SecurEnvoy IIS Web Agent

Version 7.2
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 is a pre-requisite and as such, must be installed before other SecurEnvoy applications will function.
SecurEnvoy IIS Agent Installation and Admin Guide v7.2

© 2014 SecurEnvoy

Publisher
SecurEnvoy Publishing

Managing Editor
SecurEnvoy Training Dept

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

Cover Designer
SecurEnvoy Marketing

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.9 AK</td>
<td>05/3/2012</td>
</tr>
<tr>
<td>V2.0 SM</td>
<td>13/5/2013</td>
</tr>
<tr>
<td>V2.1 TD</td>
<td>16/1/2014</td>
</tr>
</tbody>
</table>

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.

Foreword

SecurEnvoy is the trusted global leader of tokenless two-factor authentication. As the pioneers of mobile phone based tokenless authentication; SecurEnvoy leads the way with ground-breaking solutions that others aspire to.

Our innovative approach to the tokenless market demonstrates that thousands of users are benefitting from our solutions all over the world.

With users deployed across five continents, our customers benefit from a significantly reduced time to deploy and a zero footprint approach means there is no remote software deployment and administrators enjoy our comprehensive management tools allowing them to rapidly deploy up to 100,000 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 hardware token manufacturing, distribution and maintenance costs as users can make use of existing mobile phone or Email technology the return on investment (ROI) is so much more acceptable to businesses and organizations. A zero carbon footprint is also very beneficial for environmentally responsible purchasers. We are truly 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 established 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. Over a decade has passed since our initial incorporation and we are very proud of our happy customer base across the five continents and with regional support for them.

Business levels have more than doubled year on year due to our subscription sales model that 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 Microsoft IIS Agent Install & Configuration ............................................. 6
  2.1 Agent Architecture................................................................................... 6
  2.2 Installing the Microsoft IIS Agent ........................................................... 7
  2.3 Upgrading Microsoft IIS Agent ............................................................... 8
  2.4 Microsoft IIS Agent Administration ......................................................... 10

3.0 Single Sign on.................................................................................................. 14

4.0 IIS Agent Advanced Administration .......................................................... 16

5.0 IIS Agent Application Pools ........................................................................ 18

6.0 Supporting Previous versions of Microsoft IIS Agent ............................... 20
  6.1 Microsoft IIS Agent Administration Pre v5.4 ............................................ 21

7.0 Notes ............................................................................................................ 25

Note

*If you are running version 6.1 or earlier it is strongly recommended you upgrade as this agent has enhanced security*
1.0 Overview of Installation Files

Microsoft 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

IIS Pre-Requisites

Supported IIS Versions:

- IIS V6 running on Windows 2003 - all service packs (x32 and x64 bit).
- IIS V6.2 running on Windows 2008 SP1-2 (x32 and x64 bit) and R2.
- IIS V7 running on Windows 2008 SP1-2 (x32 and x64 bit) and R2.
- IIS V8 running on Windows 2012 and R2.

It is highly recommended that any protected web server should have SSL (https) enabled. Microsoft .NET 2.0 is installed.

2.0 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 Microsoft IIS Agent

Pre-Requisites: IIS must be installed and running on one of the following:
- Windows 2003
- Windows 2008 & R2
- Windows 2012 & R2

**SecurEnvoy Security Server Version 5.4 or higher is required for this version of Microsoft IIS Agent.**

Microsoft Dot Net v2.0 installed.

There must be a network connection via RADIUS (UDP Port 1812 -default) between the IIS server and the security server(s).

**Note**

*A RADIUS profile must be created upon each authenticating SecurEnvoy Security Server. See Security Server Administration Guide for further details.*

To install the Microsoft 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 have a RADIUS profile created upon each.)

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

The “Test Server” button allows a RADIUS communication test to see if the Security server is reachable.

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

Response codes are shown below:

- OK
  - All settings are correct

- Error, Shared Secret Does Not Match the Server
  - Shared secret mismatch

- Error, Connection Timed Out
  - IP address or Port issue

This completes the Microsoft IIS Agent installation.
2.3 Upgrading Microsoft IIS Agent

**Note**

*If you are running version 6.1 or earlier it is strongly recommended you upgrade as this agent has enhanced security*

If you are upgrading from version 5.3 or earlier the agent communications protocol has changed from http (port 80 TCP) to RADIUS (port 1812 UDP). Make sure any firewalls between the IIS Agent and the Security server allow the radius ports 1812 UDP. Next setup the IP address of this agent in the security server’s radius settings (when upgrading you will be prompted for the security server’s radius settings).

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

Backup the seiis.ini file resides under C:\windows\.

If you have changed the login web templates then backup the WEBAUTHTEMPLATE directory under Microsoft IIS Agent

Install the new Microsoft IIS Agent over the existing install by running setup.exe

**Note**

*Upgrading will automatically preserve your current settings and any custom login templates*

**Note**

*Do NOT un-install the existing IIS Agent or you will lose your configuration settings*
2.4 Microsoft IIS Agent Administration

Administration is performed on Windows 2003 via Microsoft’s Management Console (MMC) or for Windows 2008 / Windows 2012 via Information Services (IIS) Manager.

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

**For Windows 2008 & Windows 2012 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. Enable the Microsoft 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 Microsoft IIS Agent by checking the box “Enable Microsoft 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”.

![Internet Information Services (IIS) Manager](image)

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.

![SecurEnvoy Configuration](image)

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 & Windows 2012 deployments**

Check the "Enable Authentication" box to enable authentication on this resource and contents within.

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 HTTP Basic Authentication then Microsoft LDAP password must be used as the pin. See Config Section of Security Server Admin Guide for further details. 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. In addition, “Passcode prompt is on a separate dialog (requires Access Challenge) must be disabled from within the Radius tab for Basic HTTP Authentication to work correctly.*

---

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 & Windows 2012 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, select from inactivity timeout or timeout after authentication
- Override Hostname information
- Allow http connectivity
- Trusted Networks, networks and single machines that are trusted and do not require a 2FA can be entered here.
- Logoff URL’s, existing application logoff URL’s can be entered and these will then be called when the browser is closed or user logoff's.

**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, select either inactivity timeout or timeout after authentication
- Override Hostname information
- Allow http connectivity
- Trusted Networks, networks and single machines that are trusted and do not require a 2FA can be entered here.
- Logoff URL’s, existing application logoff URL’s can be entered and these will then be called when the browser is closed or user logoff's.

Domain and passcode parameters are controlled within the RADIUS profile upon the SecurEnvoy Security Server.
3.0 Single Sign on

Any application that makes use of IIS basic authentication (Not Integrated Windows authentication), users will be automatically signed into the application after a 2FA with either HTTP 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 entry 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 Microsoft IIS Agent upon the Exchange 2003 Front end server.

1. Click – start – programs – SecurEnvoy – IIS Config MMC
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://servername/exchange
Enter UserID, windows password and passcode
4.0 IIS Agent Advanced Administration

The seiis.ini file is located in c:\WINDOWS\ and is the main control file for the IIS Agent and contains the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>This is set by the installer and defines the current version</td>
</tr>
<tr>
<td>Webauth_Debug</td>
<td>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</td>
</tr>
<tr>
<td>Webauthfilter_Debug</td>
<td>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</td>
</tr>
<tr>
<td>MMC_Debug</td>
<td>Can be set to True or False. If set to True, creates debug information from the MMC snapin and writes it to c:\DEBUG\ismmc.txt. Default=False</td>
</tr>
<tr>
<td>WebTemplateDir</td>
<td>Set by the Installer, this is the location where the IIS Agent authentication templates are stored.</td>
</tr>
<tr>
<td>WebauthPath</td>
<td>Set by the Installer, this is the full path to the webauth.exe program.</td>
</tr>
<tr>
<td>Passpin</td>
<td># Pass Pin in a Cookie called TMPPIN, set to False or True, default = False</td>
</tr>
<tr>
<td>IsapiFilterLocation</td>
<td>Set by the Installer, this is the full path to the webauthfilter.exe program.</td>
</tr>
<tr>
<td>iis7 admin path</td>
<td>Set by the Installer, this is the full path to the IIS 7 admin program.</td>
</tr>
<tr>
<td>SecurityServer1</td>
<td>Set by the Installer, this is the Host Name of the first Security Server.</td>
</tr>
<tr>
<td>SecurityServer2</td>
<td>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.</td>
</tr>
<tr>
<td>ServerTimeout</td>
<td>The timeout in seconds the agent waits before trying the next security server. Default is 25</td>
</tr>
<tr>
<td>ServerRetry</td>
<td>The number of retries the agent uses when trying to connect to the security server. Default is 0</td>
</tr>
<tr>
<td>Securectrl_URI</td>
<td>This is the URI of the security server’s main secserver resource. Default is =/secserver/securectrl.exe</td>
</tr>
<tr>
<td>Allow_http</td>
<td>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</td>
</tr>
<tr>
<td>RedirectHttp</td>
<td>If Allow_http=False and RedirectHttp=True then http requests will be redirected to https</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cookie Timeout</td>
<td>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 360.</td>
</tr>
<tr>
<td>UseInactivity</td>
<td>Timeout is based on inactivity (True) or a fixed time after last authentication (False).</td>
</tr>
<tr>
<td>HTTP_HOST</td>
<td>Override host received in URL.</td>
</tr>
<tr>
<td>SSOAuth</td>
<td># Single sign on authentication. Accepted values are none, basic (default), auto (negotiation SSO for both Basic and Integrated Windows Login).</td>
</tr>
<tr>
<td>TrustedClient</td>
<td>Trusted networks to bypass authentication format. TrustedClient=ipaddress or subnet*</td>
</tr>
<tr>
<td>URL</td>
<td>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.</td>
</tr>
</tbody>
</table>
5.0 IIS Agent Application Pools

To allow successful use of the Microsoft IIS Agent, the web site or virtual directory (application) that requires protecting uses the correct “Application pool”.

For Windows 2008 & Windows 2012

Within Internet Information Services (IIS Manager) navigate to the Application pools, by default SecurEnvoy will be within the Default App pool. Make sure the virtual directory is using the same application pool as the SecurEnvoyAuth.

To view the virtual directory application pool, navigate to the required virtual directory and then select “Basic Settings” on the “Action pane” which is located on the right hand side of the IIS Manager window.

The Application pool identity will then be shown, if required the application pool can be changed.
For Windows 2003

Within Internet Information Services (IIS Manager) navigate to the Application pools, by default SecurEnvoy will be within the Default App pool. Make sure the virtual directory is using the same application pool as the SecurEnvoyAuth.

Depending upon deployment the SecurEnvoyAuth may reside in a different application pool. See below: In this example the SecurEnvoyAuth resides within the SecurEnvoy Application pool.

To protect a virtual directory (application), this virtual directory must use the same application pool as SecurEnvoy.

Navigate to the virtual directory then select properties.

In the Application Pool drop down menu, select the pool SecurEnvoy.

Click OK when complete.
6.0 Supporting previous versions of Microsoft IIS Agent

SecurEnvoy IIS agents that are already deployed and do not require upgrading to v7.1 and will continue to work.
6.1 Microsoft IIS Agent Administration Pre v5.4

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. 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 protect. Select the virtual directory, you will then see a SecurEnvoy Icon displayed in the “Features View window – Other”.

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.
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.

![SecurEnvoy Two Factor Authentication](image)

The following parameters can be changed:

- Authentication timeout in minutes, select either inactivity timeout or timeout after authentication.
- 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.
- Logoff URL’s, existing application logoff URL’s can be entered and these will then be called when the browser is closed or user logoff’s.

**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.

![SecurEnvoy Two Factor Authentication](image)

Select the SecurEnvoy Tab

The following parameters can be changed:

- Authentication timeout in minutes, select either inactivity timeout or timeout after authentication.
- 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.
- Logoff URL’s, existing application logoff URL’s can be entered and these will then be called when the browser is closed or user logoff’s.
7.0 Notes