Microsoft Outlook Web Access 2013

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	

Microsoft Outlook Web Access 2013 Integration Guide

This document describes how to integrate Microsoft Outlook Web Access 2013 (OWA 2013) with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

OWA 2013 provides Secure Remote Access to the internal corporate email.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as OWA 2013), 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:

OWA 2013

Microsoft Server 2012 R2
Microsoft Exchange Server 2013

SecurEnvoy

Microsoft Server 2012 R2
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 v7.2.503

© 2014 SecurEnvoy Ltd. All rights reserved

Index

1.0 Prerequisites 3
1.1 Configure the IIS Agent for Default website 4
1.2 Configure the IIS Agent for Outlook Web Access 5
2.0 Configure logout URL 6
2.1 Configure Outlook Web Access Template 6
3.0 Test the Two Factor Authentication 7
4.0 Notes 9

1.0 Prerequisites

It is assumed that the Exchange 2013 has been installed and is authenticating with a username and password.

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 Exchange server(s), additional open ports will be required.

IIS Agent has been installed as per the SecurEnvoy IIS Agent Installation and Admin Guide: https://www.securenvoy.com/integrationguides/iis%20agent%20installation%20guide.pdf

The following table shows what token types are supported.

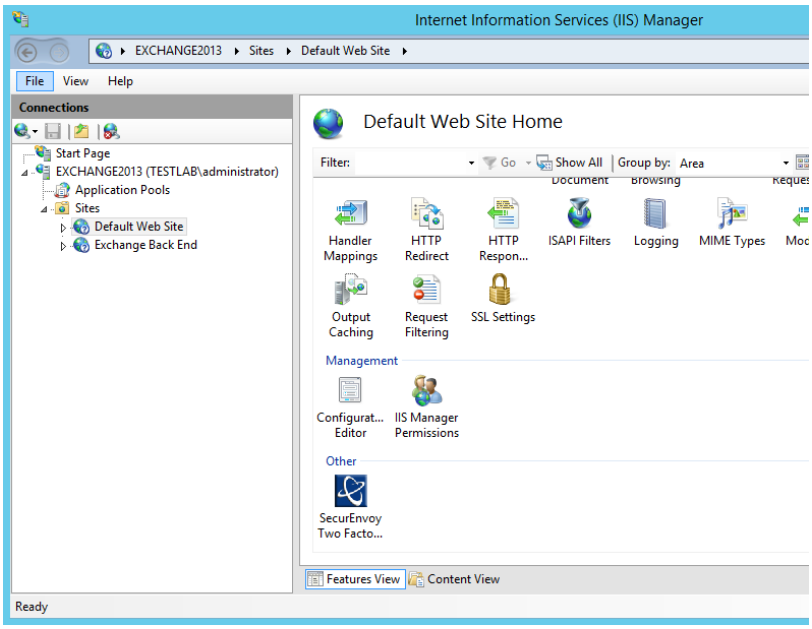
Token Type Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓
One Swipe	✓

© 2014 SecurEnvoy Ltd. All rights reserved

1.1 Configure the IIS Agent for Default website

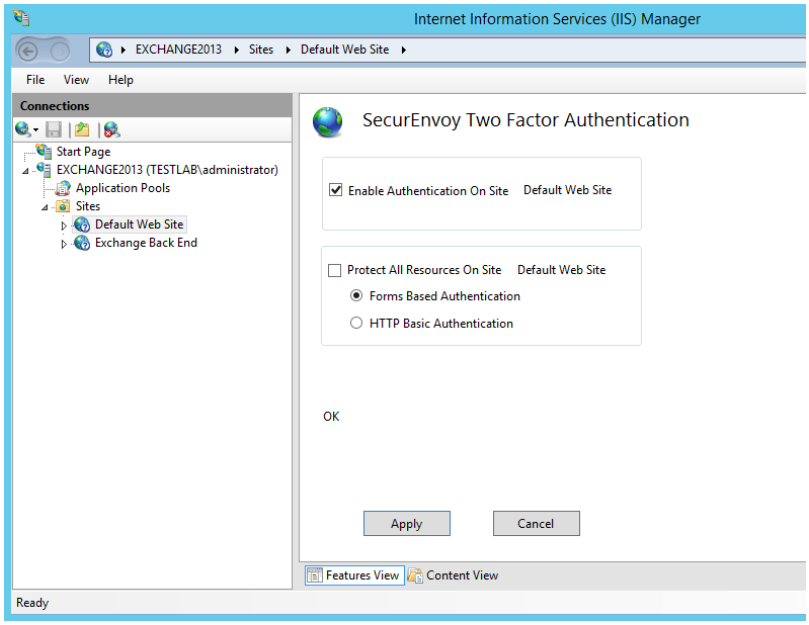
Launch the IIS management interface, either from "Start", "Administration Tools" or from the Server Manager

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"

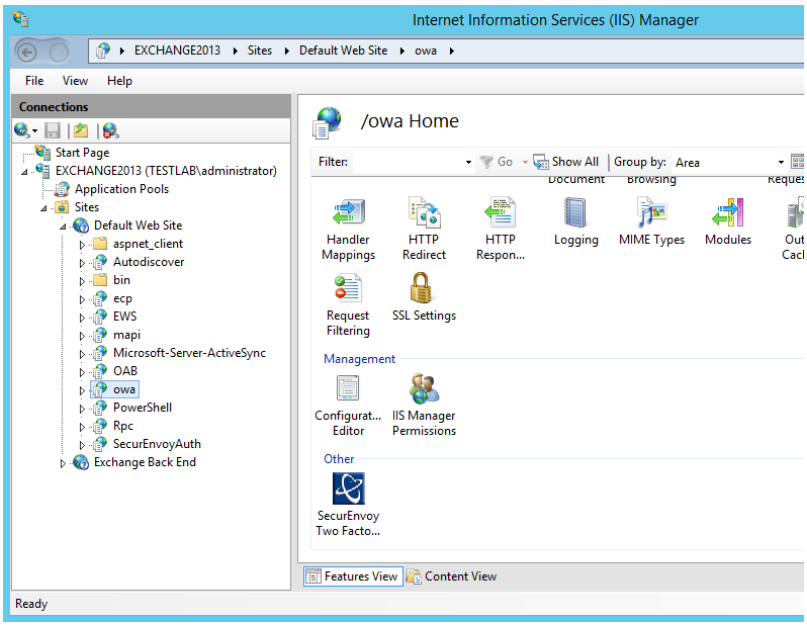
Click "Apply" when complete.



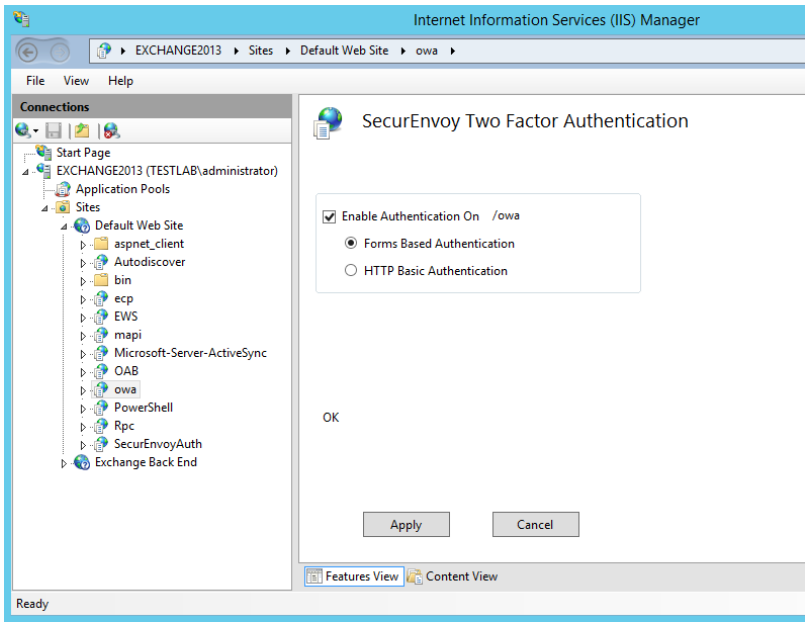
© 2014 SecurEnvoy Ltd. All rights reserved

1.2 Configure the IIS Agent for Outlook Web Access

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



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.

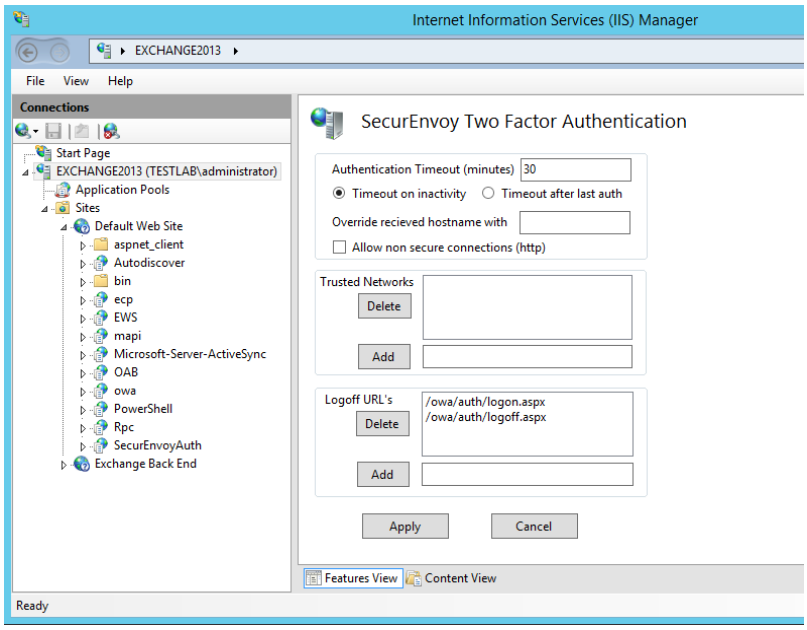
© 2014 SecurEnvoy Ltd. All rights reserved

2.0 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 **/owa/auth/logon.aspx**
/owa/auth/logoff.aspx

Restart IIS when prompted.



2.1 Configure Outlook Web Access Template

Copy the contents of OWA2013 (C:\Program Files (x86)\SecurEnvoy\Microsoft IIS Agent\SAMPLES) to

WEBAUTHTEMPLATE (C:\Program Files (x86)\SecurEnvoy\Microsoft IIS Agent), backing up existing files.

© 2014 SecurEnvoy Ltd. All rights reserved

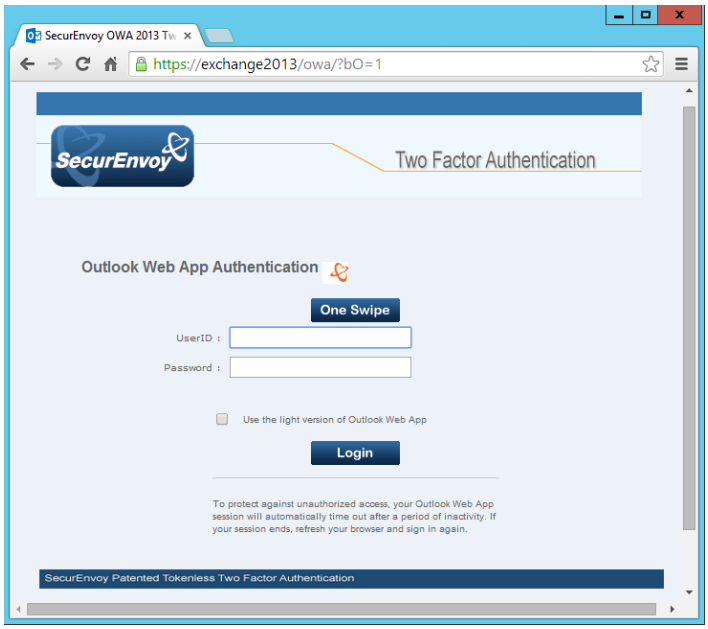
3.0 Test the Two Factor Authentication

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/owa (Don't forget the https)

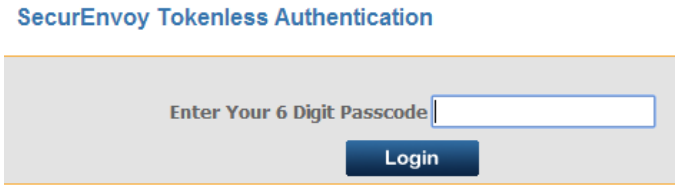
User logon screen is shown.

Enter your UsedID and Password:

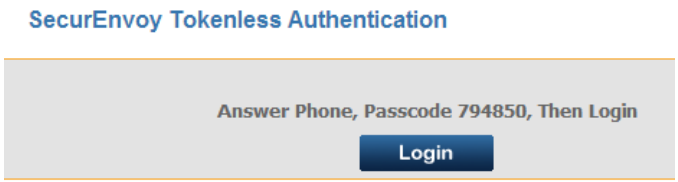


User is then presented with their two factor authentication type:

- Pre load, Realtime and Soft tokens:



- VOICE tokens:

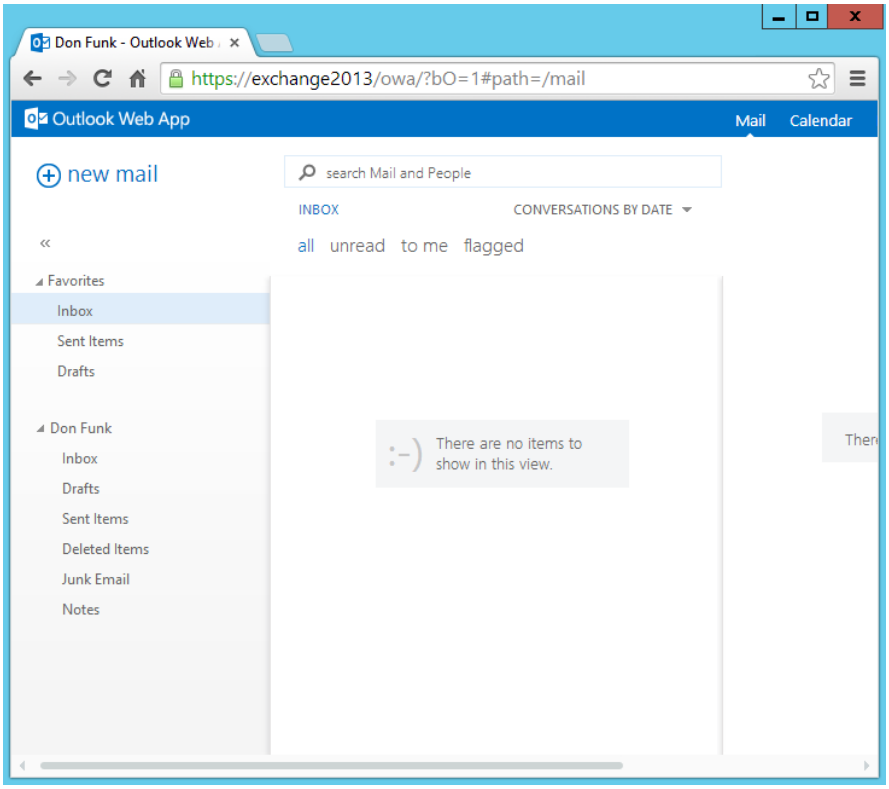


- One Swipe:



© 2014 SecurEnvoy Ltd. All rights reserved

User authenticates successfully and is presented with OWA 2013:



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 OWA without specifying the domain name:
domain\UserID

© 2014 SecurEnvoy Ltd. All rights reserved

4.0 Notes

© 2014 SecurEnvoy Ltd. All rights reserved