Cloud Services with Active Directory Federated Services (ADFS) v2.0

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House Brunel Road Theale Reading RG7 4AB	
Tony Davis	tdavis@securenvoy.com	

Cloud Services with Active Directory Federated Services (ADFS) v2.0

This document describes how to integrate Cloud Services configured for SSO to a local ADFS 2.0 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 ADFS V2 Compatible Application or Cloud Service

Microsoft

Microsoft Server 2008 R2 with ADFS 2.0 Installed

SecurEnvoy

Microsoft Server (can be installed on the same server as ADFS or on a separate server)
IIS installed with SSL certificate (required for management and remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v7.2.504

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.

IIS Agent has been installed as per the SecurEnvoy IIS Agent Installation and Admin Guide:

IIS Agent Installation Guide.pdf

The following table shows what token types are supported.

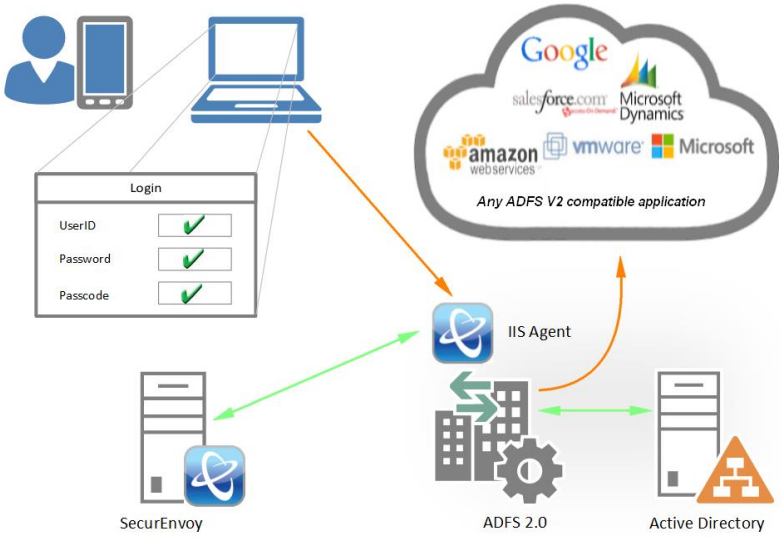
Token Type Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓
One Swipe	✓

1.1 Configure ADFS with a Cloud Service account

Install and configure ADFS V2 with your SAML claims aware application or other cloud service that support ADFS V2. The following is a list of examples:

AD FS 2.0 Step-by-Step and How To Guides
Amazon web services
Microsoft Dynamics CRM
VMware

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.

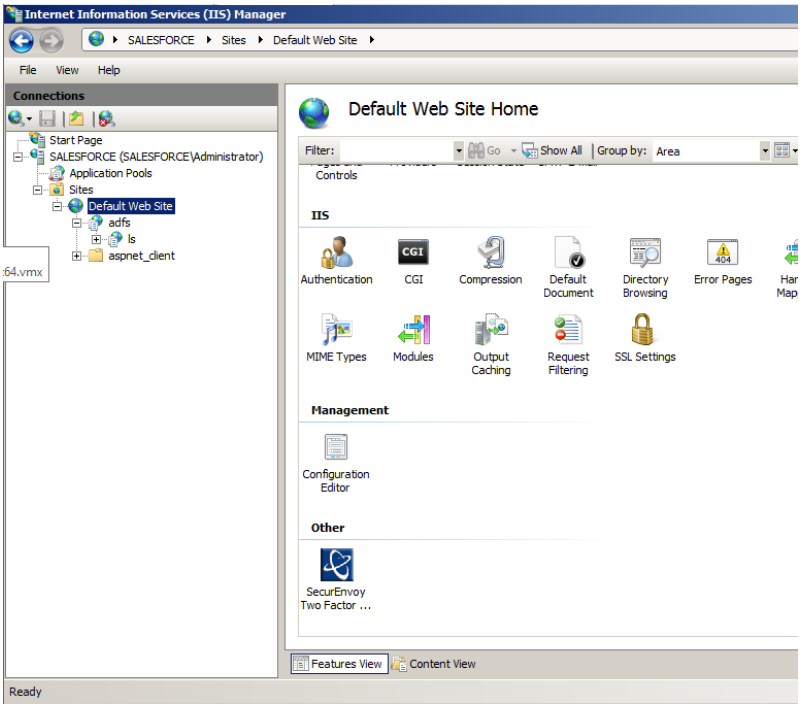
On the other side (the Resources side), another federation server validates the token and issues another token for the local servers to accept the claimed identity. This allows a system to provide controlled access to its resources or services to a user that belongs to another security realm without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

SecurEnvoy IIS agent monitors all requests by using the ISAPI filter program "webauthfilter". If a request to ADFS is detected, the filter checks to see if a valid un-tampered cookie is available and that it hasn't timed out. If the cookie is OK then the request is passed on. If the cookie is unavailable or has timed out the ISAPI filter redirects the request to SecuEnvoyAuth/webauth.exe. This program requests a UserID, Pin and Passcode and sends it to the security server for authentication. If the security server returns AUTH OK then webauth.exe creates a valid cookie and redirects the request back to the original page.

2.0 Configure IIS Agent for Default Website

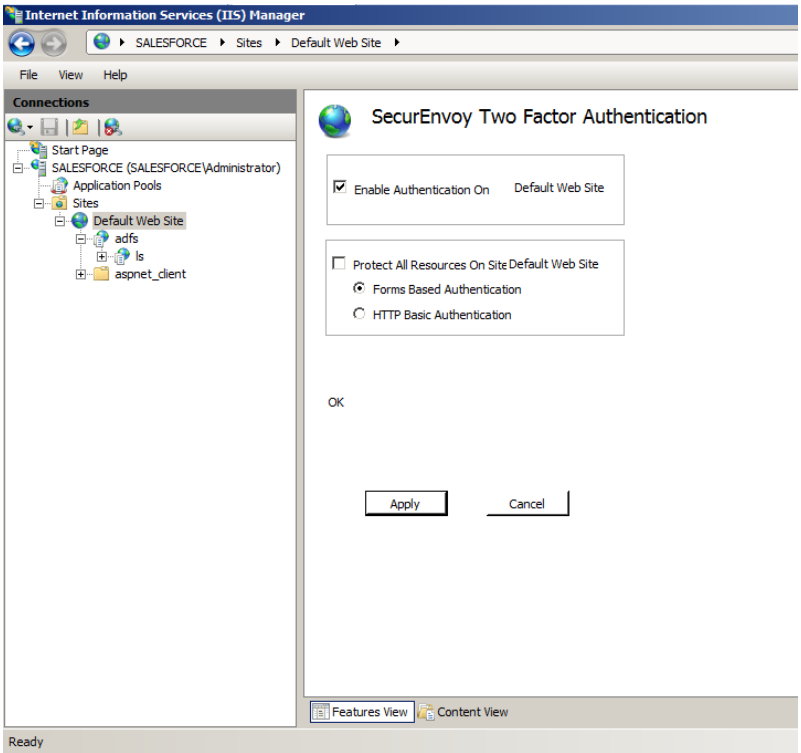
Launch the IIS management interface, either from "Start", "Administration Tools" or from the Server Manager

Expand the sites list on the navigation pane and select "Default Web Site", then scroll down the centre panel and press the "SecurEnvoy Two Factor" icon.



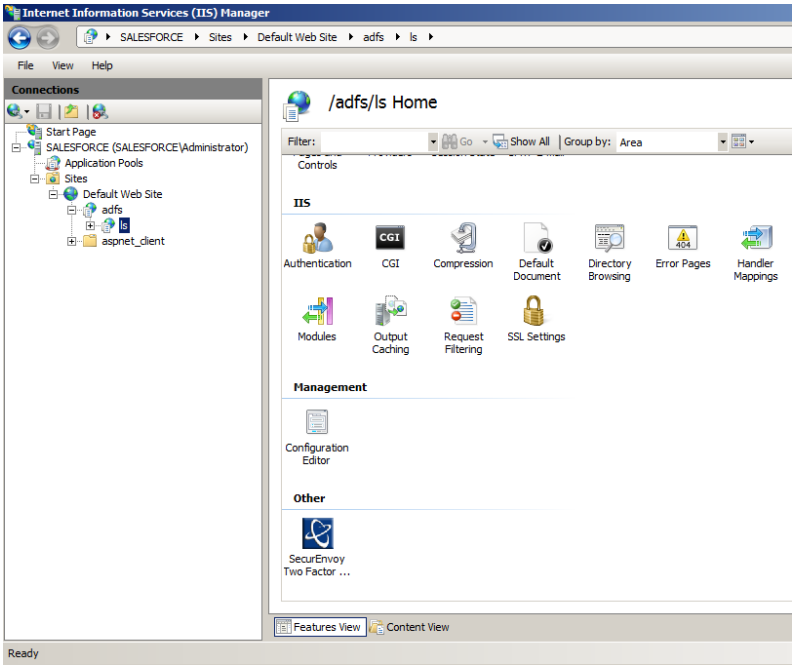
Enable the tick box to "Enable Authentication On Site Default Web Site"

Click "Apply" when complete.

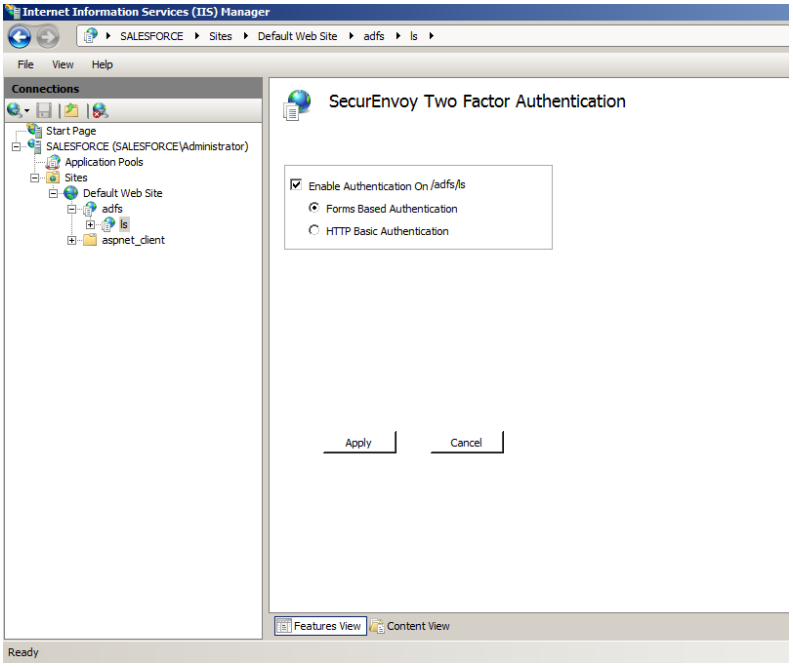


2.1 Configure IIS Agent for ADFS

Under Default Web Site, expand adfs and select ls, scroll down the centre panel and select "SecurEnvoy Two Factor"



Select the check box "Enable Authentication On /adfs/ls"
Select "Form Based Authentication" (The Default)
Click "Apply" to finish
Cancel restart IIS when prompted.



Note

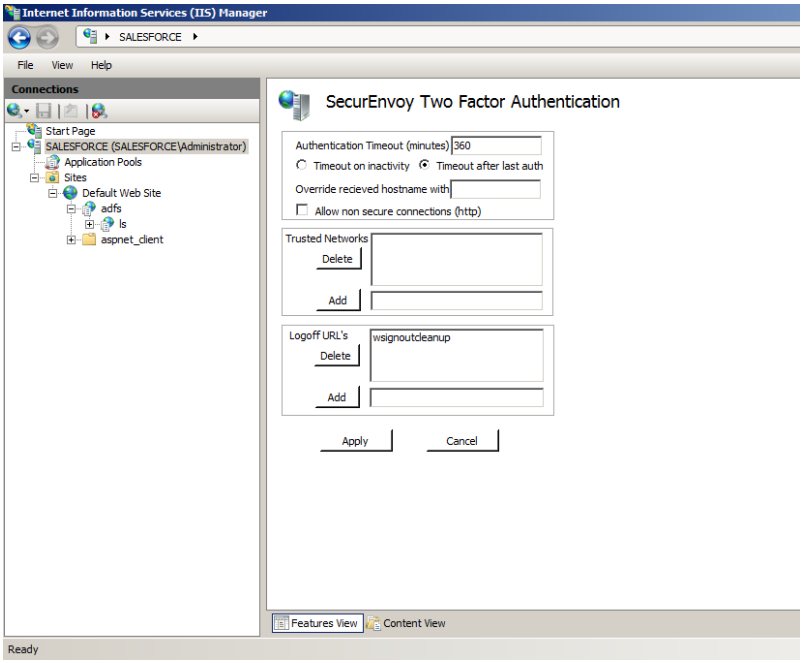
The virtual directory SecurEnvoyAuth MUST be a member of the ADFSAppPool

2.2 Configure logout URL

In the Navigation pane, select top level host name (the 2nd line down).
Scroll down the centre panel and press the "SecurEnvoy Two Factor" icon.
Setup your required inactivity timeout.

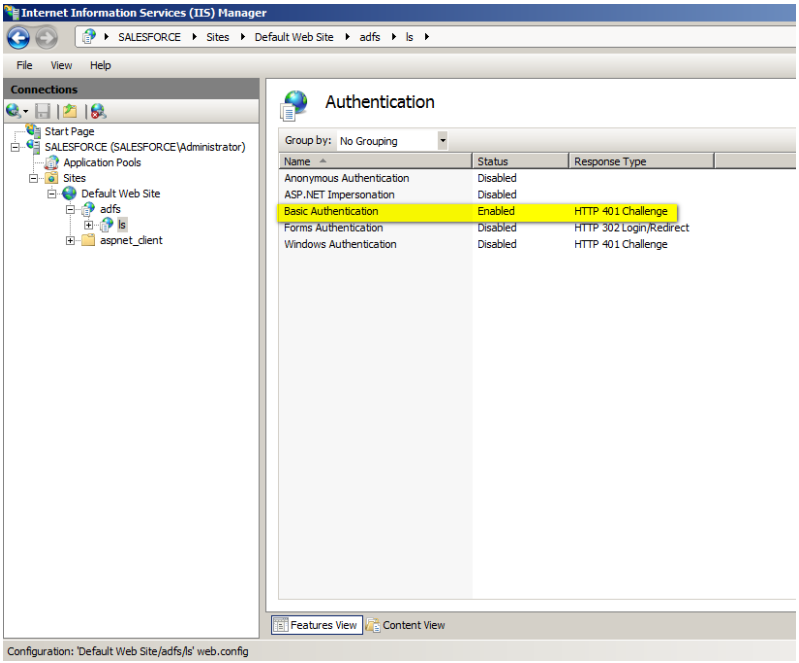
Add the logout URL **wsignoutcleanup**

Restart IIS when prompted.



2.3 Configure Basic Authentication

Navigate back to Default Web Site > adfs > ls and select the Authentication icon
Make sure that **only** Basic Authentication is Enabled



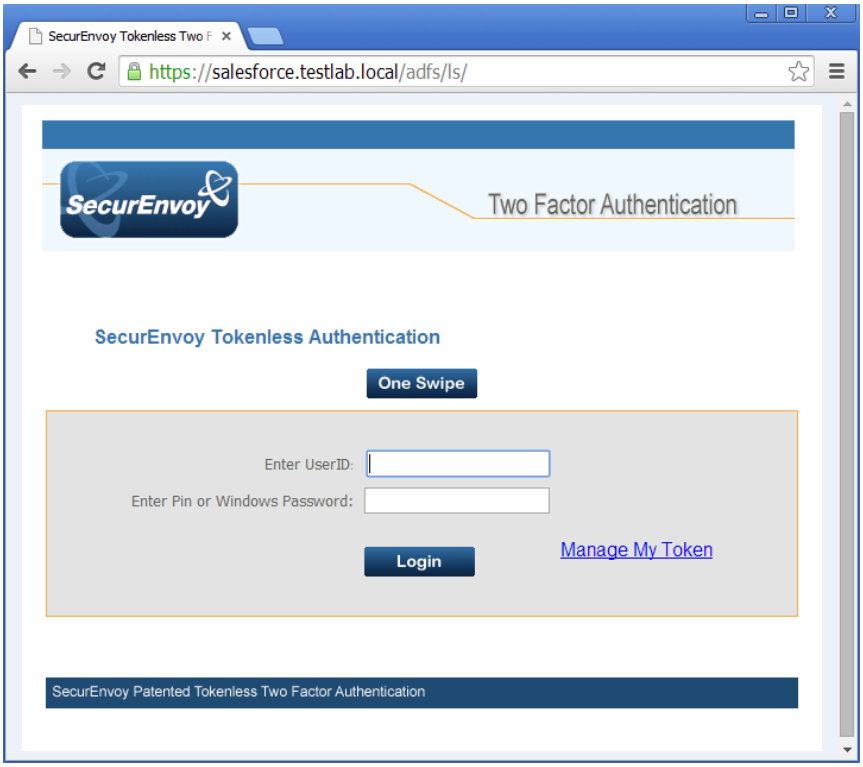
3.0 Test the Two Factor Authentication

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/adfs/ls (Don't forget the https)

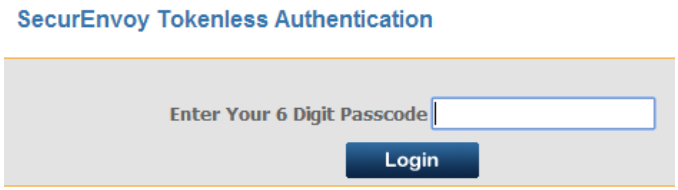
User logon screen is shown.

Enter your UsedID and Password:

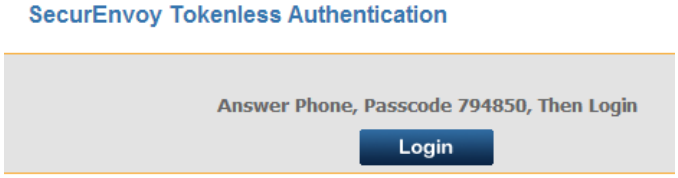


User is then presented with their two factor authentication type:

- Pre load, Realtime and Soft tokens:



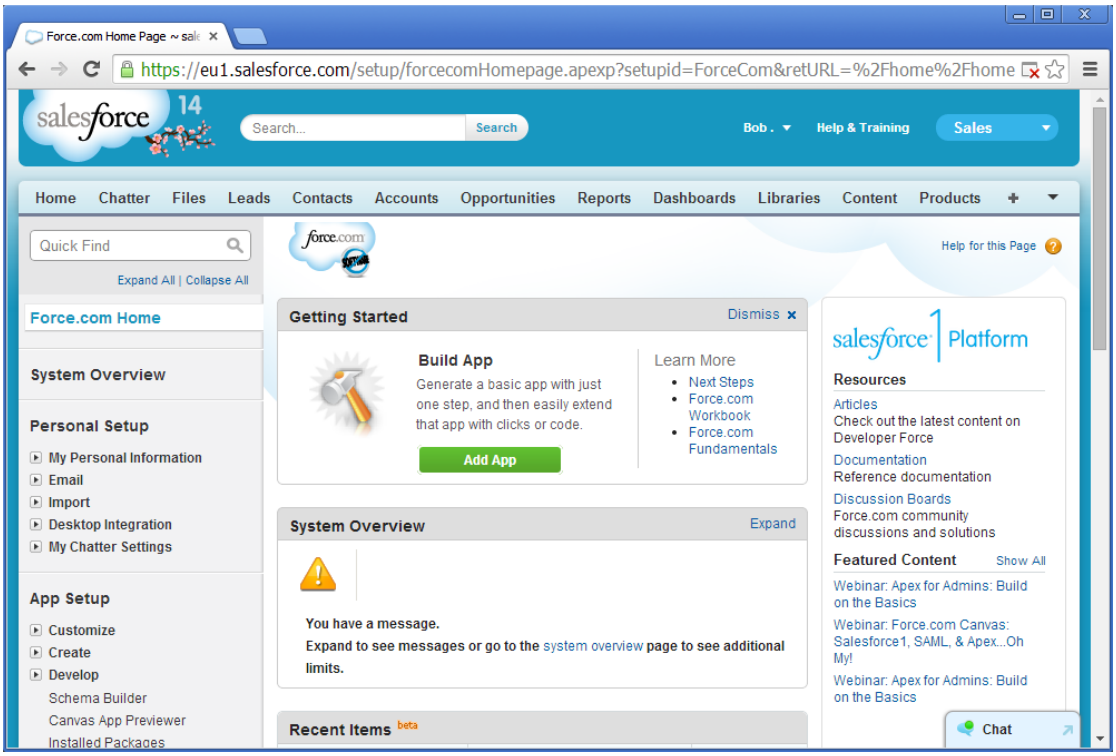
- VOICE tokens:



- One Swipe:

3.1 Successful Logon with 2FA

User authenticates successfully and is presented with their Cloud Services login screen:



Note

Configure your domain name within seiis.ini (C:\Windows):

# Default Domain Name to use if no domain information is included in this UserID (leave blank if not required)
DefaultDomain="yourdomain"

This will allow your users to logon to SalesForce without specifying the domain name:
domain\UserID

4.0 Notes