SecurEnvoy PC Soft Token

Version 7.3

SecurEnvoy Global HQ
Merlin House, Brunel Road, Theale, Reading. RG7 4TY
Tel: 0845 2600010 Fax: 0845 260014 **www.SecurEnvoy.com**

SecurEnvoy PC Soft Token

Installation and Admin Guide v7.3

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 One Directory Server and Linux Open LDAP Directory Server) for access to user information. SecurEnvoy Security Server controls and manages the authentication and sending of SMS passcodes and Emails. This must be installed for SecurAccess, SecurICE, SecurPassword and SecurMail.

SecurEnvoy PC Soft Token

Installation and Admin Guide v7.3

Printed: 2014 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	
V1.0 PU	21/03/2012
V1.1 PU	20/4/2012
V1.2 SM	8/05/2013
V1.3 TD	17/1/2014

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

This agent is required if you are installing SecurAccess and you require a soft token to be installed upon a personal computer (PC).

A setup and MSI file are included to cater for standalone and Group Policy installation. This agent utilises the HTTP(S) protocol to communicate from the SecurEnvoy PC Soft Token to the SecurEnvoy SecurAccess server.

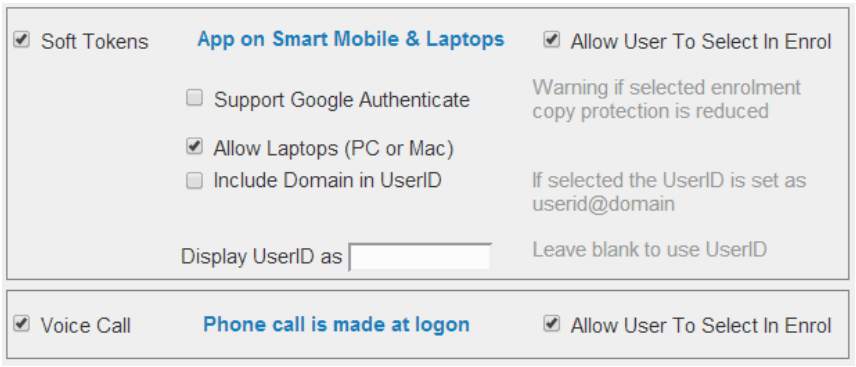
1.1 SecurEnvoy PC Soft Token

Supported Microsoft Versions:

Windows XP
Windows Vista
Windows 7
Windows 8
Windows 2003 server
Windows 2008 (R2) server
Windows 2012 (R2) server

2.0 SecurEnvoy PC Soft Token Install & Configuration

To facilitate the use of PC Soft tokens, please make sure that this setting is enabled in the SecurEnvoy Administration GUI: Navigate to Config – Token Types. Select Allow Laptops (PC or Mac).



2.1 Agent Functionality

The SecurEnvoy PC Soft Token allows users to generate a One Time Passcode (OTP) directly upon their personal computer. The passcode is valid for 30 seconds, then a new passcode is generated and displayed for the next 30 seconds and so on.

The SecurEnvoy PC Soft Token has the following functionality:

1. All users are first enabled and deployed, the user can then enrol directly with the SecurEnvoy PC Soft Token and have the seed (Token algorithm) deployed directly to the PC Soft Token. This will be with the HTTP protocol; both HTTP and HTTPS are supported.

2. Users have the ability to add multiple PC Soft Tokens, so can have one for a Portal logon and one for a corporate VPN logon. Users can also re-enrol to obtain a new seed if required.

3. The PC Soft Token resides within the PC Systray, mouse clicking upon the SecurEnvoy icon can invoke this and also a right mouse click will allow more menu options.

4. The PC Soft Token can be installed either as a single standalone installation or via a Microsoft Group Policy installation. A sesofttoken.ini file allows configuration parameters to be detailed so there is no user interaction at time of installation.

2.2 Installing and Configuring the PC Soft Token (Standalone installation)

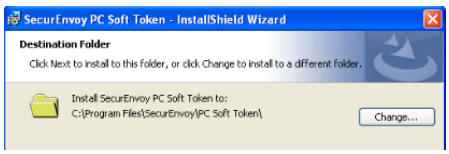
For Windows Vista, 7, Server 2008 & Server 2012 deployments

Pre-requisites:

Http(s) connectivity must exist from each PC or server and the SecurEnvoy Security server for enrolment.

To install the SecurEnvoy PC Soft Token run "PC Soft Token\setup.exe"

Click "Next" to continue.
The following page is displayed.



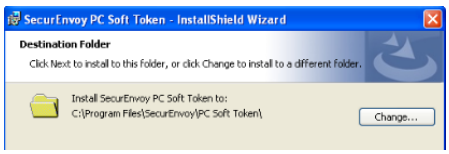
For Windows XP and Server 2003 deployments

Pre-requisites:

Http(s) connectivity must exist from each PC or server and the SecurEnvoy Security server for enrolment.

To install the SecurEnvoy PC Soft Token run "PC Soft Token\setup.exe"

Click "Next" to continue.
The following page is displayed.



After the Installation is complete, you can directly edit the sesofttoken.ini file, which resides in the c:\windows directory, the output is shown below:

[Settings]
Full URL to SecurEnvoy server /secenrol
E.G. https://example.com/secenrol
EnrolURL=

# Allow HTTP connection to SecurEnvoy server
AllowHTTP=False

Language resources

Enrolment authentication prompts

Strings: This allows configuration and customisation of all user prompts.

StrUsername=Username
StrPassword=Password
StrPasscode=Passcode

Note

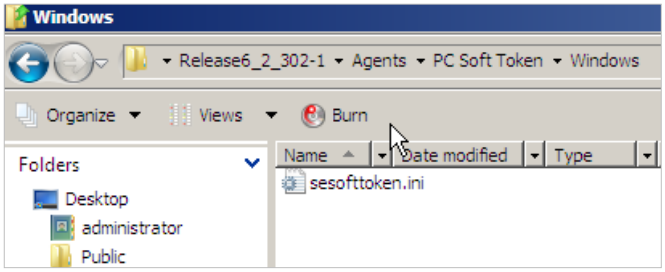
The enrolment page can be set for the SecurEnvoy Security server, SecurEnvoy recommend that HTTPS be used. E.g. https://machine_name/secnrol
However HTTP is supported if the network is trusted, but the "AllowHTTP" setting must then be set to "True" in both "setoken.ini" on the PC and "local.ini" on the SecurEnvoy Server.

2.3 Installing and Configuring the PC Soft Token (Group Policy Install)

This is a Microsoft configuration of Active Directory; please see the following web link for full information. http://support.microsoft.com/kb/816102

Prior to completing the Group Policy install, it is required that a standalone installation is completed; this will allow all configurations settings to be saved into the sesofttoken.ini file, which then can be copied to the PC Soft Token – Windows folder of the agents directory.

On the test installation PC, install the SecurEnvoy PC Soft Token as described in section 2.2, once completed the configuration settings can be copied.



Navigate to:

C:\Windows\sesofttoken.ini file

Copy this file to the MSI package and replace the sesofttoken.ini file that exists under:

MSI Package\PC Soft Token\Windows

The MSI Package is now ready for a Group Policy Install.

Note

It is recommended that the SecurEnvoy PC Soft Token should be applied on a per computer basis.

Windows 2003 Server

Create a Distribution Point

To publish or assign a computer program, you must create a distribution point on the publishing server: Log on to the server computer as an administrator.

1. Create a shared network folder where you will put a copy of all the agent's MSI install files including the .msi file and all other associated files and directories.
2. Set permissions on the share to allow access to the distribution package.
3. Copy or install the package to the distribution point. (Make sure all agent files are available)

Create a Group Policy Object

To create a Group Policy object (GPO) to use to distribute the software package:

1. Start the Active Directory Users and Computers snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click the **Group Policy** tab, and then click **New**.
4. Type a name for this new policy (for example, **Office XP distribution**), and then press ENTER.
5. Click **Properties**, and then click the **Security** tab.
6. Click to clear the **Apply Group Policy** check box for the security groups that you want to prevent from having this policy applied.
7. Click to select the **Apply Group Policy** check box for the groups that you want this policy to apply to.
8. When you are finished, click **OK**.

To Assign a Package

To assign a program to computers that are running Windows Server 2003, Windows 2000, or Microsoft Windows XP Professional, or to users who are logging on to one of these workstations:

1. Start the Active Directory Users and Computers snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, right-click your domain, and then click **Properties**.
3. Click the **Group Policy** tab, select the group policy object that you want, and then click **Edit**.
4. Under **Computer Configuration**, expand **Software Settings**.

5. Right-click **Software installation**, point to **New**, and then click **Package**.

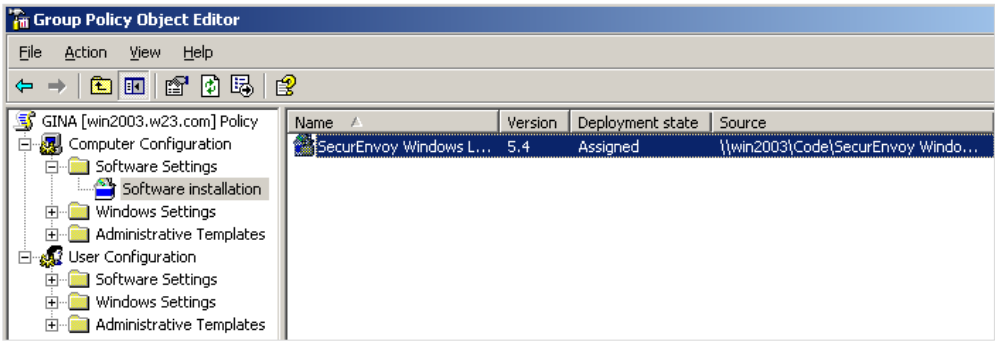
6. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, *file server**share**file name*.msi.
   Important do not use the Browse button to access the location. Make sure that you use the UNC path to the shared installer package. (Make sure all agent files are available)

7. Click **Open**.

8. Click **Assigned**, and then click **OK**. The package is listed in the right pane of the **Group Policy** window.

9. Close the **Group Policy** snap-in, click **OK**, and then quit the Active Directory Users and Computers snap-in.

10. When the client computer starts, the managed software package is automatically installed.



Windows 2008 Server

Create a Distribution Point

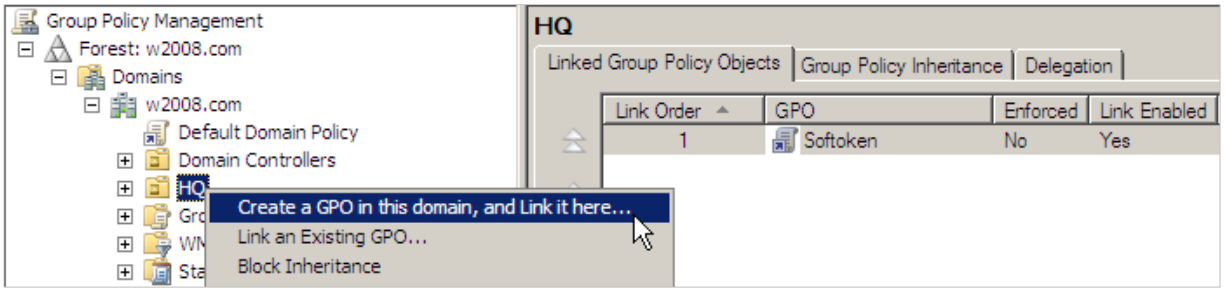
To publish or assign a computer program, you must create a distribution point on the publishing server: Log on to the server computer as an administrator.

1. Create a shared network folder where you will put a copy of all the agent's MSI install files including the .msi file and all other associated files and directories.
2. Set permissions on the share to allow access to the distribution package.
3. Copy or install the package to the distribution point. (Make sure all agent files are available)

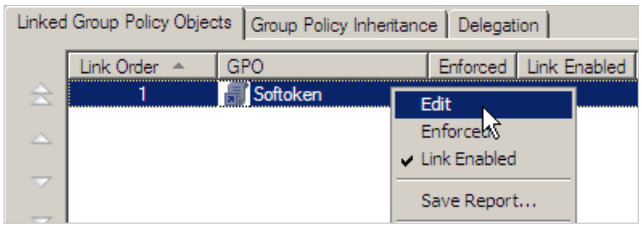
Create a Group Policy Object

To create a Group Policy object (GPO) to use to distribute the software package:

1. Start the Group Policy Management snap-in. To do this, click **Start**, point to **Administrative Tools**, and then click **Group Policy Management**.
2. In the console tree, select where you want the GPO applied. Right-click and select **"Create a GPO in this domain, and link it here**".

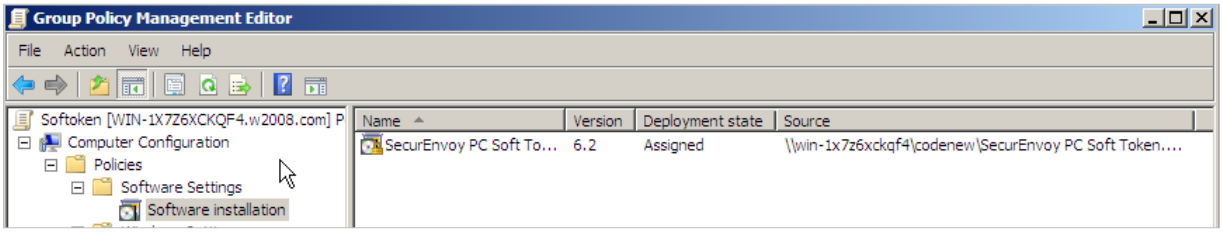


3. In the **Linked Group Policy Objects** tab, right mouse click and select **Edit**.



4. Under **Computer Configuration**, expand **Software Settings**.
5. Right-click **Software installation**, point to **New**, and then click **Package**.
6. In the **Open** dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, *file server**share**file name*.msi.
   Important do not use the Browse button to access the location. Make sure that you use the UNC path to the shared installer package. (Make sure all agent files are available)
7. Click **Open**.

8. Click **Assigned**, and then click **OK**. The package is listed in the right pane of the **Group Policy** window.

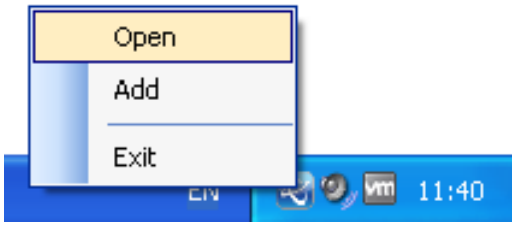


9. Close the **Group Policy** snap-in, click **OK**, and then quit the Active Directory Users and Computers snap-in.

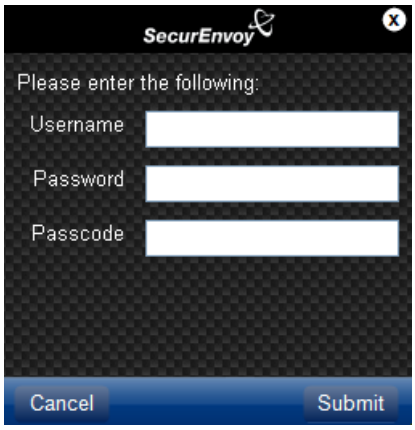
10. When the client computer starts, the managed software package is automatically installed.

3.0 User Experience

The SecurEnvoy PC Soft Token can be accessed from the "Systray", by either just mouse clicking upon the icon or using a right mouse click and selecting "Open".



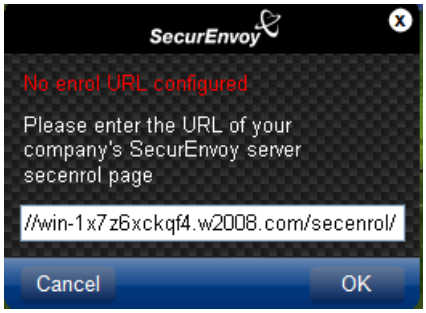
The user can then select "Add", the following screen will appear:



The user can then enrol to the SecurEnvoy Security Server to allow the "seed" record to be automatically downloaded to the PC Soft Token.

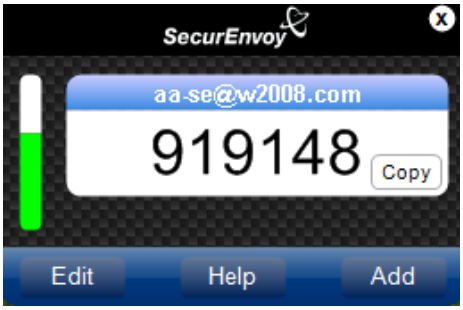
The user will authenticate with their existing Microsoft Active Directory UserID and domain password, plus the passcode that was sent to the user either by SMS or Email.

Click Submit to complete the enrolment process.



If the user sees the following screen, it will occur due to the sesofttoken.ini file not having a SecurEnvoy Security Server declared.

In this case, the user will have to enter the correct URL and then click "OK".



Once the enrolment process is complete, all the user has to do, is to open the PC Soft Token by either clicking upon the SecurEnvoy icon in the "Systray" or by right mouse click upon the icon and selecting "Open".

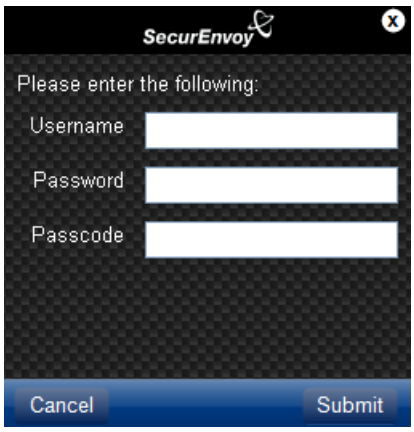
The user will then see the following screen. To help with a logon process, the user can copy the "Live" displayed code.

Edit – Gives the user the ability to rename or delete the token.

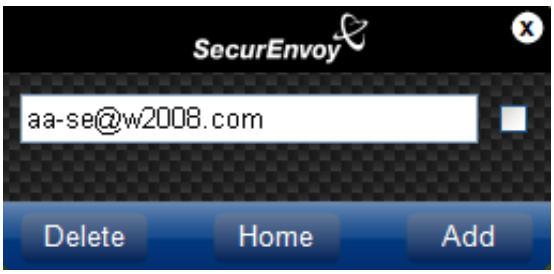
Help – "*Getting Started*" Directs user to online help pages.
– "*Manage Your Token Type*" Directs user to Manage My Token – enrolment webpage, if the URL has been setup in sesofttoken.ini.
– "*About*" Displays the application version information.

Add – Allows the user to add the user login and passcode information, so as to activate the PC Soft Token.

3.1 User Configuration



After the PC Soft Token has been launched, the user can then ad additional "PC Soft Tokens" selecting the "add" button.



The user can also select "Edit" from the relevant soft token.
The following tasks can be selected:

Delete	This will delete the selected Pc Soft Token.
Home	This will revert to the home screen and show the PC Soft Token displaying a passcode(s).
Add	This will enable the PC Soft Token to enrol for a new Soft Token.

3.2 Secret Question Enrolment

If the user has been activated for SecurPassword with secret questions or for Helpdesk, the user will be prompted to complete 2 secret questions which will be encrypted and saved to LDAP. The user when enrolling for SoftToken, will see the following prompts appear in the PC SoftToken App

Appendix Common Questions and Answers

Q: Does SecurEnvoy allow the Client to run in a multi-user environment, like "Microsoft Terminal Services Application" and "Citrix"?
A: Yes, SecurEnvoy support terminal service environments.

Q: How is proxy communications supported if the soft token needs to communicate with a SecurEnvoy server hosted in the cloud on the Internet?
A: The SecurEnvoy soft token automatically uses the local browser's proxy settings.

Q: Does the user need access rights to write to %SystemRoot% (normally c:\windows) and %ProgramFiles%?
A: No, normal users should not change any of the files located in windows or Program Files, all user specific settings are stored in the registry (a more secure place than %APPDATA%) .

Q: Is it possible to rollout the solution via MSI to install in silent mode and with a Transform file (*.MST) to define all specific corporate settings like Install Destination Folder, Full URL to SecurEnvoy server, Proxy Settings, etc.?
A: Yes, most setting can be easy changed in the sesofttoken.ini file that is deliberately kept separate to the msi file to make customization easier. The included msi file then allows for installing in silent mode via Microsoft group policy, see section 2.3 for more details. A transform file for changing other installer setting such as the Destination Folder can be created if required via standard Microsoft tools such as Orca by editing the properties table of the supplied msi file.

Q: Does the user need to run with enabled UAC (User Account Control)?
A: Elevated permissions are only required at install time. A silent install via the group policy will run under administrator permission so users will not be prompted by UAC. After installation the SecurEnvoy PC soft token will run under normal user permissions with or without UAC enabled.