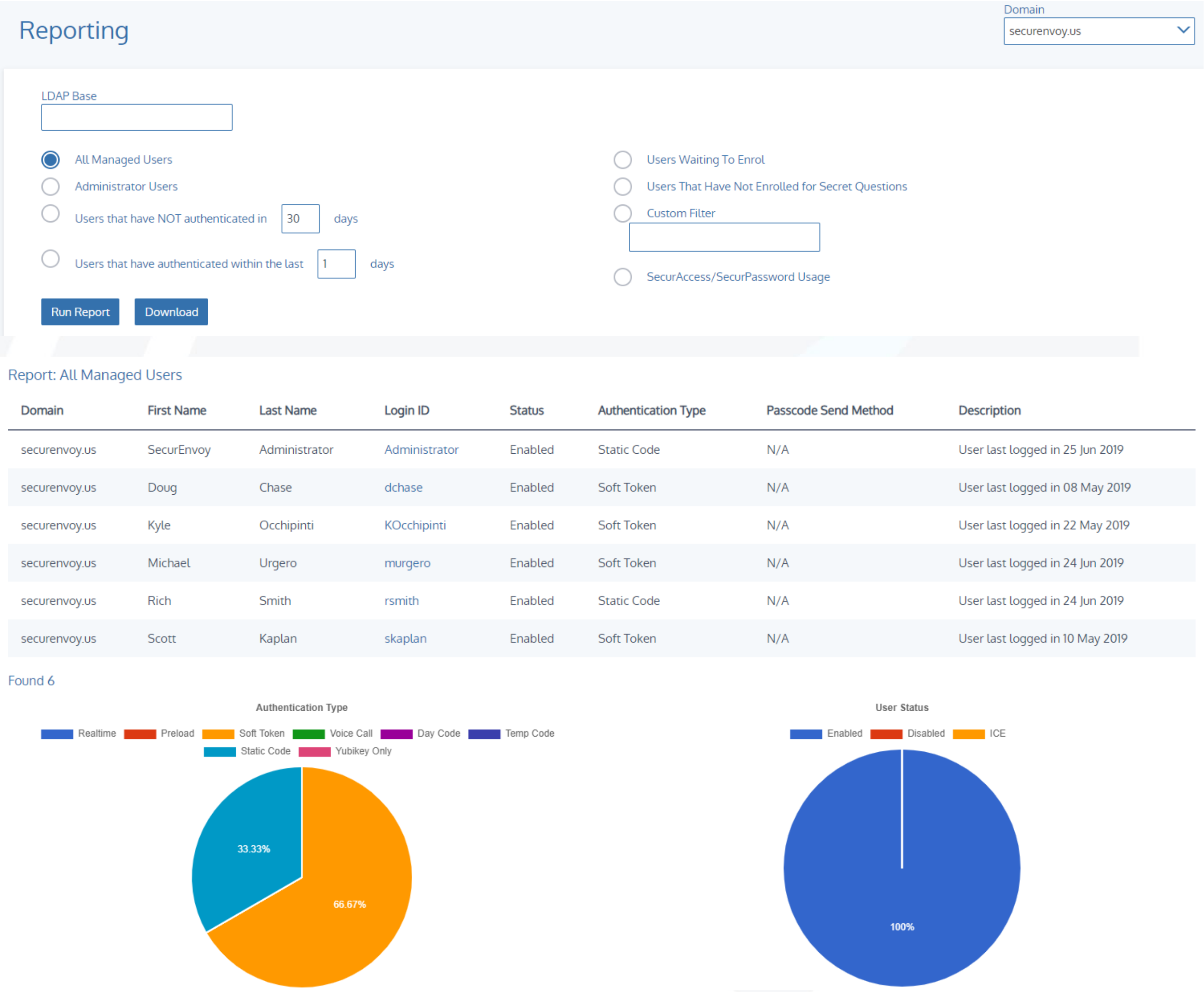
Automatic Time Re-sync

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 Worldwide travel for the user

Reporting

There are 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)

Once the designated report has run the output is displayed as a list and graphical format. The list format allows for an Admin or Helpdesk operator to directly manage the listed user from within the Admin GUI.



Reporting

Domain: securenvoy.us

LDAP Base:

● All Managed Users
○ Administrator Users
○ Users that have NOT authenticated in 30 days
○ Users that have authenticated within the last 1 days
○ Users Waiting To Enrol
○ Users That Have Not Enrolled for Secret Questions
○ Custom Filter
○ SecurAccess/SecurPassword Usage

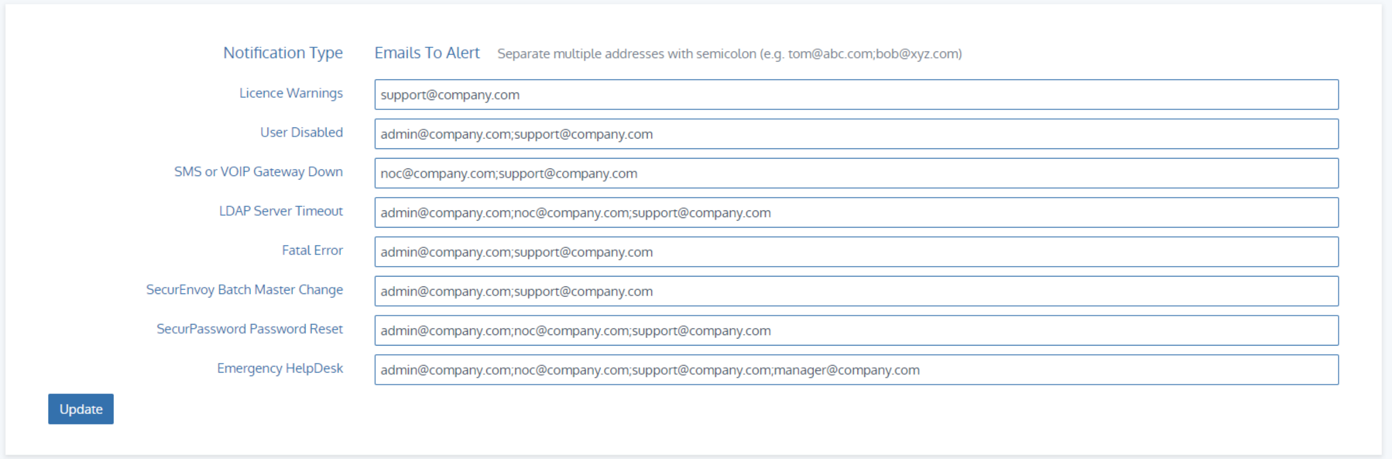
Report: All Managed Users

Domain	First Name	Last Name	Login ID	Status	Authentication Type	Passcode Send Method	Description
securenvoy.us	SecurEnvoy	Administrator	Administrator	Enabled	Static Code	N/A	User last logged in 25 Jun 2019
securenvoy.us	Doug	Chase	dchase	Enabled	Soft Token	N/A	User last logged in 08 May 2019
securenvoy.us	Kyle	Occhipinti	KOcchipinti	Enabled	Soft Token	N/A	User last logged in 22 May 2019
securenvoy.us	Michael	Urgero	murgero	Enabled	Soft Token	N/A	User last logged in 24 Jun 2019
securenvoy.us	Rich	Smith	rsmith	Enabled	Static Code	N/A	User last logged in 24 Jun 2019
securenvoy.us	Scott	Kaplan	skaplan	Enabled	Soft Token	N/A	User last logged in 10 May 2019

Found 6

Alerting

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

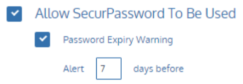


Notification Type	Emails To Alert Separate multiple addresses with semicolon (e.g. tom@abc.com;bob@xyz.com)
Licence Warnings	support@company.com
User Disabled	admin@company.com;support@company.com
SMS or VOIP Gateway Down	noc@company.com;support@company.com
LDAP Server Timeout	admin@company.com;noc@company.com;support@company.com
Fatal Error	admin@company.com;support@company.com
SecurEnvoy Batch Master Change	admin@company.com;support@company.com
SecurPassword Password Reset	admin@company.com;noc@company.com;support@company.com
Emergency HelpDesk	admin@company.com;noc@company.com;support@company.com;manager@company.com

SecurPassword

SecurPassword has the functionality to reset Microsoft Domain (AD) user password and unlock user account using Two Factor Authentication. SecurPassword can be configured to choose “Use Secret Questions” (pre-defined questions template) or “Use LDAP Data” (reference an LDAP AD Attributes).

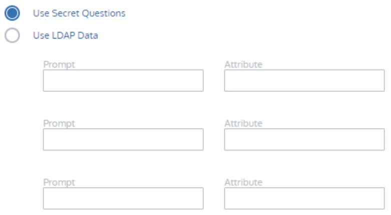
The Password expiry warning check can send via SMS/Email a warning message at (x) days before a user password expires. (Default is 7 days). Users will be automatically alerted by set number of days (configurable) prior to their password expiring.



☑ Allow SecurPassword To Be Used
☑ Password Expiry Warning
Alert 7 days before

Using Secret Questions:

The default number of secret questions used is set to 9 and cannot exceed this number. This limitation is only set on the actual number and is not limited to the questions themselves. These can be modified by editing the questions.txt file located here: \Program Files (x86)\SecurEnvoy\Security Server\Data\ENROLTEMPLATE\questions.txt



● Use Secret Questions
○ Use LDAP Data

When using this feature, users will be prompted to answer two security questions during the time that the register and enrol with the SecurEnvoy SecurAccess.

Note You can only modify the Secret Questions prior to any user enrolment, modifying these after could offset the answers that were provided to the original question, resulting in the failure for users to use this feature.

Using AD Attributes:

AD Attributes can be setup to use 1 to 3 questions. The "Prompt" field is an administrator defined setting relevant to the AD attribute. 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.

Password Maximum Age, Password Maximum Length, Upper, Lower and Number should match your AD user password polices.

Select "Update to Complete.

Note: f 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. SecurEnvoy recommends that SecurPassword uses SSL/TLS over LDAPS 636 to fully meet all of the above stated requirements of a password reset. Enabling SSL/TLS can be set within the Security server Admin -> Domain tab.

Recommended Backup procedure

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:

C:\Program Files\SecurEnvoy\Security Server\
For 64 bit installations: 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 the following is backup the following regularly.

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

- LOG files
- RADIUS configuration Data
- SMS Message Queue and Controls
- 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 and 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:

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

Example, restore all users unmanaged on the 26th March 2019 run the command ldifde -i -f 26_Mar_2019.ldf

Troubleshooting

Please visit our Knowledge Base here: https://www.securenvoy.com/kb/AllPages.aspx

Appendix

Setting Up SSL Certificates on IIS Web Servers

For this procedure, please see Microsoft's documentation here:
https://docs.microsoft.com/en-us/iis/manage/configuring-security/how-to-set-up-ssl-on-iis

Scripting with PowerShell v3

AdminAPI.dll is a 64bit assembly so you MUST start the 64bit 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”AdminAPI.dll is a 32bit assembly so you MUST start the 32bit version of PowerShell V3

SMS Gateway Options

Navigate to SecurEnvoy website for an up-to-date list of SMS Gateway options:
https://www.securenvoy.com/support/smsgateway.shtm

Web SMS Templates

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#
#PASSWORD#
UserID for Authenticating with Gateway Password for Authenticating with Gateway

Send File (POST Data)

The following dynamic strings will be replaced:
#USERID# #PASSWORD# #MOBILENUMBER# #SOURCEADDRESS# #MESSAGE# #10DIGITID# #OVERWRITE# #FLASH#
UserID for Authenticating with Gateway Password for Authenticating with Gateway Mobile Number
Source Address
SMS Message to Send Unique 10 Digit Code
Overwrite String for Setting Overwrite Last Message
Flash String to flash message on screen (Real Time Passcodes Only)

InitURI

The following dynamic strings will be replaced:
#USERID# #PASSWORD#
UserID for Authenticating with Gateway Password for Authenticating with Gateway

SendURI

The following dynamic strings will be replaced:

#USERID# #PASSWORD# #MOBILENUMBER# #SOURCEADDRESS# #MESSAGE# #10DIGITID# #OVERWRITE#

UserID for Authenticating with Gateway Password for Authenticating with Gateway Mobile Number
Source Address

SMS Message to Send Unique 10 Digit Code
Overwrite String for Setting Overwrite Last Message

Certificate Enrolment

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
Create the pkcs#10 certificate request in a cmd window certreq –v –New c:\certpol.txt c:\certreq.txt
After third party SMS Gateway CA have signed this request import the user certificate and root certificate

Move the cert and private key to the local machine store as follows:
With IE export cert and private key to cert.pfx

Start mmc with certificate plug-in for local machine
Right click “personal/certificates” “All Tasks/Imports”
Import cert.pfx

With mmc certificate plug-in, select this cert and export the cert without the private key: For 32 bit installations:
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
‘ = &apos;
" = "
& = &
> = >
< = <
LineFeed =CR =
XMLONLY
The following characters are converted (not url encoded)
‘ = &apos; ‘ = &apos; " = "
& = &
> = >
< = <
LineFeed =

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

URL
Characters are URL encoded with ISO-8859-1

Supported ASCII Data CodesServer.ini

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 http://www.ascii-code.net

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

Belvedere House, Basing View
Basingstoke, Hampshire
RG21 4HG, UK

Sales

E **sales@SecurEnvoy.com**
T **44 (0) 845 2600011**

Technical Support

E **support@SecurEnvoy.com**
T **44 (0) 845 2600012**

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E **info@SecurEnvoy.com**
T **+49 89 70074522**

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E **info@SecurEnvoy.com**
T **+612 9911 7778**

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E **info@SecurEnvoy.com**
T **(866)777-6211**

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E **info@SecurEnvoy.com**
T **(866)777-6211**

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E **info@SecurEnvoy.com**
T **(866)777-6211**

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

SecurEnvoy HQ, Octagon Point, 5 Cheapside, St Paul's, London, EC2V 6AA E: info@SecurEnvoy.com T: 44 (0) 845 2600010
Company No. **04866711** VAT Number **GB 862076128**