Cloud Services via Active Directory Federated Services (ADFS) v3.0

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House Brunel Road Theale Reading RG7 4AB	
Dorian Tomkins	dtomkins@securenvoy.com	

Cloud Services with Active Directory Federated Services (ADFS) v3.0

This document describes how to integrate Cloud Services configured for SSO to a local ADFS 3.0 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 V3 Claims Aware Application or Cloud Service

Microsoft

Microsoft Windows Server 2012, Windows Server 2012 R2

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 v7.3.501

Index

1.0 Prerequisites

SecurEnvoy Security Server has been installed with the Radius service and has 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 token types are supported.

Token Type Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓
One Swipe	✓

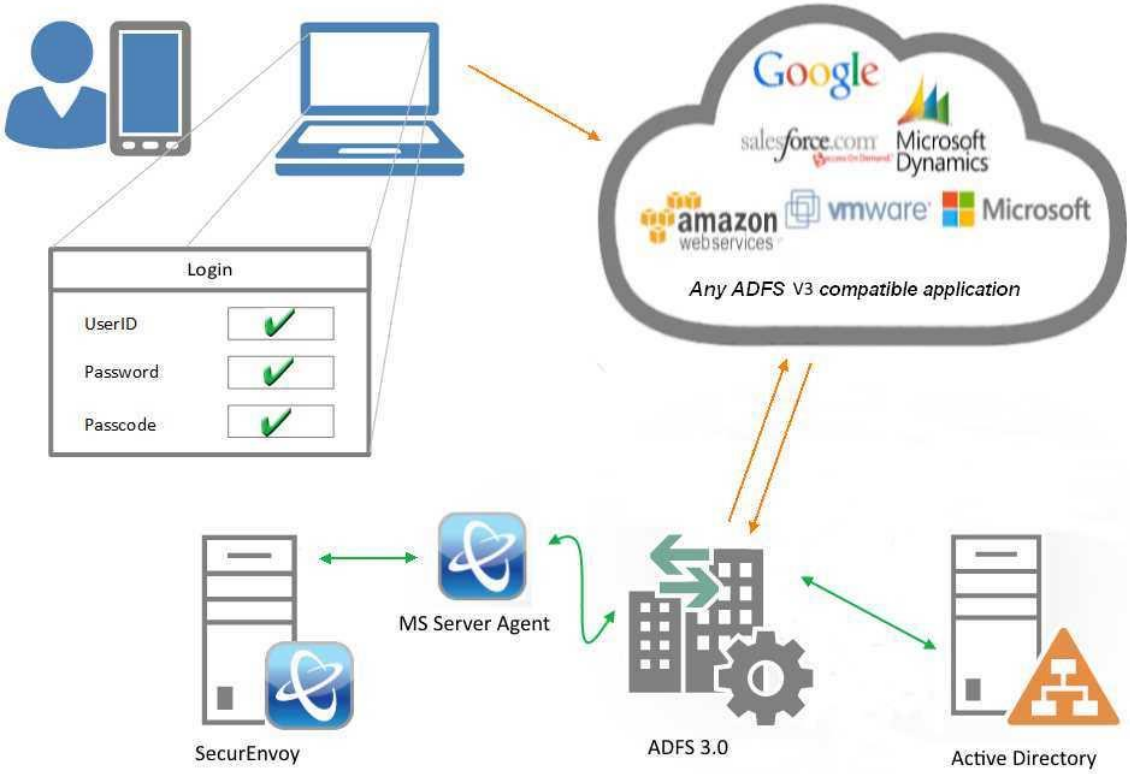
1.1 Configure ADFS with a Cloud Service account

Install and configure ADFS V3 with your SAML claims aware application or other cloud service that supports ADFS V3. The following is a list of examples:

Active Directory Federation Services Overview

Set up CRM 2015 IFD on Windows 2012 and ADFS 3.0
How To Install ADFS 2012 R2 For Office 365

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 V3 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 Install Microsoft Server Agent on your Microsoft 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

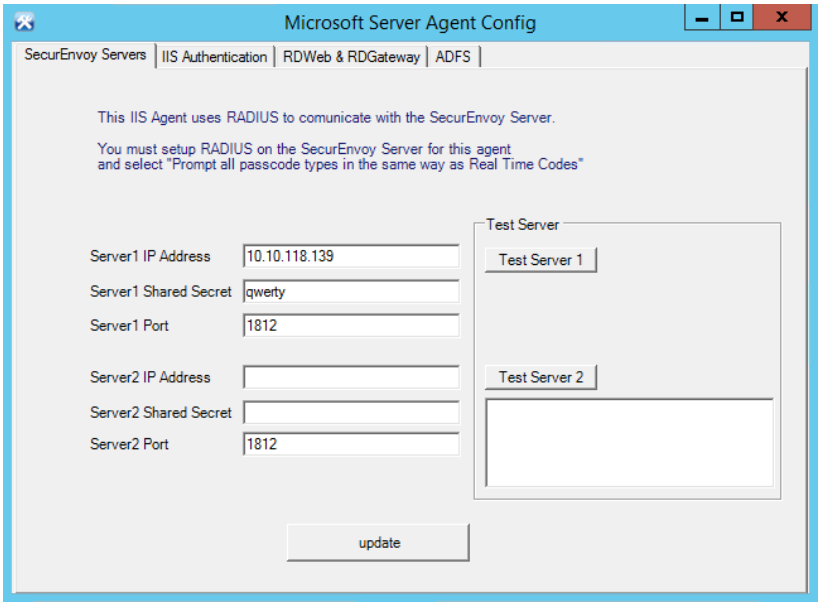
The following page is displayed for user input.

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	All settings are correct
Error, Shared Secret Does Not Match the Server	Shared secret mismatch
Error, Connection Timed Out	IP address or Port issue

This completes the Microsoft Server Agent installation.

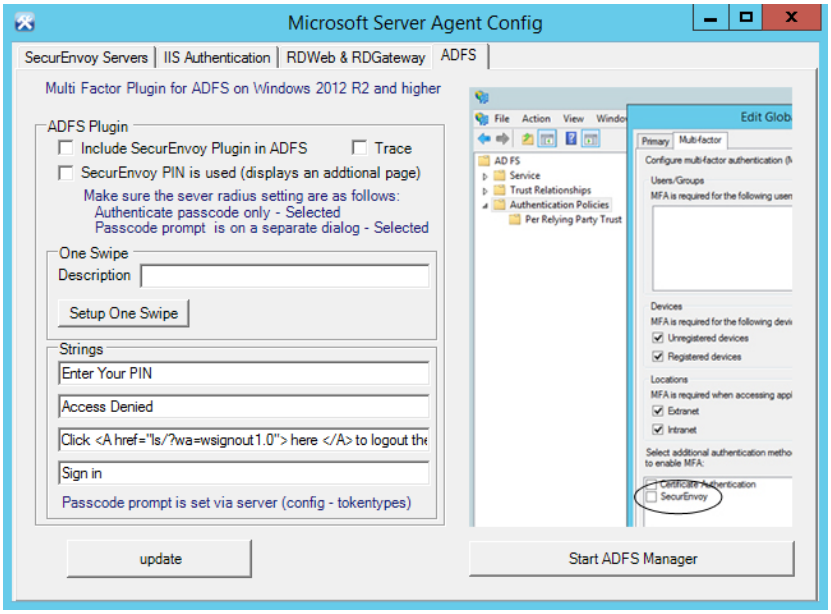
2.1 Configure Microsoft Server Agent for use with ADFS

Select the ADFS tab.

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

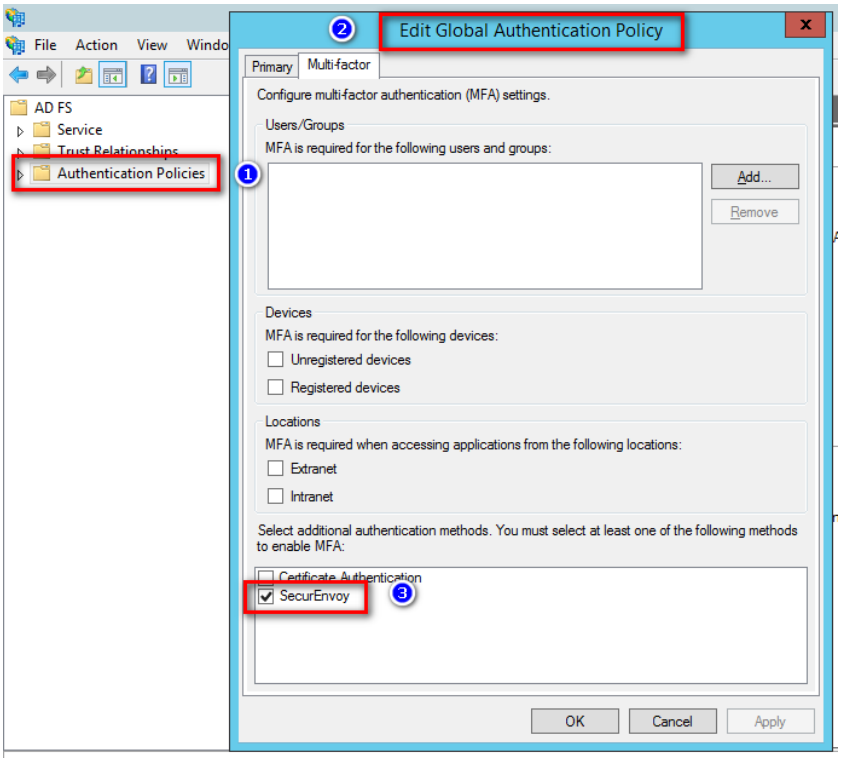
Place a check in the checkbox for 'SecurEnvoy PIN is used', if you wish to use SecurEnvoy's built in PIN management.

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



Once ADFS Manager has launched, select 'Authentication Policies' then click 'Edit Global Authentication Policy'.

Within additional authentication methods, place a check in the checkbox for 'SecurEnvoy' and click 'OK'.



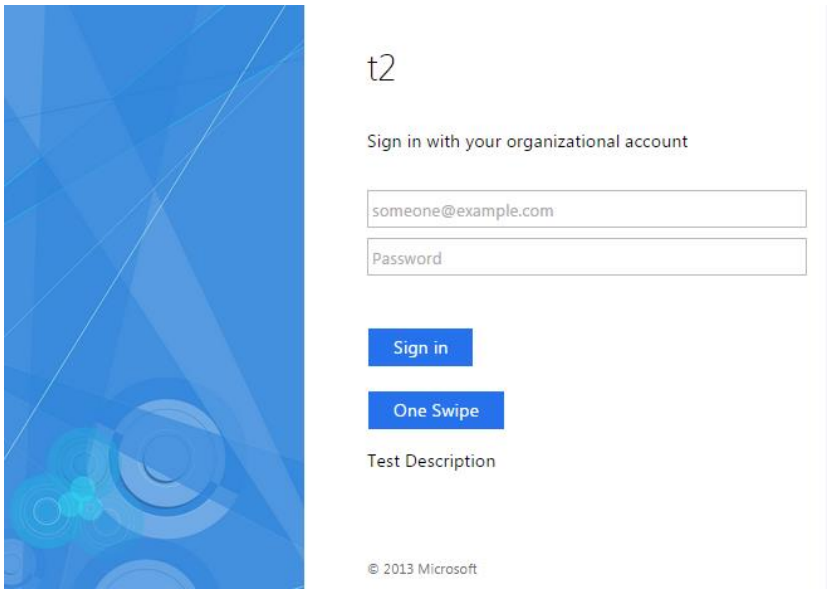
3.0 Test the Two Factor Authentication

Test the Two Factor Web authentication by opening a browser and going to the URL for the Web server i.e.

https://your_server_name/rdweb (Don't forget the https)

User logon screen is shown.

Enter your UsedID and Password:



User is then presented with their two factor authentication type:

4.0 Notes