

Microsoft Office365 with Active Directory Federated Services (ADFS)

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Andy Kemshall	akemshall@securenvoy.com	

This document describes how to integrate Microsoft's Online Services Office 365 configured for SSO to a local ADFS 2.0 service with SecurEnvoy two-factor Authentication solution called 'SecurAccess'

Microsoft Office 365 is a cloud based service that can be configured to use a local Active Directory Federation Service (ADFS) to enable local users to sign on with their existing AD credential to gain access to various Microsoft online services such as Office, SharePoint and Lync.

SecurAccess provides two-factor, strong authentication for remote Access and cloud solutions (such as SSL VPN, IPsec VPN and Web authentication) from any device, 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 Microsoft's Active Directory 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 or Active Directory in real time.

All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below

Microsoft

Office365 Cloud Account

Microsoft Server 2008R2 with ADFS 2.0 Installed

Optional (Microsoft Server 2008R2 with ADFS 2.0 Installed as a proxy)

SecurEnvoy

Windows 2003 server SP1 or Windows 2008 (any version)

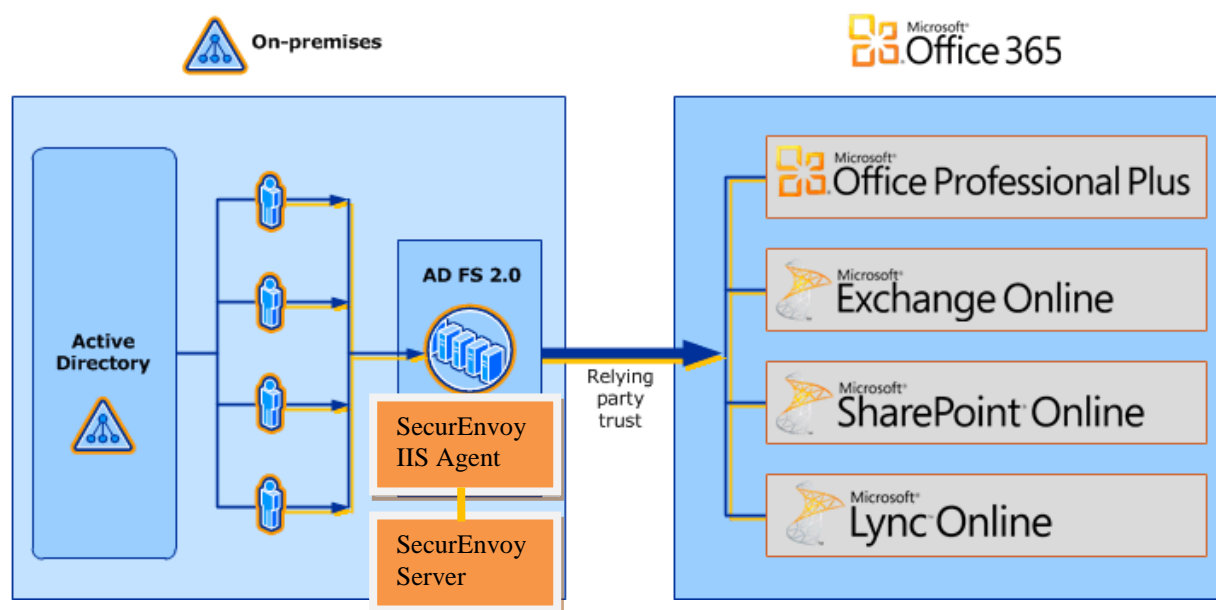
IIS installed with SSL certificate (required for management and remote administration)

Active Directory installed

SecurAccess software release v6.2

1.0 Prerequisites

Is it expected that Office365 has already been setup for SSO to an on-premise ADFS server with working SSO based on users existing AD passwords.



2.0 Installation of SecurEnvoy Microsoft IIS Agent on ADFS

The Microsoft IIS agent is located in the Agent directory of the software distribution

Install this agent on your ADFS Proxy server(s)

Note

SecurEnvoy IIS Agent MUST be version 6.2 or higher

Note

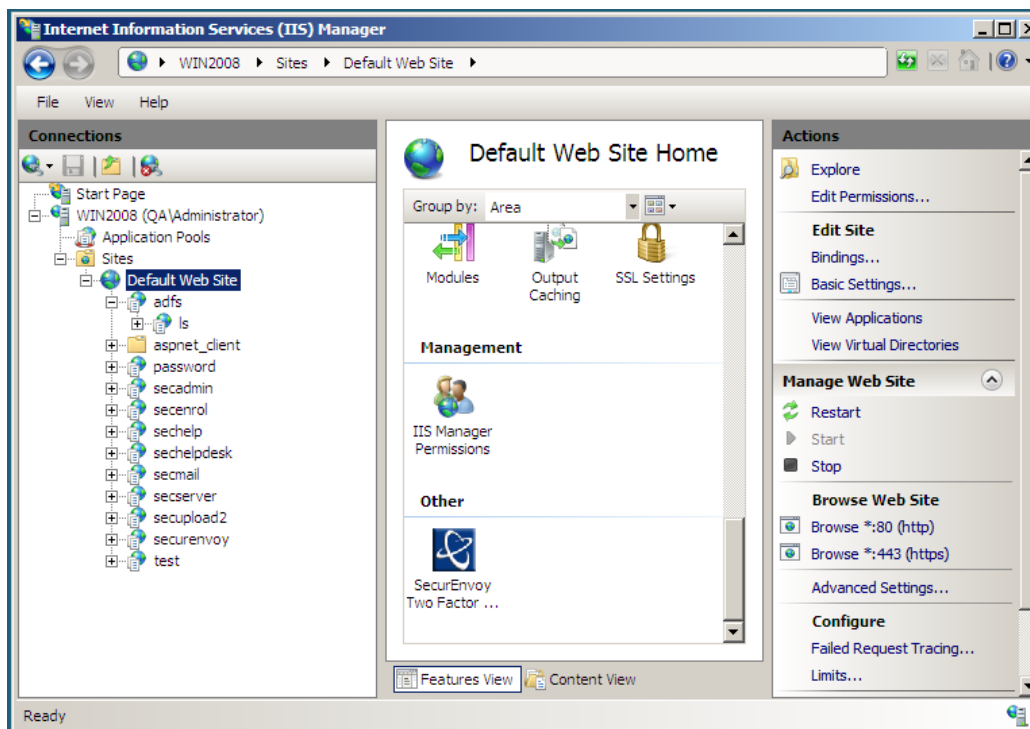
If you do not use ADFS Proxy servers then install the agent on your ADFS server(s)

Note

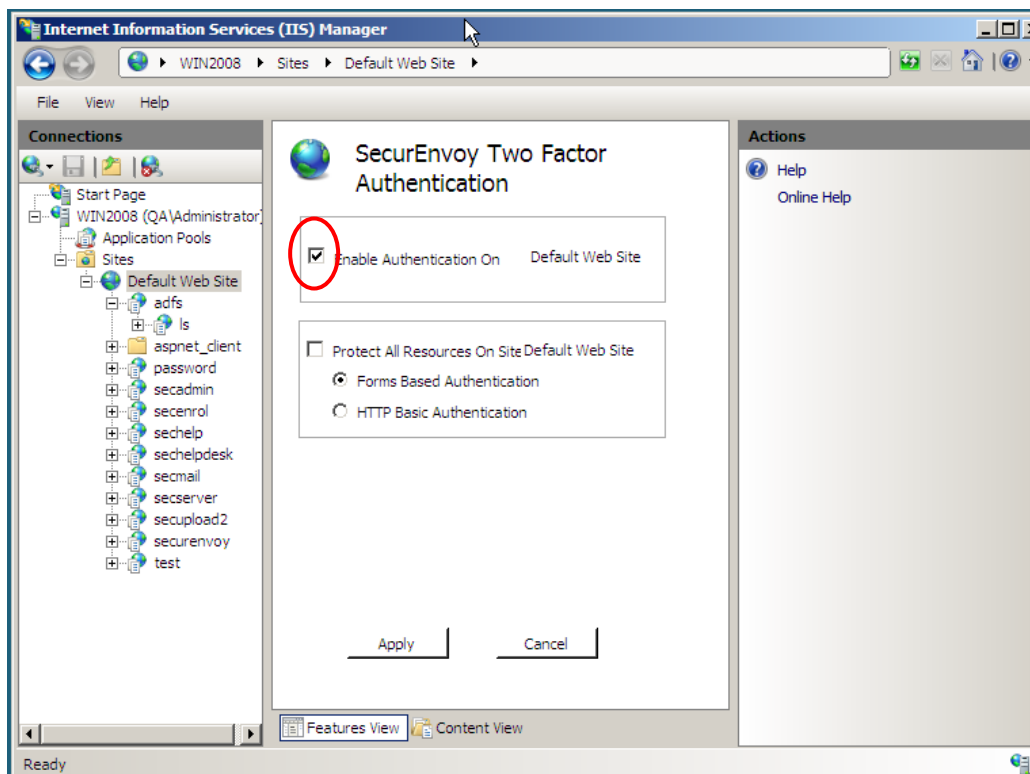
If you have published ADFS through a reverse proxy such as UAG you should authenticate SecurEnvoy at this location. Refer to the relevant reverse proxy's integration guide

2.1 Configure IIS to protect ADFS

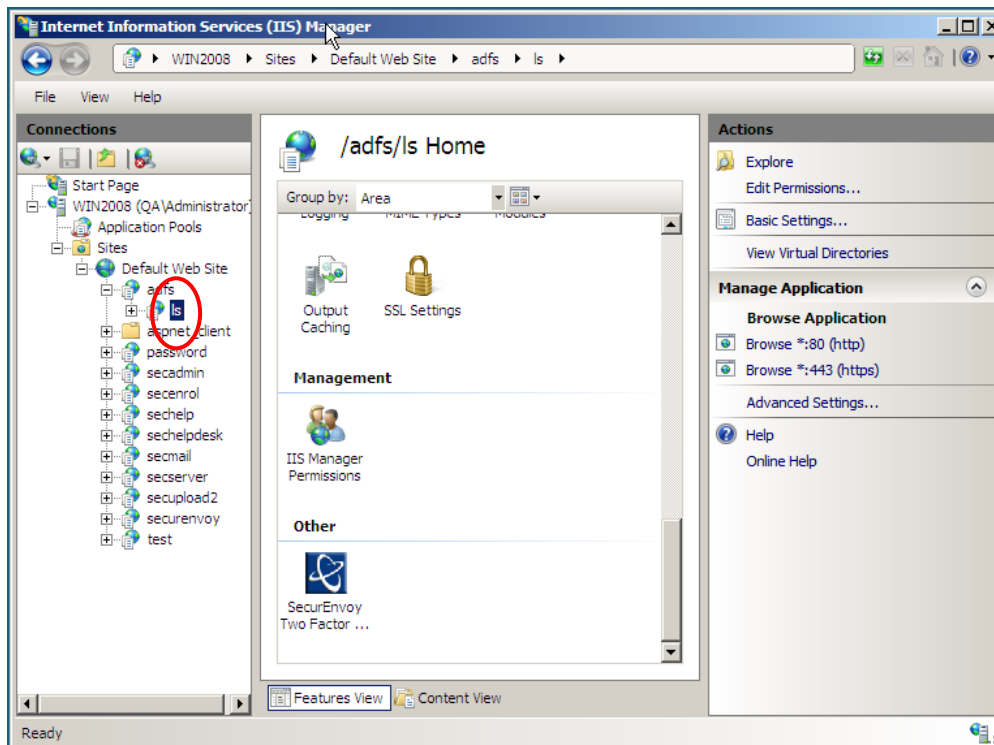
- Start the Microsoft IIS Manager
- Select Default web site under connections pane.
- Select the SecurEnvoy Icon



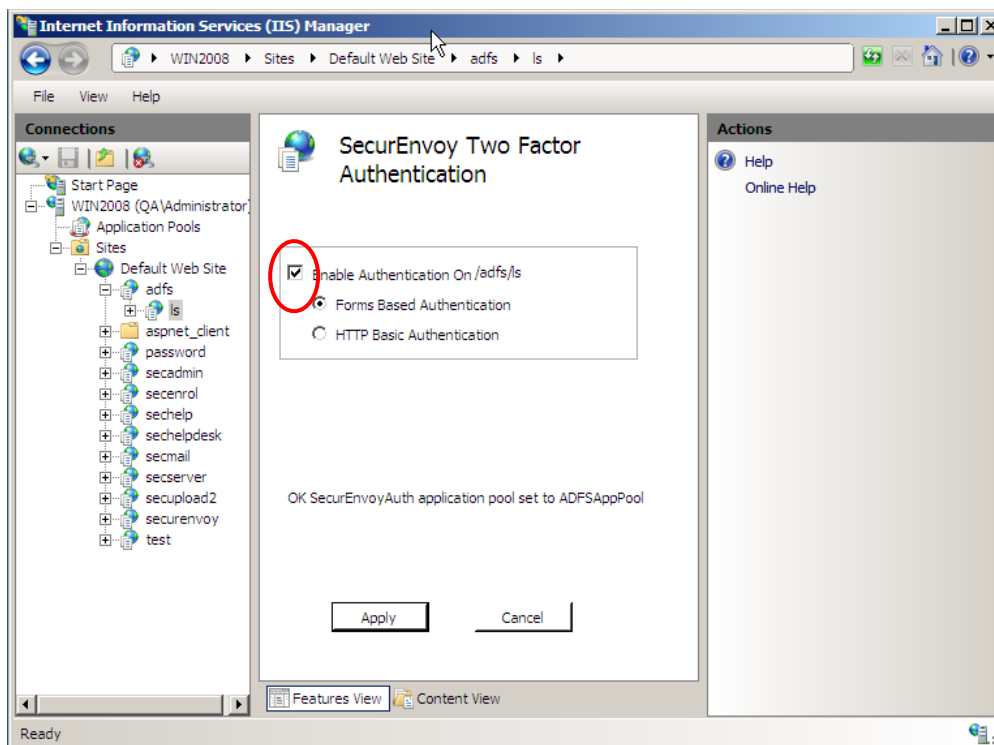
- Select **Enable Authentication On Default Web Site.**



- Apply changes
- Under **Default Web Site**, expand **adfs** and select **ls**
- Select the SecurEnvoy Icon



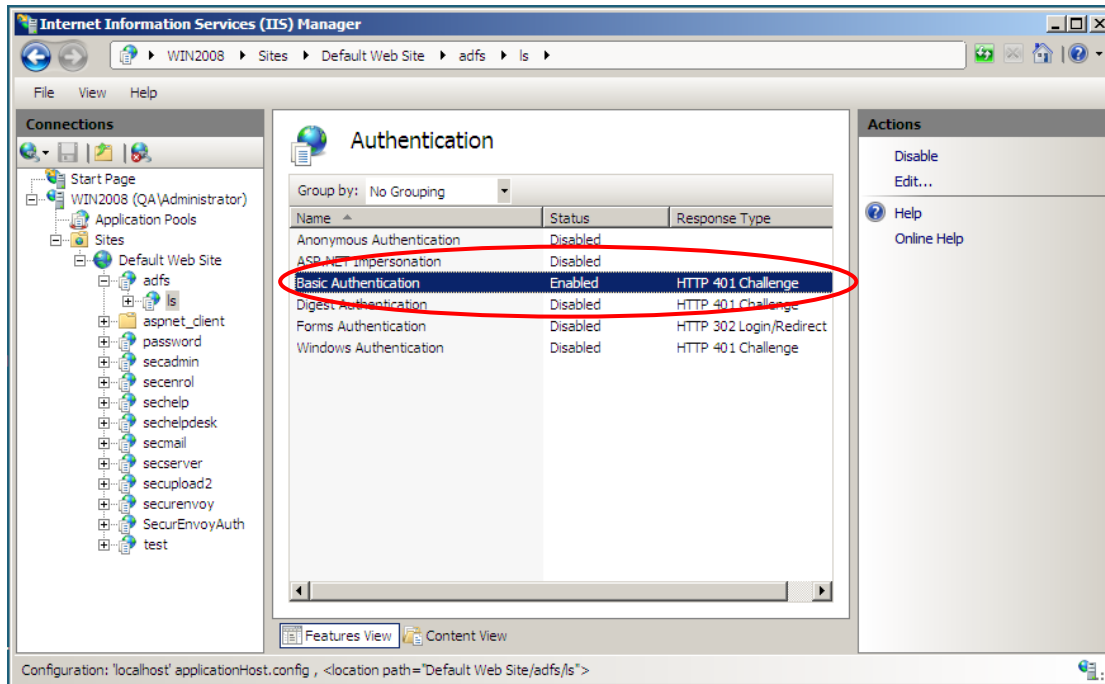
- Select the check box **Enable Authentication On /adfs/ls**



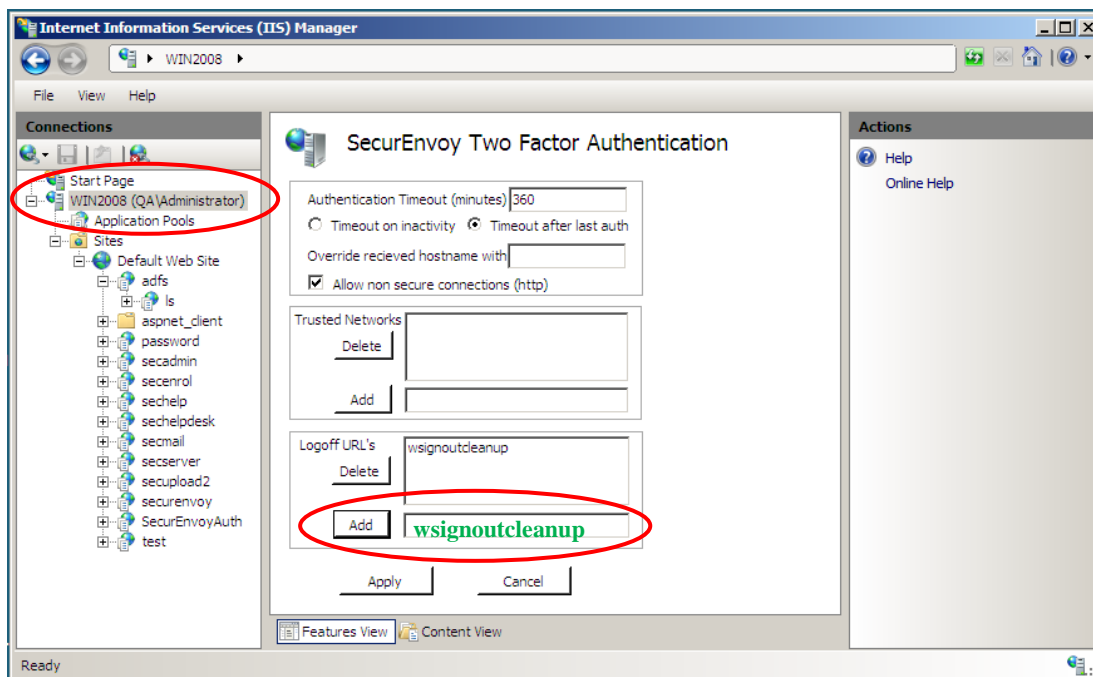
Note

The virtual directory SecurEnvoyAuth **MUST** be a member of the ADFSAppPool

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

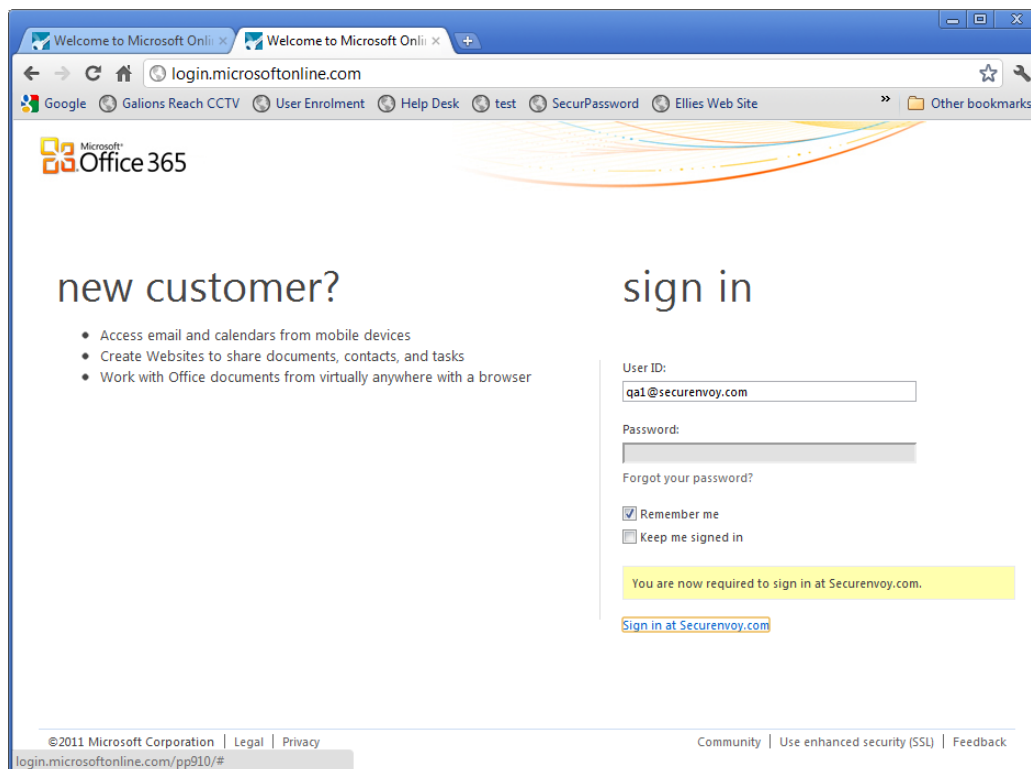


- In the left side Navigation pane, select top level host name (the 2nd line down).
- Scroll down the centre panel and press the “SecurEnvoy Two Factor” icon.
- Setup your required inactivity timeout.
- Add the logoff URL **wsignoutcleanup**
- Press Apply and restart IIS when prompted.

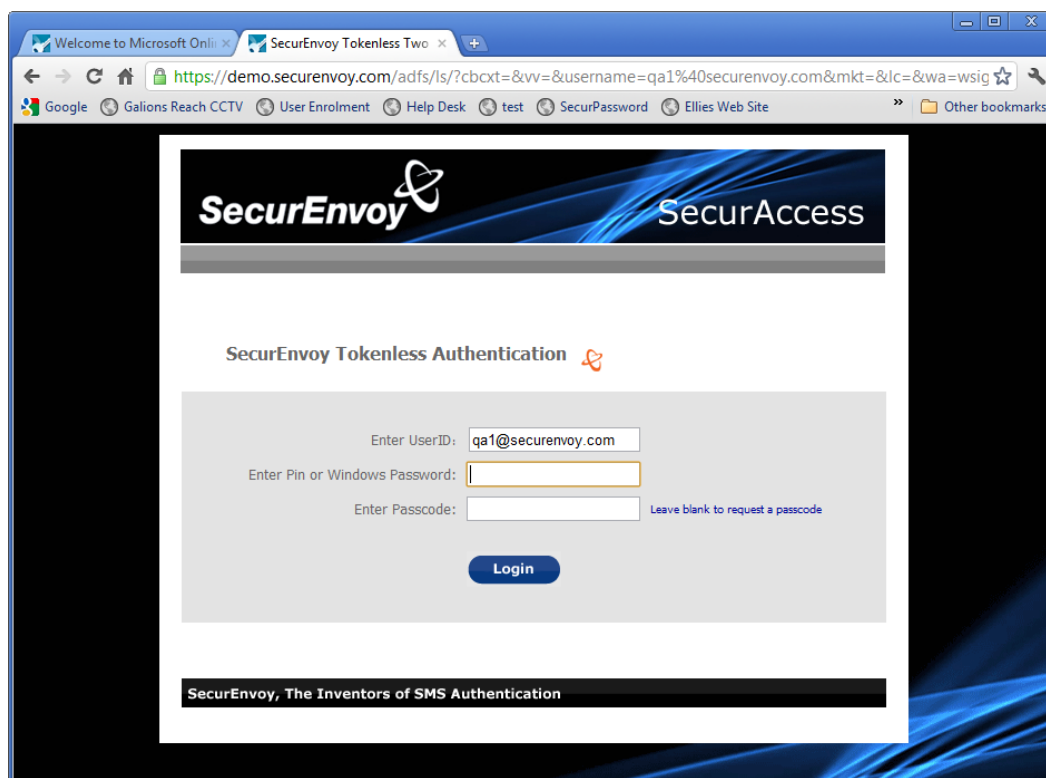


3.0 Test Logon

- Open a browser and navigate to <https://login.microsoftonline.com>
- Enter a valid userID



- Select Sign in at (your domain name)



- Enter a valid Microsoft password for this user
- Enter the passcode created by SecurEnvoy for this user

