SecurEnvoy IIS Web Agent

SecurEnvoy Ltd
1210 Parkview, Arlington Business Park, Theale, Reading. RG7 4TY
Tel: 0845 2600010 Fax: 0845 260014 **www.SecurEnvoy.com**

SecurEnvoy IIS Web Agent

Installation and Admin Guide v5.3

The SecurEnvoy Security server is the main central component of the SecurEnvoy suite of products. It has direct integration into a LDAP directory server (Microsoft Active Directory, Novell e-Dir, Sun Directory Server and Linux Open LDAP Directory Server) for user information, controls and manages the authentication of SMS passcodes and the subsequent sending of them.
This must be installed for SecurAccess, SecurPassword SecurICE and SecurMail.

SecurEnvoy IIS Agent Installation and Admin Guide v5.3

© 2009 SecurEnvoy

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Printed: 2009 in United Kingdom

Publisher
SecurEnvoy Publishing

Managing Editor
SecurEnvoy Training Dept

Technical Editors
A Kemshall Technical Director
P Underwood EMEA Pre – Sales

Cover Designer
SecurEnvoy Marketing

Revision	
v1.2 AK PU	9/1/2009
v1.3 PU	26/2/2009
V1.4 PU	24/6/2009
V1.5 PU	6/11/2009

Foreword

SecurEnvoy is the trusted global leader of tokenless two-factor authentication. As the pioneers of mobile phone based tokenless authentication; SecurEnvoy lead the way with ground breaking solutions that others aspire too.
Our innovative approach to the tokenless market now sees thousands of users benefitting from our solutions all over the world. With users deployed across five continents, our customers benefit from significant reduced time to deploy and a zero footprint approach means there is no remote software deployment and administrators enjoy the management tools allowing them to rapidly deploy up to 15000 users per hour.
Our design philosophy is based on re-using existing customer technology investments such as Microsoft Active Directory, simplifying the end user authentication experience while enhancing the overall security.
With no token manufacturing costs the return on investment (ROI) is so much more acceptable to businesses and organizations, and environmentally the green benefits of a zero carbon footprint also attract environmentally responsible purchasers. We are truly now providing solutions that have zero impact on our environment.
SecurEnvoy distribute through the channel, providing customers the value added benefits of working with local partners. We have now built up a technical and sales infrastructure that supports most languages and cultures around the world.
The business was officially incorporated in 2003 after preliminary, coding and testing in our labs. Years on we now have happy customers across the five continents and regional support. Business levels have more than doubled year on year due to our subscription sales model which is an acceptable route that allows our clients to budget more effectively. This model includes local support and annual subscriptions.
Founded by Andrew Kemshall and Stephen Watts, the two founders work relentlessly to achieve business growth worldwide. This massive growth has been possible through the quality of people and the experience within the company both from sales and technical expansion.
SecurEnvoy continues to shape the way millions of people plan their authentication requirements and purchasing decisions.

Contents

1.0 Overview of Installation Files 6
1.1 IIS Agents 6

2.0 SecurAccess Microsoft IIS Agent Install & Configuration 6
2.1 Agent Architecture 6
2.2 Installing the IIS Agent 7
2.3 Upgrading IIS Agent 8
2.4 IIS Agent Administration 10

3.0 Single Sign on 14

4.0 IIS Agent Advanced Administration 16

Note

A v5.3 IIS Agent can only ever be used with a v5.2 and above SecurEnvoy Security server.

1.0 Overview of Installation Files

SecurAccess IIS Agent

This agent is only required if you are installing SecurAccess and you need to directly authenticate an application running on an IIS Web Server.
With this agent, any existing web application can be configured for two factor authentication without the need to modify the application or make any programmatic changes.

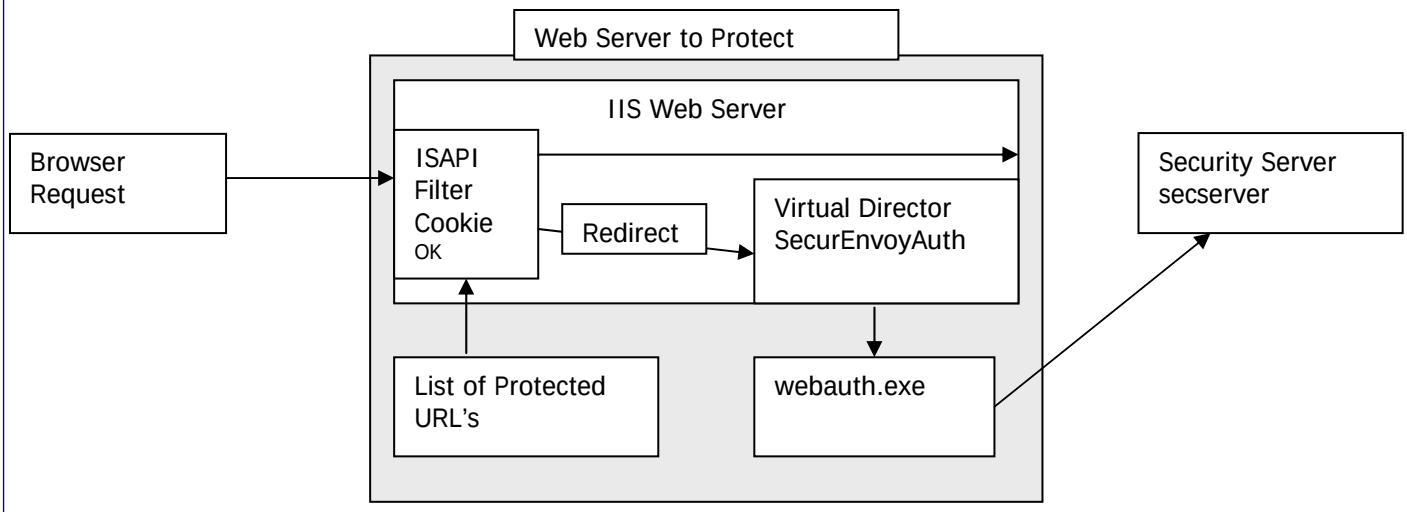
1.1 IIS Agents

Pre Requisites
Note this agent is only required for SecurAccess
Supported IIS Versions:

IIS V6 running on Windows 2003 - all service packs (x32 and x64 bit)
IIS V7 running on Windows 2008 SP1-2 (x32 and x64 bit) and R2
It is highly recommended that any protected web server should have SSL (https) enabled.
Microsoft .NET 2.0 is installed

2.0 SecurAccess Microsoft IIS Agent Install & Configuration

2.1 Agent Architecture



All web URL requests are monitored by the ISAPI filter program webauthfilter. If a protected resource is requested the filter checks to see if a valid un-tampered cookie is available and that it hasn't timed out. If the cookie is OK then the request is passed on.
If the cookie is unavailable or has timed out the ISAPI filter redirects the request to SecuEnvoyAuth/webauth.exe. This program requests a UserID, Pin and Passcode and sends it to the security server for authentication.

If the security server returns AUTH OK then webauth.exe creates a valid cookie and redirects the request back to the original page.

2.2 Installing the IIS Agent

Pre-requests: IIS must be installed and running on one of the following:-

Windows 2003
Windows 2008

Microsoft Dot Net v2.0 installed. Otherwise IIS Agent will automatically install MS Dot Net v2.0.

There must be a network connection via http (Port 80) between the IIS server and the security server(s). All authentication data is encrypted with AES 128bit.

Note

A v5.3 IIS Agent can only ever be used with a v5.2 SecurEnvoy Security server.

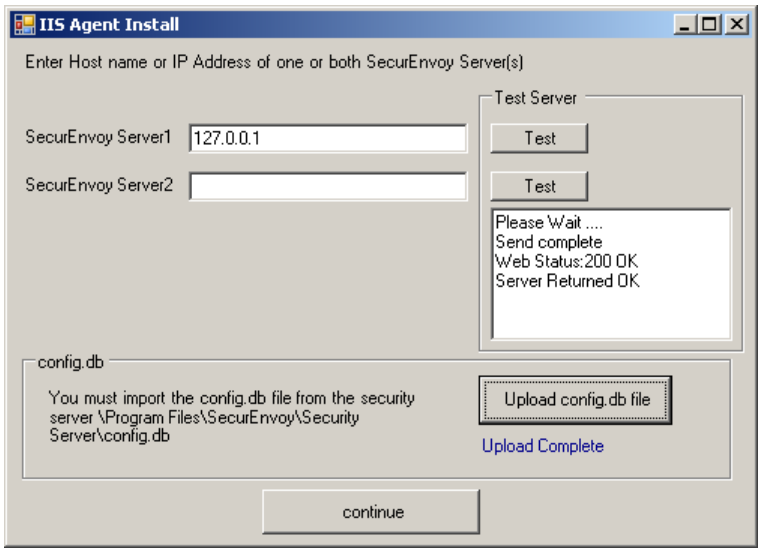
To install the IIS Agent run "Microsoft IIS Agent\setup.exe"

The following page is displayed for user input.

When prompted enter up to two security servers (note these two security servers must share the same config.db file)

If only one security server is required blank the second server entry.

Make sure all the security server names you enter can be resolved and reached. It is recommended that to start a CMD window and PING all security servers that will be entered.



Click the "Test" button to check that each Security server can be contacted.

Next click the "Get Config.db file" button

Navigate to the Security Server and point to where the config.db file resides.

Click "Open". This file is then copied across to the IIS web server.

The config.db file is located by default in C:\Program Files\SecurEnvoy\Security Server. This is copied to C:\WINDOWS for Windows 2003 and 2008 servers.

This completes the IIS Agent Installation.

2.3 Upgrading IIS Agent

To upgrade the SecurEnvoy IIS Agent, please complete the following:

For Windows 2008 deployments

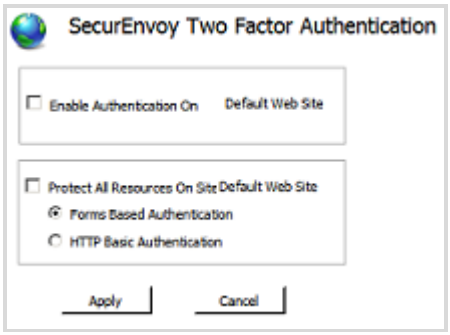
Select Start\Administrative tools\Internet Information Services (IIS) Manager

Select sites and then navigate to the site(s) that was protected.



Double click the SecurEnvoy Icon,

Disable SecurEnvoy IIS Agent by un-checking the box “Enable authentication On” click apply.



Repeat this task on all web sites.

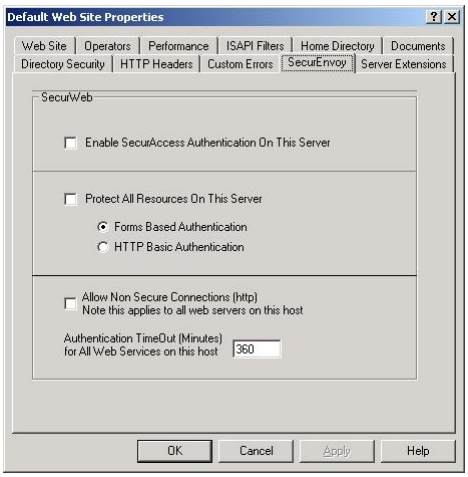
Uninstall SecurEnvoy IIS Agent.

For Windows 2003 deployments

Select Start\Programs**SecurEnvoy**\IISConfig MMC.

Right click the web site that was protected

Select the **SecurEnvoy** Tab
You should see the following screen:



Disable SecurEnvoy IIS Agent by un-checking the box “Enable SecurAccess Authentication”. Click OK.

Repeat this task on all web sites.

Uninstall SecurEnvoy IIS Agent.

2.4 IIS Agent Administration

Administration is performed via Microsoft's Management Console (MMC).

To enable the Agent and protect the whole web site carry out the following:-

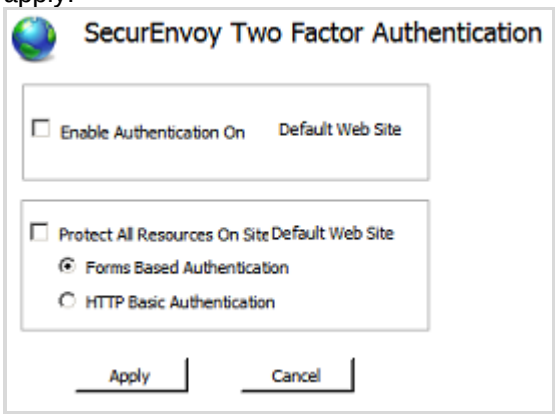
For Windows 2008 deployments

Select Start\Administrative tools\Internet Information Services (IIS) Manager

Select sites and then navigate to the web site(s) that you wish to protect.



Double click the SecurEnvoy Icon, the screen below is shown. To enable the SecurEnvoy IIS Agent by checking the box "Enable authentication On" and select the "Protect all resources" click apply.

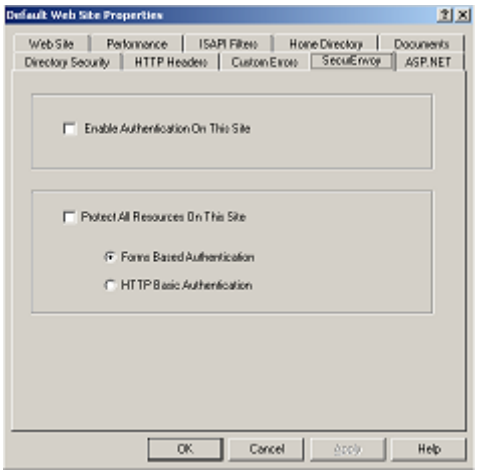


For Windows 2003 deployments

Select Start\Programs**SecurEnvoy**\IISConfig MMC.

Right click the web site that you wish to protect.

Select the **SecurEnvoy** Tab
You should see the following screen:



Enable SecurEnvoy IIS Agent by checking the box "Enable SecurAccess Authentication" and select the "Protect all resources" Click OK.

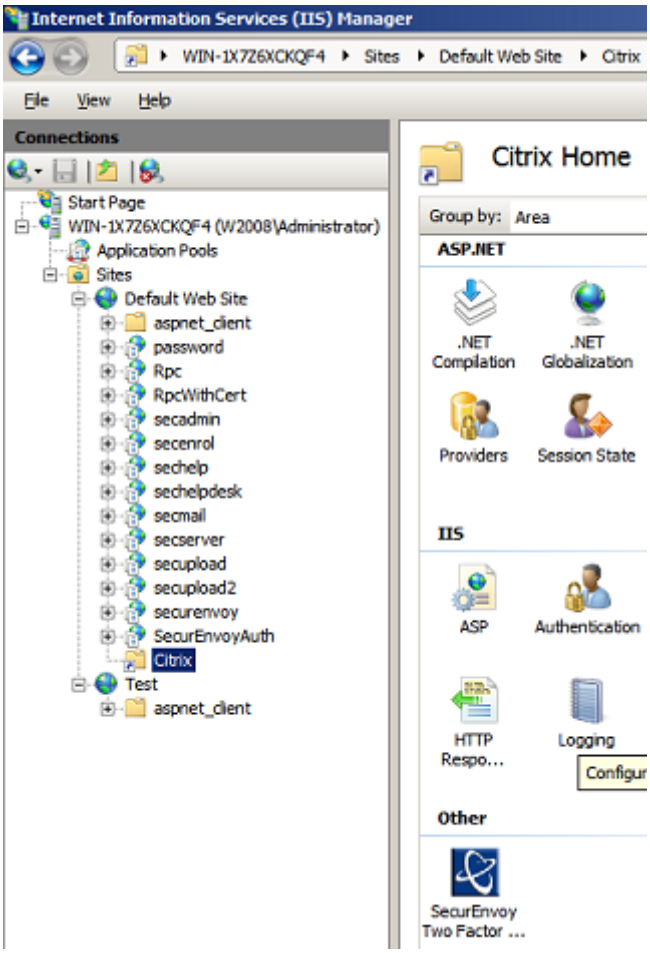
To enable two factor authentication to this server select “Enable Authentication”. If you require the whole web to be protected enable the check box “Protect all resources on this server”. If you wish a more granular approach to only protect certain resources upon the IIS web server leave this box unchecked and apply protection for each required resource. The protection can be applied at a virtual server or a virtual directory.

To protect a certain virtual directory carry out the following:-

For Windows 2008 deployments

Select Start\Administrative tools\Internet Information Services (IIS) Manager

Select sites and then navigate to the web site(s) that you wish to work with. Select the virtual directory, you will then see a SecurEnvoy Icon displayed in the “Features View window”.

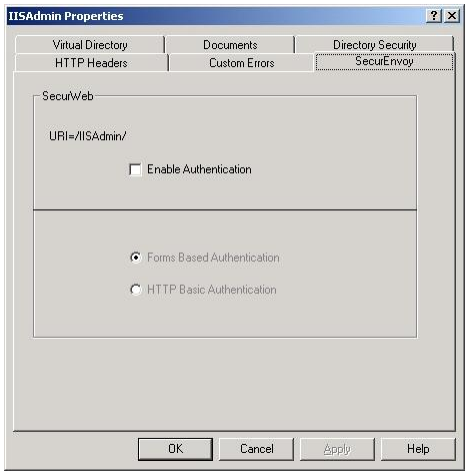


Double click the SecurEnvoy Icon; the following screen will be displayed.

For Windows 2003 deployments

Select Start\Programs**SecurEnvoy**\IISConfig MMC.

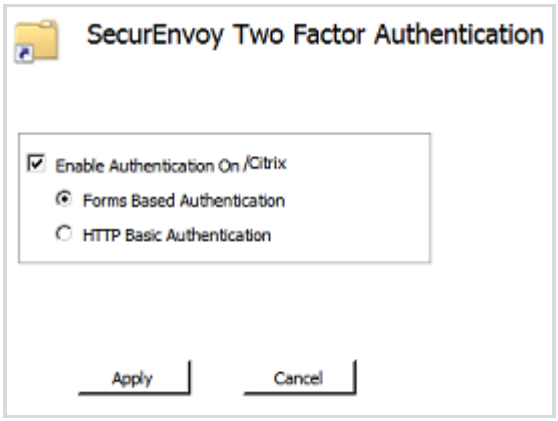
Select Web sites and then navigate to the web site that you wish to work with.
To protect a web resource (a Directory, Virtual Directory or Page) select the resource and right click it and then select properties and the **SecurEnvoy** Tab and enable the check box.



Check the “Enable Authentication” box to enable authentication on this resource and any directories or pages inside it.

There are two ways to carry out a two-factor authentication with IIS, the first is to use a form based logon, and the second is to use a HTTP basic auth. The basic auth will provide a pop up authentication screen for the web browser.

For Windows 2008 deployments



Check the "Enable Authentication" box to enable authentication on this resource and any directories or pages inside it.

There are two ways to carry out a two-factor authentication with IIS, the first is to use a form based logon, and the second is to use a HTTP basic auth. The basic auth will provide a pop up authentication screen for the web browser.

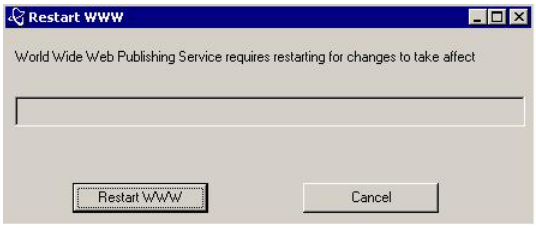
Click "Apply"

Follow prompts for restarting the IIS web server.

For Windows 2003 deployments

Click Ok

When complete the configuration will prompt for the World Wide Web publishing service to be restarted.



Note

If using the HTTP basic auth only, the following is required, you must be using the Microsoft password is the pin. (See Section Config Server Admin Guide). In addition the protected resource must be set to basic only authentication and have a default domain listed for the authentication. This will then allow a single sign on solution from a two-factor authentication to the application.

If this server doesn't have SSL (https) enabled it is recommended that a server certificate is added and SSL is enabled on this server, See Appendix A. If however you don't wish to add a server certificate and are willing to risk session cookies being intercepted as they are sent down a non-encrypted connection then you can check the box "Allow Non Secure Communications (http)"

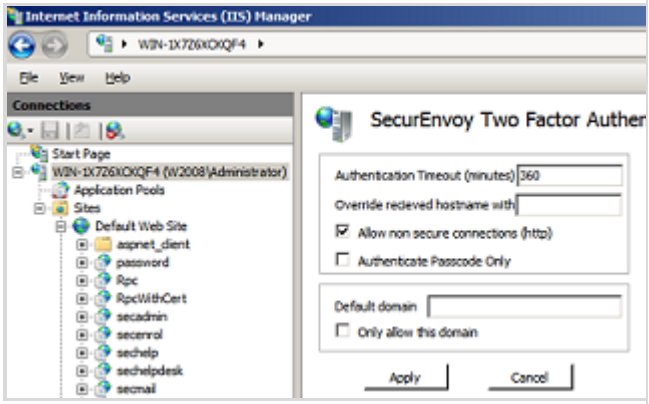
Authentication timeout is the number of minutes from the last successful authentication until the user is prompted for re-authentication. It is recommended that this is set long enough to allow a typical user to complete their session.

To change the global parameters for the IIS the Agent carry out the following:-

For Windows 2008 deployments

Select Start\Administrative tools\Internet Information Services (IIS) Manager

Select the physical machine, and then double click the SecurEnvoy Icon, the following screen will appear.



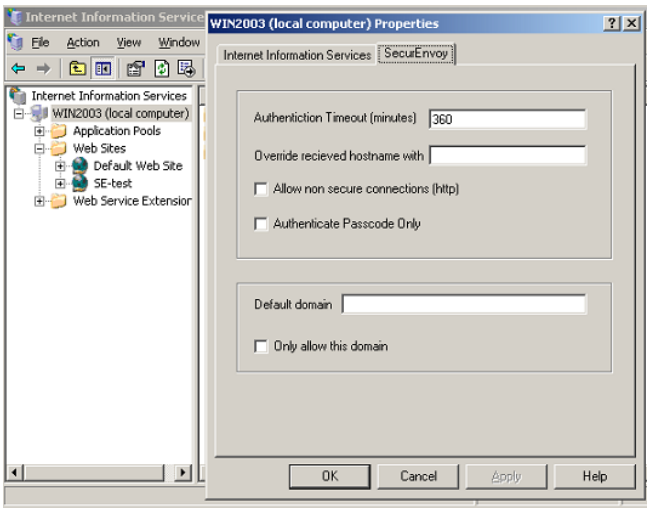
The following parameters can be changed:

Authentication timeout in minutes
Override Hostname information
Allow http connectivity
Authenticate passcode only, if an existing application is authenticating the password.
Default Domain and only allow this Domain switch.

For Windows 2003 deployments

Select Start\Programs**SecurEnvoy**\IISConfig MMC.

Select the physical machine, and right click and then select properties, the following screen will appear.



Select the **SecurEnvoy** Tab

The following parameters can be changed:

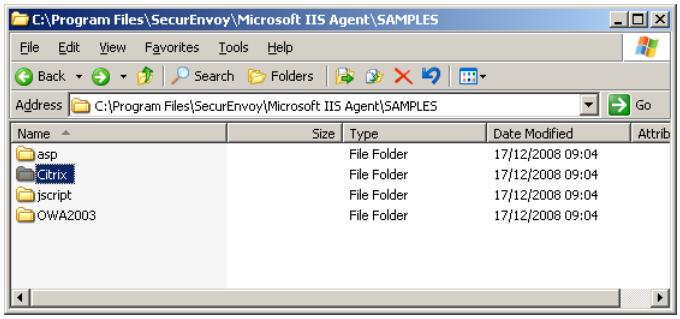
Authentication timeout in minutes
Override Hostname information
Allow http connectivity
Authenticate passcode only, if an existing application is authenticating the password.
Default Domain and only allow this Domain switch.

3.0 Single Sign on

Any application that utilises IIS basic authentication (Not Integrated Windows authentication), user's will be automatically signed into the application after a 2FA with either Basic or Form based authentication enabled.

To facilitate a simple sign on solution, SecurEnvoy has included a number of pre configured templates for the majority of mainstream applications.

Navigate to Program Files\SecurEnvoy\Microsoft IIS Agent\Samples directory, there will be a number pre configured applications.



Select the one that is correct for your environment.

Select the correct application and then copy the passcodeok.htm file to:

C:\Program Files\SecurEnvoy\Microsoft IIS Agent\WEBAUTHTEMPLATE

Overwrite the original file.

Note

It is recommended to either rename or backup the original Passcodeok.htm file prior to this process.

Note

For SSO with form based logon. If no available passcodeok.htm file exists in samples directory for your specific application. Simply create a new passcodeok.htm file and map the form elements required for authenticating. See existing sample passcodeok.htm files for reference.

You should use the same Form Action login page defined in your form element. Define hidden input entries fields that match your application logon requirements, substituting $USERID$ and $PASSWORD$ for username and password values.

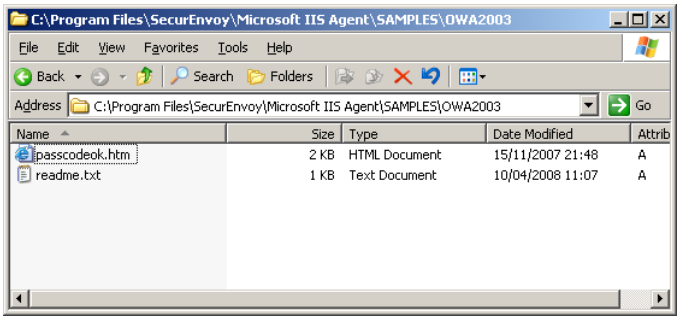
Example

To configure a Two Factor authentication for Exchange Web mail upon Microsoft Exchange 2003 server.

Install SecurEnvoy Microsoft IIS Agent upon the Exchange 2003 Front end server.

1. Click – start – programs – SecurEnvoy – IIS Config MMMC
2. Expand MMC tree to show default web site
3. Right mouse click default web site, select properties, select the SecurEnvoy tab, click “Enable SecurAccess authentication upon this server”, click OK
4. Click restart WWW
5. Navigate to Exchange virtual directory, right mouse click and select SecurEnvoy tab, check enable authentication, check Forms based authentication, click OK
6. Click restart WWW

Navigate to Program Files\SecurEnvoy\Microsoft IIS Agent\Samples\OWA2003



Copy the passcodeok.htm file to:
C:\Program Files\SecurEnvoy\Microsoft IIS Agent\WEBAUTHTEMPLATE

Overwrite the original file.

Note

It is recommended to either rename or backup the original Passcodeok.htm file prior to this process.

Carry out a test authentication by going to https://*servernamel*exchange
Enter UserID, windows password and passcode

4.0 IIS Agent Advanced Administration

The seiis.ini file is located in WINDOWS and is the main control file for the IIS agent and contains the following settings:-

Version	This is set by the installer and defines the current version
Webauth_Debug	Can be set to True or False If set to True, creates debug information from the webauth.exe program and writes it to c:\DEBUG\webauth.txt. Default=False
Webauthfilter_Debug	Can be set to True or False If set to True, creates debug information from the webauthfilter ISAPI plugin and writes it to c:\DEBUG\webauthfilter.txt Default=False
MMC_Debug	Can be set to True or False If set to True, creates debug information from the MMC snapin and writes it to c:\DEBUG\iismmc.txt. Default=False
WebTemplateDir	Set by the Installer, this is the location were the IIS Agent authentication templates are stored
WebauthPath	Set by the Installer, this is the full path to the webauth.exe program
Passpin	# Pass Pin in a Cookie called TMPPIN, set to False or True, default = False
IsapiFilterLocation	Set by the Installer, this is the full path to the webauthfilter.exe program
iis7 admin path	Set by the Installer, this is the full path to the IIS 7 admin program
SecurityServer1	Set by the Installer, This is the Host Name of the first Security Server
SecurityServer2	Set by the Installer, This is the Host Name of the second Security Server or it should be set to “None” if only one security server is required
ServerTimeout	The timeout in seconds the agent waits before trying the next security server. Default is 25
ServerRetry	The number of retries the agents uses when trying ton connect to the security server. Default is 0
Securectrl_URI	This is the URI of the security server’s main secserver resource. Default is =/secserver/securectrl.exe
Allow_http	Set by the MMC administration program. Can be set to True or False. If set to False allows unsecured web connections (http) and doesn’t require SSL connections or a server side certificate. Default=False
RedirectHttp	If Allow_http=False and RedirectHttp=True then http requests will be redirected to https

Cookie Timeout	Set by the MMC administration program. This is the time in minutes a user's web browser can continue to browse a protected resource before being re-authenticated. Default is 30
HTTP_HOST	Override host received in URL.
DefaultDomain	Default domain to use if no domain name is included in the user authentication request
OnlyAllowThisDomain	UserID that contain domain names that are not the default domain will be denied.
URL	Set by the MMC administration program. One or more URI's of a protected web resource /F dictates forms based /B dictates HTTP basic auth