Microsoft Outlook Web Access 2003 using Microsoft Internet Information Server v6.0

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	

This document describes how to integrate Microsoft Outlook Web Access 2003 (OWA) with SecurEnvoy two-factor Authentication solution called 'SecurAccess'

Microsoft Outlook Web Access enables you to gain access to your messages, calendars, contacts, tasks, and public folders from any mobile device that's supports an Internet connection and a Web browser. Leveraging Microsoft Exchange Server, businesses can deploy Corporate email through a browser to their remote workforce.

SecurAccess provides two-factor, strong authentication for remote Access 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

For OWA
Microsoft Server 2003
Microsoft Exchange Server 2003

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 v5.3.503

Installation of the SecurEnvoy Microsoft IIS Web agent

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

Install this agent on your Outlook Web Access IIS server

Configure the IIS Agent For Outlook Web Access

Launch the IIS management interface, either from “Start”, “Programs”, “Administration Tools” or from Microsoft’s MMC.

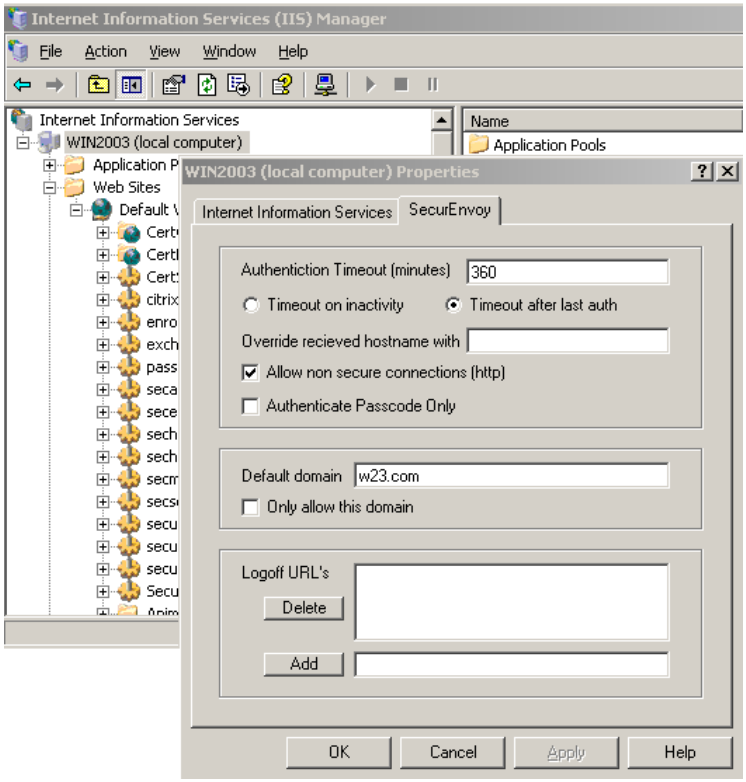
Navigate to the “local computer”, right mouse click and then select the SecurEnvoy tab. The following screen will be displayed.

Enter the time allowed before re-authentication is required in the “Authentication TimeOut” entry box

Click “OK” when complete.

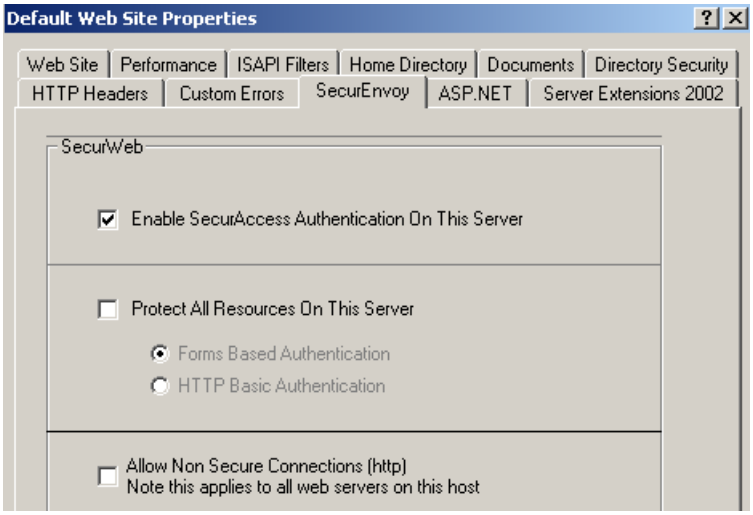
To help provide a seamless logout sequence, add the following line to the Logoff URL’s.

exchweb/bin/auth/owalogon.asp?url=https://test.domain.com/exchange/&reason=1
Substitute “test.domain.com” with the FQDN of your server.
When a user log’s off, both the Microsoft cookie and SecurEnvoy cookie are flushed.



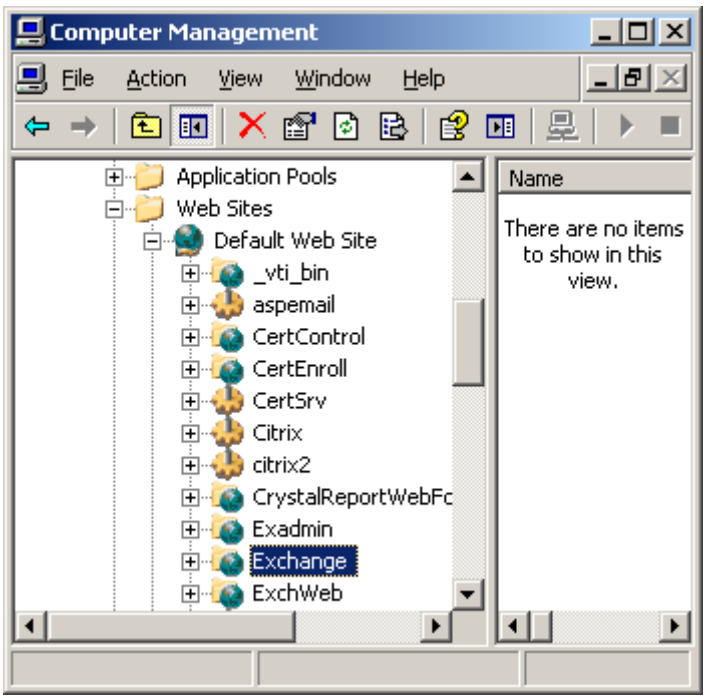
Expand the Web site list on the navigation pane and right mouse click “Default Web Site”, then select “Properties”.

Select the SecurEnvoy Tab and enable the tick box to “Enable SecurAccess Authentication”



Click “OK” when complete.

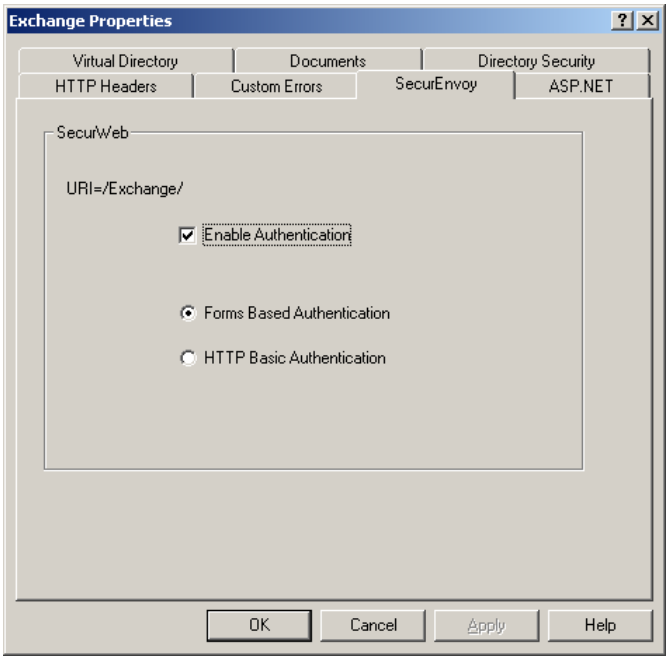
Next select the virtual web site you want to protect in the navigation pane. For OWA select “Exchange” Right mouse click and select properties.



Select the SecurEnvoy tab and enable the tick box to “Enable Authentication”

If your Exchange environment is setup for forms based authentication then select “Form Based Authentication” else select “HTTP Basic Authentication”

Click “OK” to finish

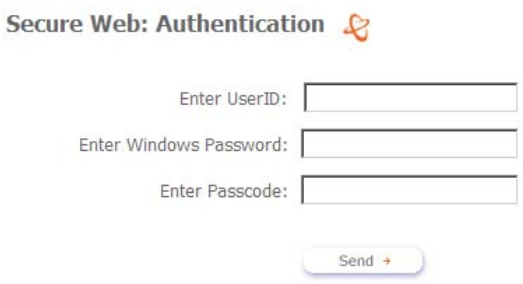


Test the Two Factor Web authentication by opening a browser and going to the URL for the Web server i.e.

https://test.domain.com/Exchange (Don’t forget the https)

User logon screen is shown below.





For single sign-on to the forms based exchange authentication page refer to the following:
C:\Program Files\SecurEnvoy\Microsoft IIS Agent\SAMPLES\OWA2003