Microsoft Outlook Web Access 2010

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 Outlook Web Access 2010 (OWA) with SecurEnvoy two-factor Authentication solution called 'SecurAccess'

The equipment used for the integration process is listed below

Microsoft Server 2008 R2 with Microsoft Exchange Server 2010

Windows Server 2008 R2 with SecurAccess Release v5.3.502

Installation of the SecurEnvoy Microsoft IIS Web agent

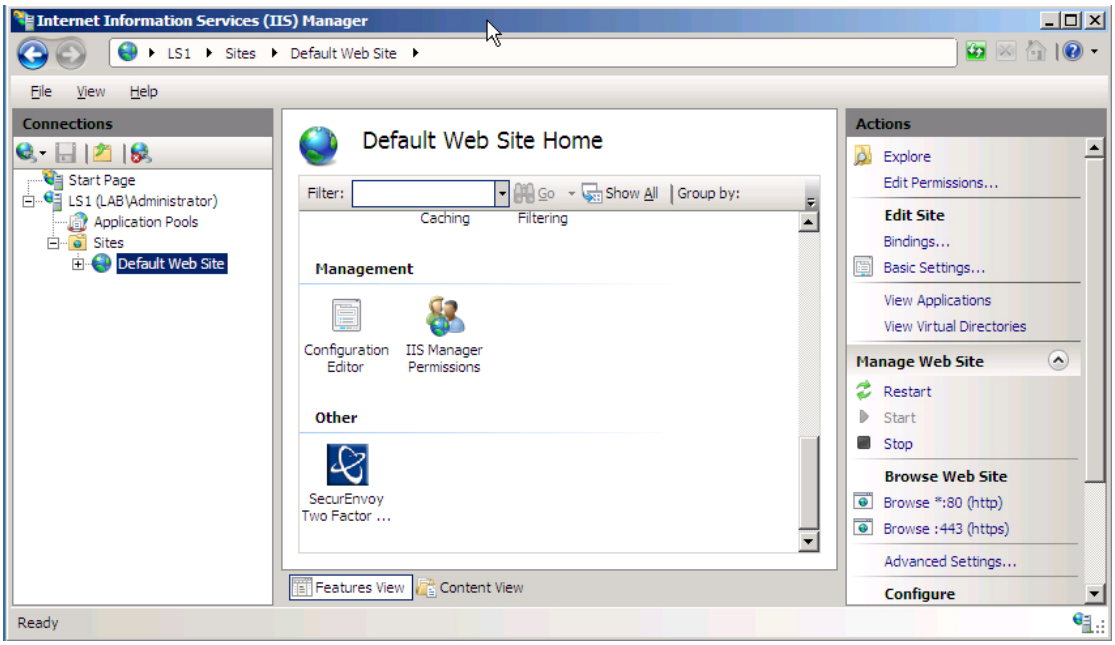
The Microsoft IIS agent is located in the Agent directory of the software distribution

Install this agent on your Outlook Web Access IIS server

Configure the IIS Agent for Outlook Web Access

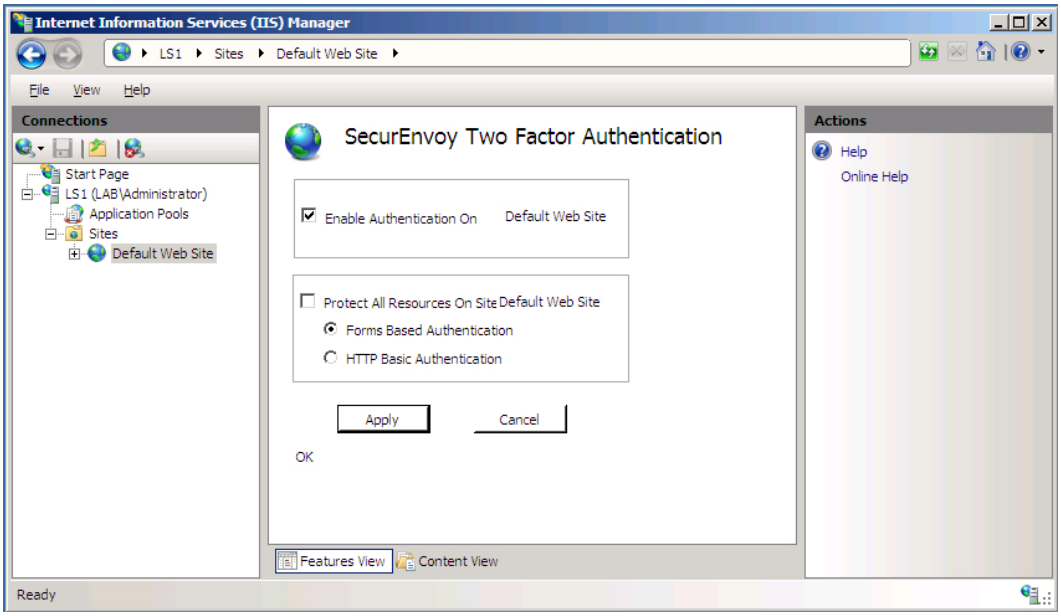
Launch the IIS7 management interface, either from "Start", "Administration Tools" or from the Server Manager

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.



If OWA is installed on a Windows 2003 server then right click “Default Web Site” and select Properties and select the SecurEnvoy tab.
Enable the tick box to “Enable Authentication On Default Web Site”

Click “OK” when complete.

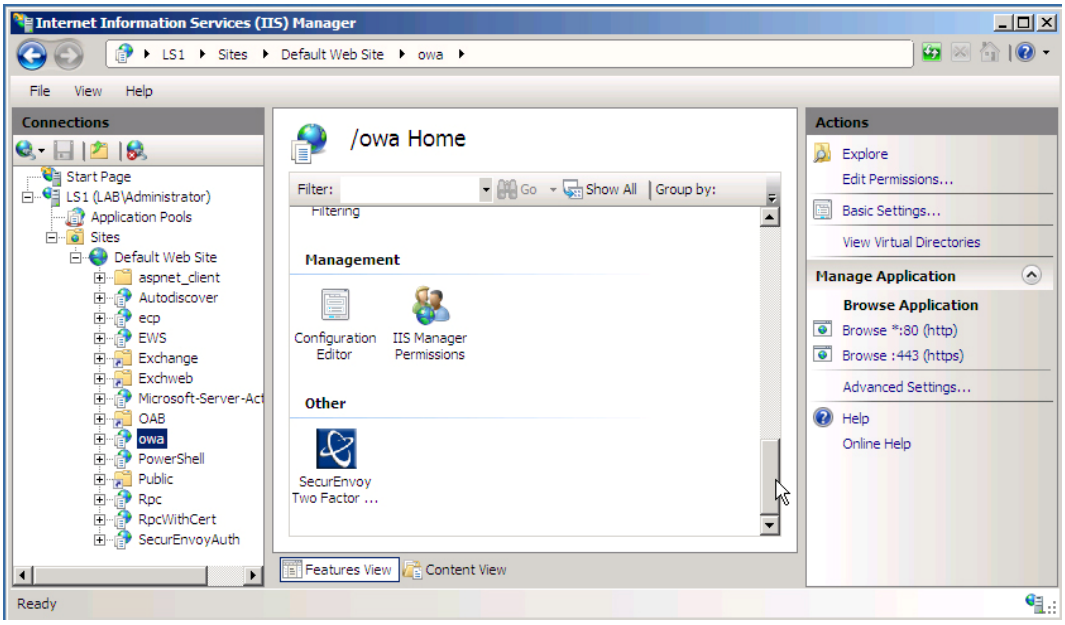


Next select the virtual web site you want to protect. For OWA select “owa”, scroll down the centre panel and select “SecurEnvoy Two Factor”

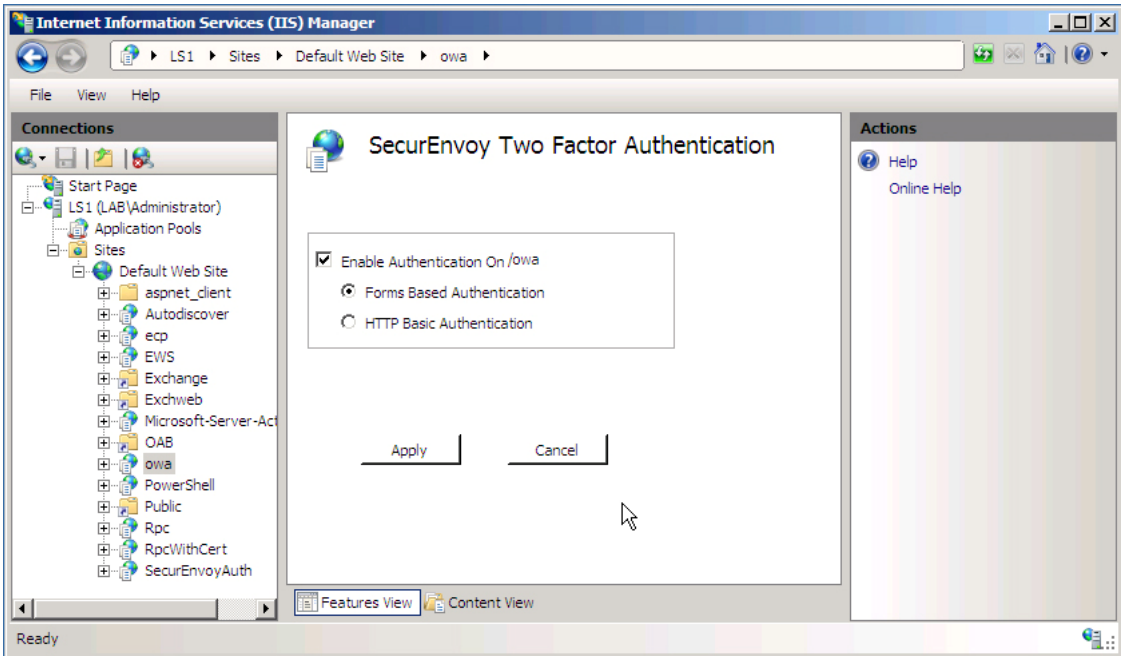
If OWA is installed on a Windows 2003 server then right click “owa” and select Properties and select the SecurEnvoy tab.

Note

If you wish to use Exchange Sync / Email Push to mobile phones then you should create a separate OWA instance and authenticate this instead and restrict your existing instance to internal / local users only as Exchange Sync needs to authenticate to its self.



Select the tick box “Enable Authentication On /owa”
Select “Form Based Authentication” (The Default)
Click “Apply” to finish
Cancel restart IIS when prompted.

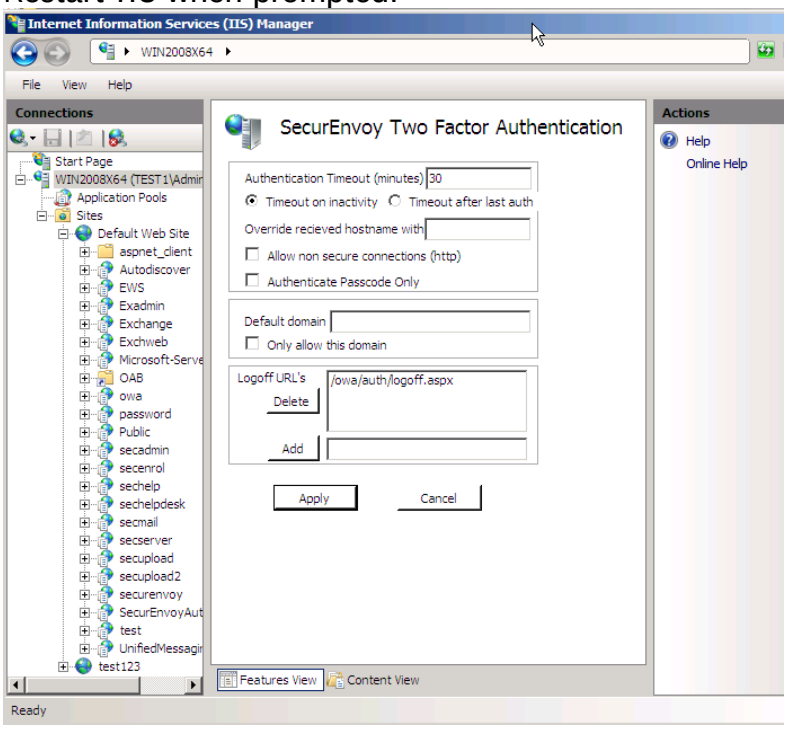


Note

The virtual directory SecurEnvoyAuth is automatically set to the application pool “MSExchangeOWAAppPool”. This must be maintains for correct operation.

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.

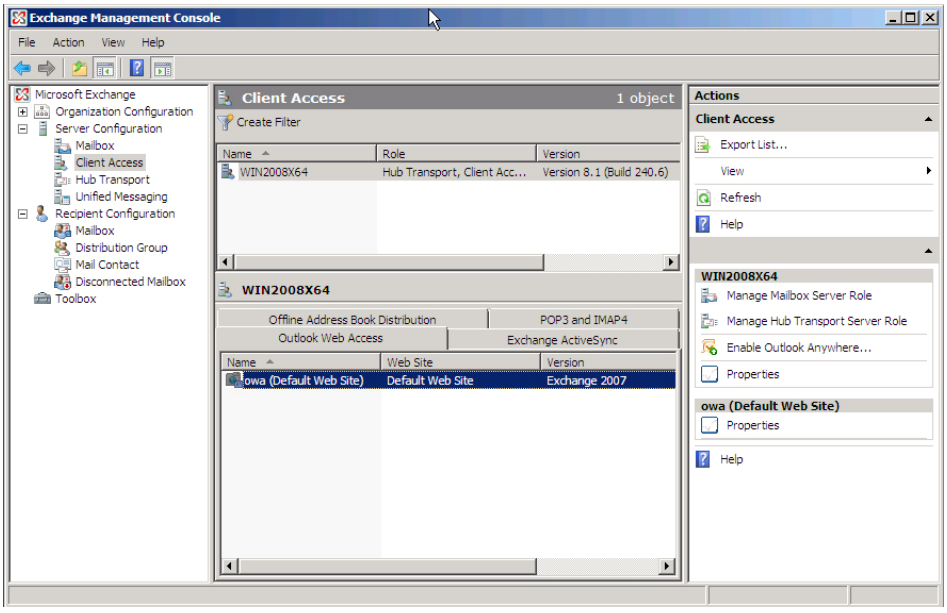
Add the logout URL **/owa/auth/logoff.aspx**
Restart IIS when prompted.



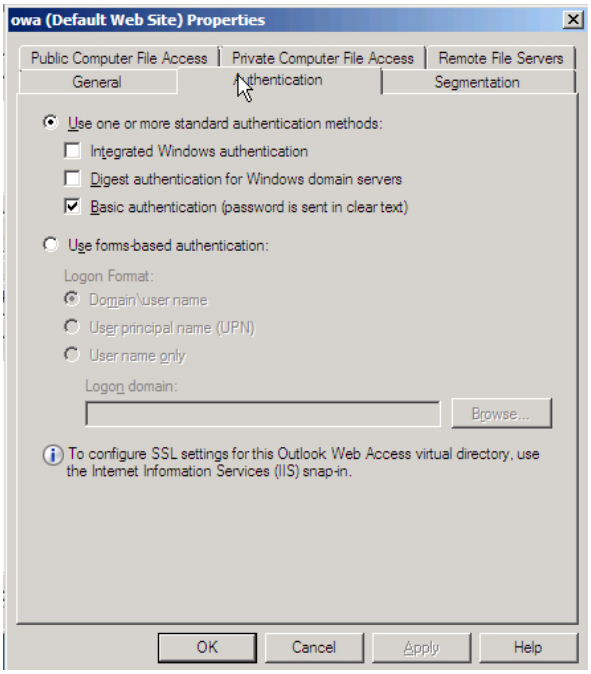
Note

LogoffURL require IIS agent version 5.3.502 or higher

Change OWA to use basic authentication to allow single sign-on as follows:
1. Start Exchange Management Console and expand
Server Configuration – Client Access and click on “owa (Default Web Site)”



2. Select the Authentication Tab and select “Use one or more standard authentication methods:” and then select “Basic authentication”



3. Press OK and Restart IIS.

Note

Basic authentication passwords are only sent between the SecurEnvoy IIS agent and the OWA application within the same server and are not used between OWA and browser.

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/owa (Don’t forget the https)
User logon screen is shown below.

