

SecurEnvoy Windows Logon Agent

Installation and Admin Guide v9.3
Including support for
SecurPassword

SecurEnvoy Windows Logon Agent Guide

Contents

1.1	OVERVIEW OF INSTALLATION FILES.....	3
	SECURENVOY WINDOWS LOGIN AGENT.....	3
1.2	SECURENVOY WINDOWS LOGIN AGENT INSTALL & CONFIGURATION.....	4
	AGENT FUNCTIONALITY.....	4
	INSTALLING AND CONFIGURING THE SECURENVOY WINDOWS LOGIN AGENT (STANDALONE INSTALLATION).....	5
	INSTALLING AND CONFIGURING THE SECURENVOY WINDOWS LOGIN AGENT (GROUP POLICY INSTALL).....	7
1.3	USER EXPERIENCE	9
1.4	USER CONFIGURATION.....	10
1.5	EMERGENCY ACCESS	10
1.6	SECURPASSWORD.....	11
1.7	RESET PASSWORD WITH EXISTING AD INFORMATION	12
1.8	USER EXPERIENCE - RESET PASSWORD WITH EXISTING AD INFORMATION.....	13
1.9	RESET PASSWORD WITH SECURENVOY SECRET QUESTIONS.....	14
1.10	USER EXPERIENCE - RESET PASSWORD WITH SECURENVOY SECRET QUESTIONS.....	15
1.11	OFFLINE SUPPORT (SOFT TOKEN).....	15
1.12	SECURENVOY SERVER USER CONFIGURATION	16
1.13	OFF-LINE USER EXPERIENCE.....	16

1.1 Overview of Installation Files

This agent is required if you are installing SecurAccess and it is required to directly authenticate upon a Windows PC or a Windows server. This agent is also required if you are using SecurPassword and requires a Self-Service Password Reset (SSPR) solution directly from a Windows PC or a Windows server. A setup and MSI file are included to cater for standalone and Group Policy installation.

This agent utilizes the HTTP(S) protocol to communicate from the SecurEnvoy Windows logon agent SecurEnvoy SecurAccess server.

SecurEnvoy Windows Login Agent

Note

For SecurAccess ONLY operation with the Windows Logon Agent (WLA), existing v6 WLA clients are supported, but this will not support the new VOICE token.

Note this agent is only required for SecurAccess and SecurPassword.

For SecurPassword via the WLA, this MUST be upgraded at the same time as the SecurEnvoy Security Server is upgraded to v7.

Supported Microsoft Versions: -

- Windows Vista, Windows 7, Windows 8 / 8.1 & Windows 10
- Windows 2008 server - all versions including R2 and Terminal Server configurations
- Windows 2012 server - all versions including R2 and Terminal Server configurations
- Windows 2016 server - all versions including Terminal Server configurations

Note

For SecurAccess ONLY operation with the Windows Logon Agent (WLA) can now support 2FA for a user's laptop working offline.

ONLY Soft Tokens are supported and allows users to 2FA whilst working in a disconnected state away from the company domain.

Supported Token Types

Token Type	Supported
SMS and Email Preload (Email client must be on another device)	✓
SMS and Email Realtime (Email client must be on another device)	✓
Voice Call	✓
Smartphone Soft Token App	✓
Smartphone App Online Push	✓
Smartphone App QR Code	✗
PC/MAC Soft Token App	✗
NFC	✗

1.2 SecurEnvoy Windows Login Agent Install & Configuration

Prior to installing the SecurEnvoy Windows Login Agent, it is essential that there is a network connection via https (or http if the network is trusted) between the Windows Login Agent and the security server.

Confirm this is true by browsing to the following:

`https://[my Security Server]/secserver`

example `https://www.abc.com/secserver`

You should get the following returned: "ERR, Unknown Flag"

Agent Functionality

All existing Microsoft logon capabilities are preserved; the SecurEnvoy agent provides a second factor of authentication via HTTP(S) using a 6-digit passcode sent to the end user.

The SecurEnvoy Windows login Agent has the following functionality:

1. All users are authenticated to the Microsoft Domain and SecurEnvoy, the Microsoft domain manages and authenticates the UserID and domain password and SecurEnvoy authenticates the UserID and 6 digit passcode. Only when access has been granted by both the Microsoft Domain and SecurEnvoy is the user allowed access to the Microsoft environment.
2. Authentication can be provided by way of Group membership, where only a designated Window group requires a 2FA logon. Thereby allowing other user groups to logon without 2FA. Group logic can be applied for users who are a member of a specific group or who are not a member of a specific group.
The two-factor authentication is used for initial logon, lock workstation and screen lock.
3. SecurEnvoy Windows Login Agent has the ability to allow an "Emergency Access account" which will allow logon with a UserID and password. This account must be either a Domain or local account upon the machine. This can be used when Server client communication has failed.
4. Users, who utilize a soft token for authentication, now have the ability to work offline and still use 2FA at time of logon. Users in this mode must use a soft token and authenticate once in a connected state so that the SEED record can be copied locally to the laptop.
5. SecurPassword allows the user to reset their domain password using Two Factor authentication, the user will supply the 6 digit passcode and answer security question(s).
6. New connections feature, where a connection port can be specified to be protected or unprotected from 2FA. This is useful, where you want to 2FA external users but exclude internal users.

Installing and Configuring the SecurEnvoy Windows Login Agent (Standalone installation)

Pre-requests:

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

To install the SecurEnvoy Windows Login Agent run "SecurEnvoy Windows Login Agent\setup.exe"

Click "Next" to continue.

The following page is displayed.

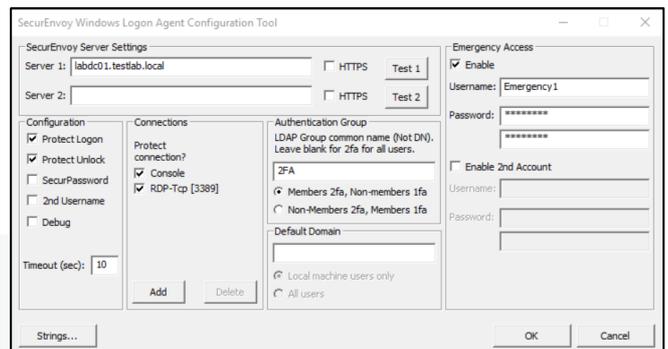
The configuration utility will run automatically. Populate details for:

Security server address and whether HTTPS is required.

Select options for configuration

These are:

- Protect logon
- Protect unlock



Authentication group:

Select group for which users should provide a 2FA to logon.

Debug, provides debug output to c:\debug\

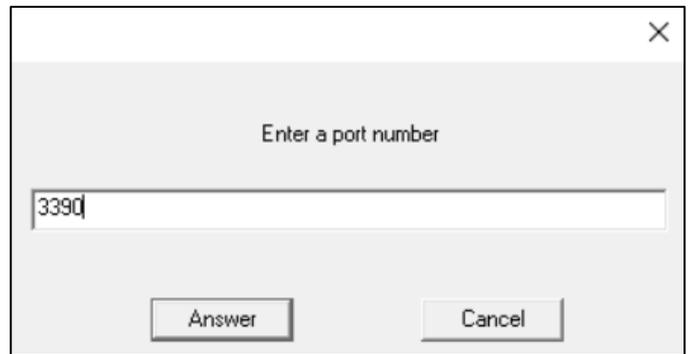
Emergency Access: set an account that can be used for when Server client communication has failed.

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

Connections: By default, the Windows Login agent protects both Console and the default RDP port. If you would like only external users to be authenticated with 2FA, a custom port can be specified.

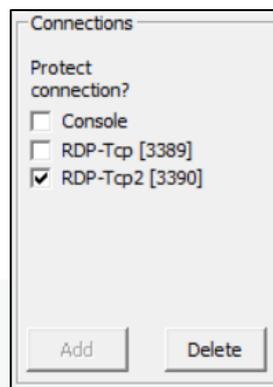
Click the "Add" button within the connections dialog.

Enter a port number that external users will be forced to use and click "Answer"



If you would like only external users to have 2FA,

Uncheck Console and 3389(default). This ensures only external users will be 2FA



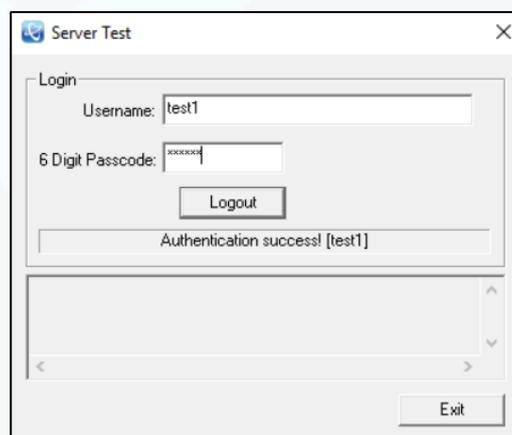
Note

Configure your firewall to use Network-Address-Translation (NAT) regarding all RDP requests on port 3390 from the external network. NAT should be configured to transfer all RDP requests from port 3389 to port 3390. This means that all external RDP requests will connect to the target machine using the new custom RDP Listener.

To check that all parameters are correct, click the "Test" button for each configured SecurEnvoy server, the following screen will be shown.

Enter the UserID and passcode and click "login".

Click "Exit" when finished testing



Click "Finish"

Click "Yes" to reboot



Installing and Configuring the SecurEnvoy Windows Login Agent (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 exported and saved to the MSI package.

On the test installation PC, install the SecurEnvoy Windows login Agent as described on Page 5, once completed the configuration settings can be exported.

Run Regedit and Navigate to:

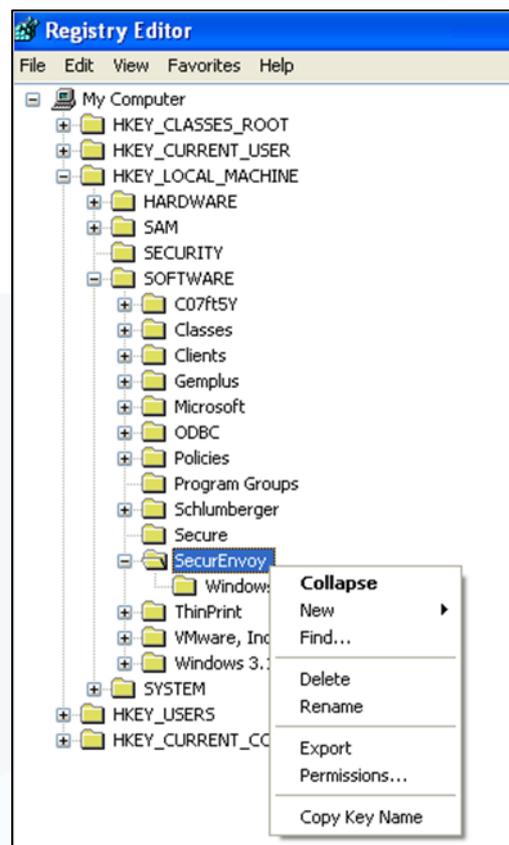
HKLM\software\SecurEnvoy

Right mouse click and select export, save the file as config.reg.

Copy this file to the MSI package and replace the config.reg file that exists under:

MSI Package\Program
Files\SecurEnvoy\Windows Login Agent

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



Note

It is recommended that the SecurEnvoy Windows login Agent should be applied on a computer basis.

Windows 2008 R2, 2012 R2 & 2016 Server

Create a Distribution Point

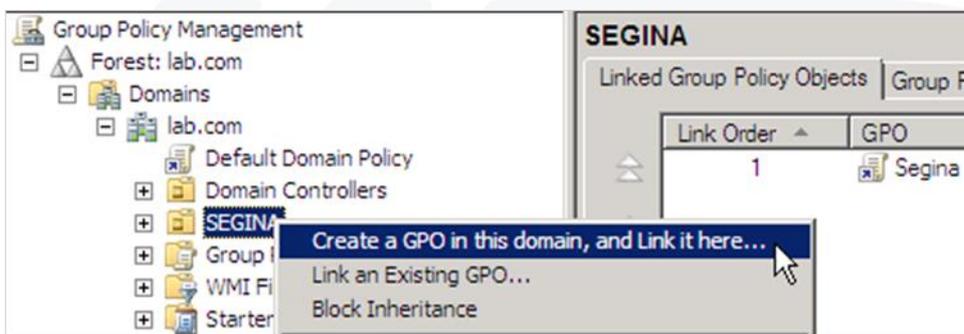
To publish or assign a computer program, you must create a distribution point on the publishing server:
 Log on to the server computer as an administrator.

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.

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.
7. Important, do not use the Browse button to access the location. Make sure that you use the UNC path to the shared installer package.
8. Click Open.
9. Click Assigned, and then click OK. The package is listed in the right pane of the Group Policy window.
10. Close the Group Policy snap-in, click OK, and then quit Active Directory Users and Computers snap-in.
11. When the client computer starts, the managed software package is automatically installed.

1.3 User Experience

User invokes CTRL ALT DEL to initiate the logon sequence

Windows Credential provider

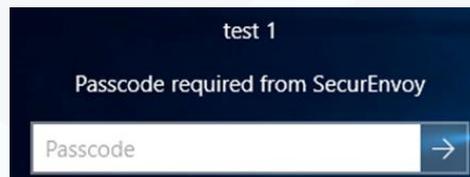
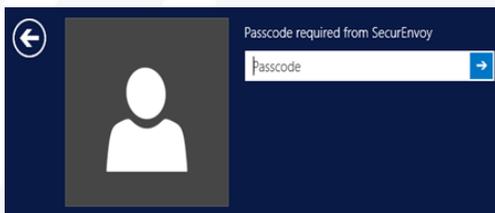


User enters UserID, domain password



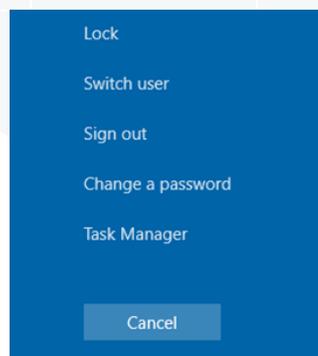
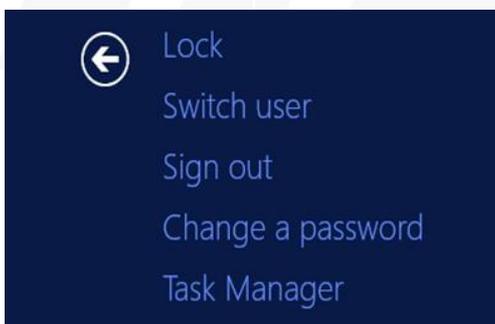
If the user is configured for 2FA the following screen prompt is shown, otherwise the user is granted access to the domain.

If using "Pre-Load" or "Daycode" mode the user enters the passcode from their mobile phone. If the user is in "Real-Time" delivery mode the passcode is sent at time of logon.



User has all the same Microsoft functionality.

Ability to:	Lock Computer	Log off	Shut Down
	Change Password	Task Manger	Cancel



1.4 User Configuration

User can access the SecurEnvoy Windows login Agent from the "Start All programs menu" or using Windows search:



The following programs can be searched/selected; this requires Administrative permissions to achieve these tasks.

- | | |
|---------|--|
| Config | This executes the Config utility program, all settings can be configured, these are described on Page 5. |
| Disable | This will disable the SecurEnvoy Windows Login Agent, a reboot is required to confirm change, user will now authenticate with a Microsoft login. |
| Enable | This will enable the SecurEnvoy Windows Login Agent, a reboot is required to confirm change, user will now authenticate with a SecurEnvoy 2FA login. |

1.5 Emergency Access

SecurEnvoy Windows Login Agent has the ability to allow an "Emergency Access account" which will allow logon with a UserID and password. This account must be either a Domain or local account upon the machine. This can be used when client/server communication has failed due to network, interface card or server issue.

The following screen shot will be displayed to indicate a timeout issue.

Access can then be gained by logging in with the emergency access account that was previously setup in section 1.4.



1.6 SecurPassword

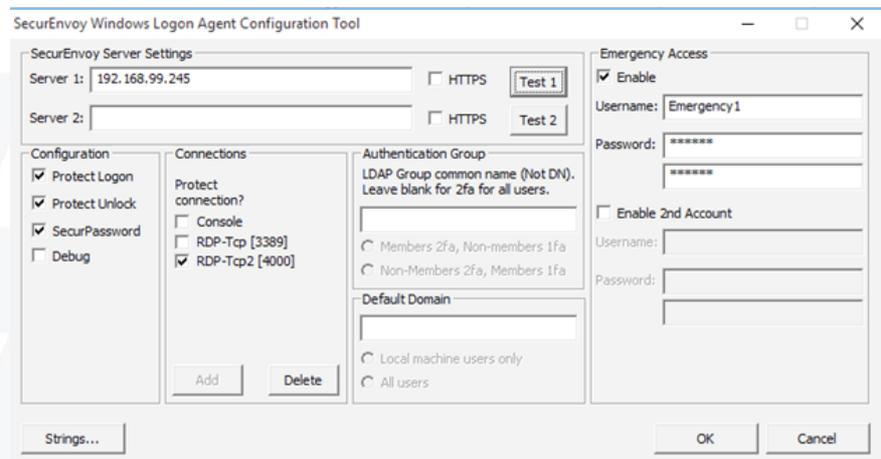
SecurPassword allows a user to reset their Microsoft Domain password using Two Factor Authentication. In addition to the passcode, up to three attributes of data can be used to help validate the authentication request for a password reset. Also, the user can use security questions that were answered within the enrolment process. Any data that is held within the Directory Server can provide further checks to the user's credentials. Attributes like employee number, department etc can provide additional authentications parameters.

To enable SecurPassword it must be first enabled upon the SecurEnvoy Security server, as such a valid license must be installed. Enable the Allow SecurPassword checkbox must be ticked. The only decision is to either use existing attributes to check for authentication, or use the security questions a user has enrolled with

User can be automatically sent a "Password expiry warning" via SMS, this feature will send out a SMS warning message at x days before their user password expires. (Default is 7 days). These settings are configured upon the SecurEnvoy Security server(s).

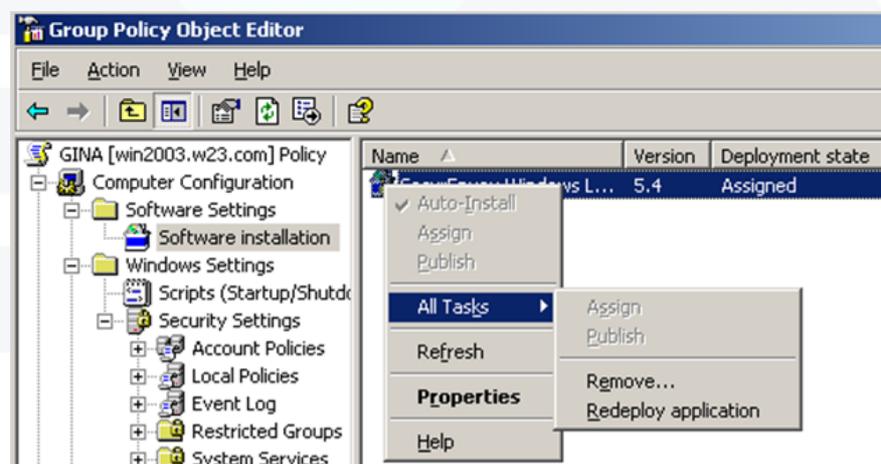
To enable the SecurEnvoy Windows Login Agent to support SecurPassword, run the configuration utility and tick the SecurPassword checkbox. Click OK when complete.

For standalone installations this will have to be completed for all machines that have the SecurEnvoy Windows Login Agent that require SecurPassword.



To enable the SecurEnvoy Windows Login Agent to support SecurPassword via a Group Policy install.

A new config.reg file must be created, once completed the package can be redeployed with the updated config.reg file.



1.7 Reset password with existing AD information

Domain password reset, using existing AD information. The system can be setup so that existing AD information can be used to reset the domain password. Within the SecurEnvoy Admin GUI select "config" and then go to the SecurPassword settings.

When "secret questions" is un-ticked it will prompt for exiting AD attributes and a prompt to be assigned. In addition, the user can be reminded by a SMS alert that their password is about to expire, the default alert time is 7 days.



SecurPassword - Microsoft and Other LDAP Self Help Password Management Domain:

Allow SecurPassword To Be Used

Password Expiry Warning Alert: Days Before

Use Secret Questions

Prompt: Attribute:

Prompt: Attribute:

Prompt: Attribute:

Password Maximum Age: Days

Password Minimum Length:

Password Must Include: Upper Lower Number Other

Update

Note

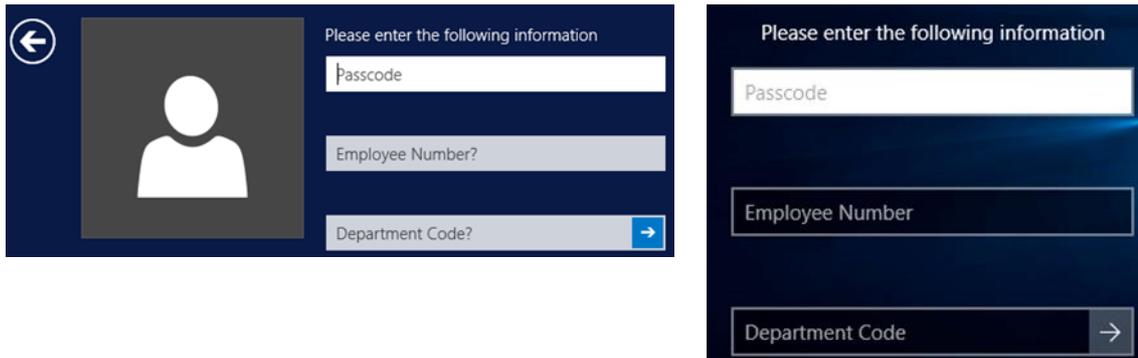
Up to three questions can be set up, although only two are shown in the admin GUI, the third question can be set up directly within the server.ini file.

The Windows password can be reset by the user selecting the "Reset" link on either the GINA or the Credential provider login.



1.8 User experience - Reset password with existing AD information

When the user selects the reset password link they will then be prompted to reply with answers as shown below:

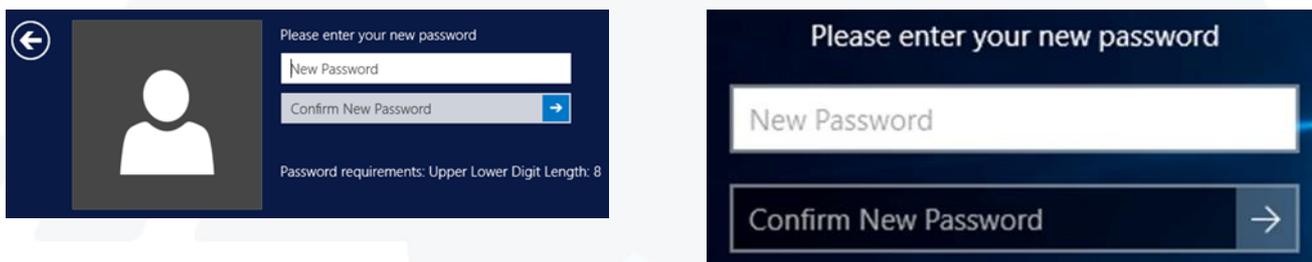


The first screenshot shows a dark blue dialog box with a back arrow in the top left. On the left is a white silhouette of a person. The text reads "Please enter the following information". There are three input fields: "Passcode", "Employee Number?", and "Department Code?". A blue arrow is on the right of the "Department Code?" field.

The second screenshot shows the same dialog box, but the input fields now contain the text "Passcode", "Employee Number", and "Department Code". A right-pointing arrow is on the right of the "Department Code" field.

If a Domain password policy is in force, the Gina or credential provider will display what components are required to make a good password.

When a user responds with the relevant component i.e. Upper-case letter or numeric, the requirements that have been met will then be grayed out.



The first screenshot shows a dark blue dialog box with a back arrow in the top left. On the left is a white silhouette of a person. The text reads "Please enter your new password". There are two input fields: "New Password" and "Confirm New Password". Below the fields is the text "Password requirements: Upper Lower Digit Length: 8".

The second screenshot shows the same dialog box, but the input fields now contain the text "New Password" and "Confirm New Password". The text "Password requirements: Upper Lower Digit Length: 8" is now grayed out.

Note

The Password complexity prompt within the GINA or credential provider requires that the LDAP base is set. This can be configured directly within the server.ini file.

1.9 Reset password with SecurEnvoy secret questions

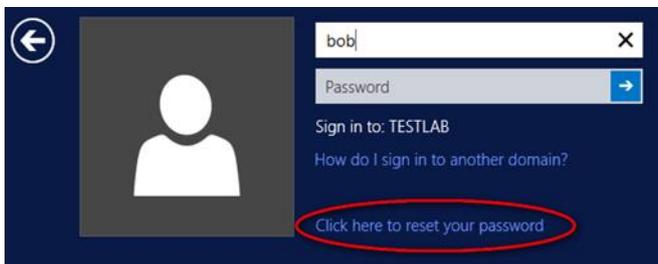
Domain password reset, using SecurEnvoy secret questions. The system can be setup so that the user enrolls at <https://securenvoy-server/secenrol> and selects two security questions existing and provides relevant answers.

Within the SecurEnvoy Admin GUI select "config" and then go to the SecurPassword settings box.

When "secret questions" is ticked the user will respond with a security questions answer. Only one security question is used and these questions are then cycled each time one it used.

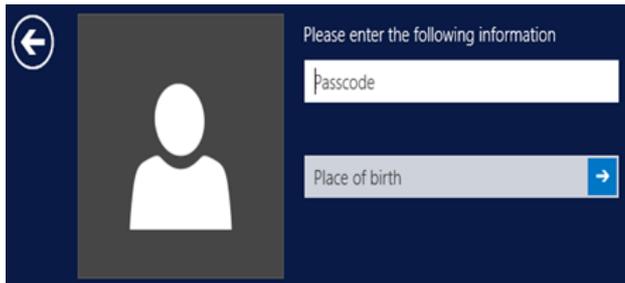
In addition, the user can be reminded by a SMS alert that their password is about to expire, the default alert time is 7 days.

The Windows password can be reset by the user selecting the "Reset" link on either the GINA or the Credential provider login.



1.10 User experience - Reset password with SecurEnvoy secret questions

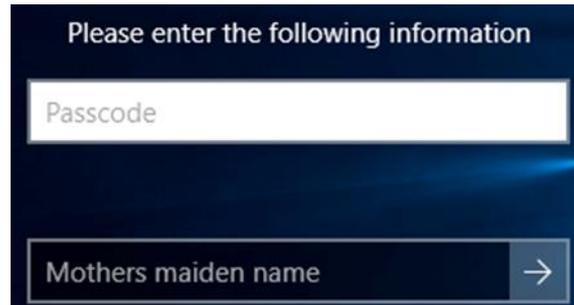
When the user selects the reset password link they will then be prompted to reply with answers as shown below:



Please enter the following information

Passcode

Place of birth

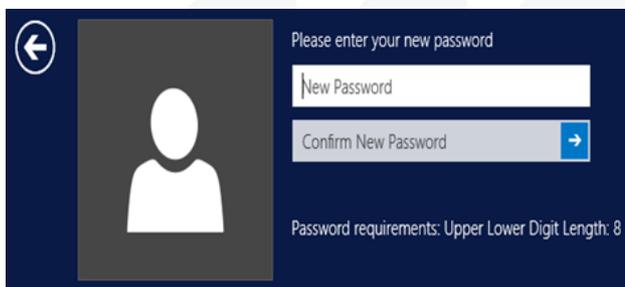


Please enter the following information

Passcode

Mothers maiden name

If a Domain password policy is in force the Gina or credential provider will display what components are required to make a good password.



Please enter your new password

New Password

Confirm New Password

Password requirements: Upper Lower Digit Length: 8

When a user responds with the relevant component i.e. Upper-case letter or numeric, the requirements that have been met will then be grayed out.

Note

The Password complexity prompt within the GINA or credential provider requires that the LDAP base is set. This can be configured directly within the server.ini file.

1.11 Offline Support (Soft Token)

To support users who are required to work in an offline state, the following are required:

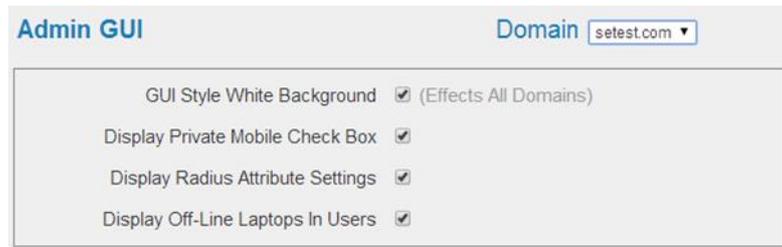
- User MUST be using a Soft Token
- User MUST be setup for Offline mode
- User MUST have authenticated with Soft Token at least once, in a connected state (this action copies the SEED record from the server to the user's machine)
- If a user updates their Soft Token SEED record to a new one, they must authenticate with the new Soft Token at least once, in a connected state

1.12 SecurEnvoy server User configuration

Setup the SecurEnvoy server to support offline passcodes for a Soft Token.

Launch the Admin GUI, Config then select Admin GUI options.

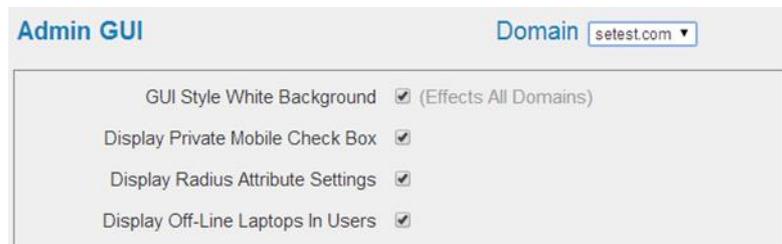
Select the domain you wish to work with and finally select the checkbox "Display Off-line Laptops".



Once complete then select the user(s) that require this setup, within the user profile.

Select the checkbox "Off-line Laptop"
Click update when complete

This MUST be completed for all users who require Off-Line passcodes support for a Soft Token.



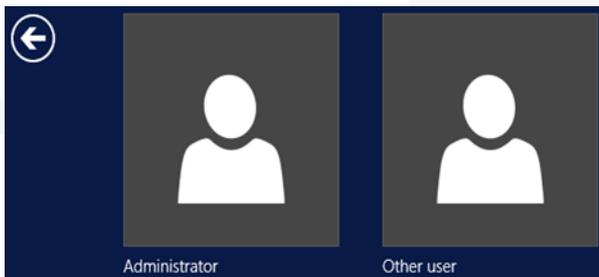
1.13 Off-Line User experience

Users have exactly the same experience as if they were logging on in a connected state. The local machine will validate the passcode.

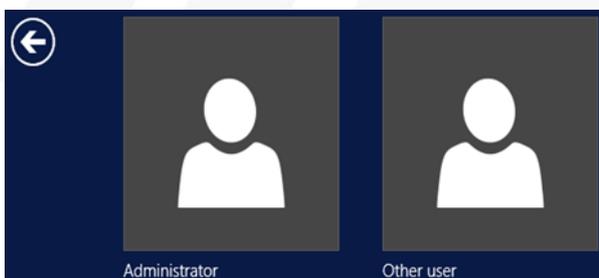
If there is any clock drift, the user is presented with a "Next Token Code" prompt.

The user is simply presented to enter in the next token passcode displayed upon their device.

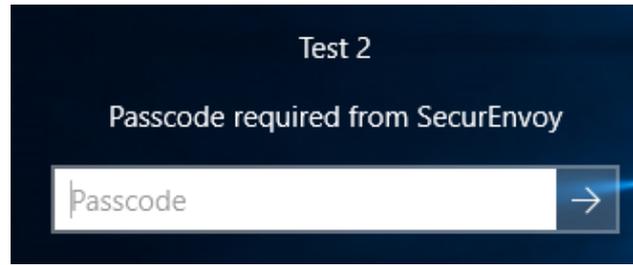
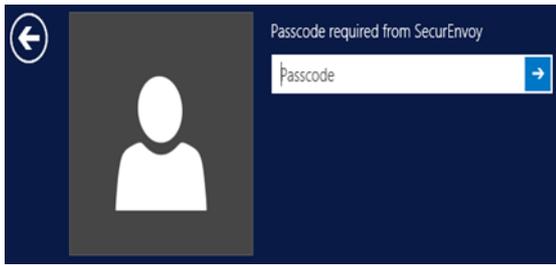
Windows Credential provider



User enters UserID, domain password.



If the user is configured for 2FA the following screen prompt is shown, otherwise the user is granted access to the domain.



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



A Shearwater Group plc Company

www.securenvoy.com