

SecurEnvoy Cloud Administration Guide

Authenticating Users Using SecurEnvoy Cloud

Contents

SECURENVOY CLOUD ADMINISTRATION AND CONFIGURATION GUIDE	4
Copyright	4
UNDERSTANDING SMS DELIVERY DELAYS	5
Location Issues	5
Mobile Device Issues	5
Different Networks	5
Network Traffic	5
Delivery Receipts	5
TOKEN TYPES	6
One Time Passcode Delivery Options	6
Pre-Load SMS Delivery	6
Real Time SMS Delivery	6
Mobile Authenticator (Soft Token)	7
Mobile Authenticator - Locked Token Screen	7
Hardware Tokens	7
USER SELF-ENROLMENT	8
User Self-Enrolment Process	8
DOMAIN MODEL FOR LDAP	9
SUPPORT FOR MULTI LDAP ENVIRONMENTS	9
Company with Internal users requiring 2FA	9
Company requiring a Business to Consumer 2FA	9
Company requiring 2FA for an ASP/ISP type model	9
SECURENVOY CLOUD DEPLOYMENT	10
Single Domain Deployment Options	10
INITIAL CONFIGURATION	12
Completing Initial Setup Wizard	13
Licence	13
Domain	14
Setup Complete	14
CONNECTOR AGENT INSTALL	15
Connector Agent Config File	15
Software Installation	16
Connector Agent Config	17
ADMINISTRATION INTERFACE	19
Multi-Domain Configuration	19
Config	19
Licence Upgrades	20
Authentication Types	20
Apps	20
Protect Mobile Authenticator App (TouchID/PIN)	21
SMS/Email	22
Hardware Tokens	23
Temp and Static Code	24
Pin Management	25
Mobile Settings	25
Account Lockout Settings	26
Automatic Group Deployment	27
Send Passcodes to Mobile / Email Example	27
Misc GUI Settings	28
USER MANAGEMENT	28
One Time Codes	30
Day Codes	30
Soft Token	31
Static Passcode	31
Mobile Authenticator	32
Mobile Authenticator "Soft Token"	33
Mobile Authenticator Security	33
CONNECTED APPS	34

Microsoft Office365	35
Goggle G-Suite	36
TIMEZONE	37
REPORTING WIZARD (ADMIN GUI)	37
ALERTING	38
WEB SMS TEMPLATES	38



SecurEnvoy Cloud Administration and Configuration Guide

Copyright

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.



Understanding SMS Delivery Delays

- What causes a delay in delivering SMS messages?
- Why did it take so long for my SMS to arrive?
- How long is it normal to wait for delivery of SMS?
- Why was my SMS so slow to be sent?

Whilst we are accustomed to messages arriving within a few minutes, SMS isn't an instant messaging service. For example, even within network, service providers guarantee delivery within a certain time, and that time is 24 hours.

Below are some reasons why your SMS might not be delivered instantly.

Location Issues

The location of the sender or recipient can create a delay in text message delivery. What causes this varies from handset to handset, but common reasons are being on the border of two cell coverage areas or travelling at speeds above about 50km/h. This is most likely happening if messages arrive all at once. If a mobile device is located outside a network's coverage area or in a spot where the network signal is blocked such as in a mountainous region, a delay in transmission may occur. In urban areas, tall buildings can also cause transmission issues. Being in an old building with poor cell reception is another possible culprit.

Mobile Device Issues

Problems with a mobile device may cause delays in text message transmission. The most obvious cause is a device that has been turned off, but a weak or uncharged battery may also negatively impact message delivery. Devices that have an adjustable antenna may experience transmission difficulties if the antenna has sustained damage or has not been fully raised.

Different Networks

A text sender and receiver using different networks may have a greater chance of experiencing texting delays than those using the same network, because of communication between networks or the carrier prioritizing their own traffic.

Network Traffic

Texting during periods of heavy network use impacts text delivery speed. Periods of increased traffic may create congestion on the local network and delay arrival of messages to the handset.

Delivery Receipts

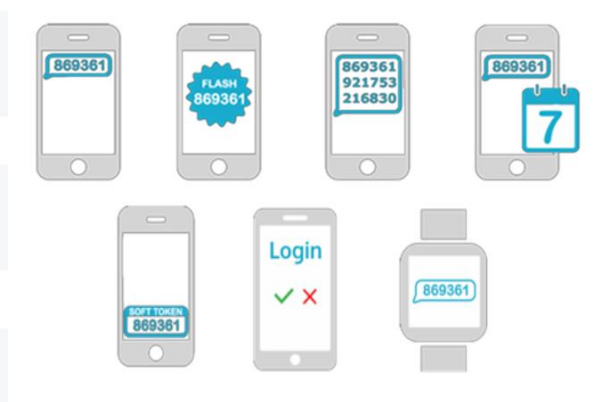
It should also be noted that the arrival of delivery receipts (DLRs) are not always a good measure of when the SMS was delivered. Delivery receipts are often prioritised lower than other traffic (i.e. lower than the SMS traffic) on networks, and at busy times or when networks approach maximum capacity, they will de-prioritise delivery of delivery receipts further in favour of SMS content, leading to potentially very delayed arrival of delivery receipts in your account.

Token Types

One Time Passcode Delivery Options

The users' mobile phone can receive a one-time passcode (OTP) via the following methods

- SMS (Realtime and Pre-Load) – *(More on each option is described later in the guide)*
- SMS (Reusable Day code)
- SecurEnvoy's Mobile Authenticator *(including the latest Push Notification authentication option)* – Available for Apple and Android OS's
- Email Token - Email based delivery of tokens is not user selectable from within the Enrolment portal unless specifically enabled by an administrator.. SecurEnvoy does not recommend that this method of passcode delivery is utilised without first understanding the implications of using an insecure method of delivery *(SMTP traffic is not an encrypted protocol and brings a threat of OTP compromise).*
- Hardware Token – USB based OTP token



Pre-Load SMS Delivery

The key strategy for successful use of SMS for delivering passcodes is resolving intermittent network coverage and SMS delivery delays. SecurEnvoy Cloud 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.

Mobile Authenticator (Soft Token)

SecurEnvoy's approach to mobile 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 mobile authenticator app.

Available free of charge SecurEnvoy Mobile Authenticator is suitable for most types of mobile devices i.e. Apple iPhones, iPad's, and Android phone operating systems.

Mobile Authenticator - Locked Token Screen

The Authenticator locked screen is an additional interaction security feature above 2FA/MFA where you have the facility to protect the authenticator app with a password or biometric finger print.

Functions where the lock screen is activated:

- Pressing the power button on the phone to lock the phone OS.
- Pressing the home button on the phone to return to the OS home screen.
- If the phone is left to timeout through OS screen/lock timeout settings.
- If the phone has no settings enabled to timeout or lock then the SecurEnvoy token will auto lock after

Hardware Tokens

SecurEnvoy's approach to hardware tokens is with support of YubiKey's Series 4 & 5 USB tokens. Yubikey is a hardware authentication device manufactured by Yubico that supports 44-character one-time passwords as an alternative to the traditional SMS or Mobile Authenticator tokens. The token is supported in laptops that have had their USB ports locked down due the token being recognised by the devices OS as a standard keyboard.



User Self-Enrolment

SecurEnvoy utilises a self-serve user management portal known as "Manage My Token".

The web portal allows the user to initially enrol their authentication token and thereafter manage the life cycle of their device.

For instance, re-provisioning Mobile Authenticator tokens from their new mobile phone and automatically revoking any previous tokens from original phones. SecurEnvoy's Mobile Authenticator tokens are only supported on a single mobile device.

The process of enrolling users is through a self-enrolment portal, allowing the user to select their preferred token type of SMS or Soft Token (Mobile). Authentication Types can be locked down by the Administrator preventing this selection if necessary.

User Self-Enrolment Process

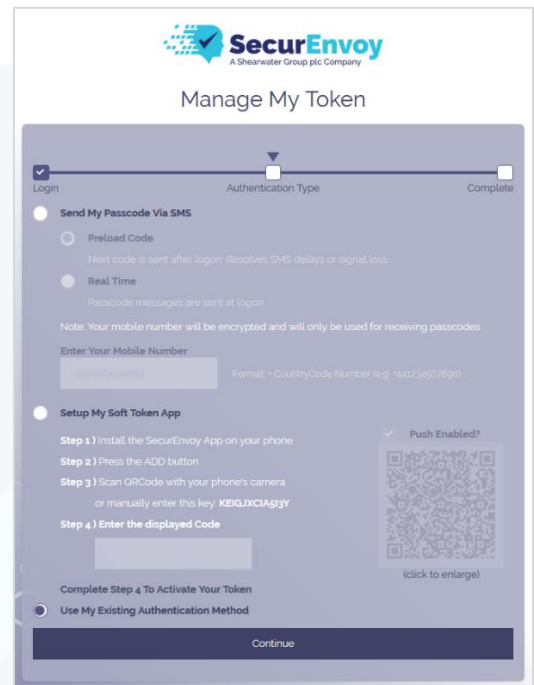
User receives and enrolment email (*wording is customisable per customer requirements – please request via your SecurEnvoy Account Manager*), including a link to the customer specific enrolment portal eg:
"http(s)://*customername*.securenvoy.cloud/secenrol"

Each enrolment email will include a link to the respective app store for iOS or Android download of the SecurEnvoy Mobile Authenticator app.

Log into the SecurEnvoy enrolment page – cleverly they can authenticate themselves with their current Active Directory (AD) user name and passcode.

A QR Code appears on the screen which the user scans with the camera on their phone.

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



Domain Model For LDAP

SecurEnvoy has the ability to fully support direct integration with the following LDAP servers:
Microsoft Active Directory & OpenLDAP

In addition, SecurEnvoy can support a fully heterogeneous environment, allowing various vendor's LDAP servers to coexist and interoperate with SecurEnvoy Cloud. This allows companies exceptional scope to manage a truly heterogeneous LDAP environment.

Support for Multi LDAP Environments

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 or OpenLDAP) requires very little configuration. All that is needed is a service account upon the SecurEnvoy Connector Agent server that has read and write privileges to the "telex number" attribute within AD or OpenLDAP.

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 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 a managed Microsoft LDAP environment through the SecurEnvoy Cloud admin GUI.

Note: If you require SecurEnvoy Managed Users functionality, please engage with your SecurEnvoy Account Manager or representative.

Company requiring 2FA for an ASP/ISP type model

Managed customers allow connectivity to their own LDAP servers for user management (2FA, this requires read and write access to the telexnumber attribute) through the SecurEnvoy Connector Agent. 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 'Automatic Group Deployment' section below).

SecurEnvoy Cloud Deployment

Single Domain Deployment Options

Below you will find a number of deployment options that are supported by SecurEnvoy Cloud and the SecurEnvoy Cloud Connector Agent within a single domain.

Multiple instances of the SecurEnvoy Cloud Connector Agent can be run simultaneously across several servers within a single domain to provide resilience for the SecurEnvoy Cloud solution.

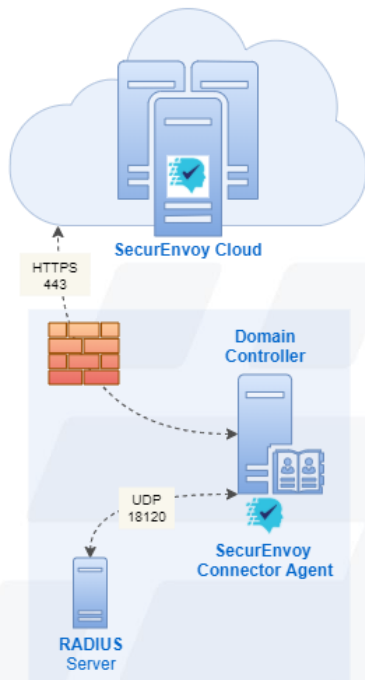


Figure 1 - Deployment Option 1

In a simple, non-resilient SecurEnvoy Cloud deployment the Domain Controller would typically host a single instance of the SecurEnvoy Cloud Connector Agent. The Connector Agent will connect outbound to the SecurEnvoy Cloud via HTTPS port 443.

The Connector Agent service will have a direct local connection to AD in order to make LDAP queries for user authentication. In this example you can see that the SecurEnvoy Connector Agent can also authenticate against a separate RADIUS server via UDP port 18120.

To provide a level of redundancy and resilience for the SecurEnvoy Cloud solution, multiple instances of the SecurEnvoy Connector Agent can be deployed on each of the Domain Controllers within your domain.

As seen previously, the SecurEnvoy Connector Agent will connect outbound to the SecurEnvoy Cloud via HTTPS port 443. Each respective Connector Agent service will make a direct local connection to AD on the Domain Controller where it is hosted. The Connector Agent can also authenticate against a separate RADIUS server via UDP port 18120.

In this particular deployment, if a Domain Controller was to fail or be shut down the redundant Domain Controller and Connector Agent service would be able to continue authenticating SecurEnvoy Cloud users.

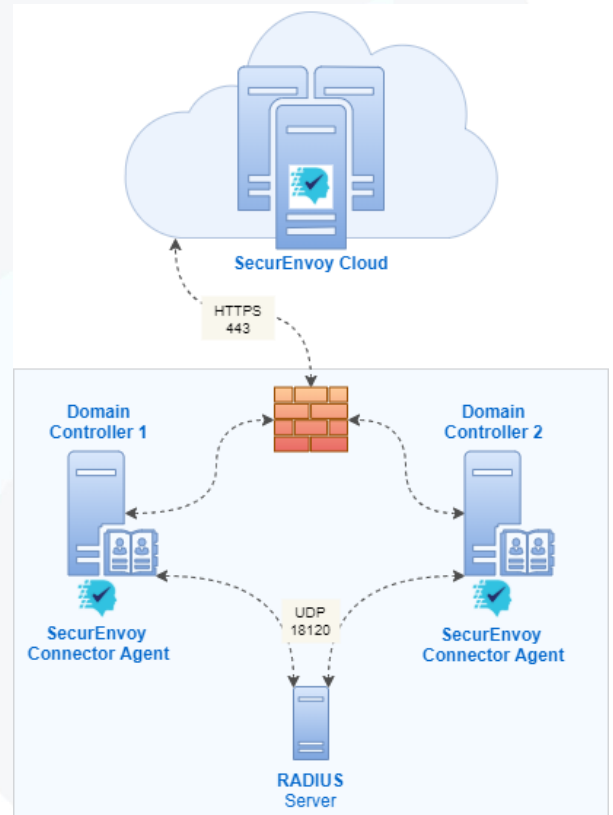
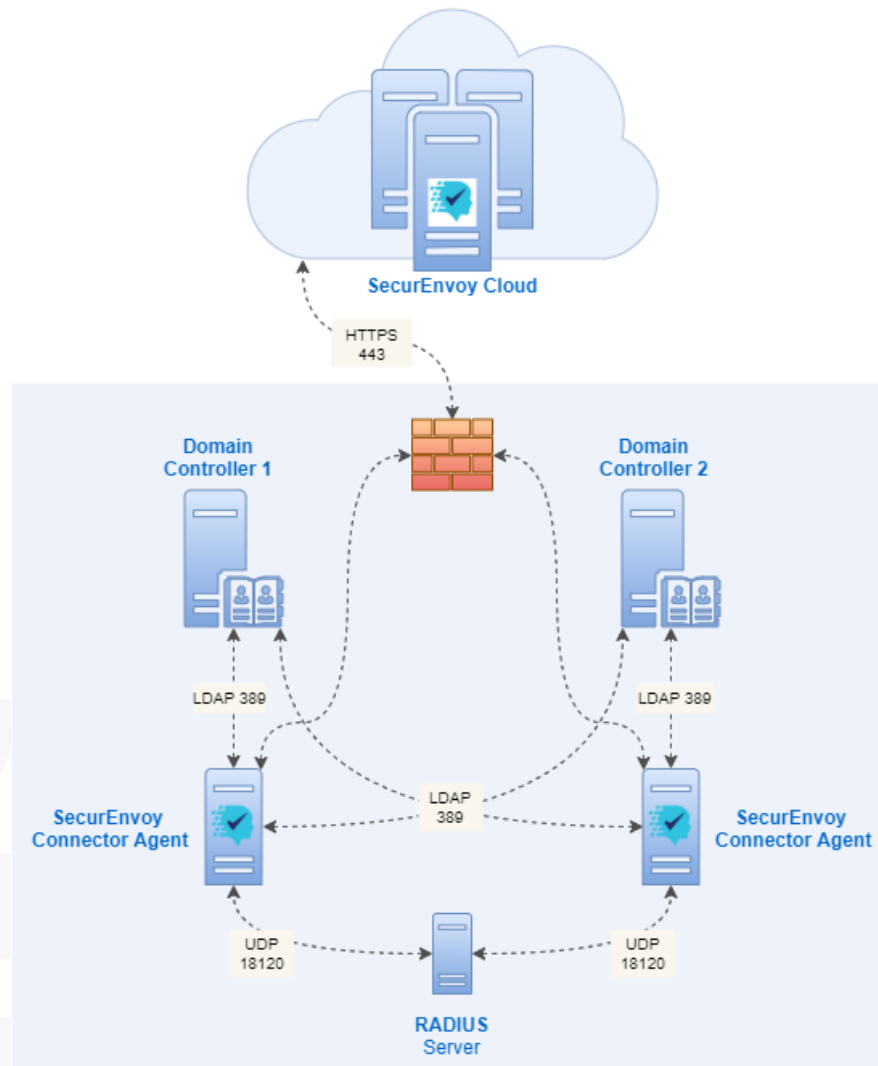


Figure 2 - Deployment Option 2



For security or operational reasons it may not be feasible to host the SecurEnvoy Cloud Connector Agent directly on your Domain Controller/s. In this instance, the Connector Agent service can be hosted on a separate server or servers. This deployment will also provide a greater level of redundancy and resilience as each Connector Agent service has multiple LDAP connections to each Domain Controller.

The configuration file for the Connector Agent would need to be configured with the IP addresses of each of the Domain Controllers within the domain. Doing so will allow the Connector Agent services to connect to each Domain Controller to make LDAP queries for user authentication.

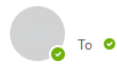
As seen previously, the SecurEnvoy Connector Agent will connect outbound to the SecurEnvoy Cloud via HTTPS port 443, as well as authenticating against a separate RADIUS server via UDP port 18120.

Initial Configuration

To access the SecurEnvoy Cloud GUI, open a web browser and enter the following "http(s)://*customername*.securenvoy.cloud/secadmin/" (replace with customer name provided in your onboarding email)

For the initial setup of SecurEnvoy Cloud, your SecurEnvoy Account Manager will send to you an email with a URL to your SecurEnvoy Cloud GUI as well as the Administrator username and password.

SecurEnvoy Cloud Administration



Welcome to the SecurEnvoy Cloud Multi-Factor Authentication Service.

Your SecurEnvoy Cloud admin portal address is: <https://your-company.securenvoy.cloud/secadmin>

Your administrator account details for the admin portal are as follows:

Username: jsmith@admin.securenvoy.cloud

Password: *****

You will shortly receive a one-time 6 digit passcode via email to allow you to complete the login process.


Upon entering the Administrator credentials into the SecurEnvoy Cloud GUI a One Time Passcode will be sent to your email address. Enter this 6-digit code into the field and click 'Login'. You are now logged in with the Administrator account for your SecurEnvoy Cloud GUI.

Two Factor Authentication Passcode



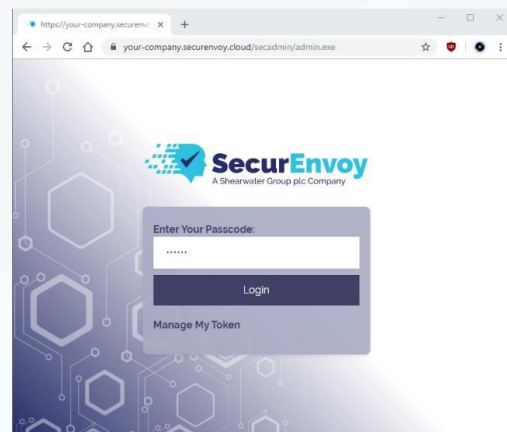
no-reply@securenvoy.cloud

To

 This message was sent with High importance.

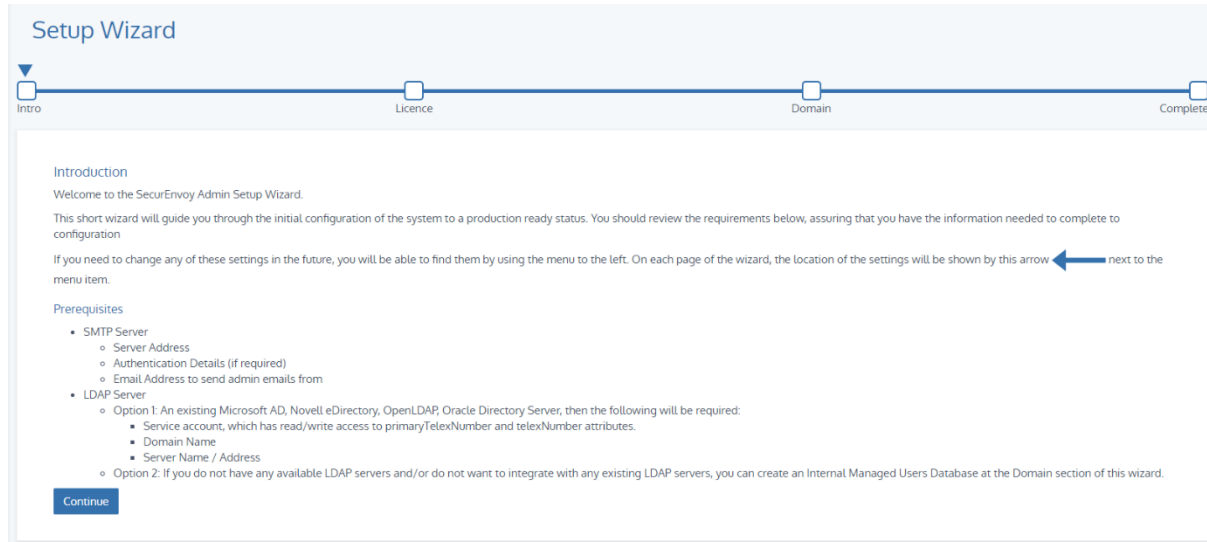
269495 default Passcode

Powered by SecurEnvoy



Completing Initial Setup Wizard

The SecurEnvoy "Setup Wizard" is the first stage in setting up all configuration data of the SecurEnvoy Security Cloud.



Setup Wizard

Intro Licence Domain Complete

Introduction
Welcome to the SecurEnvoy Admin Setup Wizard.
This short wizard will guide you through the initial configuration of the system to a production ready status. You should review the requirements below, assuring that you have the information needed to complete to configuration
If you need to change any of these settings in the future, you will be able to find them by using the menu to the left. On each page of the wizard, the location of the settings will be shown by this arrow ← next to the menu item.

Prerequisites

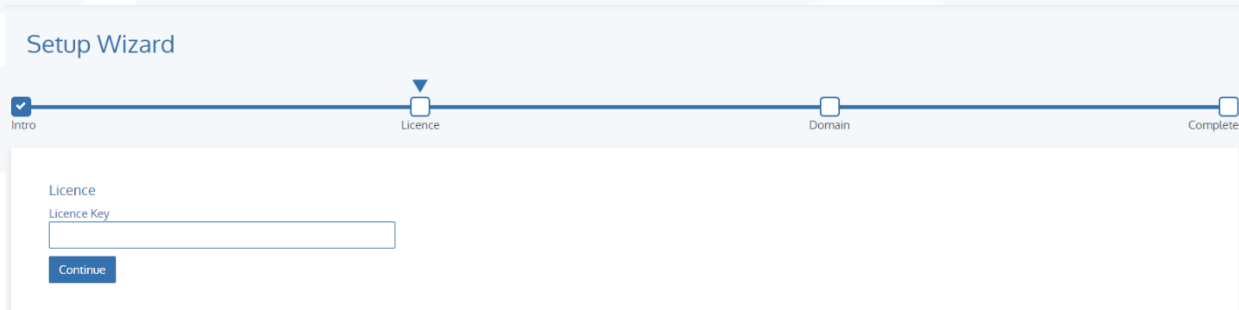
- SMTP Server
 - Server Address
 - Authentication Details (if required)
 - Email Address to send admin emails from
- LDAP Server
 - Option 1: An existing Microsoft AD, Novell eDirectory, OpenLDAP, Oracle Directory Server, then the following will be required:
 - Service account, which has read/write access to primary/telexNumber and telexNumber attributes.
 - Domain Name
 - Server Name / Address
 - Option 2: If you do not have any available LDAP servers and/or do not want to integrate with any existing LDAP servers, you can create an Internal Managed Users Database at the Domain section of this wizard.

Continue

By default, the setup wizard will launch to the Intro tab through each relevant section until the complete tab.

Licence

Your trial or full licence key is entered here. Take extra care when copying the key that it doesn't include any spacing.



Setup Wizard

Intro Licence Domain Complete

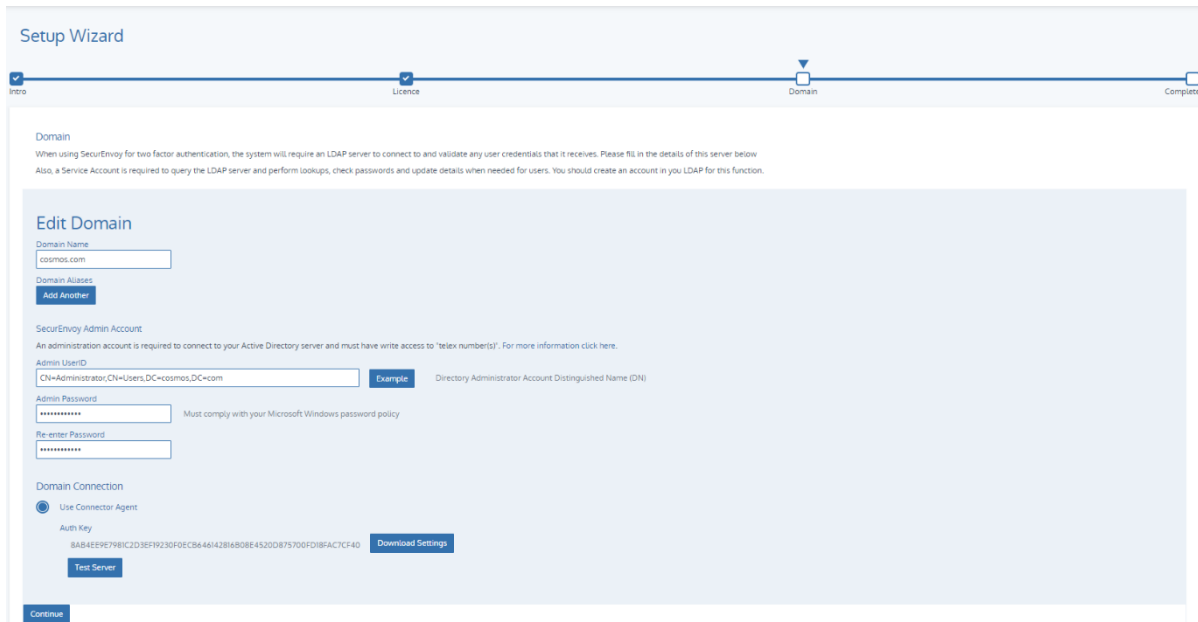
Licence
Licence Key

Continue

Domain

At this stage you will need to enter your domain details to allow SecurEnvoy Cloud to authenticate your Active Directory (AD) users.

You will need to enter your domain name, followed by Administrator or Service Account credentials to connect to your Active Directory server (this account must have write access to LDAP attributes "primary telex and telex other "). The format of the Admin UserID must be in the format of LDAP Distinguished Name (for example; "CN=Administrator,CN=Users,DC=your-company,DC=com").

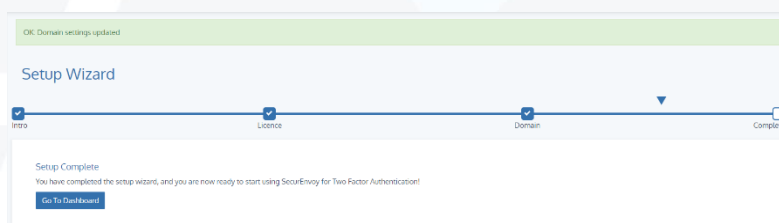


At this stage **DO NOT** click the "test server" button, when the domain details have been entered, click 'Continue'.

Setup Complete

Setup wizard complete!

Select "Go to Dashboard" to complete the setup and continue with your personalised settings.



Connector Agent Install

Connector Agent Config File

On the left admin panel, navigate to Domains > Edit Domain (Figure 10);

- Click on 'Download Settings' and 'Download'.
 - i. This will download a file called 'ConnectorClient.ini' to your local machine.
- Remember where 'ConnectorClient.ini' is downloaded to, as it is required later in this process.

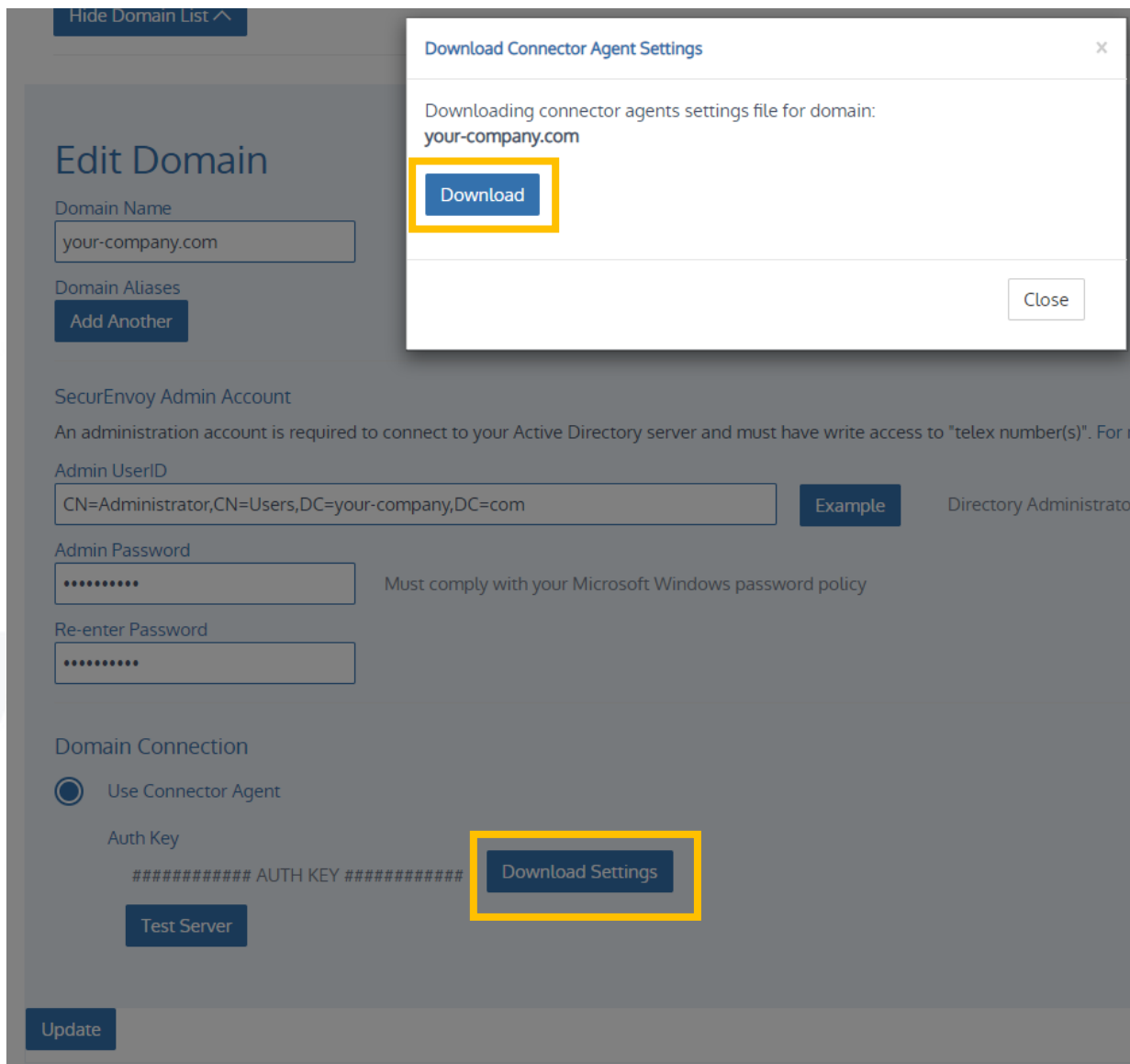


Figure 3 SecurEnvoy Cloud Domain Configuration

Software Installation

Navigate to SecurEnvoy Support Downloads (<https://www.securenvoy.com/en-us/support#id4>) and download the Connector Agent setup file. When this has downloaded, install Connector Agent software on the preferred server.

- If you decide to install the Connector Agent on a server that **is not** a Domain Controller you must ensure that the server running the Connector Agent service has IP connectivity to your Domain Controller.

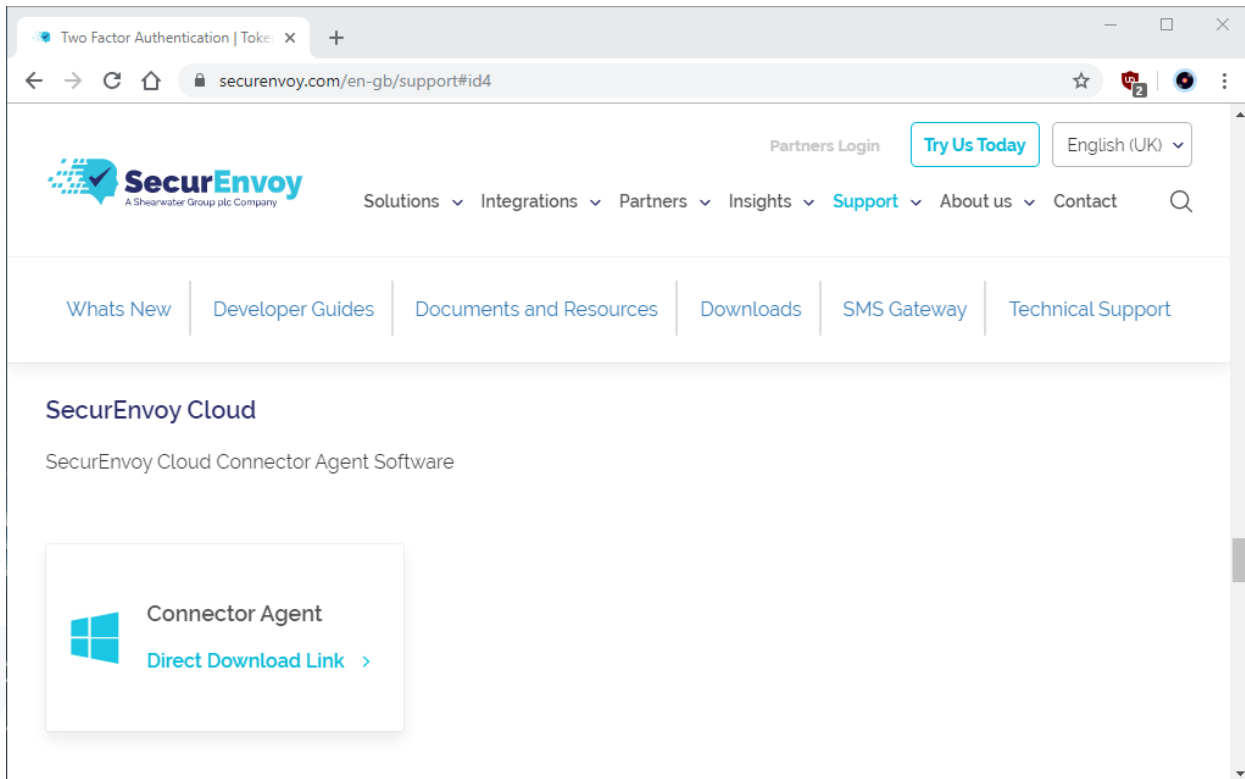


Figure 4 SecurEnvoy Downloads

Connector Agent Config

Once the ConnectorAgent software is installed, place the 'ConnectorClient.ini' file into the following SecurEnvoy Connector Agent directory [Figure 12].

- Copy and paste, or, move the 'ConnectorClient.ini' downloaded in Step 10 to the following directory;
 - i. C:\ProgramData\SecurEnvoy\ConnectorAgent (hidden directory)
 - ii. When prompted, select 'Replace the file in the destination'
- If the Server that the ConnectorAgent service is running on is not a Domain Controller, 'ConnectorClient.ini' must be updated with the IP address of the DC rather than a loopback address [Figure 13].
- To add multiple Domain Controller IPs, list the IP address of the Domain Controller with followed by port number ':389'. Separate each IP address with a Semicolon [Figure 13a].

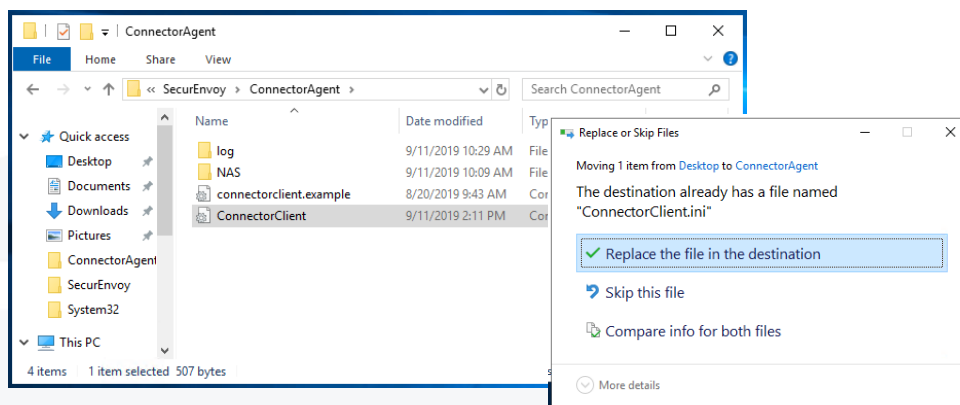


Figure 5 ConnectorClient.ini Filepath

```

ConnectorClient - Notepad
File Edit Format View Help
# Global settings

# Debug (True/False)
Debug=False

AuthKey=##### AUTH KEY #####

# Connector
ConnectorEnabled=True
ServerUri=wss://your-company.securenvoy.cloud/connector/connect

# Radius settings
RadiusEnabled=True
RadiusPort=18120
SecureCtrlUri=https://your-company.securenvoy.cloud/secserver/securectrl.exe

[Tcp_your-company.com]
Identifier=Tcp_your-company.com
Servers=127.0.0.1:389
Type=TcpClient
Domain=your-company.com
  
```

```

[Tcp_your-company.com]
Identifier=Tcp_your-company.com
Servers=10.1.1.10:389;10.2.2.10:389;10.3.3.10:389
Type=TcpClient
Domain=your-company.com
  
```

Figure 13a Adding Multiple Domain Controller IPs

Figure 6 Optional - ConnectorClient.ini LDAP Server Configuration

Following the changes to the configuration, locate the 'SecurEnvoy Connector Client' service and 'Restart' [Figure 14].

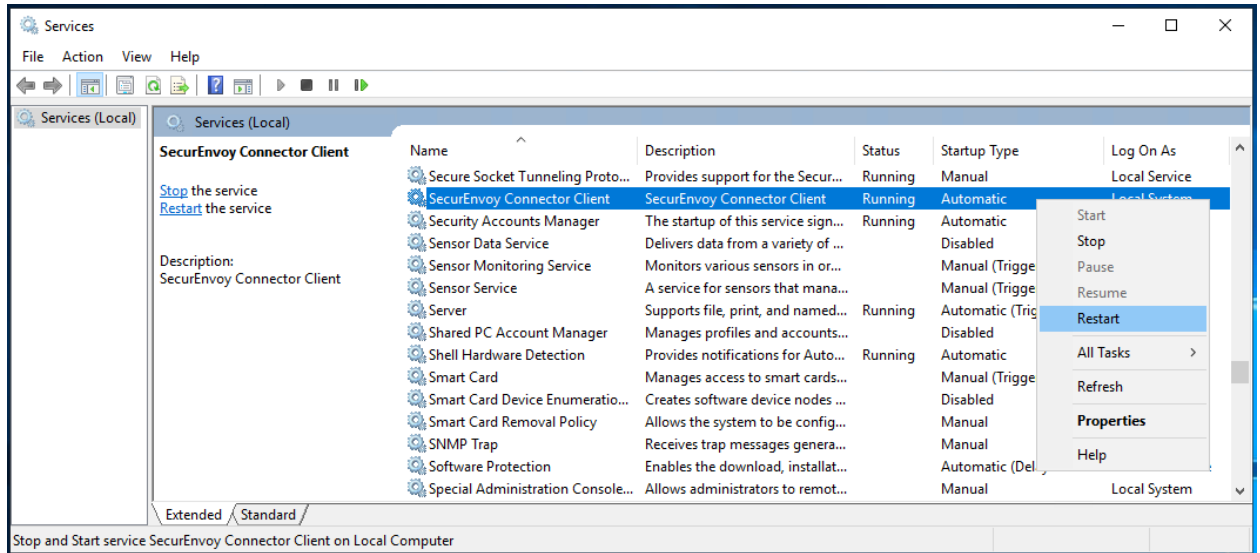


Figure 7 Windows Services - Restart Service for SecurEnvoy Connector Client

To test that the SecurEnvoy Cloud Connector is up and running, navigate to the following URL:
<https://your-company-id.secureenvoy.cloud/connector>
 If you are presented with text 'SecurEnvoy Connector' then the SecurEnvoy Cloud Connector is operational [Figure 14a].

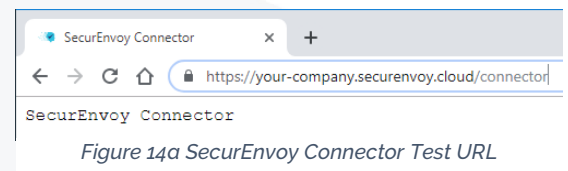


Figure 14a SecurEnvoy Connector Test URL

To test LDAP connectivity to your Domain Controller you can run ldp.exe (located in C:\Windows\System32\). Go to Connection > Bind and select 'Bind type: Bind as currently logged on user', then click 'OK'. If successful you will see that ldp.exe window title changes to 'ldap://your-domain.com/' and the text in the main window will show 'Authenticated as: "your-domain/user"'.

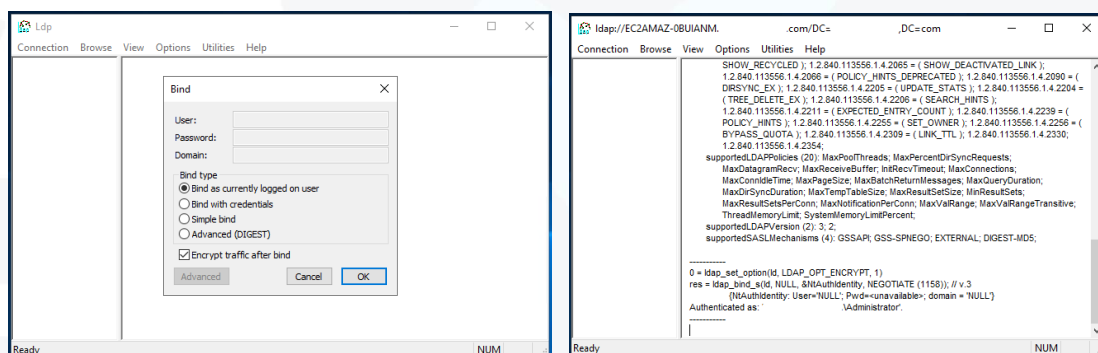


Figure 14b ldp.exe LDAP bind testing

Ldp is built into Windows Server 2008 onwards. It is available if you have the AD DS server role installed.

Administration Interface

To access the SecurEnvoy Cloud GUI, open a web browser and enter the following "http(s)://*customername*.securenvoy.cloud/secadmin/"

Multi-Domain Configuration

To add additional domain's, click "Add New Domain" and then select the domain type followed by the domain information. Select "Add" to complete.

Manage Domains

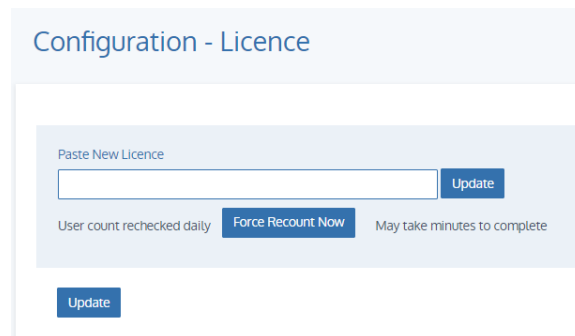
Config

Start the SecurEnvoy Cloud GUI ([http\(s\)://*customername*.securenvoy.cloud/secadmin/](http(s)://customername.securenvoy.cloud/secadmin/)) and select the "Config" menu.

The Config page has multiple sections that can be configured. These allow parameter changes to be made to the SecurEnvoy Cloud product, all of these settings can be applied on a per Domain basis. All except "Logging" as this is a global setting for the whole SecurEnvoy Cloud.

Licence Upgrades

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".



Authentication Types

Authentication types are sectioned into four sub-categories each with an option (per domain) to enable or disable via a check box. Each check box dictates what Token types are available per domain and available via the "User Tab" and "Manage My Token" page ([http\(s\)://customername.securenvoy.cloud/secenrol](http(s)://customername.securenvoy.cloud/secenrol)).

Apps

Here you have the option to enable the different app types and their functionalities.

iOS & Android Mobile Authenticator - Push Notifications

Push provides the user (smart phone) with a notification similar to SMS text or alerts but only for users who have installed our app. Push is a great way to keep cost down (no SMS cost) and secure (intended for that particular user).

SecurEnvoy's iOS and Android Mobile Authenticator application supports Push Notification functionality on a global server/per domain basis or Push notifications on a per user basis (Push per user is selectable through the "Manage my Token" portal).

When a user authenticates to their remote VPN or application with SecurEnvoy 2FA, a push notification message is sent to the Apple or Google notification centre prior to the user receiving the Push notification. The user can choose to accept or deny the authentication request from the locked screen or within their mobile authenticator application, securing the acceptance with the users Biometric or Phone PIN.

There is a way to disable push per authentication attempt using the '-no push' switch. Simply append the user's password with the string '-nopush', see an example of this below:

```
Userid = username  
Password = Password123-nopush
```

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

Note: The Mobile Authenticator App is required for the use of Push notifications.

Protect Mobile Authenticator App (TouchID/PIN)

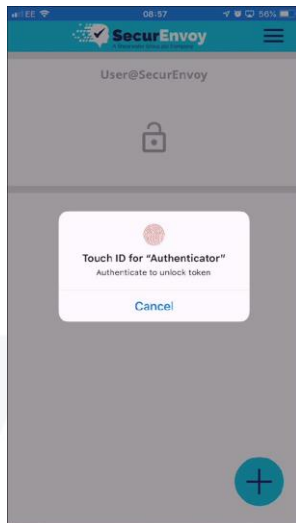
Access to SecurEnvoy Mobile Authenticator tokens can be protected by either a biometric Touch ID or the phones security access PIN code. Without the user entering a PIN or using a biometric the token will not be displayed to the user.

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.

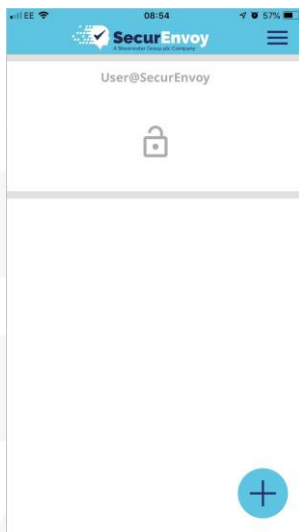
Check the option "Protect app with Touch ID or Pin" to provide additional security.

Protect App with Touch ID or Pin
 Phone's Pin/Fingerprint required

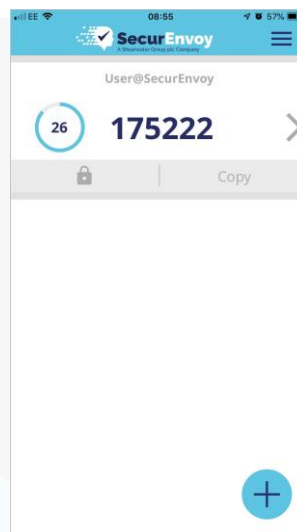
Biometric Locked Screen



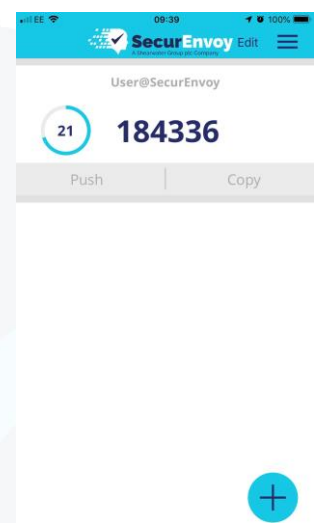
Locked Screen



Token Locked Screen



Unlocked Screen



Note: "Protect app with Touch ID or Pin" doesn't support push and should be disabled by unchecking "Allow Push".

Allow Push
 Sends Deny/Accept Notification to phone (OneSwipe online)
 Time to wait for push
 seconds (Radius timeout must be longer)

SMS/Email

Here you can select the authentication delivery method along with the authenticating feature.

Passcodes can be delivered via SMS or Email.

Caution should be taken when users are given the option to select email - as SMTP is not an encrypted protocol and may not be configured for TLS. Therefore, we believe that administrators should be in control as to whether email is used for passcode delivery.

Pre-loaded is the default SMS delivery option and is sent when a user is first enabled and refreshed at time of logon.

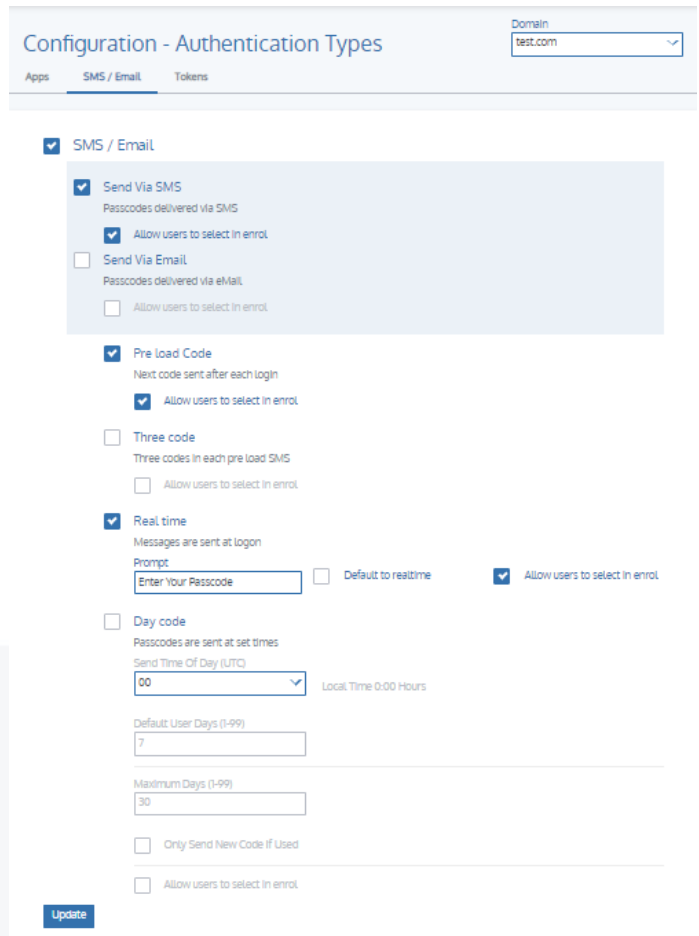
The system can be enabled so that either single or 'Three code' One Time Passcodes are sent within each SMS message (three codes are sent in each pre load SMS). This caters for users who are in an area that have weak or erratic mobile phone signal.

SecurEnvoy has 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. 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 "Default to realtime" 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.

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.

The next required passcode will be sent to this users' 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.

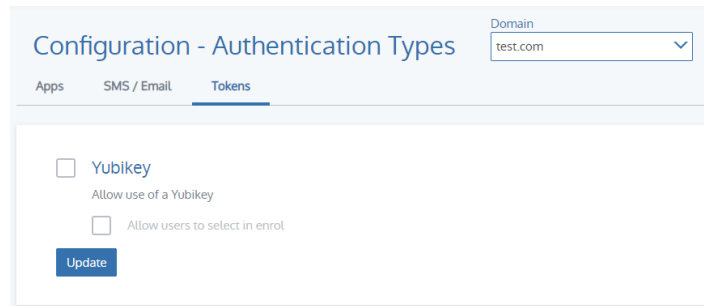


The screenshot shows the 'Configuration - Authentication Types' interface. The 'SMS / Email' tab is selected. The 'Domain' dropdown is set to 'test.com'. The 'SMS / Email' section is checked. Under 'Send Via SMS', 'Send Via SMS' is checked, and 'Allow users to select in enrol' is also checked. Under 'Send Via Email', 'Send Via Email' is unchecked, and 'Allow users to select in enrol' is also unchecked. The 'Pre Load Code' section is checked, with 'Next code sent after each login' checked and 'Allow users to select in enrol' checked. The 'Three code' section is unchecked, with 'Allow users to select in enrol' unchecked. The 'Real time' section is checked, with 'Messages are sent at logon' checked, 'Prompt' set to 'Enter Your Passcode', 'Default to realtime' unchecked, and 'Allow users to select in enrol' checked. The 'Day code' section is unchecked, with 'Send Time Of Day (UTC)' set to '00', 'Local Time 0:00 Hours', 'Default User Days (1-99)' set to '7', and 'Maximum Days (1-99)' set to '30'. The 'Only Send New Code if Used' checkbox is unchecked, and 'Allow users to select in enrol' is unchecked. An 'Update' button is at the bottom.

Hardware Tokens

Yubikey is the only authentication method that can be used alongside other authentication types. An example would be Yubikey + softtoken.

Yubikey support can be enabled via Config -> Authentication Types -> Tokens. Once enabled, you'll have the option to use it as a sole authentication method or in combination with other authentication types.



Configuration - Authentication Types Domain: test.com

Apps SMS / Email **Tokens**

Yubikey
 Allow use of a Yubikey

Allow users to select in enrol

Update

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

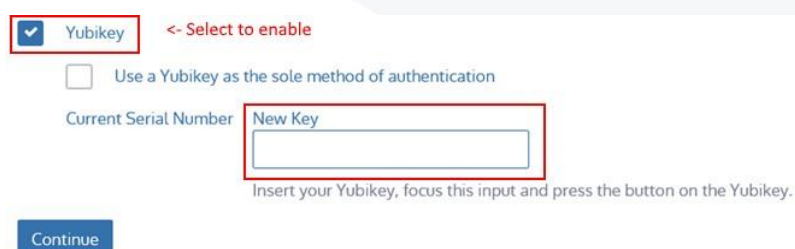
How The Process Works

1. The protected application prompts the user for their username and password and then asks for the OTP.
2. The User physically taps the Yubikey's button to trigger input to generate the OTP string.
3. The OTP string is sent from the SecurEnvoy server to the Yubico server for authentication checking.
4. Once the token check has completed, the Yubikey servers verify that the key matches.
5. 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.

Note: Yubikey will use the built-in generic keyboard drivers that are already installed. Consider Yubikey as a keyboard with a single paste key.

Enrolment Option 1 (Manage My Token Portal):

1. End-user enrolls their own key via the "Manage My Token Portal"
2. End-user can select Yubikey in combination with another token type or "Use a Yubikey as the sole method of authentication"
3. Then select the "New Key" entry form field and press the button on the Yubikey which will paste information into this field.
4. Press "Update" to complete. At which time the SecurEnvoy Server will contact Yubicloud to authenticate this key and assign the serial number marked on this key to this user account.



Yubikey <- Select to enable

Use a Yubikey as the sole method of authentication

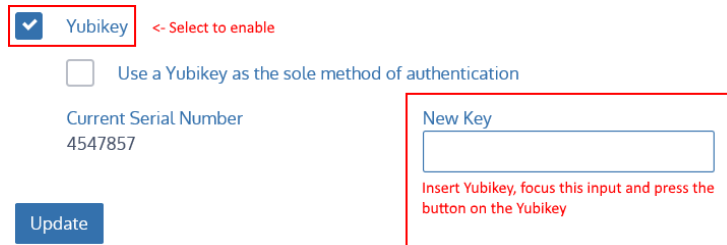
Current Serial Number **New Key**

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

Continue

Enrolment Option 2 (Admin Portal):

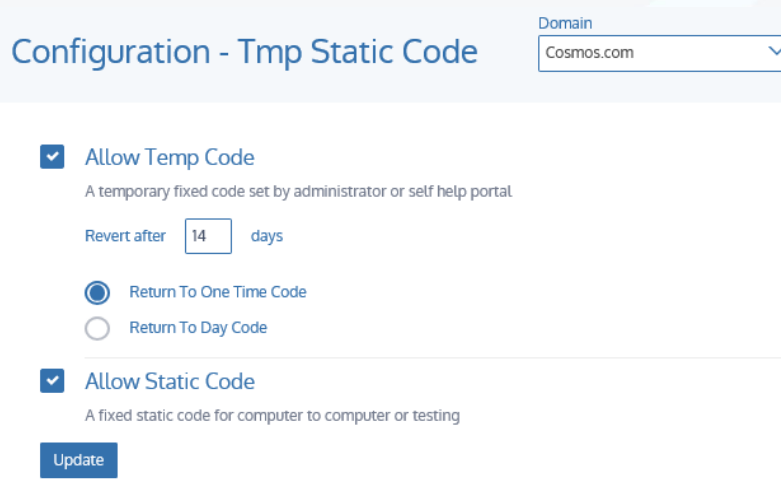
1. The Administrator manually enrolls the End-user via the SecurEnvoy Server Admin -> Users tab
2. The Administrator selects Yubikey in combination with another token type or "Use a Yubikey as the sole method of authentication"
3. Then select the "New Key" entry form field and press the button on the Yubikey which will paste information into this field.
4. Press "Update" to complete. At which time the SecurEnvoy Server will contact Yubicloud to authenticate this key and assign the serial number marked on this key to this user account.



Temp and Static Code

A fixed 6-digit Temp or Static code can be configured as an authentication type, either by an Administrator or, if enabled, by the user via the 'Manage My Token Portal'.

The Temp Code setting under the Configuration hierarchy enables Temp Code for a set period of time as an authentication type when configuring a user. When this defined period of time has lapsed, you are able to set the Temp Code to return to either a One Time Code or Day Code.



During testing it may be beneficial to have the ability to "Allow Static Code", this is a permanent, fixed 6-digit passcode. You may decide to configure this if SMS or Email passcodes are not a viable option of authentication or available to a user for testing purposes. All of these settings can be assigned upon a per domain basis.

Pin Management

Pin Management gives you the ability to choose between using Microsoft Windows password as the Pin for each respective enabled user, or configure SecurEnvoy Cloud as the Pin management authority.

If set to SecurEnvoy Cloud, you will need to configure a Pin with a length of 4-8 numeric or alphanumeric characters. 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

Configuration - Pin Management
Domain
Cosmos.com

External LDAP
Existing LDAP password is used as the pin

SecurEnvoy

PIN Length
8

Min Upper Case Characters
1

Min Lower Case Characters
0

Pin Must Be Numeric (0-9) Only

Update

Mobile Settings

The SecurEnvoy Cloud system can be setup to validate the mobile number that is entered. 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
Cosmos.com

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
0 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 44

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

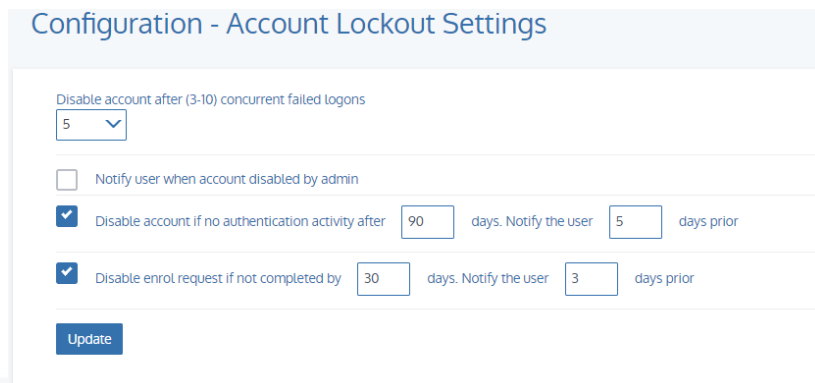
Default Users To Private Numbers
Un-check to store mobile numbers in LDAP

Update

Account Lockout Settings

The Account Lockout Settings can be configured to automatically disable a user account after 3-10 concurrent failed logons. Once disabled, no more passcodes are sent and the user will be disabled and denied access.

If using SMS as an authentication method, the user is sent an alert SMS explaining that their account is now locked.



The screenshot shows the 'Configuration - Account Lockout Settings' interface. It includes a dropdown menu for 'Disable account after (3-10) concurrent failed logons' set to '5'. There are three checkboxes: 'Notify user when account disabled by admin' (unchecked), 'Disable account if no authentication activity after 90 days. Notify the user 5 days prior' (checked), and 'Disable enrol request if not completed by 30 days. Notify the user 3 days prior' (checked). An 'Update' button is located at the bottom.

User accounts can be automatically disabled if there is no authentication activity for XX number of days. (Default value is 90 days).

In addition to this, it is possible to notify the user through SMS or Email NN number of days prior to being disabled. (Delivery of this message is dependent on the authentication type the user is enrolled with),

User accounts that do not complete an enrolment request with XX days are disabled, (Default value is 30 days).

In addition to this, it is possible to notify the user through SMS or Email NN number of days prior to having the enrolment request disabled. (Delivery of this message is dependent on the authentication type the user is enrolled with),

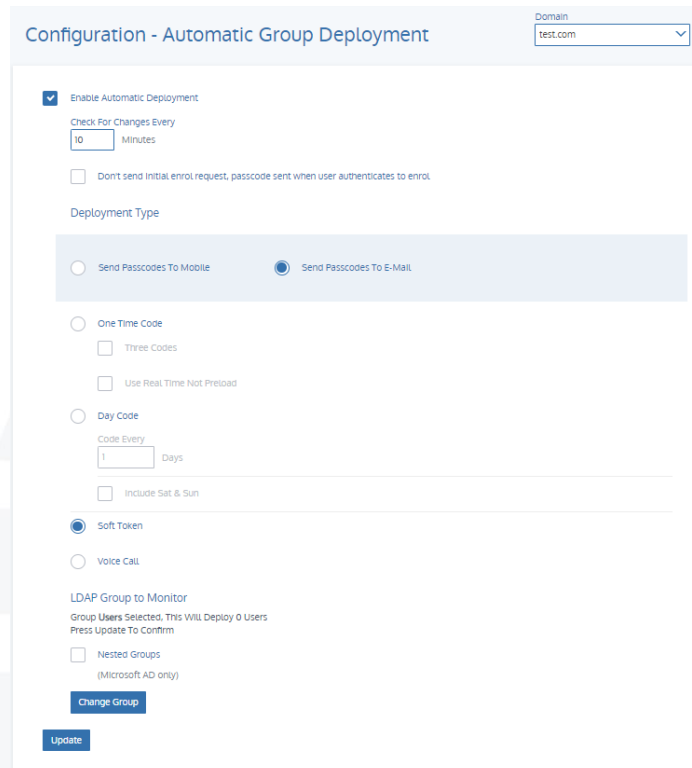
All of these settings can be assigned upon a per domain basis.

Automatic Group Deployment

The Automatic Group Deployment is an embedded feature that allows simple ongoing provisioning of users. A dedicated group of users is monitored, any user added to this group is automatically deployed with the options configured within the SecurEnvoy Cloud GUI.

Note: Only one group per domain is supported.

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



The following options are available to be set:

Send Passcodes to Mobile / Email Example

A user will remain configured with the configured method of authentication selected via Automatic Group Deployment. For example, if a group is deployed with a passcode via SMS, they will always receive a passcode via SMS. As long as the mobile attribute is populated within AD. 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 a user group is deployed to authenticate via email, they will always authenticate via email.

Note: Mobile or Email attributes must be populated within AD.

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 users to be provisioned.

Misc GUI Settings

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

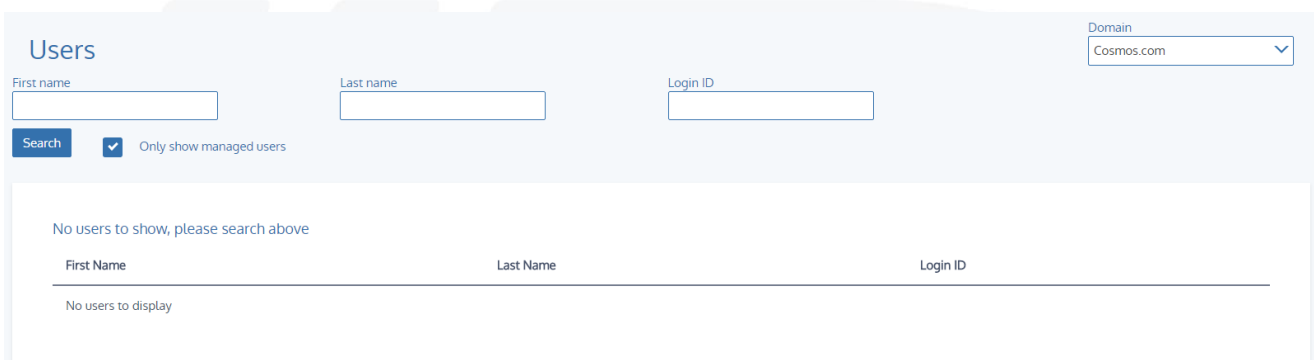
These are as follows: Hides the users' mobile settings (Encrypted) within the TelexOther attribute. Display Attributes (Not displayed by default)

User Management

Note: By default, the page will always open at the Dashboard page.

Users

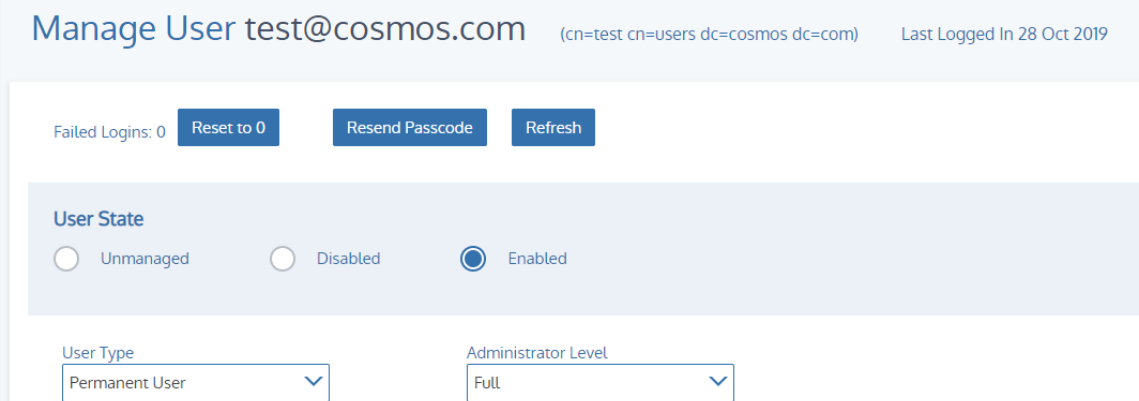
This section allows you to search and administer your LDAP (Directory Server) based users. You can enable users for two factor mobile numbers and email addresses, resend passcodes and set static passcodes



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, the first 200 users from your LDAP domain 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

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.

Authentication Type

One Time Code

Use Real Time Not Preload

Soft Token

Registered Phone Type = AndroidFirebase Resync ▾

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.

User Type

Temporary User ▾

	Date			Hour
Start	Aug ▾	30	2017	13 ▾
End	Sep ▾	30	2017	13 ▾

Send Via...
(This affects One Time Codes, Day Codes and other notifications)

Send Code to Mobile

User Enrol Private Send Simple SMS Text Some countries can't deliver dynamic sms texts

Send Code to Email

Administrator Privileges

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.

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

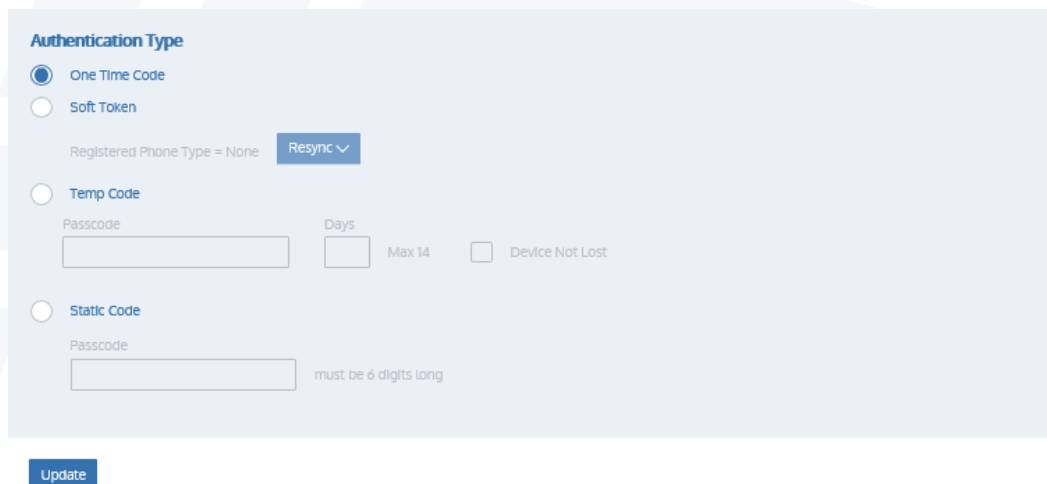
This option is displayed if passcodes are allowed via email.

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



The screenshot shows a configuration window titled "Authentication Type". It contains the following elements:

- Three radio buttons for selection: "One Time Code" (selected), "Soft Token", and "Temp Code".
- Below "Soft Token": "Registered Phone Type = None" and a "Resync" button with a dropdown arrow.
- Below "Temp Code": A "Passcode" input field, a "Days" input field with "Max 14" next to it, and a "Device Not Lost" checkbox.
- Below "Static Code": A "Passcode" input field with a note "must be 6 digits long".
- An "Update" button at the bottom left of the form area.

One Time Codes

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 Codes

This mode automates the process of changing passwords every xxx days. Day codes are reusable passcodes that are automatically changed every (x) 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

This mode supports the use of a "Soft Token", this will be available for main stream smart phones such as Apple's iPhone or Android. 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.

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



Authentication Type

One Time Code

Soft Token

Registered Phone Type = None **Resync** ▾

Code 1

Code 2

Resync

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

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.

Mobile Authenticator

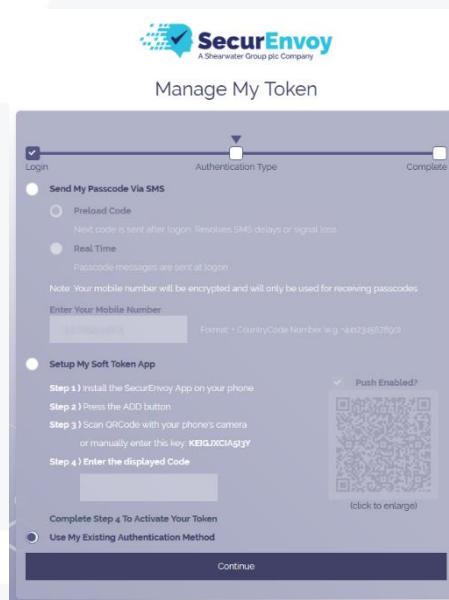
SecurEnvoy provides a Mobile Authenticator for your phone to generate one-time passcodes (OTP) for two factor authentication that can be checked by SecurEnvoy Cloud.

Multiple tokens can be enrolled and used within the same app for multiple user accounts eliminating the need to carry multiple hardware tokens or install multiple authenticator apps. SecurEnvoy cloud allows user far greater choice of security - either tokenless SMS two factor authentication or now with this Mobile Authenticator.

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

The SecurEnvoy Cloud solution allows users far greater choice of security - either tokenless SMS two factor authentication or the SecurEnvoy Cloud Mobile Authenticator app.

Available free of charge to current customers from SecurEnvoy, the SecurEnvoy Authenticator app is supported on iOS and Android, downloadable from the Apple App Store or Android Play Store.



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.

Logs into their companies SecurEnvoy Clouds enrolment page (/secenrol) – cleverly they can authenticate themselves with their current user name and passcode.

A QR Code appears in the screen which the user scans with the camera on their phone, within seconds the user is authenticated and can start using their phone as a token.

Mobile Authenticator "Soft Token"

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

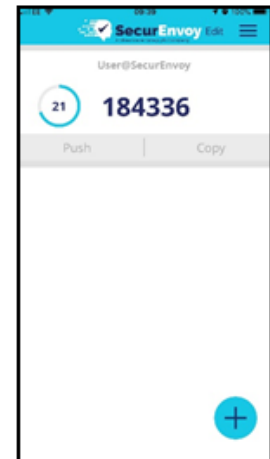
The "Soft Token" can also be re-synched by entering two following passcodes.

Send Via...
(This affects One Time Codes, Day Codes and other notifications)

Send Code to Mobile

User Enrol Private Send Simple SMS Text Some countries can't deliver dynamic sms texts

Send Code to Email



Mobile Authenticator Security

SecurEnvoy's Mobile Authenticator, 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 and Linux Open LDAP

Security Watermarking

The SecurEnvoy Cloud 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".

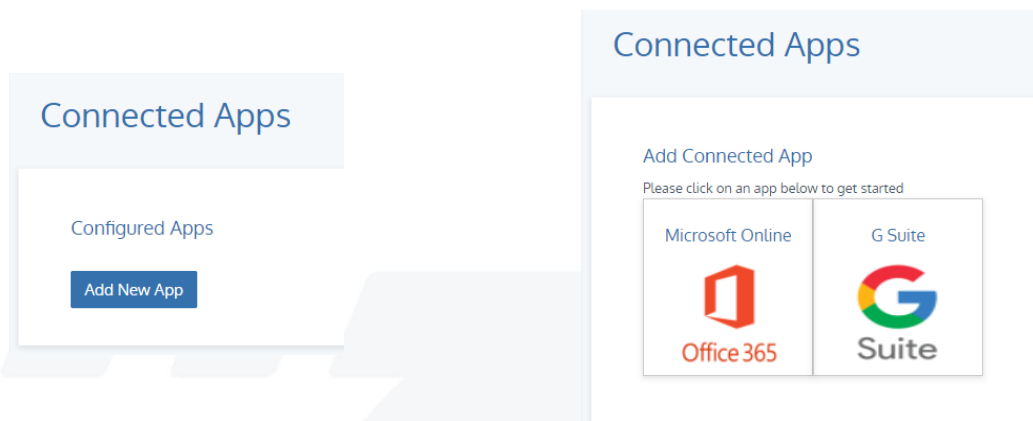
Automatic Time Re-sync

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.

Connected Apps

SecurEnvoy Cloud also supports 2FA for SaaS applications such as Microsoft Office 365 and Google G Suite. To configure these services you will need to follow the setup wizards for the respective services to integrate them with your SecurEnvoy Cloud.

The configuration of these services can be found in the left side of the SecurEnvoy Cloud GUI, under Identity > Connected Apps.



Microsoft Office365

Follow these steps to connect your Office 365 tenant

Pre-requisites

- Add company domain to corporate Office 365 Admin Account

To complete the federation of an on-premise domain to Office 365, the Azure Active Directory Connect synchronization service (Azure AD Connect) is required to take care of operations related to the synchronization of identity data between your on-premise environment and Azure AD.

1. Download and install Azure AD Connect on your domain controller.
2. On successful install, select "Customise"
3. "User Sign-In" – Select "Do not configure" and select "Next"
4. "Connect to Azure AD" - Enter Microsoft O365 Tenant authentication details e.g. `username@company.onmicrosoft.com`
5. "Connect your directories" – Select your Forest and click "Add Directory"
6. "AD Forest Account" – Select "Use existing AD account" and enter Administrator or Service Account details for the domain e.g. `domain.com\administrator`
7. "Click "Next" to continue
8. "Azure AD Sign-In configuration" – Make sure "userPrincipalname" is selected as the on-premise attribute used within Azure AD.
9. "Domain & OU Filtering" – Select "Sync all domains and OU's" unless a filter is required.
10. "Uniquely identifying your users" – Select how users are represented in your on-premise domain or select the default "Users are represented only once across all directories"
11. Select "Choose a specific attribute" to allow Azure AD to identify the users and select "objectGUID"
12. Select "Next" on remaining screens to complete configuration.
13. Select "Install" to complete the installation.

Upon completion of Azure AD Connect configuration you can select your domain and copy and paste the Windows Powershell script at the bottom of the Connected Apps – Office 365 Configuration page. See an example of this here:

On completion of Azure AD Connect, the following commands should be copied and run in a Windows Powershell window from a Desktop or Server.

First, choose the domain that you will be federating:

Domain

1. Run "Windows Powershell" in administrator mode (do not use x86 version)
2. Paste the following script into the Powershell Window

```
Install-Module MSOnline -Force  
connect-MsolService
```

Google G-Suite

Pre-requisites

- Add company domain to corporate GSuite Admin Account
- Access to a Google domain super administrator account to authorize GCDS

To complete the federation of an on-premise domain to Google GSuite, the Google Cloud Directory Sync tool (GCDS) is required to take care of operations related to the synchronization of identity data between your on-premise environment and Google.

1. Download and install Google Cloud Directory Sync on your domain controller.
2. On successful install, select "Configuration Manager" from the Google Cloud Directory Sync Folder in Windows Applications, by clicking on the windows start button.
3. Once the Google Configuration Manager starts, enter the "Primary Domain Name" that will be synced e.g. domain.com and select "Authorize Now", enter your Google Administrator login details to complete Authorisation.
4. Select "LDAP Configuration" from the left-hand menu and select the required "Server Type"
5. Select "Connection Type" – Selecting standard LDAP unless running Secure LDAP
6. Enter the Hostname or IP address of the LDAP domain controller you intend on syncing to Google.
7. Enter an Authorised User and password in the form
CN=administrator,CN=Users,DC=domain,DC=com
8. Enter you LDAP Base DN in the form of CN=Users,DC=Domain,DC=com and select "Test Connection" to confirm connectivity to your LDAP server.
9. Select "General Settings" – Use defaults, "User Accounts" and "Groups selected"
10. Select "User Accounts" (User Attributes Tab) and select "Use Defaults" Button.
11. Select the "Search Rules" tab at the top of "User Accounts" and select "Use Defaults" button.
12. Select Groups from the left pane and select the "Use Defaults" button.
13. Notifications – Enter required details to receive notifications.
14. Select "Sync" from the let pane and click "Sync & Apply Changes" unless a simulation is required beforehand.

On completion of Google Cloud Directory Sync, the following changes need to be made to the federated domain within the Google Admin Console, see example below:

On completion of Google Cloud Directory Sync, the following changes need to be made to the federated domain within the Google Admin Console.

1. Login to Google Admin Console and navigate to Security and select **"Setup Single Sign-on (SSO)"**

2. Under **"Setup SSO with third party identity provider"** enter the details listed below:

Sign-in Page URL

<https://cosmos.securenvoy.cloud/saml2>

Sign-out Page URL

<https://cosmos.securenvoy.cloud/logout>

[Download Certificate](#)

[Add](#)

Timezone

You can update your timezone for reporting and logging purposes within the SecurEnvoy Cloud configuration, to do this navigate to Config > Timezone.

Note: Timezones are in UTC time format only, they do not reflect Daylight Saving time.

Timezone

(UTC+00:00) Dublin, Edinburgh, Lisbon, London

Update

Reporting Wizard (Admin GUI)

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)

Reporting

Domain
 Cosmos.com

Show Report Options

Report: All Managed Users

Domain	First Name	Last Name	Login ID	Status	Authentication Type	Passcode Send Method	Description
Cosmos.com	Dorian	Tomkins	dtomkins	Enabled	Static Code	N/A	User last logged in 30 Aug 2017
Cosmos.com	Jack	Black	jblack	Enabled	Static Code	N/A	User last logged in 30 Aug 2017
Cosmos.com	Sales	One	Sales1	ICE	Static Code	N/A	No authentication since last enabled
Cosmos.com	Temp	One	temp1	Enabled	Voice Call	N/A	No authentication since last enabled
Cosmos.com	Temp	Two	temp2	Enabled	Temp Code	N/A	User last logged in 06 Jul 2017

Found 5

Authentication Type

Type	Percentage
Realtime	60%
Voice Call	20%
Temp Code	20%

User Status

Status	Percentage
Enabled	80%
ICE	20%

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.

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

Alerting Domain
test.com

Notification Type Emails To Alert Separate multiple addresses with semicolon (e.g. tom@abc.com;bob@xyz.com)

Licence Warnings

User Disabled

LDAP Server Timeout

Emergency HelpDesk

Web SMS Templates

Note: If you need to change the wording in the SMS Template that is sent to the user, then please contact your local SecurEnvoy Account Manager or SecurEnvoy Partner.

Please Reach Out to Your Local SecurEnvoy Team...



UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, 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

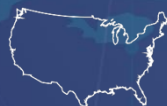


USA - Mid West

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



www.securenvoy.com