SecurEnvoy Enrol Integration Guide

Guide for integrating with SecurEnvoy's Enrolment System

Contents

Version History

Version	Author	Date	Changes
1.1	Matt Wood	09/02/2021	Updating styling
1.0	Matt Wood	26/03/2021	Initial version

Document Purpose

The purpose of this document is to demonstrate how a developer can integrate with the SecurEnvoy enrolment functionality in order to enrol a user with a Soft Token programmatically.

General Details

The functionality described in this document allows a developer to integrate soft token enrolment functionality into their own custom application, without needing the end user to visit the standard "SecEnrol" page.

The steps to do this are:

1. Authenticate with end user's credentials
2. Receive base64 encoded QR code image and token seed
3. Prompt user to scan QR code with their SecurEnvoy Soft Token App
4. Poll server to check for enrolment completion
5. (Optional) Manually send check code to complete enrolment

Authenticate User (1st step)

Description	Authenticate the user with userid and password, receive either "success" with qr code data, or "challenge" with a session key
URL	/secenrol/
Method	POST
URL Parameters	None
Data Parameters	action = GETQRONLY userid = <string> - The UserID of the user to enrol PASSWORD = <string> - The password/PIN of the user integrationmode = true

Success Responses	Challenge
	{
	    "result":"challenge",
	    "session":"<session key>",
	    "userid":"<the userid of the user>"
	}
	
	Success (will only happen with soft token push login)
	{
	    "result":"success",
	    "base64image":"<base 64 encoded image>",
	    "seed":"ABCD1234",
	    "enrolurl":"<url>",
	    "domain":"1"
	}

Cookie Returned	SecurEnvoyPin=<cookie content> (this is only returned with a "success" result)

Error Responses	**Access Denied**
	{
	    "result":"accessdenied"
	}
	
	Unexpected Error
	{
	    "result":"error",
	    "message":"<error message>"
	}

Sample Call	POST /secenrol/ HTTP/1.1 Host: www.host.com Content-Type: application/x-www-form-urlencoded Cache-Control: no-cache action=GETQRONLY&userid=bob&PASSWORD=secretpassword& PASSCODE=123456&integrationmode=true
Notes	If the authentication is successful (a status of "success"), this request will return a cookie named **SecurEnvoyPIN.** This cookie should be sent with every request after this until enrolment is completed.

2nd Authentication Step and Get QR Code

Description	Authenticate the user with userid, session key and passcode and get information back to enable enrolment to softtoken
URL	/secenrol/
Method	POST
URL Parameters	None
Data Parameters	**action = GETQRONLY** **userid = \<string\>** - The UserID of the user to enrol **SESSION = \<string\>** - The session key returned in the last step **PASSCODE = \<string\>** - The one time passcode of the user **integrationmode = true**

Success Response	{
	    "result":"success",
	    "base64image":"\<base 64 encoded image\>",
	    "seed":"ABCD1234",
	    "enrolurl":"\<url\>",
	    "domain":"1"
	}

Cookie Returned	SecurEnvoyPin=\<cookie content\>

Error Responses	**Access Denied**
	{
	    "result":"accessdenied"
	}
	
	Unexpected Error
	{
	    "result":"error",
	    "message":"\<error message\>"
	}

Sample Call	POST /secenrol/ HTTP/1.1 Host: www.host.com Content-Type: application/x-www-form-urlencoded Cache-Control: no-cache action=GETQRONLY&userid=bob&PASSWORD=secretpassword& PASSCODE=123456&integrationmode=true
Notes	If the authentication is successful, this request will return a cookie named **SecurEnvoyPIN.** This cookie should be sent with every request after this until enrolment is completed.

Poll Server for Auto Enrolment Completion

Description	Poll the enrolment server to check if the phone has completed auto enrolment
URL	/secenrol/
Method	POST
URL Parameters	None
Data Parameters	action = QUERYSOFTTOKEN seed = <string> - The seed passed back from the previous request integrationmode = true
Success Responses	**CONTINUE** – this is returned when auto enrol has not yet completed, you should keep polling until OK is returned or the "CheckCode" is manually entered **OK** - this is returned when auto enrolment has completed successfully
Error Responses	<Error Message>
Sample Call	POST /secenrol/ HTTP/1.1 Host: www.host.com Content-Type: application/x-www-form-urlencoded Cache-Control: no-cache Cookie: SecurEnvoyPIN=<cookie content from previous response> action=QUERYSOFTTOKEN&seed=ABCD1234&integrationmode=true
Notes	You must include the cookie **SecurEnvoyPIN,** returned from the authentication request in this request

Manually Send Check Code

Description	Manually send check code from phone if auto enrolment is not possible
URL	/secenrol/
Method	POST
URL Parameters	None
Data Parameters	**action = SETINFO** **domain = \<string\>** - The domain number returned from the authentication request **tokentype = softtoken** **SOFTTOKENURL = \<string\>** - The "enrolurl" returned from the authentication request **CHECKCODE = \<string\>** - The code displayed on the user's phone if auto enrolment fails **integrationmode = true**

Success Response	{
	     "result":"success"
	}

Error Responses	**Access Denied**
	{
	     "result":"accessdenied"
	}
	
	Unexpected Error
	{
	     "result":"error",
	     "message":"\<error message\>"
	}

Sample Call	POST /secenrol/ HTTP/1.1 Host: www.host.com Content-Type: application/x-www-form-urlencoded Cache-Control: no-cache Cookie: SecurEnvoyPIN=\<cookie content from previous response\> action=SETINFO&domain=1&tokentype=softtoken&CHECKCODE=ABCD1234& SOFTTOKENURL=\<enrol url\>
Notes	You must include the cookie **SecurEnvoyPIN,** returned from the authentication request in this request