SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

Microsoft Outlook Web Access 2013 Installation Guide

SecurAccess Integration Guide

Version 2.0 – 12/18

Microsoft Outlook Web Access 2013 Integration Guide

Contents

1.1 SOLUTION SUMMARY 3

1.2 GUIDE USAGE 3

1.3 PREREQUISITES 3

1.4 AUTHENTICATION 4

1.41 SETUP RADIUS - SECURACCESS 4
1.42 SECURENVOY MICROSOFT SERVER AGENT INSTALLATION 5
1.43 SETUP RADIUS IIS AUTHENTICATION 5
1.44 CONFIGURE IIS FOR SECURENVOY MFA AUTHENTICATION 6
1.46 CONFIGURE OUTLOOK WEB ACCESS 2013 MFA AUTHENTICATION 9
1.47 CONFIGURE OUTLOOK WEB ACCESS TEMPLATES 10

1.5 TEST FOR TWO FACTOR AUTHENTICATION 11

1.1 Solution Summary

SecurEnvoy's SecurAccess MFA provides Two Factor Authentication for remote access solutions (such as OWA 2013)

The software used for the integration process is listed below:

OWA 2013
SecurEnvoy Microsoft Server Agent
Microsoft Exchange Server 2013
Microsoft Internet Information Services

SecurEnvoy
SecurEnvoy Microsoft Server Agent
SecurAccess software Release V9.3.502

1.2 Guide Usage

The information in this guide describes the configuration required for integration with SecurEnvoy and common to most deployments. It is important to note two things:

- Every organization is different and may require additional or different configuration.
- Some configurations may have other methods to accomplish the same task than those described.

1.3 Prerequisites

The following conditions are required to set up SecurEnvoy's MFA Solution:

- Microsoft Exchange Server 2013
- Microsoft Internet Information Services
- SecurEnvoy SecurAccess Server installed with the RADIUS service
- SecurEnvoy Microsoft Server Agent
- If firewalls are between the SecurEnvoy SecurAccess Server, Active Directory Servers and Exchange Servers additional open ports will be required.

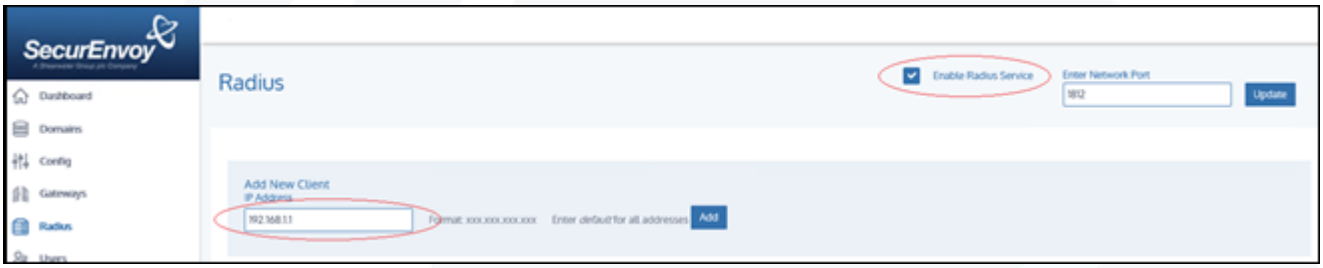
1.4 Authentication

The following section describes the steps required to configure SecurEnvoy Microsoft Server Agent to authenticate users via RADIUS through the SecurEnvoy SecurAccess Solution.

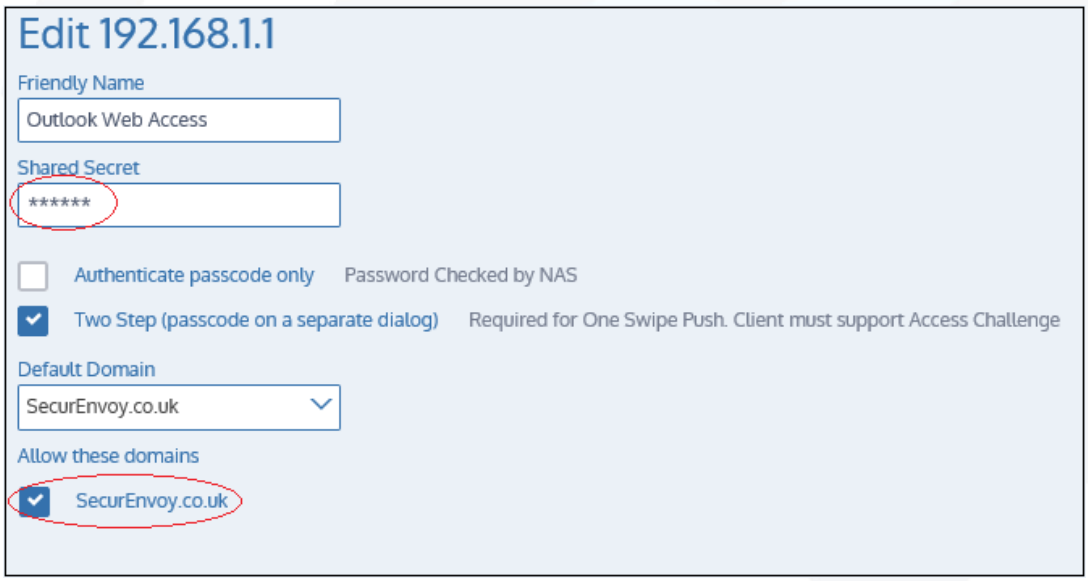
1.41 Setup RADIUS - SecurAccess

Within the SecurAccess configuration, we will need to configure the Outlook Web Access server to communicate and authenticate as an authorised RADIUS client.

- Navigate to RADIUS in the administrator dashboard.
- Ensure the RADIUS Service is enabled in the top right-hand side of the screen and make sure the port number is left as default 1812.
- Enter the IP address of the Outlook Web Access server and click “Add”



- Enter in a shared secret or common password and select the domains that will be authenticated against (if there is more than one domain configured in SecurAccess)
- Click Update

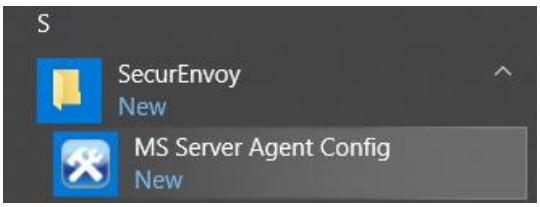


1.42 SecurEnvoy Microsoft Server Agent Installation

From the SecurEnvoy SecurAccess console, locate and run the SecurEnvoy Server Agent installer which can be found in the latest downloaded SecurEnvoy software folder or ZIP file.

securenvoy.zip\Releasex.x.xxx\Agents\Microsoft Server Agent\setup.exe

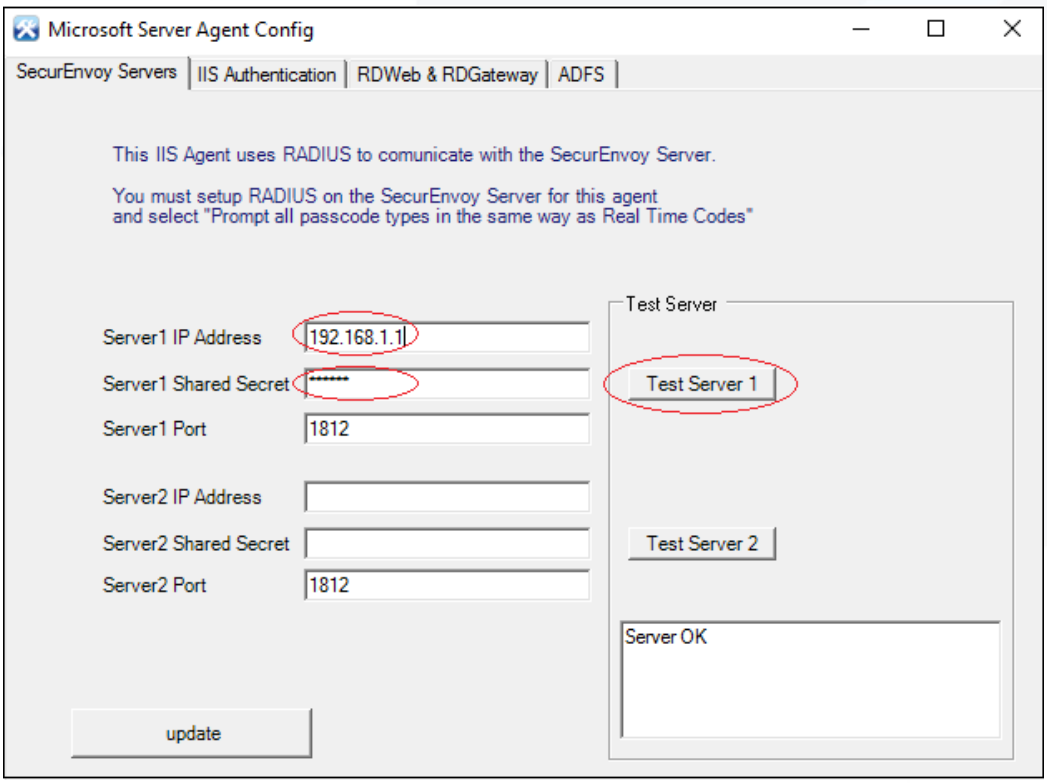
On successful installation of the agent, locate and run the server agent



1.43 Setup RADIUS IIS Authentication

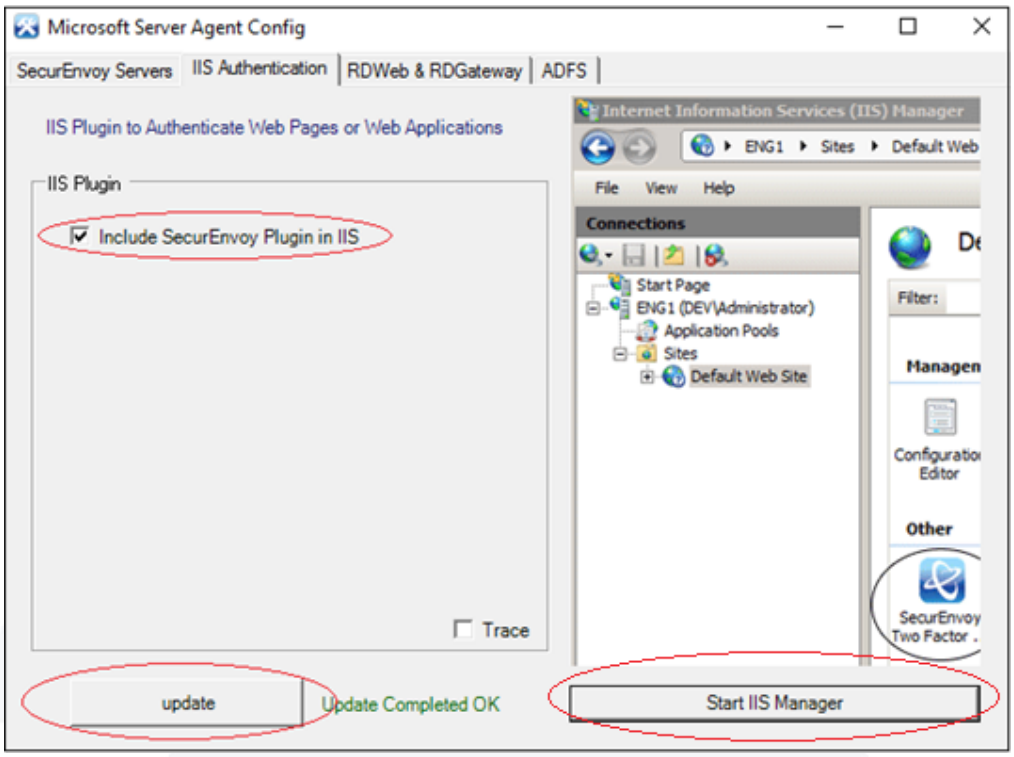
From the configuration console, we will configure the details of the SecurEnvoy Server that will authenticate the Outlook Web Access 2013 server.

Enter in the IP address of the SecurEnvoy Server and the Shared Secret, configured in section 1.41 of this document.
Once details have been entered click on Test Server 1 to confirm that the SecurAccess server is IP reachable and is accepting authentication challenges with the correct shared key.



By selecting the IIS Authentication tab at the top of the Microsoft Server Agent Config, this will allow us to configure the Microsoft Server Agent to support the redirection of user authentication to SecurEnvoy MFA.

Tick "Include SecurEnvoy Plugin in IIS" and click Update at the bottom of the page

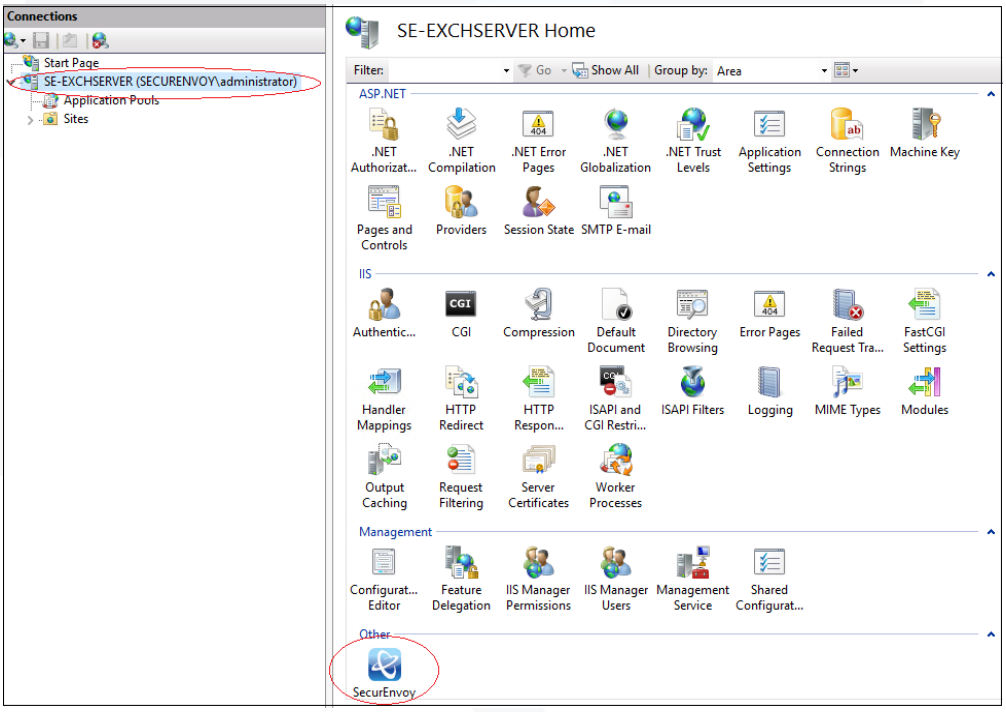


Click on "Start IIS Manager" to load IIS Manager.

1.44 Configure IIS for SecurEnvoy MFA Authentication

On loading of the Internet Information Services Manager, we will look to configure OWA to utilise SecurEnvoy as the Multi-Factor Authentication method.

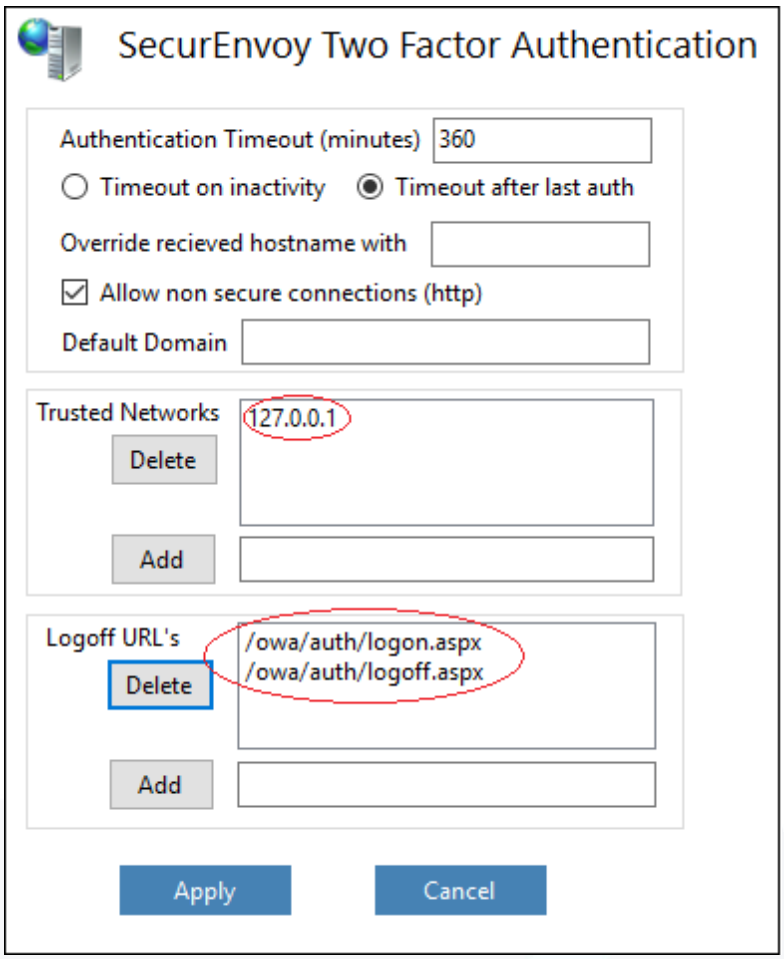
In the "Connections" pane select the top-level name, then in the Centre pane select the SecurEnvoy icon at the bottom of the centre pane.



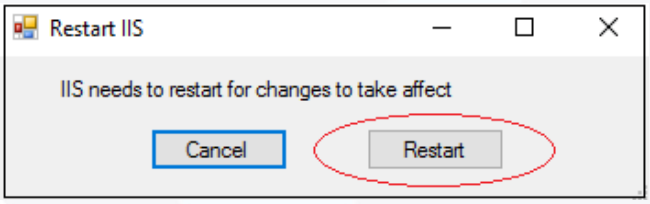
In centre pane "SecurEnvoy Two Factor Authentication" add the two following URL's then select Apply.

/owa/auth/logon.aspx
/owa/auth/logoff.aspx

Since the release of Outlook 2013 OWA and ECP use the same landing page.
To stop administrators from getting a 2FA challenge On ECP entering loopback address 127.0.0.1 as a trusted site will stop this.



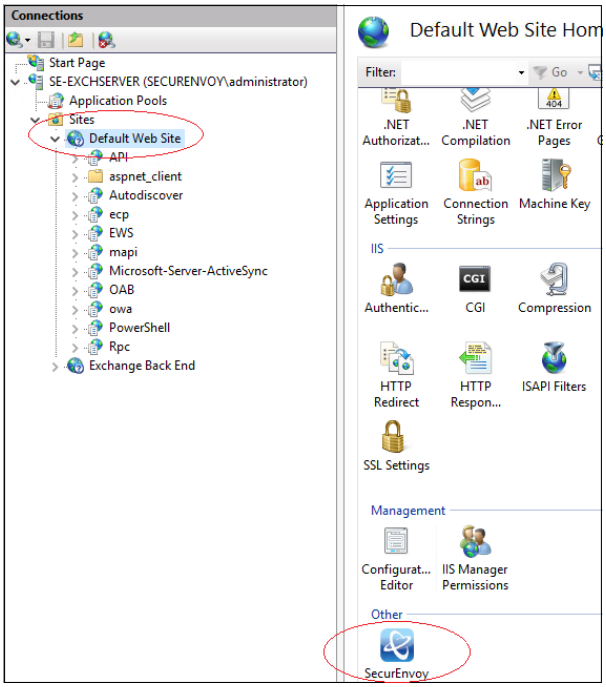
Select Restart when prompted



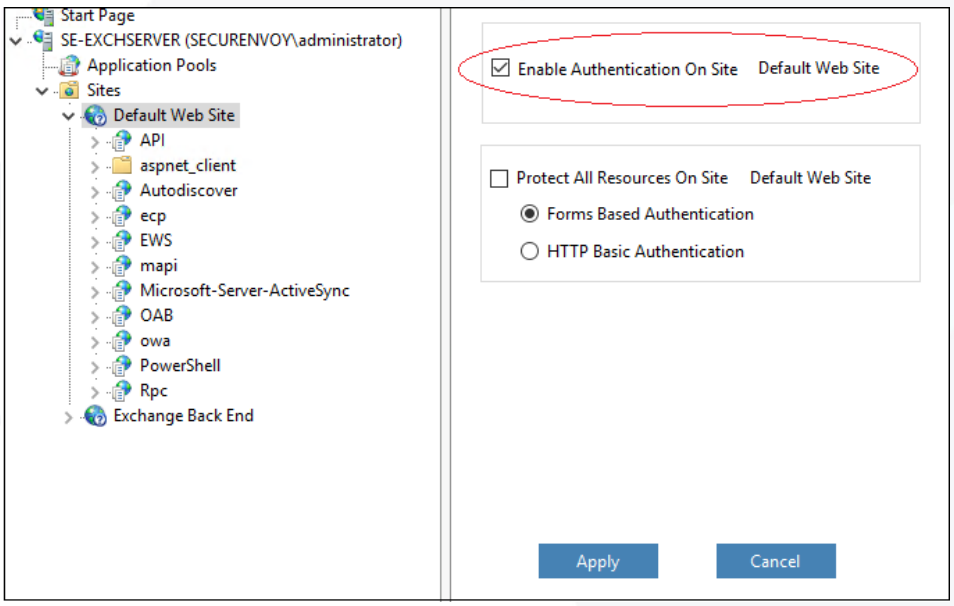
Warning - before applying our ISAPI filter:

- Recommend installation out-of-hours or least busy times.
- Logout existing OWA users.
- Users that are already logged into OWA will be required to reauthenticate (2fa enabled?) with 2fa.

In “Connections” pane select Default Web Site
Then in centre pane
“Default Web Site Home”
select SecurEnvoy.

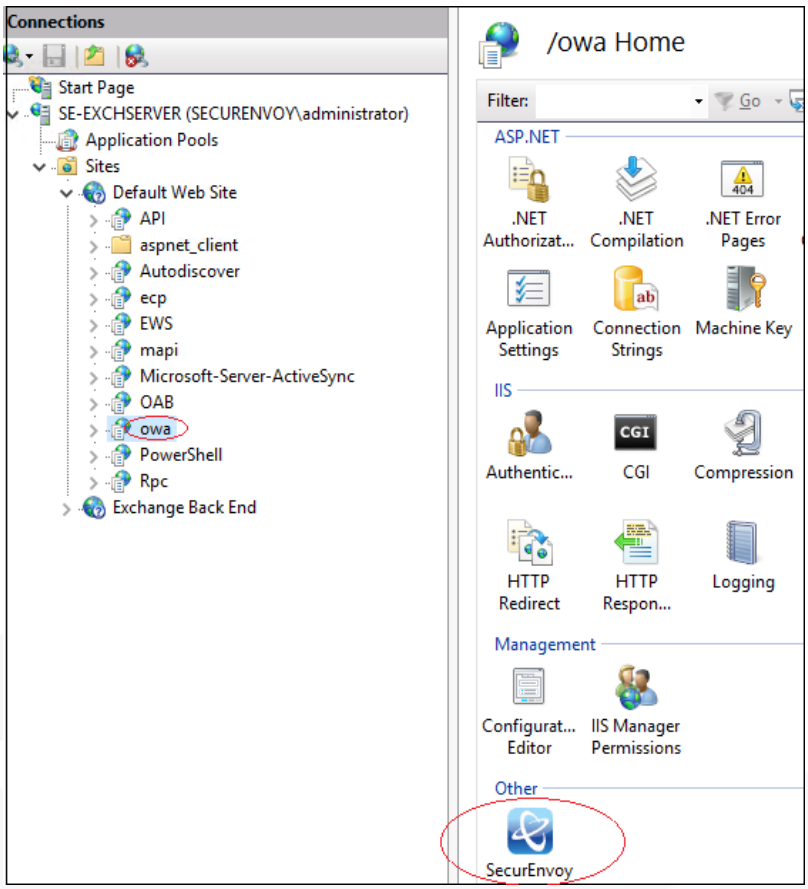


Select tick box Enable Authentication on Site Default Web Site
then select Apply.



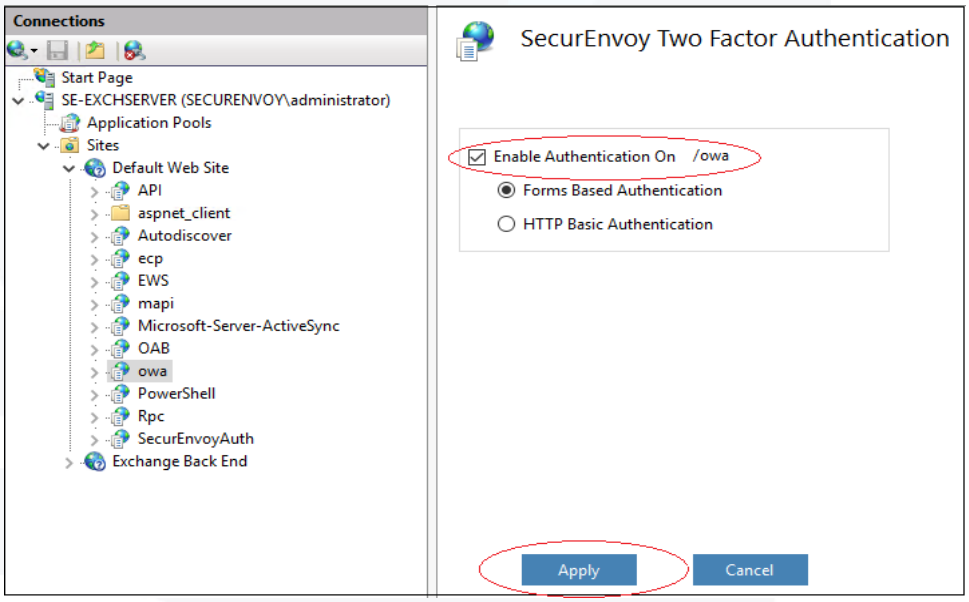
1.46 Configure Outlook Web Access 2013 MFA Authentication

In “Connections” pane select owa, then in centre pane “/owa Home” select SecurEnvoy.

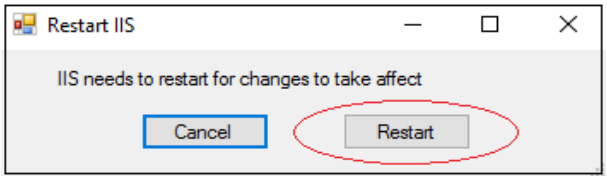


Select Tick Box
Enable Authentication on /OWA

Then select Apply.

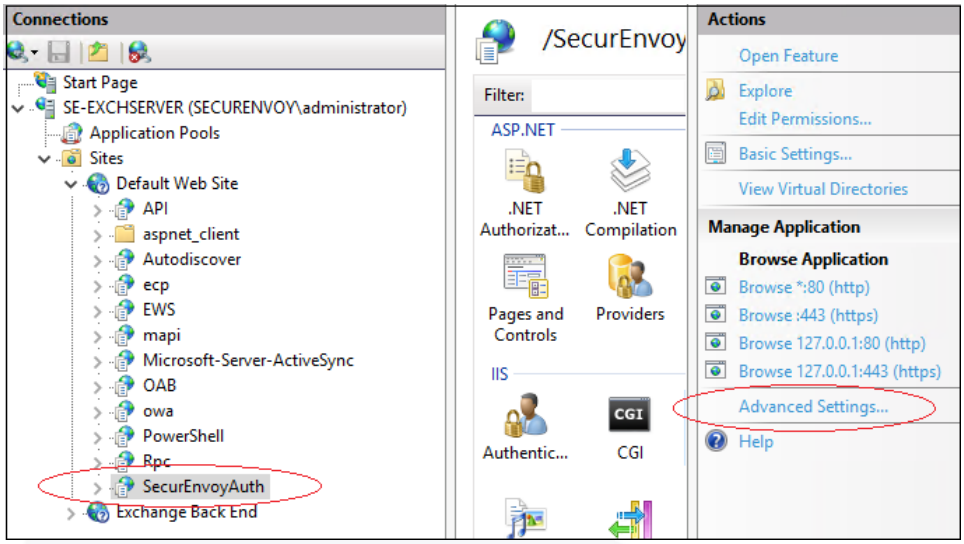


Select Restart when prompted



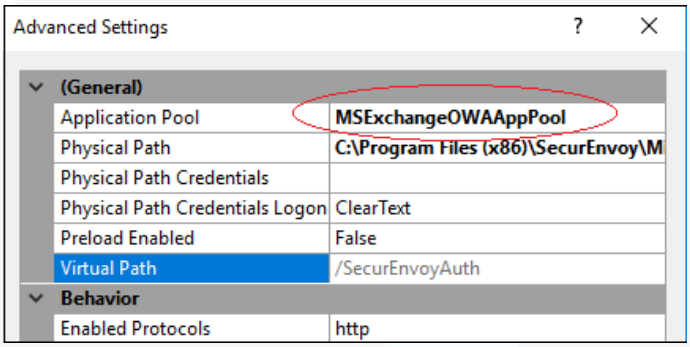
In “Connections” pane select SecurEnvoyAuth

Then in the “Actions” Pane select Advanced Settings



Under the (General) tab

Check that “Application Pool” is set to MSExchangeOWAAppPool



1.47 Configure Outlook Web Access Templates

On the Exchange Server copy the contents from folder

C:\Program Files (x86)\SecurEnvoy\Microsoft Server Agent\SAMPLES\OWA2013

To folder

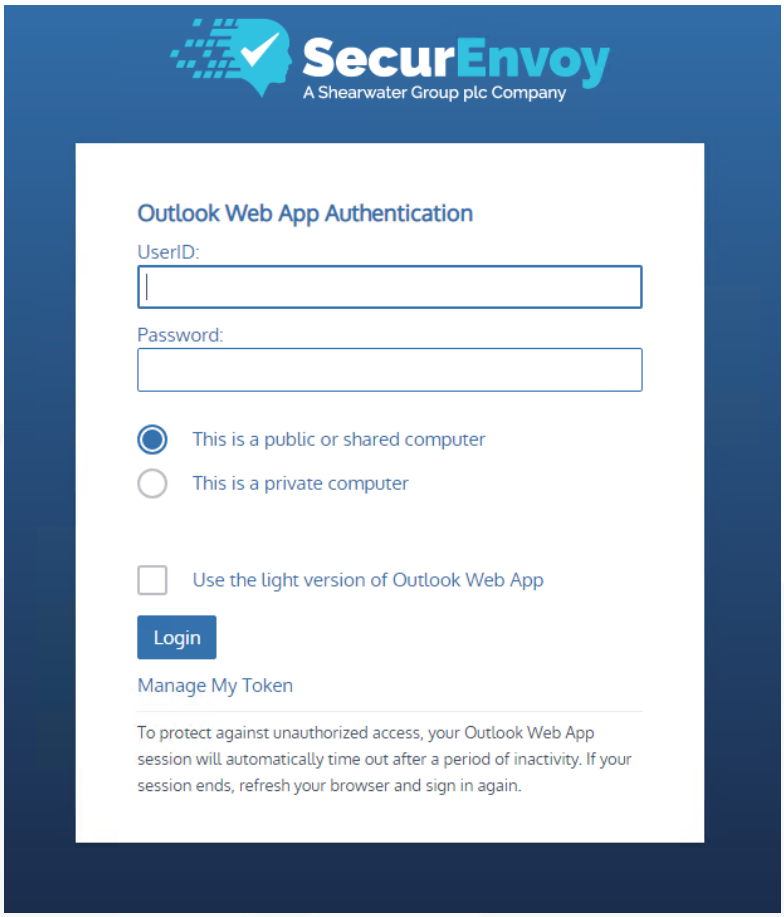
C:\Program Files (x86)\SecurEnvoy\Microsoft Server Agent\WEBAUTHTEMPLATE

1.5 Test for Two Factor Authentication

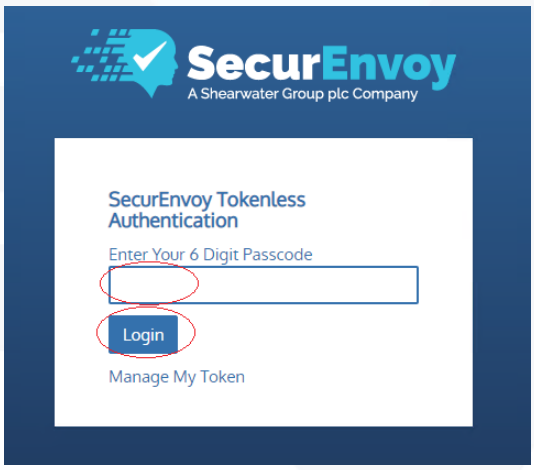
Test the two-factor web authentication by opening a web browser and going to the URL for the web server.

https://your_Server_Iname/owa (Don't forget https:)

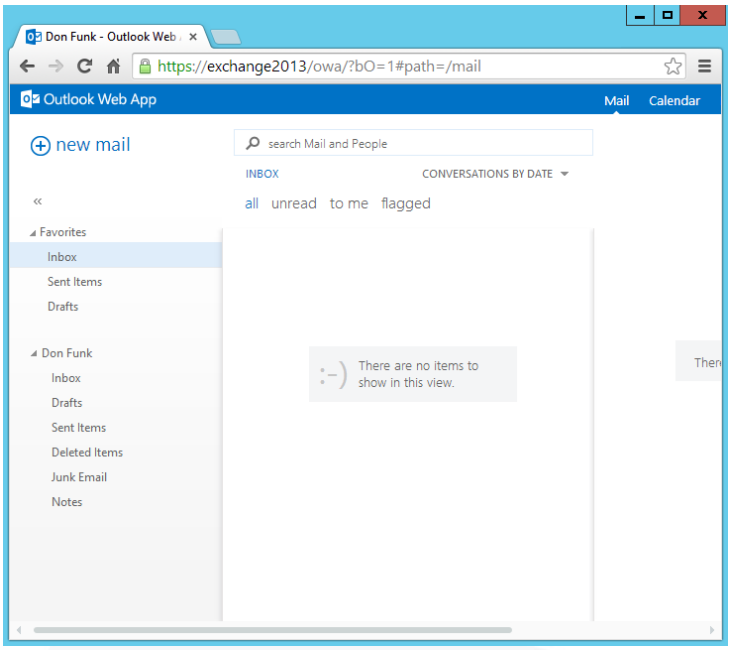
Enter your UserID and Password:
then select Login.



Enter Your 6 Digit Code
Then select Login



On a successful authentication the user will be presented with OWA 2013



Note

Configure your domain name by modifying the following line within seiis.ini in folder (C:\Windows): (Please make a backup copy first)

# 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

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com