

# Cloud Services via Active Directory Federated Services (ADFS) V4.0

**Authenticating Users Using SecurAccess  
Server by SecurEnvoy**

# ADFS V4.0

## Contents

1.0	CLOUD SERVICES WITH ADFS V4.0.....	3
1.1	PREREQUISITES.....	4
1.1.1	CONFIGURE ADFS WITH A CLOUD SERVICE ACCOUNT .....	5
1.1.2	OVERVIEW OF ADFS WITH SECURENVOY AND CLOUD SERVICES .....	5
2.0	CONFIGURING SECURENVOY RADIUS CLIENT .....	6
2.1	RADIUS CLIENT SETUP.....	6
3.0	INSTALLING THE MS SERVER AGENT ON YOUR MS ADFS SERVER .....	7
3.1	CONFIGURING THE MICROSOFT SERVER AGENT FOR ADFS .....	7
3.2	CONFIGURING THE MICROSOFT SERVER AGENT FOR ADFS .....	8
3.3	ENABLING MFA AUTHENTICATION POLICY.....	8
4.0	TESTING MFA AUTHENTICATION.....	9
5.0	NOTES .....	10

## 1.0 Cloud Services with ADFS v4.0

This document describes how to integrate Cloud Services configured for SSO to a local ADFS 4.0 service with SecurEnvoy two-factor Authentication solution called 'SecurAccess'

Cloud services are designed to provide easy, scalable access to applications, resources and services that can be configured to use a local Active Directory Federation Service (ADFS) and enable local users to sign on with their existing AD credentials.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Cloud Services), without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into any LDAP server and negates the need for additional User Security databases. SecurAccess consists of two core elements: A Radius Server and Authentication server. The Authentication server is directly integrated with LDAP in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing LDAP password. Utilizing the LDAP password as the PIN, allows the User to enter their UserID, Domain password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. It provides a seamless login into the Windows Server environment by entering three pieces of information. SecurEnvoy utilizes a web GUI for configuration. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

### Cloud Services

Any SAML ADFS V4 Claims Aware Application or Cloud Service

### Microsoft

Microsoft Windows Server 2016

### SecurEnvoy

SecurEnvoy Server (can be installed on the same server as ADFS or on a separate server)

SecurEnvoy Microsoft Server Agent must be installed on the ADFS server

SecurAccess software release v9.3.502

## 1.1 Prerequisites

SecurEnvoy Security Server has been installed with the Radius service configured with a suitable account that has read and write privileges to the Active Directory. If firewalls are between the SecurEnvoy Security server, Active Directory servers, and the ADFS server(s), additional open ports will be required.

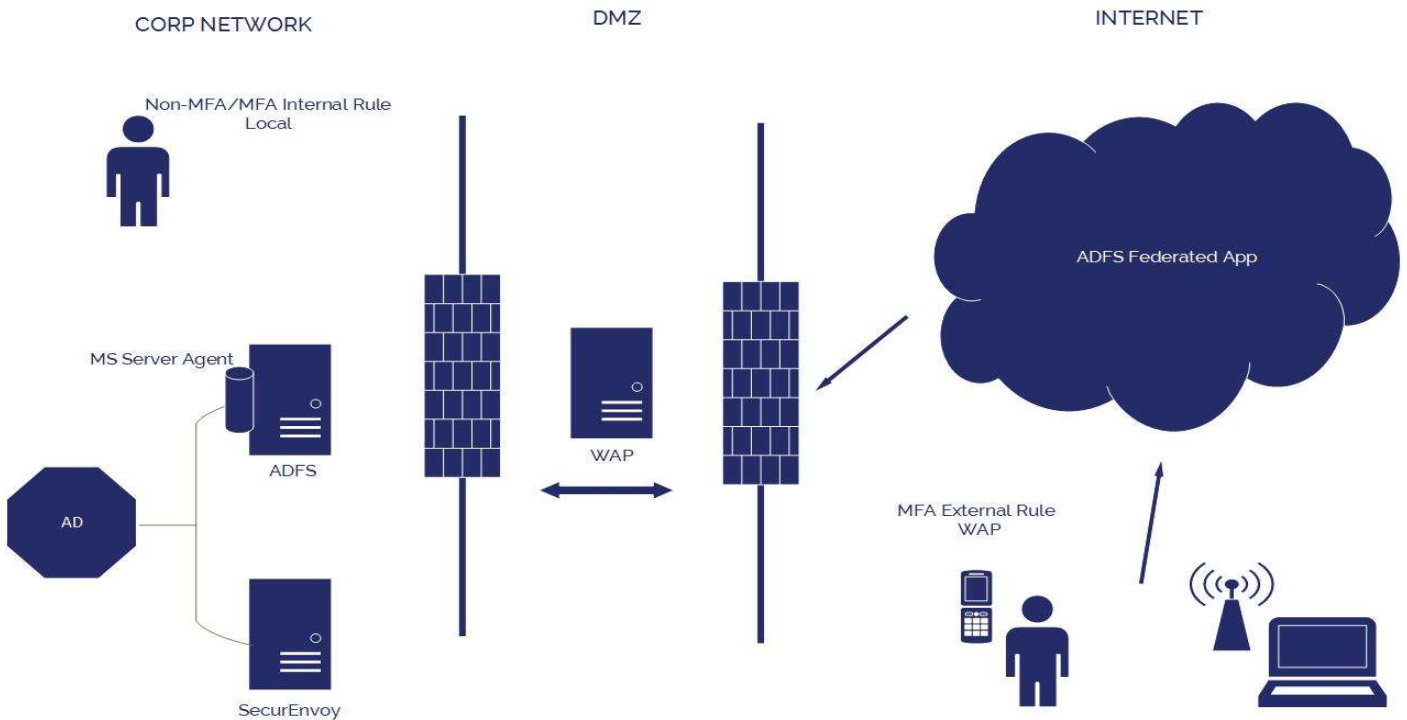
The following table shows what tokens types are supported.

Token Type Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓
Online Push	✓

### 1.1.1 Configure ADFS with a Cloud Service Account

Install and configure ADFS V4 with your SAML claims aware application or other cloud service that supports ADFS V4.

### 1.1.2 Overview of ADFS with SecurEnvoy and Cloud Services



Active Directory Federation Service (ADFS) is a software component from Microsoft® that allows users to use single sign-on (SSO) to authenticate to multiple web applications which may be located across organization boundaries.

Identity federation is established between two organizations by establishing trust between two security realms. A federation server on one side (the Accounts side) authenticates the user through the standard means in Active Directory Domain Services and then issues a token containing a series of claims about the user, including its identity.

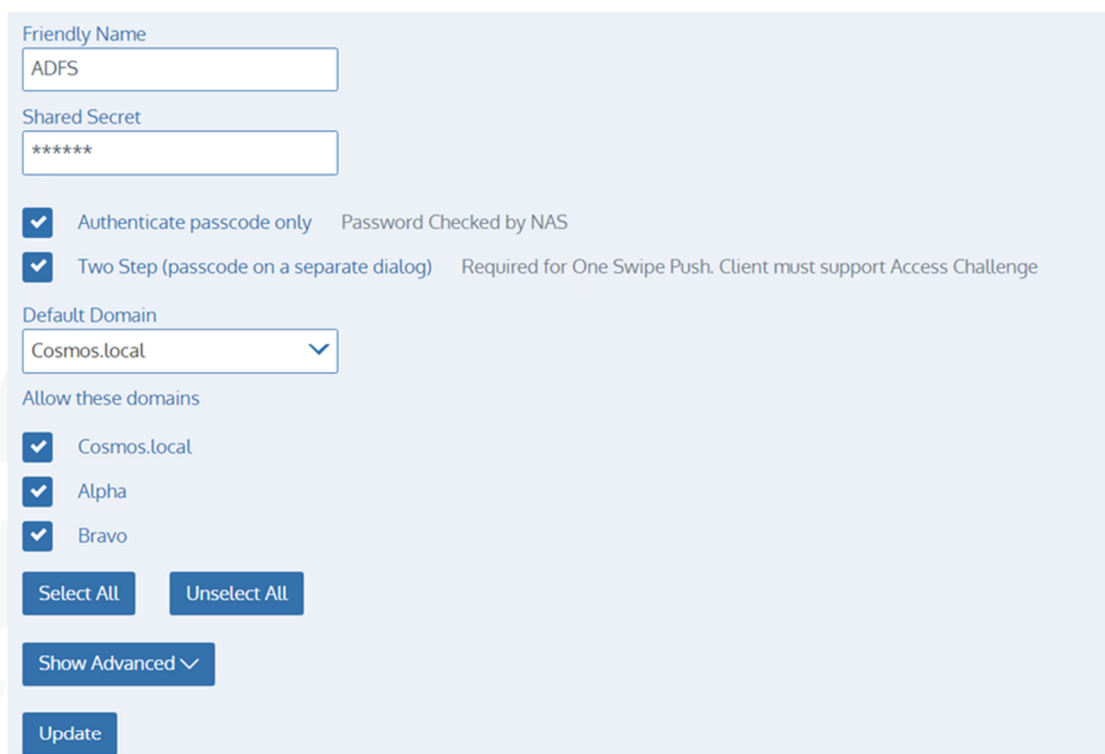
On the other side (the Resources side), another federation server validates the token and issues another token for the local servers to accept the claimed identity. This allows a system to provide controlled access to its resources or services to a user that belongs to another security realm without requiring the user to authenticate directly to the system and without the two systems sharing a database of user identities or passwords.

SecurEnvoy Microsoft server agent plugs into ADFS V4 and can be configured within ADFS Manager for multi-factor authentication. When enabled in ADFS, a UserID, Pin (optional) and Passcode are sent to the security server for authentication. If the security server returns AUTHOK then ADFS is instructed to continue.

## 2.0 Configuring SecurEnvoy Radius Client

### 2.1 Radius Client Setup

- From the SecurEnvoy Security Server Admin navigate to the Radius Tab and select "Add".
- Enter the Friendly name, shared Secret and authenticating domains.
- Check both "Authenticate Passcode Only" and "Two Step (Password on a Separate dialog)"
- Check "Update" to complete.



The screenshot shows the 'Add' configuration form for a Radius Client in SecurEnvoy. The form includes the following fields and options:

- Friendly Name:** A text input field containing 'ADFS'.
- Shared Secret:** A text input field containing '\*\*\*\*\*'.
- Authentication Options:** Two checked checkboxes: 'Authenticate passcode only Password Checked by NAS' and 'Two Step (passcode on a separate dialog) Required for One Swipe Push. Client must support Access Challenge'.
- Default Domain:** A dropdown menu with 'Cosmos.local' selected.
- Allow these domains:** A list of domains with checkboxes: 'Cosmos.local', 'Alpha', and 'Bravo', all of which are checked.
- Buttons:** 'Select All', 'Unselect All', 'Show Advanced' (with a dropdown arrow), and 'Update'.

#### Note

To allow Radius traffic through the network firewall, open inbound and outbound listening rules on UDP (default 1812)



## 3.0 Installing the MS server Agent on your MS ADFS Server

To install the Microsoft Server Agent run "Microsoft Server Agent \setup.exe" which is included in the Agents directory of your SecurEnvoy Server software download package.

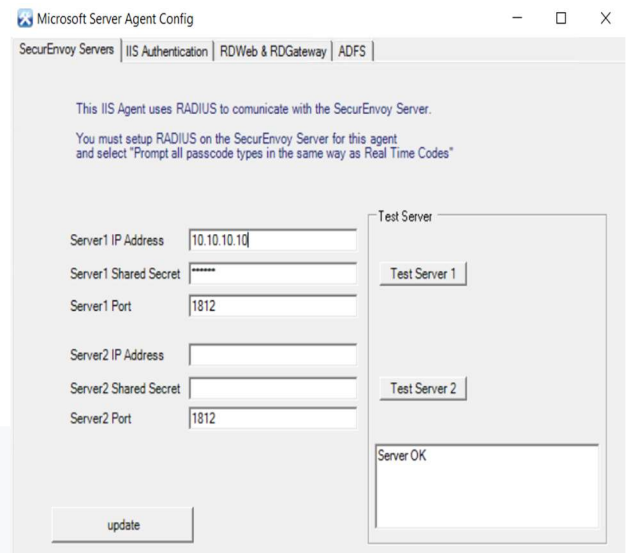
The following page is displayed for user input.

When prompted; enter up to two security servers (note these two security servers must have a RADIUS profile created upon each.)

If only one security server is required, blank the second server entry.

The "Test Server" button allows a RADIUS communication test to see if the Security server is reachable.

Make sure all the security server names you enter can be resolved and reached. It is recommended to start a CMD window and PING all security servers that will be entered.



Response codes are shown below:

OK  
 Error, Shared Secret Does Not Match the Server  
 Error, Connection Timed Out

All settings are correct  
 Shared secret mismatch  
 IP address or Port issue

This completes the Microsoft Server Agent installation.

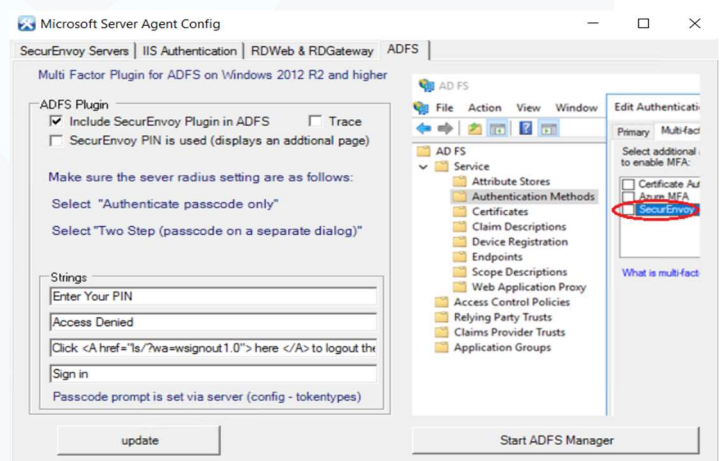
### 3.1 Configuring the Microsoft server Agent for ADFS

Select the ADFS tab.

Place a check in the checkbox for 'Include SecurEnvoy Plugin in ADFS'.

Place a check in the checkbox for 'SecurEnvoy PIN is used', if you wish to use SecurEnvoy's built in PIN management.

Click 'Update' to apply settings then click 'Start ADFS Manager'.



### 3.2 Configuring the Microsoft server Agent for ADFS

Launch ADFS Manager and navigate to "Relaying Party Trusts" -> Select -> "Add Relaying Party Trust" from the "Actions" Window.

Select "Claims aware" and then select "Start" -> From the "Select Data Source" add your Federation metadata details and select "Next".

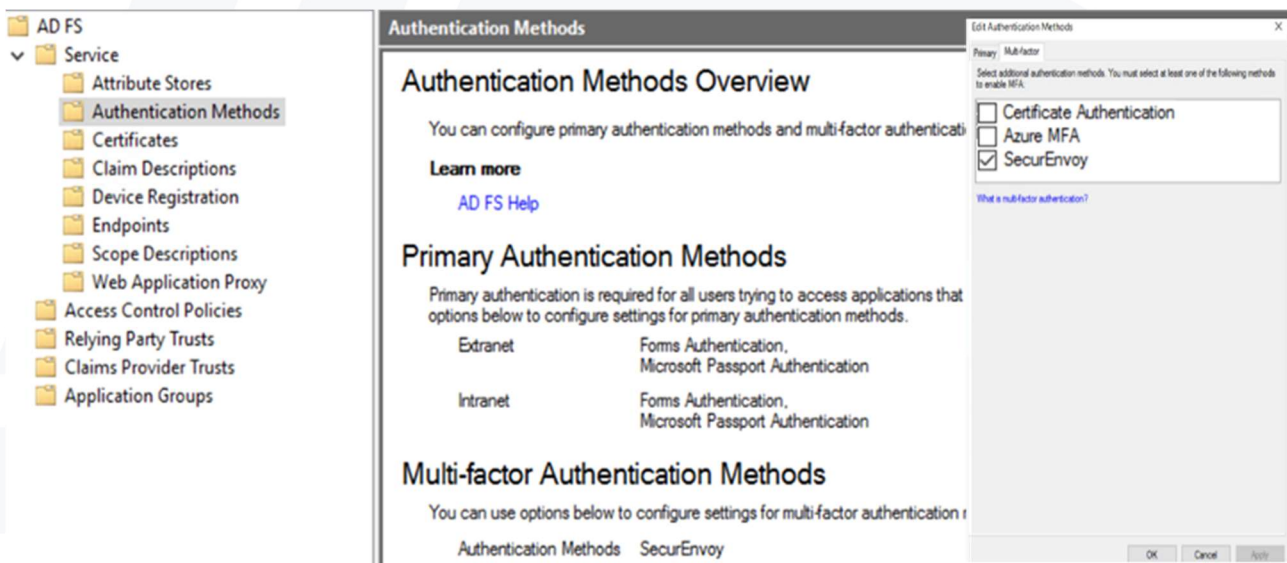
Display Name enter "MFA" and select "Nest".

From the "Access control Policy" screen, select "Permit everyone and require MFA" or your choice of policy = select "Next" and then "Next" to complete.

### 3.3 Enabling MFA Authentication Policy

From the ADFS Manager select -> "Authentication Policies" then click 'Edit' "Primary authentication Methods".

Within "Edit Authentication Methods" -> Multi-factor, place a check in the checkbox for 'SecurEnvoy' and click 'OK'.

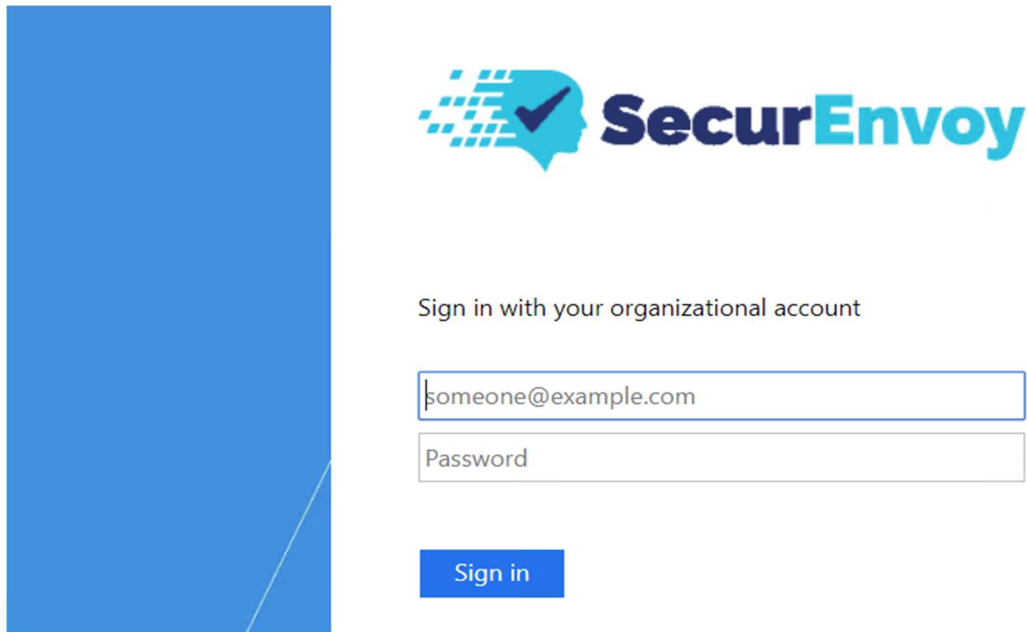




## 4.0 Testing MFA authentication

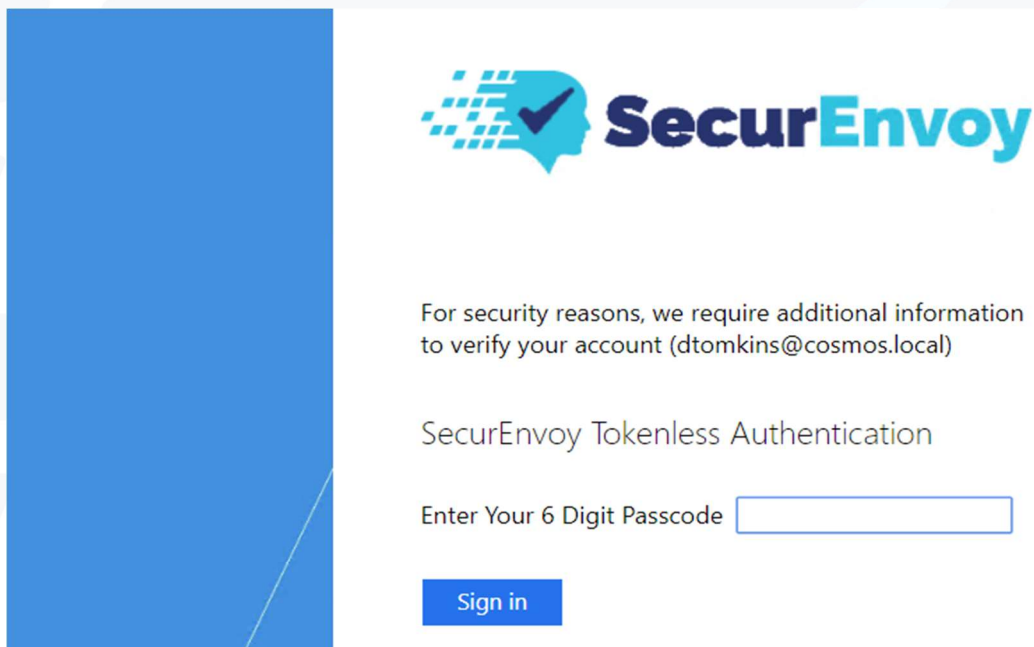
Test the Two Factor Web authentication by opening up a browser and going to your ADFS URL.

First you're prompt for the UserID and Password



The screenshot shows the SecurEnvoy login interface. On the left, there is a large blue rectangular area. To the right, the SecurEnvoy logo is displayed at the top. Below the logo, the text "Sign in with your organizational account" is centered. Underneath, there are two input fields: the first contains the email address "someone@example.com" and the second is labeled "Password". A blue "Sign in" button is positioned below the password field.

User is then presented with their two factor authentication type:



The screenshot shows the SecurEnvoy two-factor authentication page. On the left, there is a large blue rectangular area. To the right, the SecurEnvoy logo is displayed at the top. Below the logo, the text "For security reasons, we require additional information to verify your account (dtomkins@cosmos.local)" is centered. Underneath, the text "SecurEnvoy Tokenless Authentication" is displayed. Below this, the text "Enter Your 6 Digit Passcode" is followed by a text input field. A blue "Sign in" button is positioned below the passcode field.

Please make sure to read the contents of the End User Licensing Agreement. There are updates from previous versions.

## 5.0 Notes

Checking that you have the correct SecurEnvoyADFS.dll loaded.

On the ADFS server navigate to: \Program Files (x86)\SecurEnvoy\Microsoft Server Agent\ADFS and check that SecurEnvoyADFS.dll exists.

Compare that the correct SecurEnvoyADFS.dll file is present in the root of the ADFS folder.

- ADFS 3.0 the file date is 11/07/2017 (Size 72Kb)
- ADFS 4.0 the file date is 04/09/2017 (Size 71Kb)



# Please Reach Out to Your Local SecurEnvoy Team...



## UK & IRELAND

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

### Sales

E [sales@SecurEnvoy.com](mailto:sales@SecurEnvoy.com)  
T 44 (0) 845 2600011

### Technical Support

E [support@SecurEnvoy.com](mailto:support@SecurEnvoy.com)  
T 44 (0) 845 2600012



## EUROPE

Freibadstraße 30,  
81543 München,  
Germany

### General Information

E [info@SecurEnvoy.com](mailto:info@SecurEnvoy.com)  
T +49 89 70074522



## ASIA-PAC

Level 40 100 Miller Street  
North Sydney  
NSW 2060

### Sales

E [info@SecurEnvoy.com](mailto: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](mailto:info@SecurEnvoy.com)  
T (866)777-6211



## USA - Mid West

3333 Warrenville Rd  
Suite #200  
Lisle, IL 60532

### General Information

E [info@SecurEnvoy.com](mailto:info@SecurEnvoy.com)  
T (866)777-6211



## USA - East Coast

373 Park Ave South  
New York,  
NY 10016

### General Information

E [info@SecurEnvoy.com](mailto:info@SecurEnvoy.com)  
T (866)777-6211



[www.securenvoy.com](http://www.securenvoy.com)