SecurEnvoy Cloud
Connector Agent Deployment

Guide

SecurEnvoy
A Shearwater Group plc Company

Table of Contents

		Page
I.	**Prerequisites**	3
II.	**Admin Portal Enrolment**	4
III.	**Domain & Connector Configuration**	8
IV.	**Enrolling an Admin User**	13
V.	**Device Enrolment**	16

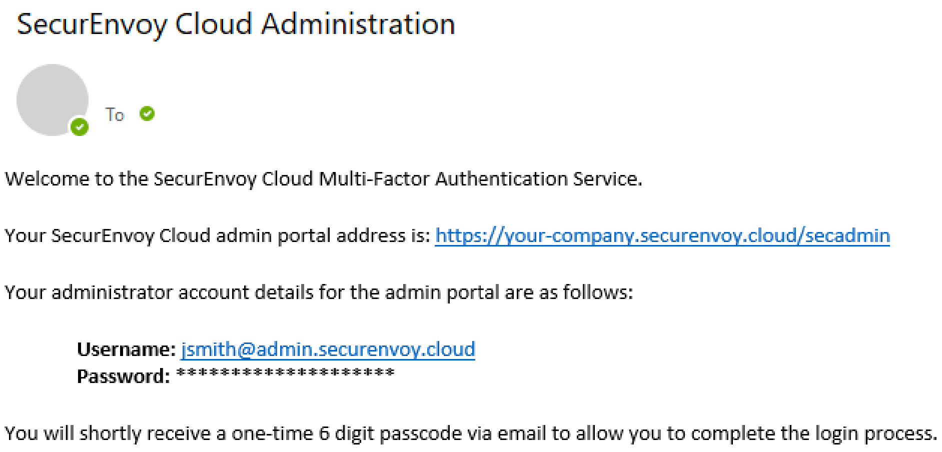
Prerequisites

SecurEnvoy Connector Agent Minimum System Requirements:

- Windows Server 2016 with;
    - Minimum of 1x vCPU
    - Minimum of 4GB RAM

Part I: Admin Portal Enrolment

1. In order to login to the SecurEnvoy Cloud Admin portal you will need your one-time Administrator username and password, which will be provided to you via email from your SecurEnvoy Account Manager/Representative [Figure 1].



SecurEnvoy Cloud Administration

To

Welcome to the SecurEnvoy Cloud Multi-Factor Authentication Service.

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

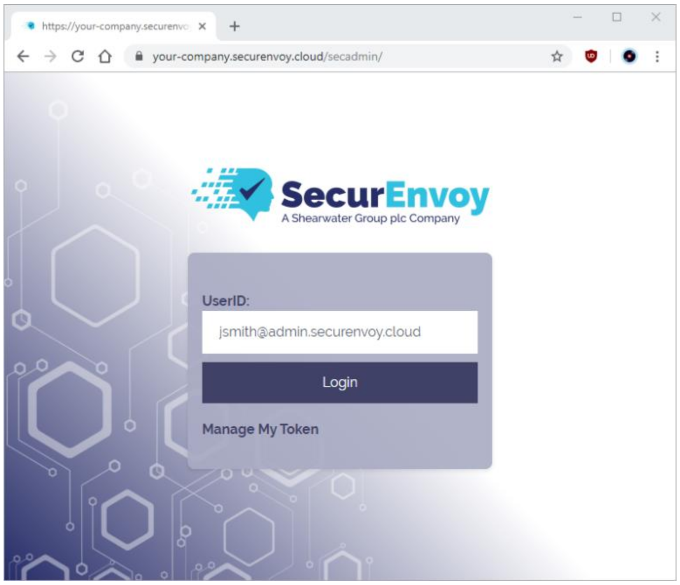
Your administrator account details for the admin portal are as follows:

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.

Figure 1 SecurEnvoy Cloud Administration Email

2. Navigate to the URL provided in the SecurEnvoy Cloud Administration email and enter the administrator username, then click ‘Login’ [Figure 2].



https://your-company.securenvo
your-company.securenvoy.cloud/secadmin/
SecurEnvoy
A Shearwater Group plc Company
Login
Manage My Token

UserID: jsmith@admin.securenvoy.cloud

Figure 2 SecurEnvoy Cloud Secadmin Web Portal – UserID

3. Enter the 20-character password provided in the SecurEnvoy Cloud Administration email and click ‘Login’ [Figure 3].

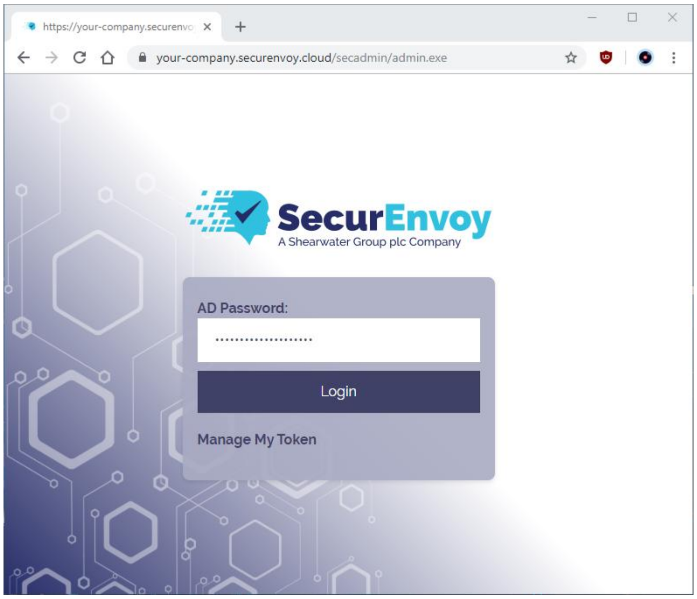
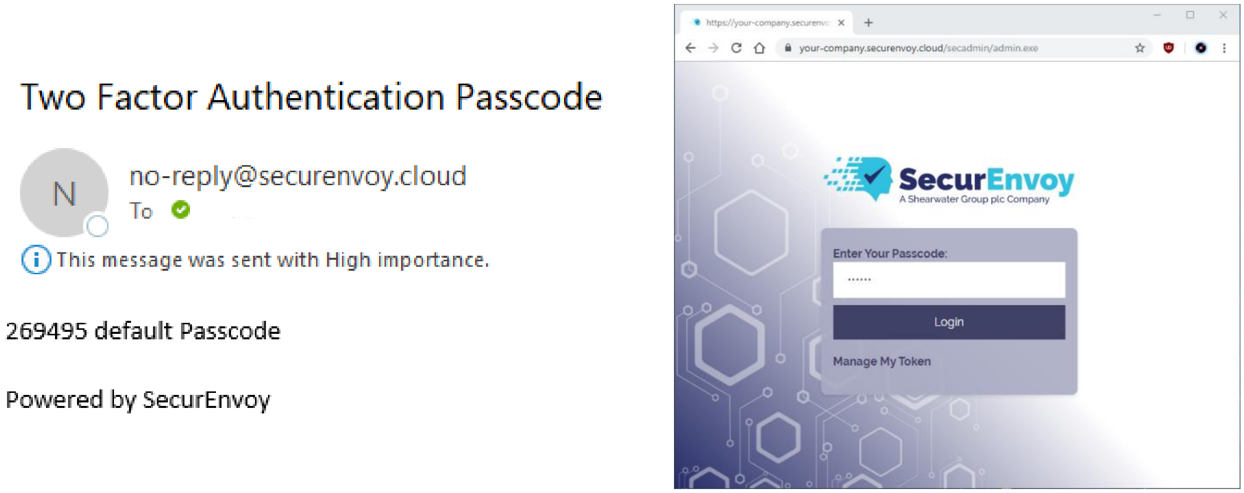

https://your-company.securenvo
your-company.securenvoy.cloud/secadmin/admin.exe
SecurEnvoy
A Shearwater Group plc Company
AD Password:
Login
Manage My Token

Figure 3 SecurEnvoy Cloud SecAdmin Web Portal – AD Password

4. If the correct username and password have been entered previously, you will receive an email from with your 6-digit Two Factor Authentication Passcode from SecurEnvoy.

- Copy and paste the 6-digit code into the field and click ‘Login’ [Figure 4].



Two Factor Authentication Passcode

no-reply@securenvoy.cloud
To

This message was sent with High importance.

269495 default Passcode

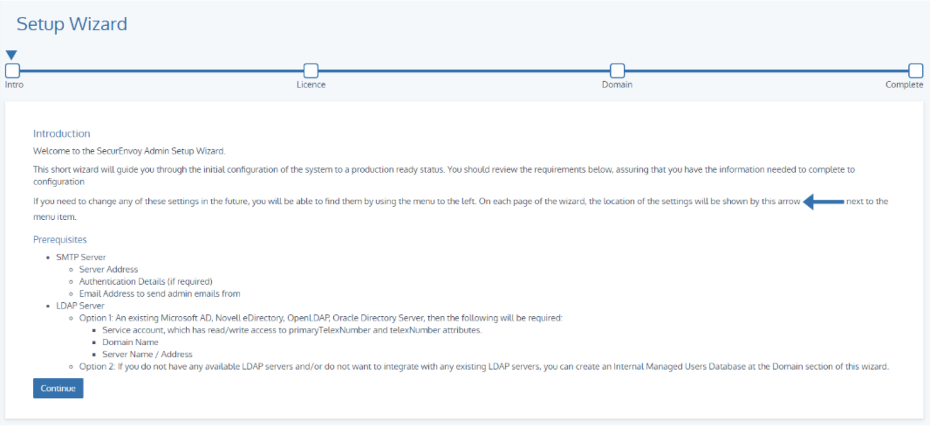
Powered by SecurEnvoy

N
https://your-company.securenvo
your-company.securenvoy.cloud/secadmin/admin.exe
SecurEnvoy
A Shearwater Group plc Company
Enter Your Passcode:
Login
Manage My Token

Figure 4 SecurEnvoy Cloud Secadmin Web Portal Enrolment – Two Factor Authentication Passcode

5. You will now be presented with the SecurEnvoy Cloud Setup Wizard [Figure 5].

    - To complete this process you will need:
        1. SecurEnvoy Cloud Licence Key
            - Provided to you by your SecurEnvoy Account Manager/Rep
        2. LDAP Domain Name
            - Administrator or Service Account credentials for the above domain
    - Click ‘Continue’.



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.

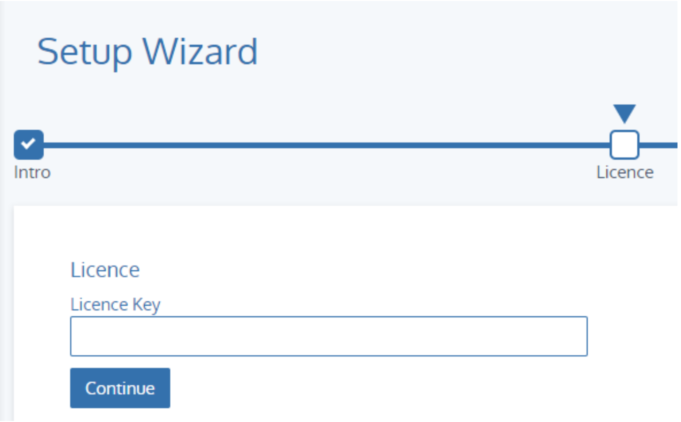
Prerequisites

- 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 primaryTelexNumber 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.

Figure 5 SecurEnvoy Cloud Setup Wizard

> 🔔 If you are using a Service Account rather than Administrator credentials, please ensure that the Service Account has read/write permissions for the following attributes;
> - primaryTelexNumber
> - telexNumber
> - mobile

6. When prompted, enter your ‘Licence Key’ and click ‘Continue’ [Figure 6].



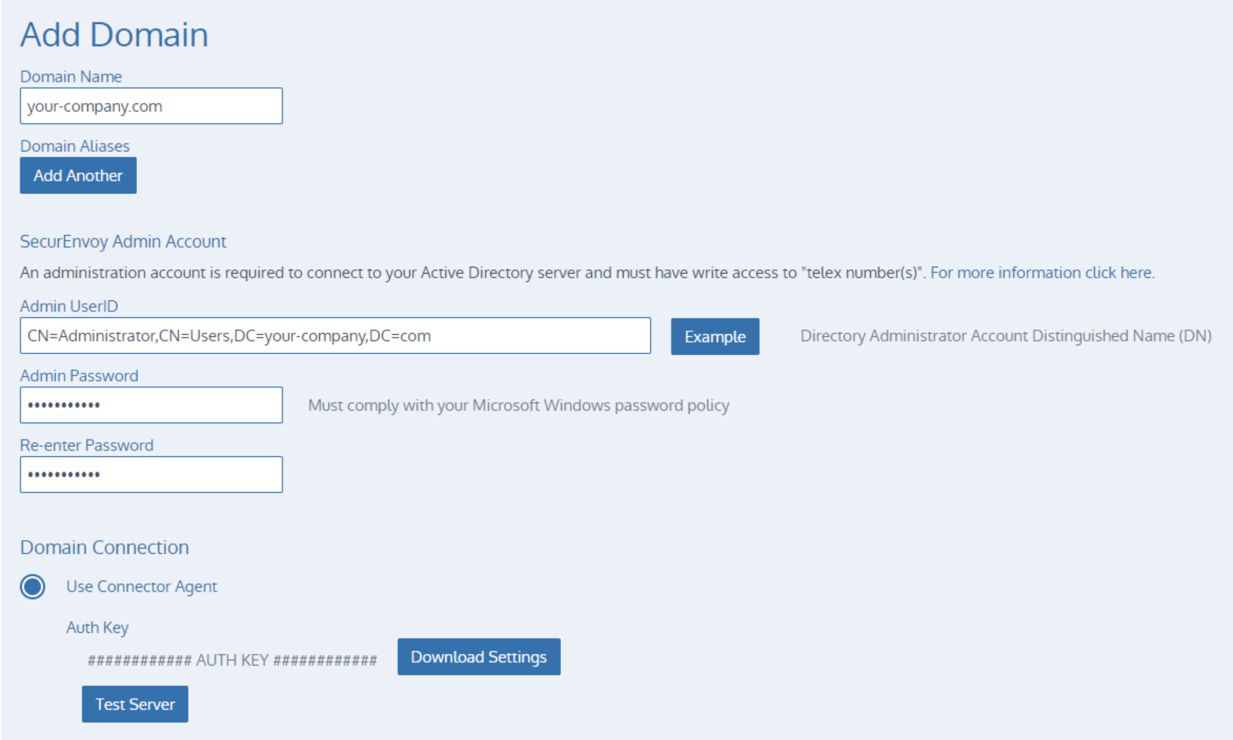
Licence

Licence Key

Figure 6 SecurEnvoy Cloud Setup Wizard – Licence Key

7. Next you will need to complete the domain configuration [Figure 7]:

- Enter LDAP Domain Name
- SecurEnvoy Admin Account, Admin UserID
    1. Copy and paste from your AD the 'distinguishedName' of the Administrator or Service Account you are using to enrol.
        - Or
    2. Click 'Example' and replace the relevant CN and DC fields with valid values for your domain of the Administrator or Service Account you are using to enrol.
- Enter the AD password for the Administrator or Service Account.
- Select the 'Use Connector Agent' check-box.
- Do not click Download Settings or Test Server at this stage.
- Click 'Continue'.



Add Domain

Domain Name: your-company.com

Domain Aliases

SecurEnvoy Admin Account

An administration account is required to connect to your Active Directory server and must have write access to "telex number(s)". For more information click here.

Admin UserID: CN=Administrator,CN=Users,DC=your-company,DC=com

Directory Administrator Account Distinguished Name (DN)

Admin Password: •••••••••••

Must comply with your Microsoft Windows password policy

Re-enter Password: •••••••••••

Domain Connection

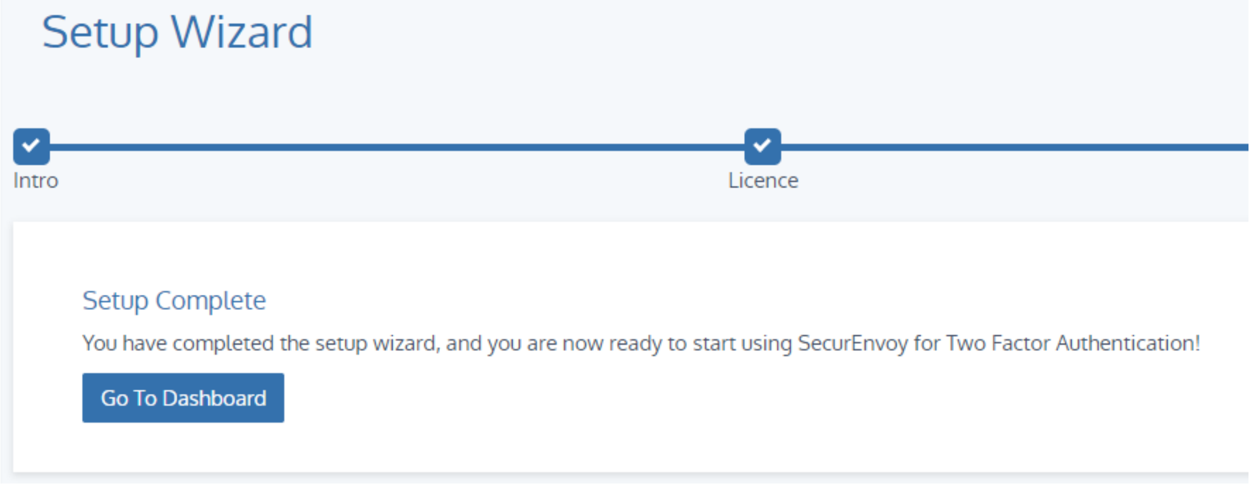
● Use Connector Agent

Auth Key: ############ AUTH KEY ############

Figure 7 SecurEnvoy Cloud Setup Wizard – Add Domain

PART II: Domain & Connector Configuration

8. After completing the Setup Wizard, click on ‘Go To Dashboard’ [Figure 8].



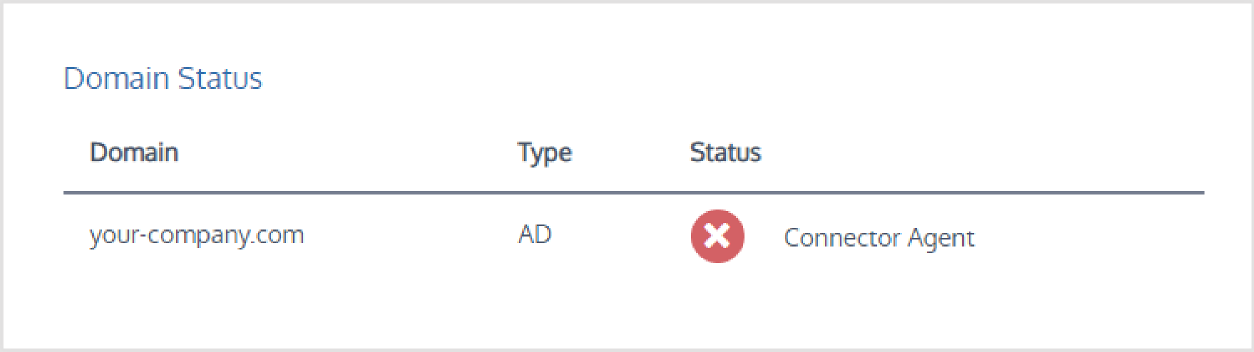
Setup Wizard

Setup Complete

You have completed the setup wizard, and you are now ready to start using SecurEnvoy for Two Factor Authentication!

Figure 8 SecurEnvoy Cloud Setup Wizard - Completion

9. You will notice on the dashboard that the ‘Domain Status’ should show as Down, this is not an error and is expected at this stage of the process [Figure 9].



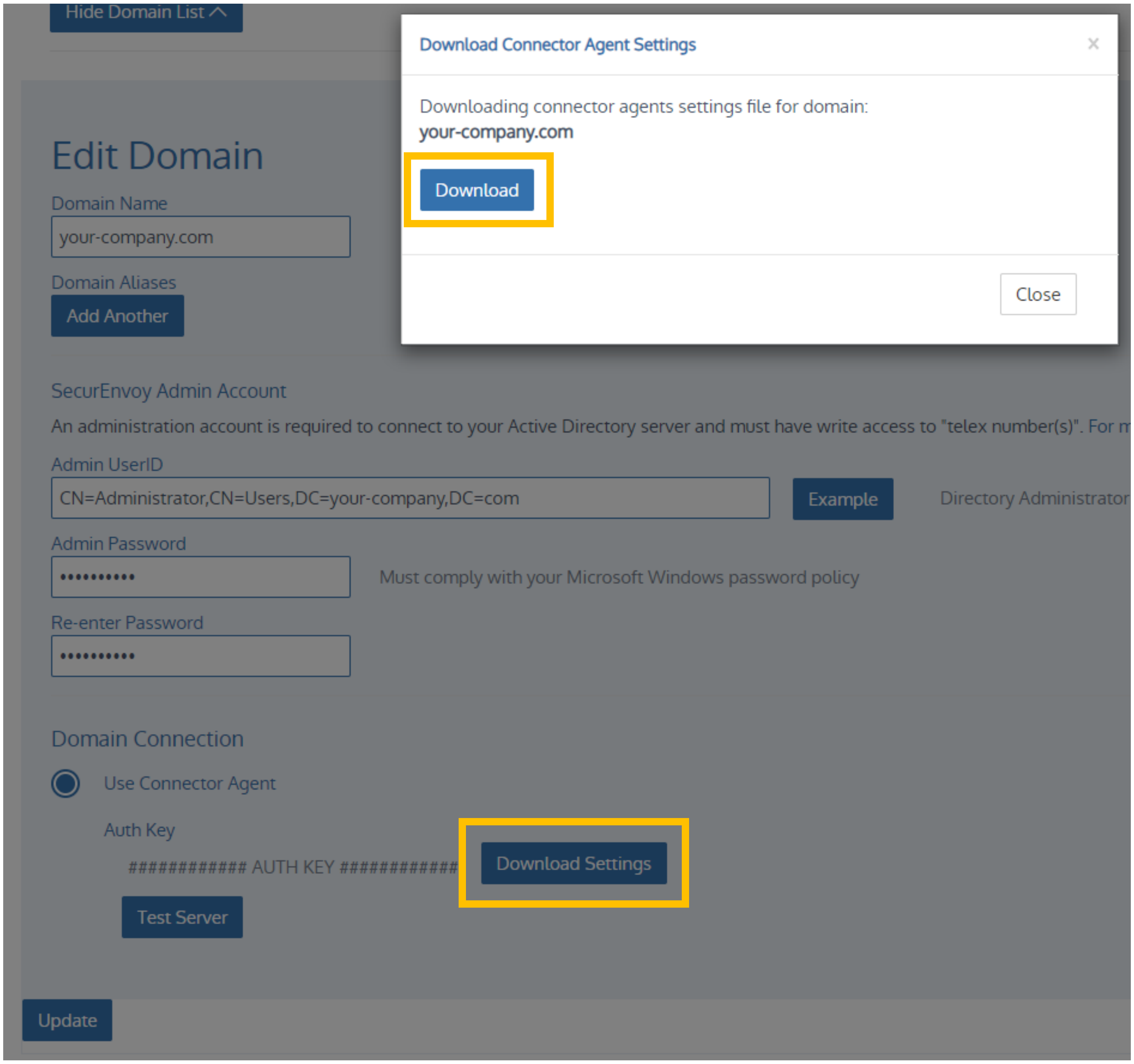
Domain Status

Domain	Type	Status
your-company.com	AD	✗ Connector Agent

Figure 9 SecurEnvoy Cloud Dashboard Domain Status

10. On the left 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 on in this process.



Download Connector Agent Settings

Downloading connector agents settings file for domain:
your-company.com

Edit Domain

Domain Name: your-company.com

Domain Aliases

SecurEnvoy Admin Account

An administration account is required to connect to your Active Directory server and must have write access to "telex number(s)". For m

Admin UserID: CN=Administrator,CN=Users,DC=your-company,DC=com

Directory Administrator

Admin Password: ••••••••••

Must comply with your Microsoft Windows password policy

Re-enter Password: ••••••••••

Domain Connection

● Use Connector Agent

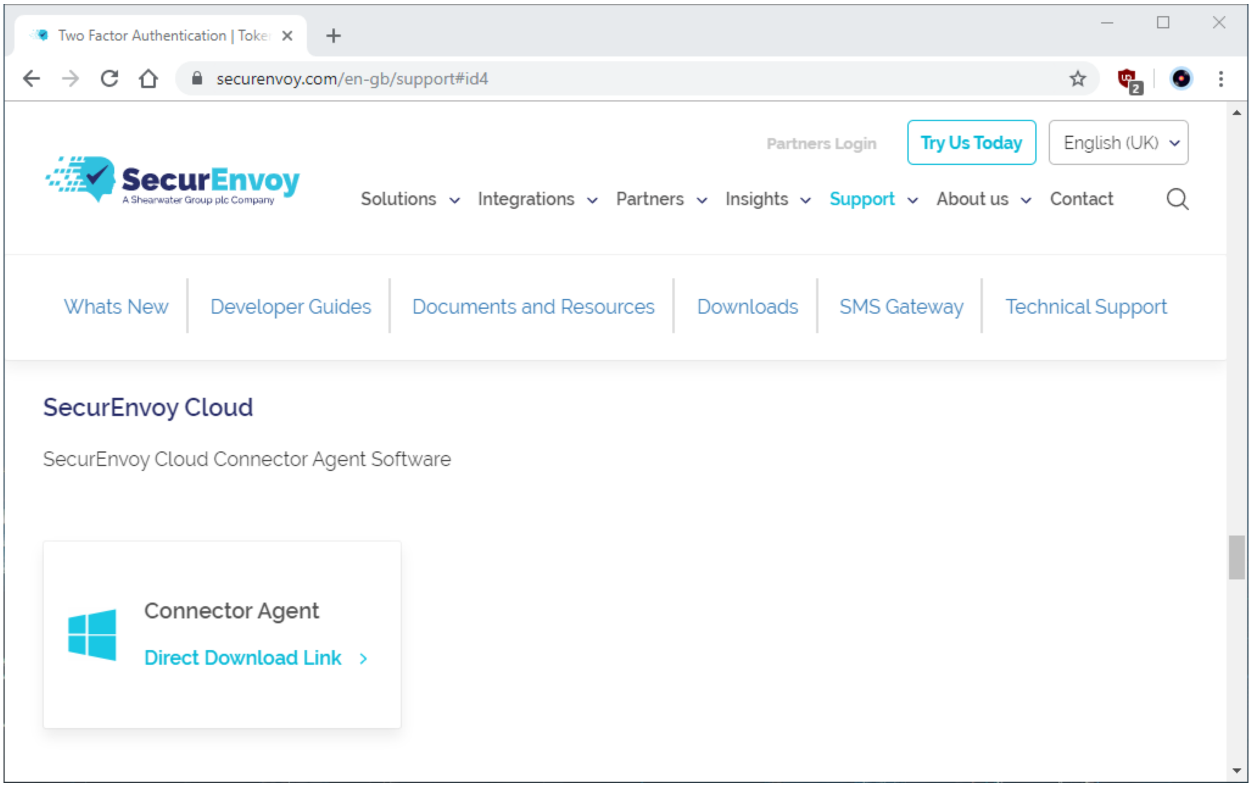
Auth Key

############ AUTH KEY ############

Figure 10 SecurEnvoy Cloud Domain Configuration

11. 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 can route to your Domain Controller.



SecurEnvoy Cloud

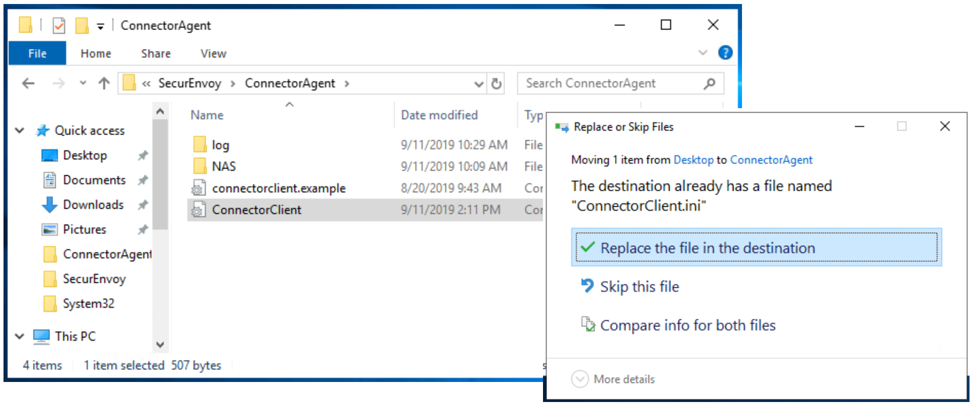
SecurEnvoy Cloud Connector Agent Software

Figure 11 SecurEnvoy Downloads

12. Now that ConnectorAgent is installed, you can move the 'ConnectorClient.ini' file to the 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
  ii. When prompted, select 'Replace the file in the destination'

- If 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].


ConnectorAgent

File Home Share View

« SecurEnvoy › ConnectorAgent ›

Search ConnectorAgent

Name	Date modified	Typ
log	9/11/2019 10:29 AM	File
NAS	9/11/2019 10:09 AM	File
connectorclient.example	8/20/2019 9:43 AM	Cor
ConnectorClient	9/11/2019 2:11 PM	Cor

4 items 1 item selected 507 bytes

Replace or Skip Files

Moving 1 item from Desktop to ConnectorAgent

The destination already has a file named "ConnectorClient.ini"

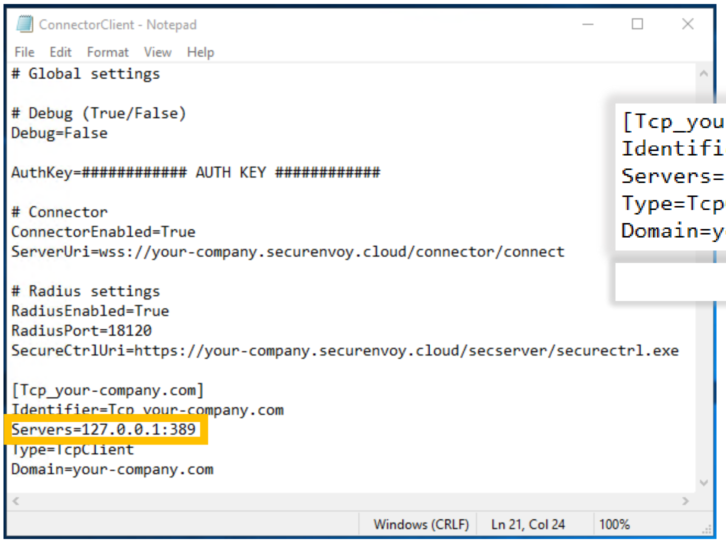
✓ Replace the file in the destination

Skip this file

Compare info for both files

More details

Figure 12 ConnectorClient.ini Filepath


ConnectorClient - Notepad

```
# 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
```

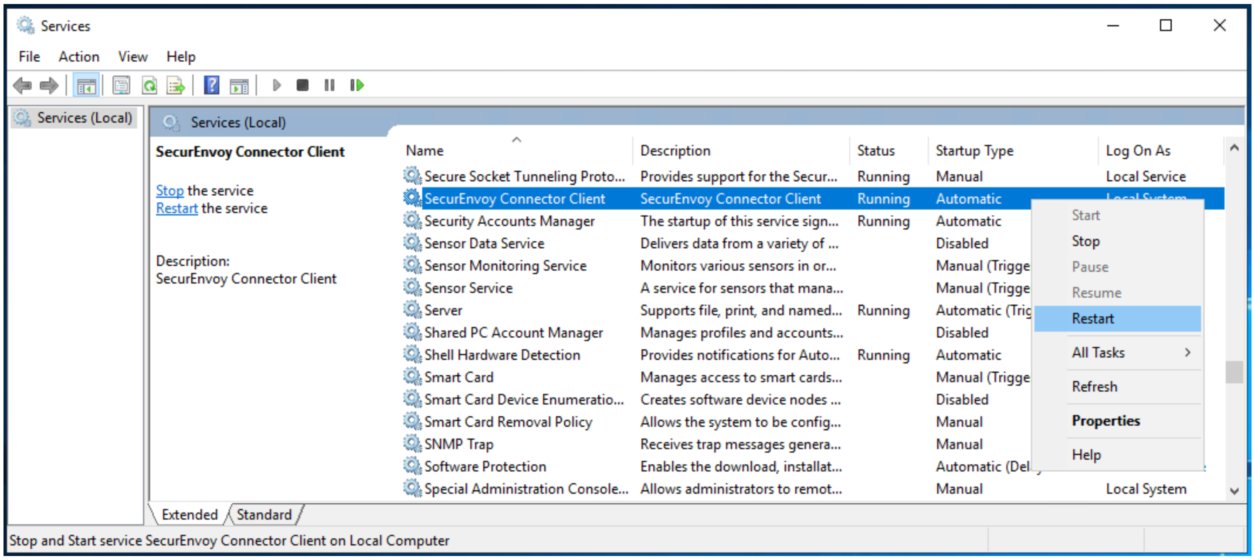
Windows (CRLF) Ln 21, Col 24 100%

```
[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 13 Optional - ConnectorClient.ini LDAP Server Configuration

13. Go to Windows Services, locate the ‘SecurEnvoy Connector Client’ service, right-click, and click ‘Restart’ [Figure 14].



SecurEnvoy Connector Client

Stop the service
Restart the service

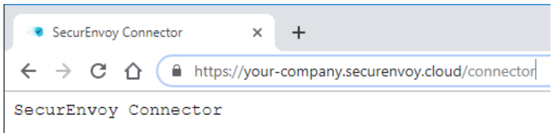
Description:
SecurEnvoy Connector Client

Name	Description	Status	Startup Type	Log On As
Secure Socket Tunneling Proto...	Provides support for the Secur...	Running	Manual	Local Service
SecurEnvoy Connector Client	SecurEnvoy Connector Client	Running	Automatic	Local System
Security Accounts Manager	The startup of this service sign...	Running	Automatic	
Sensor Data Service	Delivers data from a variety of ...		Disabled	
Sensor Monitoring Service	Monitors various sensors in or...		Manual (Trigge	
Sensor Service	A service for sensors that mana...		Manual (Trigge	
Server	Supports file, print, and named...	Running	Automatic (Tric	
Shared PC Account Manager	Manages profiles and accounts...		Disabled	
Shell Hardware Detection	Provides notifications for Auto...	Running	Automatic	
Smart Card	Manages access to smart cards...		Manual (Trigge	
Smart Card Device Enumeratio...	Creates software device nodes ...		Disabled	
Smart Card Removal Policy	Allows the system to be config...		Manual	
SNMP Trap	Receives trap messages genera...		Manual	
Software Protection	Enables the download, installat...		Automatic (Del	
Special Administration Console...	Allows administrators to remot...		Manual	Local System

Stop and Start service SecurEnvoy Connector Client on Local Computer

Figure 14 Windows Services - Restart Service for SecurEnvoy Connector Client

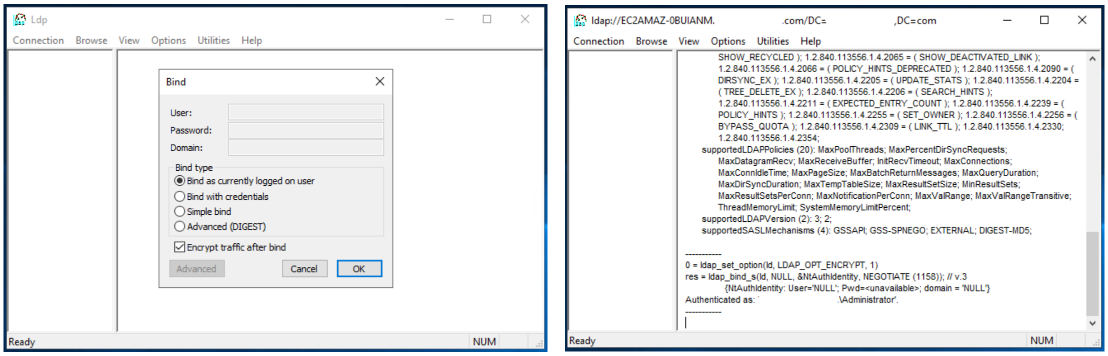
To test that the SecurEnvoy Cloud Connector is up and running, navigate to the following URL:
https://***{your-company-ID}***.securenvoy.cloud/connector
If you are presented with text ‘SecurEnvoy Connector’ then the SecurEnvoy Cloud Connector is operational [Figure 14a].



```
SecurEnvoy Connector
```

Figure 14a SecurEnvoy Connector Test URL

14. 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”’.


Ldp
Connection Browse View Options Utilities Help
Bind
Advanced
Cancel
OK
Ready
NUM
ldap://EC2AMAZ-0BUIANM. .com/DC= ,DC=com
Connection Browse View Options Utilities Help
Ready
NUM

User:
Password:
Domain:

Bind type
● Bind as currently logged on user
○ Bind with credentials
○ Simple bind
○ Advanced (DIGEST)

☑ Encrypt traffic after bind

```
          SHOW_RECYCLED ); 1.2.840.113556.1.4.2065 = ( SHOW_DEACTIVATED_LINK );
          1.2.840.113556.1.4.2066 = ( POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = (
          DIRSYNC_EX ); 1.2.840.113556.1.4.2205 = ( UPDATE_STATS ); 1.2.840.113556.1.4.2204 =
          ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = ( SEARCH_HINTS );
          1.2.840.113556.1.4.2211 = ( EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = (
          POLICY_HINTS ); 1.2.840.113556.1.4.2255 = ( SET_OWNER ); 1.2.840.113556.1.4.2256 = (
          BYPASS_QUOTA ); 1.2.840.113556.1.4.2309 = ( LINK_TTL ); 1.2.840.113556.1.4.2330;
          1.2.840.113556.1.4.2354;
      supportedLDAPPolicies (20): MaxPoolThreads; MaxPercentDirSyncRequests;
          MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout; MaxConnections;
          MaxConnIdleTime; MaxPageSize; MaxBatchReturnMessages; MaxQueryDuration;
          MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets;
          MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive;
          ThreadMemoryLimit; SystemMemoryLimitPercent;
      supportedLDAPVersion (2): 3; 2;
      supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
0 = ldap_set_option(ld, LDAP_OPT_ENCRYPT, 1)
res = ldap_bind_s(ld, NULL, &NtAuthIdentity, NEGOTIATE (1158)); // v.3
          {NtAuthIdentity: User='NULL'; Pwd=<unavailable>; domain = 'NULL'}
Authenticated as: '                    .\Administrator'.
-----------
```

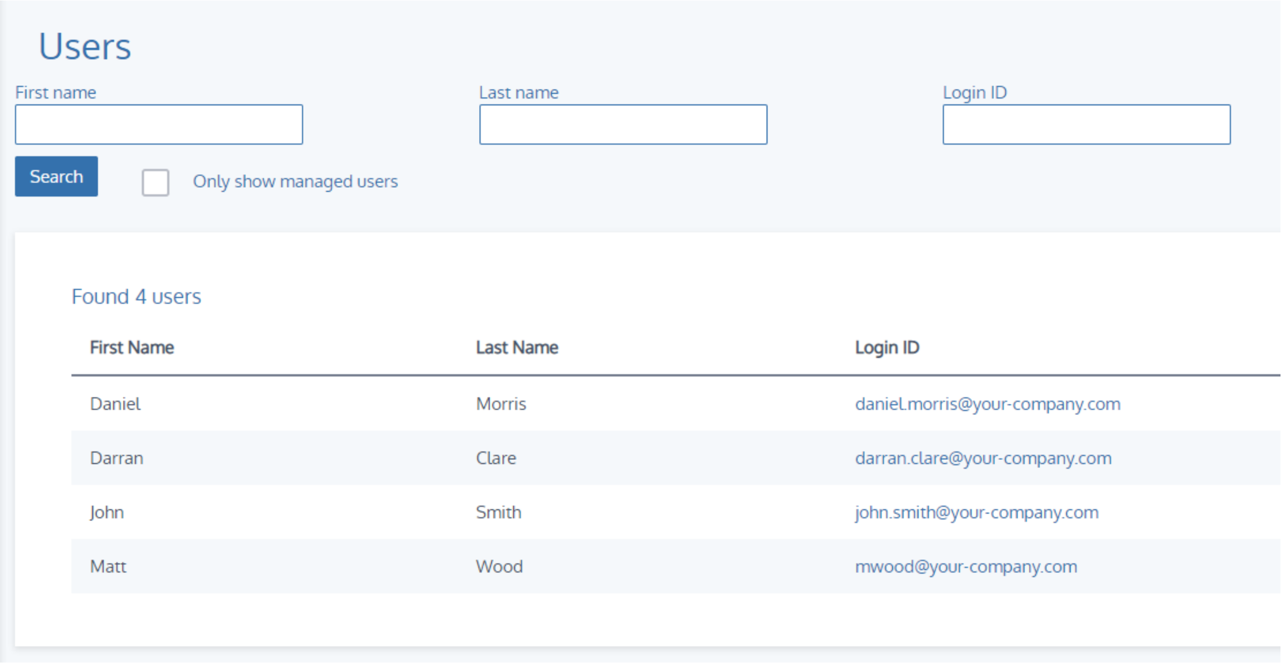
Figure 14b ldp.exe LDAP bind testing

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

Part III: Enrolling An Admin User

15. Return to the SecurEnvoy Cloud Dashboard and on the left side panel, click on ‘Users’ [Figure 15].

- Click ‘Search’ and select the user you wish to enable for admin access to SecurEnvoy Cloud and MFA.



Users

First name

Last name

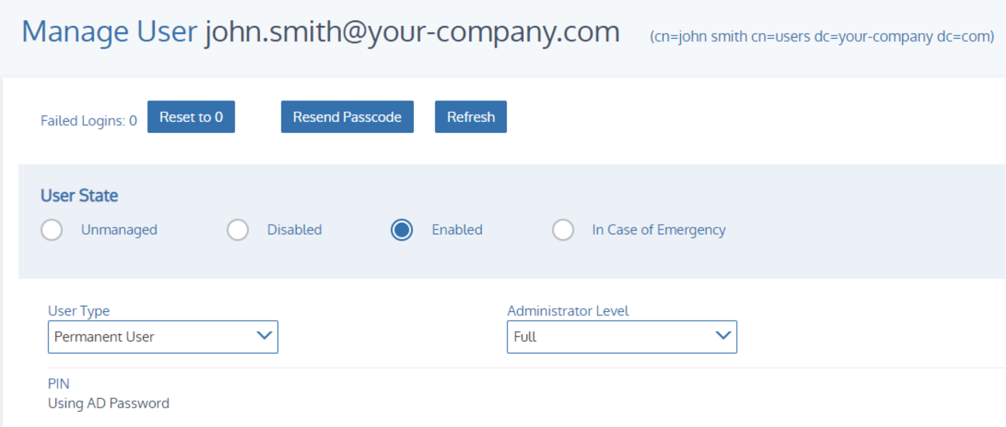
Login ID

Found 4 users

First Name	Last Name	Login ID
Daniel	Morris	daniel.morris@your-company.com
Darran	Clare	darran.clare@your-company.com
John	Smith	john.smith@your-company.com
Matt	Wood	mwood@your-company.com

Figure 15 SecurEnvoy Cloud Users

16. Click Enabled and change the Administrator Level to Full [Figure 16].



Manage User john.smith@your-company.com (cn=john smith cn=users dc=your-company dc=com)

Failed Logins: 0

User State

○ Unmanaged ○ Disabled ● Enabled ○ In Case of Emergency

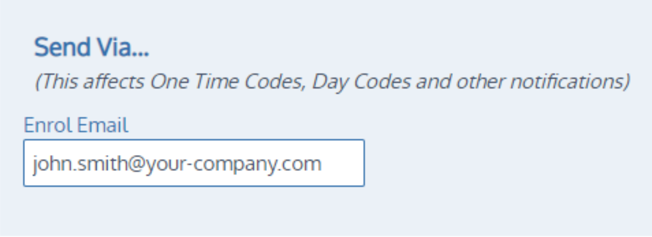
User Type: Permanent User

Administrator Level: Full

PIN
Using AD Password

Figure 16 SecurEnvoy Cloud Enable Administrator User

17. Check that the email field contains the correct email address [Figure 17].



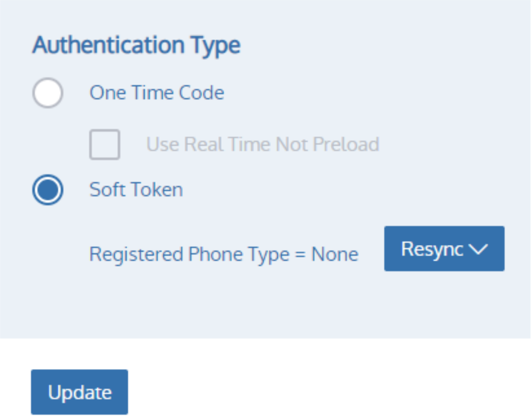
Send Via...

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

Enrol Email: john.smith@your-company.com

Figure 17 SecurEnvoy Cloud Administrator Enrolment Email Address

18. Choose Authentication Type 'Soft Token' [Figure 18].



Authentication Type

○ One Time Code

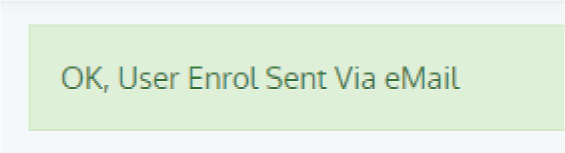
□ Use Real Time Not Preload

● Soft Token

Registered Phone Type = None

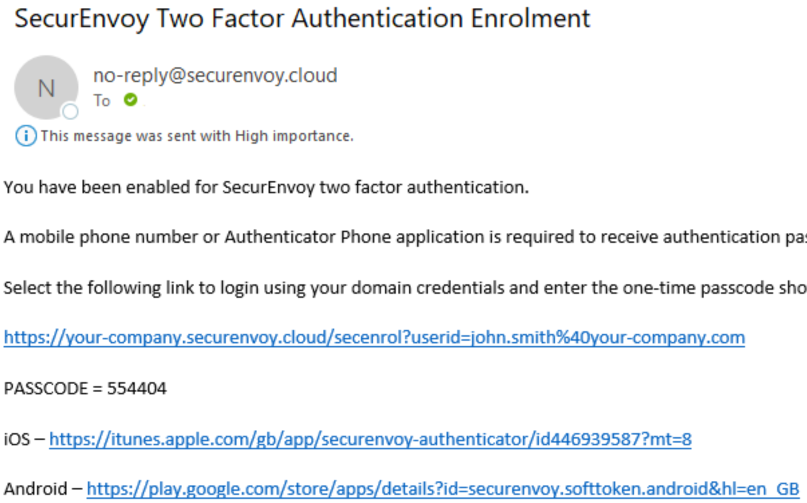
Figure 18 SecurEnvoy Cloud Administrator Authentication Type

19. Click ‘Update’, this should trigger an enrolment email to be sent to the above email address from Step 16. [Figure 19 & Figure 20].



OK, User Enrol Sent Via eMail

Figure 20 SecurEnvoy Cloud Enrolment Email Sent to Administrator User



SecurEnvoy Two Factor Authentication Enrolment

no-reply@securenvoy.cloud
To

This message was sent with High importance.

You have been enabled for SecurEnvoy two factor authentication.

A mobile phone number or Authenticator Phone application is required to receive authentication passcodes.

Select the following link to login using your domain credentials and enter the one-time passcode shown below.

https://your-company.securenvoy.cloud/secenrol?userid=john.smith%40your-company.com

PASSCODE = 554404

iOS – https://itunes.apple.com/gb/app/securenvoy-authenticator/id446939587?mt=8

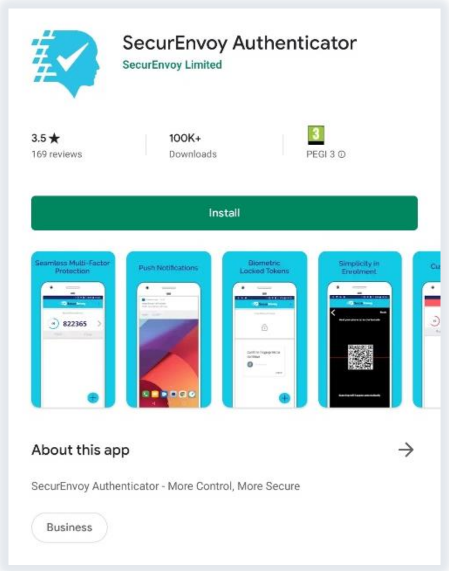
Android – https://play.google.com/store/apps/details?id=securenvoy.softtoken.android&hl=en_GB

Figure 19 SecurEnvoy 2FA Enrolment Email

Part IV: Device Enrolment

20. Install the SecurEnvoy Authenticator Application by SecurEnvoy Limited.

- Google Play Store on Android [Figure 21]
- App Store on iOS

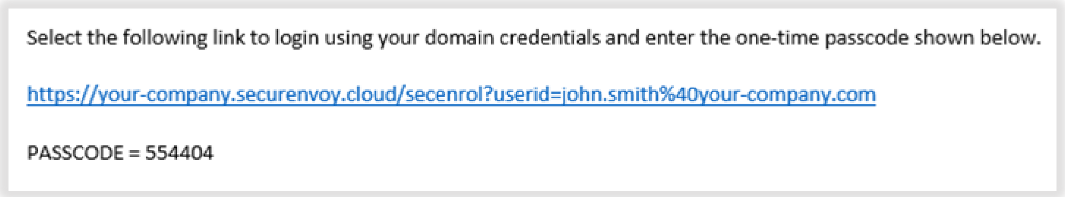


SecurEnvoy Authenticator
SecurEnvoy Limited

SecurEnvoy Authenticator - More Control, More Secure

Figure 21 SecurEnvoy Authenticator on Google Play Store

21. Click on the enrolment URL provided in the SecurEnvoy Two Factor Authentication Enrolment email [Figure 22].



Select the following link to login using your domain credentials and enter the one-time passcode shown below.

https://your-company.securenvoy.cloud/secenrol?userid=john.smith%40your-company.com

PASSCODE = 554404

Figure 22 SecurEnvoy 2FA Enrolment Email URL & Passcode

22. Enter your AD Administrator or Service Account Username and AD Password [Figure 23].

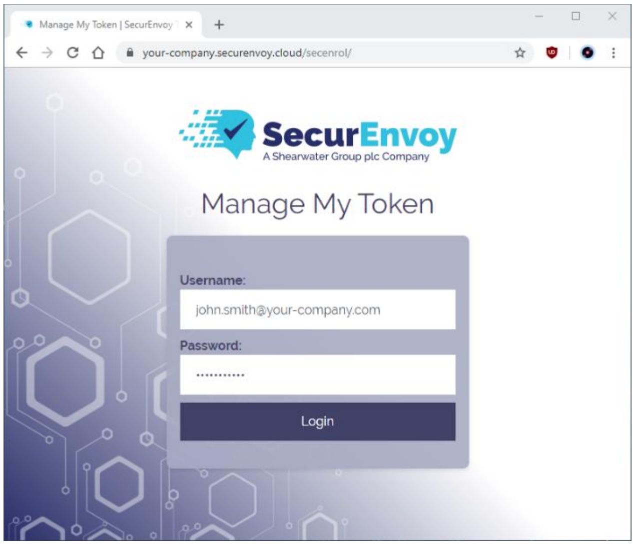

Manage My Token | SecurEnvoy
your-company.securenvoy.cloud/secenrol/
SecurEnvoy
A Shearwater Group plc Company
Manage My Token
Username:
john.smith@your-company.com
Password:
············
Login

Figure 23 SecurEnvoy SecEnrol Portal

23. Copy and paste the one-time 6-digit Passcode from the SecurEnvoy Two Factor Authentication enrolment email, from Step 18 [Figure 24].

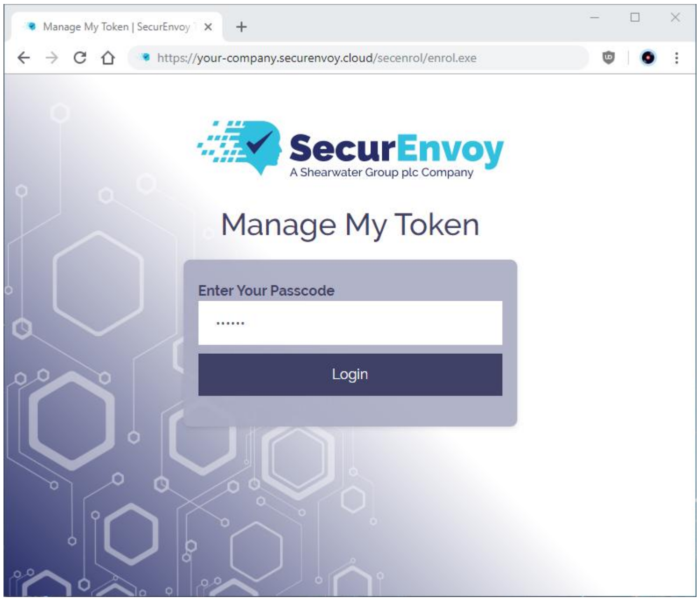
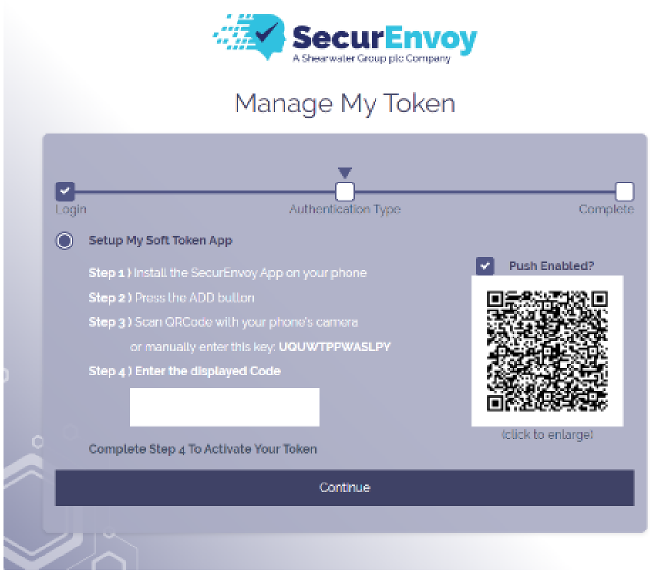

Manage My Token | SecurEnvoy
https://your-company.securenvoy.cloud/secenrol/enrol.exe
SecurEnvoy
A Shearwater Group plc Company
Manage My Token
Enter Your Passcode
······
Login

Figure 24 SecurEnvoy SecEnrol Portal Passcode

24. You will now be presented with the SecurEnvoy Manage My Token ‘Soft Token App’ setup wizard [Figure 25].



Manage My Token

○ Setup My Soft Token App

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: **UQUWTPPWASLPY**

Step 4) Enter the displayed Code

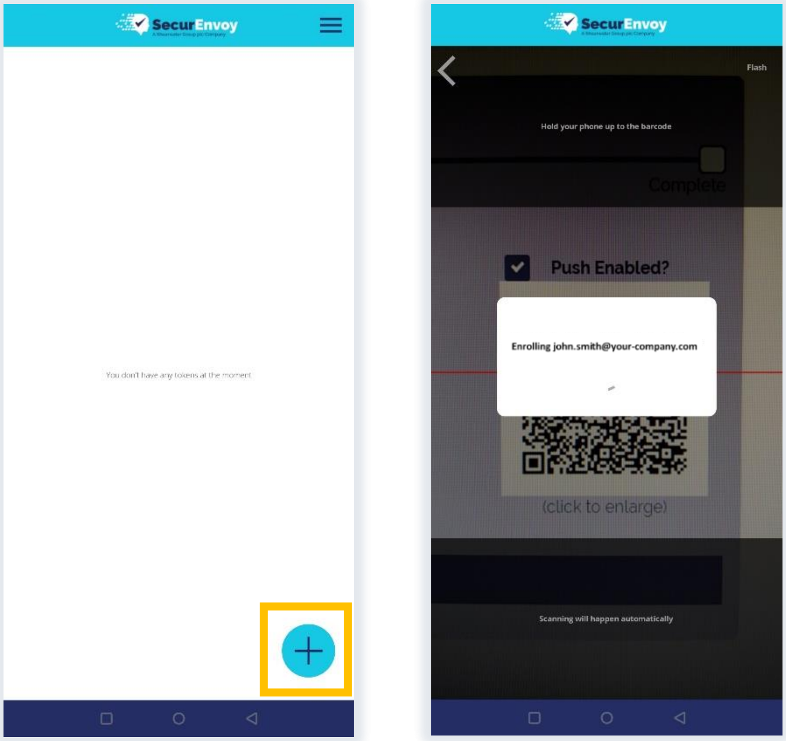
Complete Step 4 To Activate Your Token

☑ Push Enabled?

Figure 25 SecurEnvoy Cloud SecEnrol Manage My Token Wizard

25. Open the SecurEnvoy Authenticator app on your device, press the (+) symbol and scan QR code on the screen of your local machine [Figure 26].

- When prompted, allow the SecurEnvoy Authenticator app to use the device camera.



You don't have any tokens at the moment

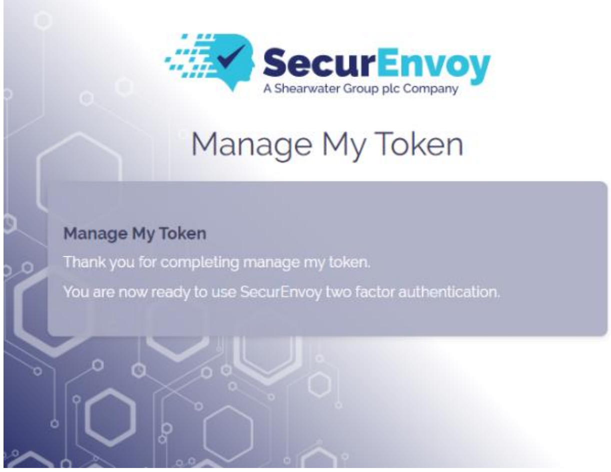
Hold your phone up to the barcode

Enrolling john.smith@your-company.com

Scanning will happen automatically

Figure 26 SecurEnvoy Authenticator App QR Code Enrolment

26. After a short period of time, the SecurEnvoy Authenticator app will be enrolled to the SecurEnvoy Cloud service [Figure 27].



SecurEnvoy
A Shearwater Group plc Company

Manage My Token

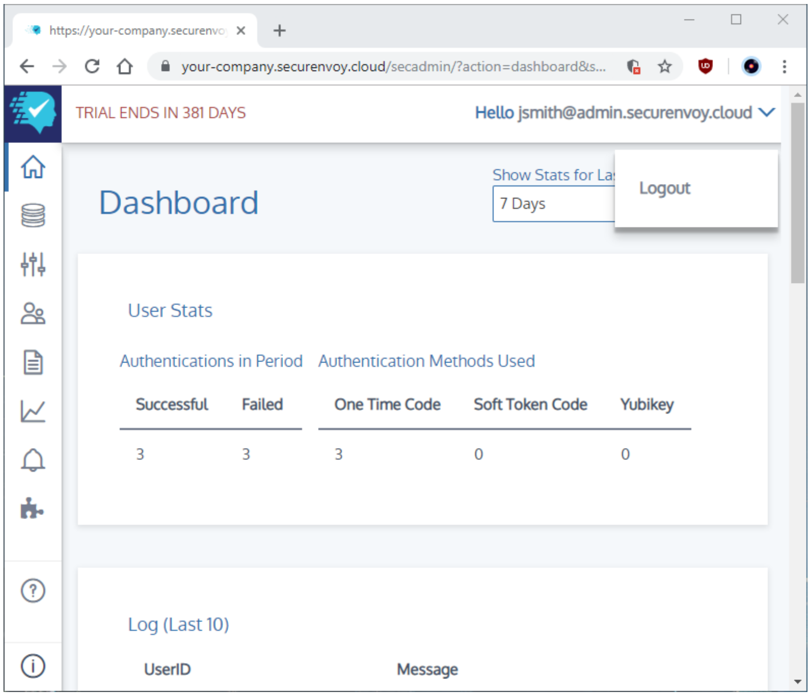
Manage My Token

Thank you for completing manage my token.

You are now ready to use SecurEnvoy two factor authentication.

Figure 27 SecurEnvoy Manage My Token Completion

27. Return to the SecurEnvoy Cloud Administrator portal, ([https://[your-company].securenvoy.cloud/secadmin/](https://[your-company].securenvoy.cloud/secadmin/)) and logout the Administrator or Service Account user [Figure 28].



https://your-company.securenvo
your-company.securenvoy.cloud/secadmin/?action=dashboard&s...

TRIAL ENDS IN 381 DAYS

Hello jsmith@admin.securenvoy.cloud

Dashboard

Show Stats for La

7 Days

Logout

User Stats

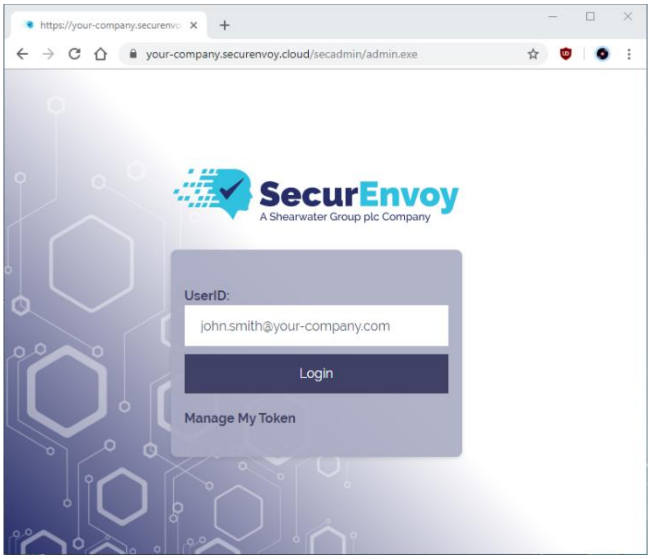
Authentications in Period		Authentication Methods Used		
Successful	Failed	One Time Code	Soft Token Code	Yubikey
3	3	3	0	0

Log (Last 10)

UserID Message

Figure 28 SecurEnvoy Cloud Secadmin Dashboard Logout Enrolment Admin

28. Login with configured user from Step 14 [Figure 29].

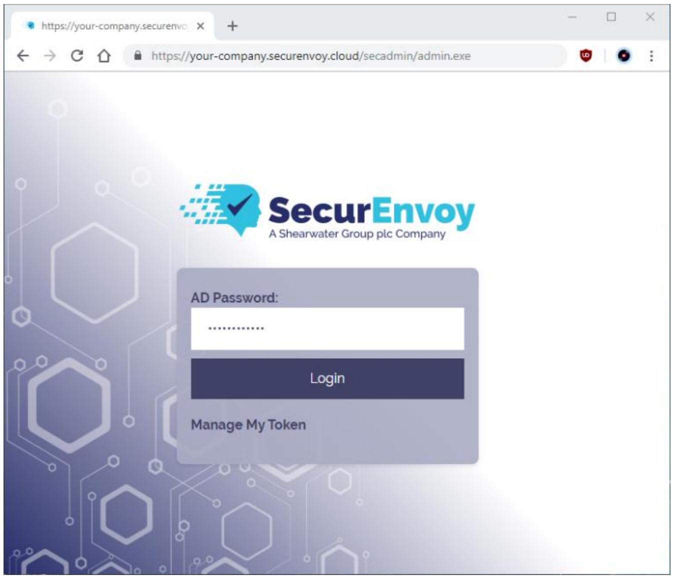

https://your-company.securenvoy.cloud/secadmin/admin.exe

UserID:

john.smith@your-company.com

Figure 29 SecurEnvoy Secadmin Web Portal Login UserID

29. Enter the AD Password for the Administrator or Service Account [Figure 30].

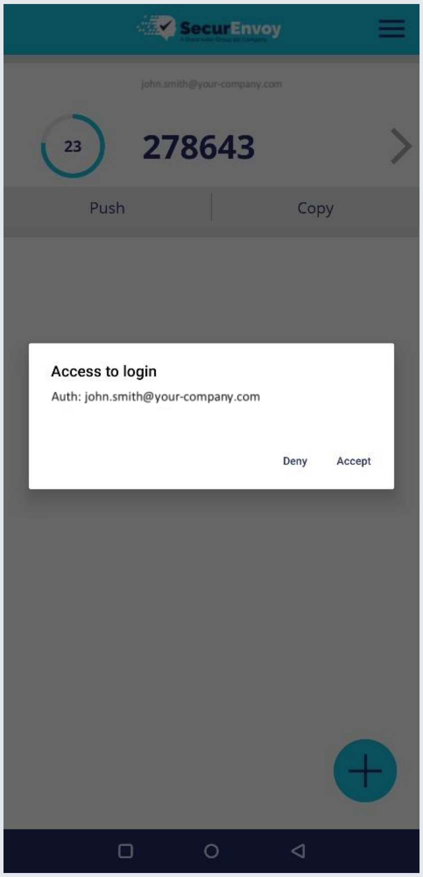

https://your-company.securenvoy.cloud/secadmin/admin.exe

AD Password:

•••••••••••••

Figure 30 SecurEnvoy Secadmin Web Portal AD Password

30. Wait for push notification on device that has SecurEnvoy app (Step 19) and press ‘Accept’ [Figure 31].

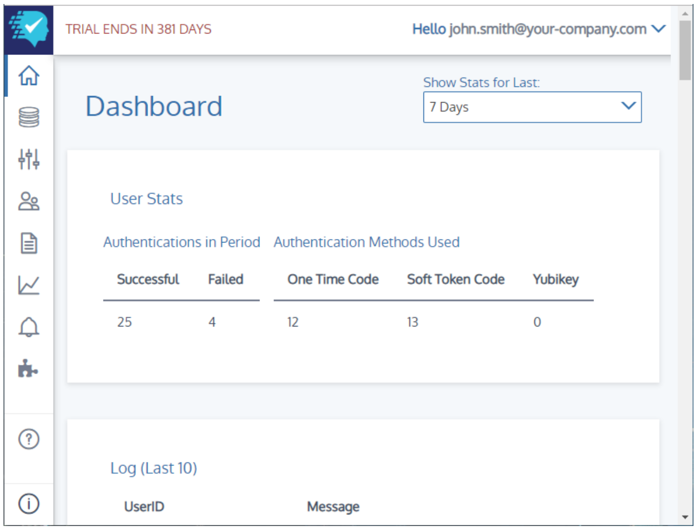


Access to login

Auth: john.smith@your-company.com

Figure 31 SecurEnvoy Authenticator App Notification

31. You should now be logged into the SecurEnvoy Dashboard with your own Administrator or Service Account credentials [Figure 32].



TRIAL ENDS IN 381 DAYS

Hello john.smith@your-company.com

Dashboard

Show Stats for Last: 7 Days

User Stats

Authentications in Period		Authentication Methods Used		
Successful	Failed	One Time Code	Soft Token Code	Yubikey
25	4	12	13	0

Log (Last 10)

UserID Message

Figure 32 SecurEnvoy Cloud Secadmin Web Portal Dashboard