External Authentication with Citrix Secure Gateway - Presentation server

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	

Citrix Integration Guide

This document describes how to integrate a Citrix Secure Gateway - Presentation server with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Citrix Secure Gateway - Presentation server provides - Secure Remote Access to the internal corporate network for all Client/Server applications.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Citrix), without the complication of deploying hardware tokens or smartcards.
Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that a Single Sign On solution can be completed. Utilising the Windows password as the PIN, allows The User enters their UserID, Windows password and One Time Passcode received upon their mobile phone. The SecurEnvoy Web agent passes this information to the Security server where it carries out a Two-Factor authentication, as the Windows password was presented, this can be passed to the back end Citrix Presentation server, where a Windows authentication takes place. All this happens without any user intervention. It provides a seemless login into the Citrix Environment by entering three pieces of information. SecurEnvoy utilizes a web GUI for configuration, whereas the Citrix environment uses a mixture of Web GUI and applications. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Citrix

Citrix Metaframe XPe feature release 3
Web Interface for Presentation Server version 3.0

Microsoft

Windows 2003 server SP1 (For Citrix Environment)
IIS installed with SSL certificate

SecurEnvoy

Windows 2003 server SP1
IIS installed with SSL certificate (required for management and remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v3.01 0100
SecurAccess Microsoft IIS web agent v3.01 agent

© 2005 SecurEnvoy Ltd. All rights reserved

Index

1.0 Pre Requisites..... 3
1.1 Installation Overview..... 3
2.0 Installation of SecurEnvoy - Microsoft IIS Web Agent..... 4
2.1 Configuration of SecurEnvoy - Microsoft IIS Web Agent..... 4
3.0 Configuration of SecurEnvoy Admin..... 6
4.0 Test Logon..... 7
5.0 Single Sign On Solution..... 8

1.0 Pre Requisites

It is assumed that Citrix Metaframe server(s) are already installed and that a SSL certificate is installed upon the Web server running the Citrix Web services, this guide is for the setup of Citrix Secure Gateway and Presentation Server (Web Interface) on one machine to integrate with SecurEnvoy. Prior to the installation of SecurEnvoy software, please make sure that a Citrix user can connect, authenticate and run applications using existing Windows Domain credentials. SecurEnvoy requires an account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security servers, SecurEnvoy IIS Web agent and Active Directory servers, additional open ports will be required.

1.1 Installation Overview

Installation of both Citrix Secure Gateway (CSG) and Citrix Web Interface upon the same physical machine. This requires additional configuration to Citrix Web interface, to allow Microsoft IIS web services to interact. Microsoft IIS is configured to use port 443 for SSL connectivity.

In this scenario the SecurEnvoy IIS Web agent is installed upon the Citrix Web Interface machine.
All references to IP addresses and machine names are taken for the Installation and Machine information tables.

Installation Information	
Domain name	Securenvoy.com
Citrix machine	Citrix.Securenvoy.com
Metaframe Farm	SecHQ Servers – 10.1.10.100, 10.1.10.101, 10.1.10.102
Secure Ticket Authority	STA01.Securenvoy.com
SecurEnvoy Server	SecAuth.Securenvoy.com

© 2005 SecurEnvoy Ltd. All rights reserved

Machine Information	
Name	**IP Address**
Citrix.Securenvoy.com	192.168.200.100
Metaframe Farm SecHQ	10.1.10.100, 10.1.10.101, 10.1.10.102
STA01.Securenvoy.com	10.1.10.22
SecAuth.Securenvoy.com	10.1.10.50

2.0 Installation of the SecurEnvoy Microsoft IIS Web agent

The Microsoft IIS agent is located in the Agent directory of the SecurEnvoy software distribution

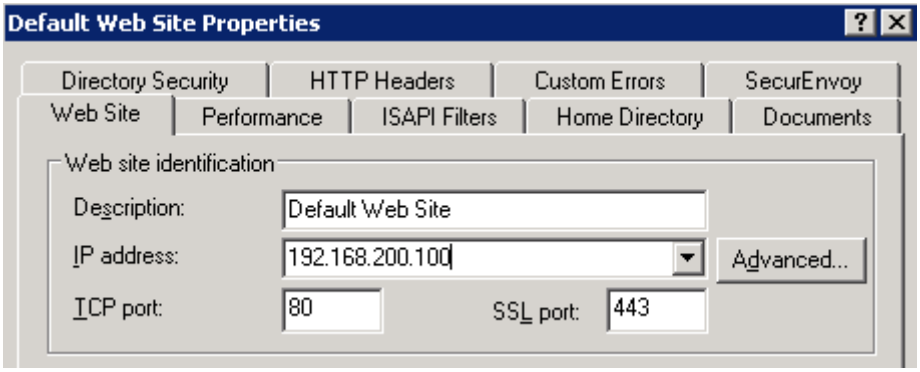
Install this agent on your Citrix Presentation Server

2.1 Configuration of SecurEnvoy - Microsoft IIS Web Agent

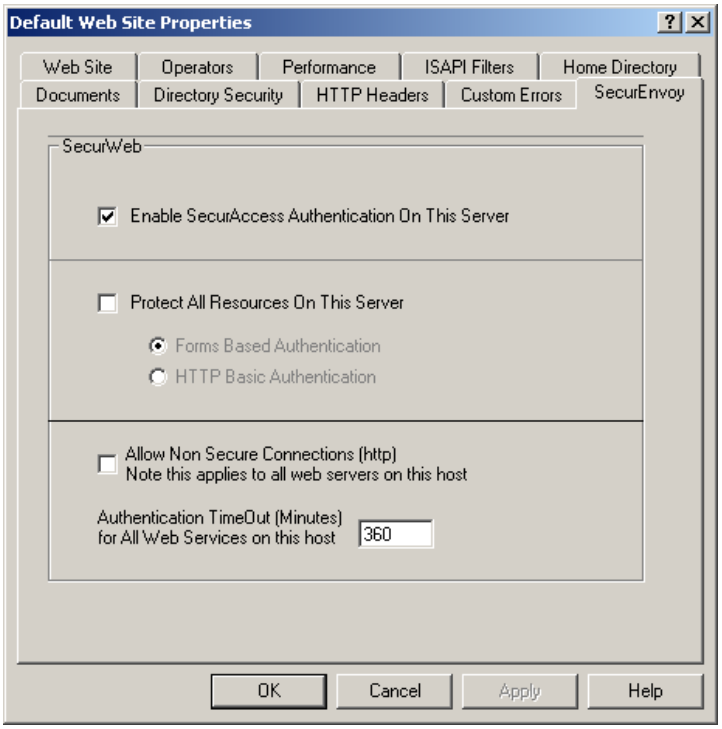
Launch the IIS management interface, either from “Start”, ”All Programs”, “SecurEnvoy”, “IIS Config MMC” or from Microsoft’s MMC for IIS.

Expand the Web site list on the navigation pane and right mouse click “Default Web Site”, then select “Properties”.

Machine Name:	**Citrix.securenvoy.com**
Citrix Service:	**CSG and Web Interface**
SecurEnvoy Security Server:	**SecAuth.securenvoy.com**
Protected web resource:	**/Citrix**

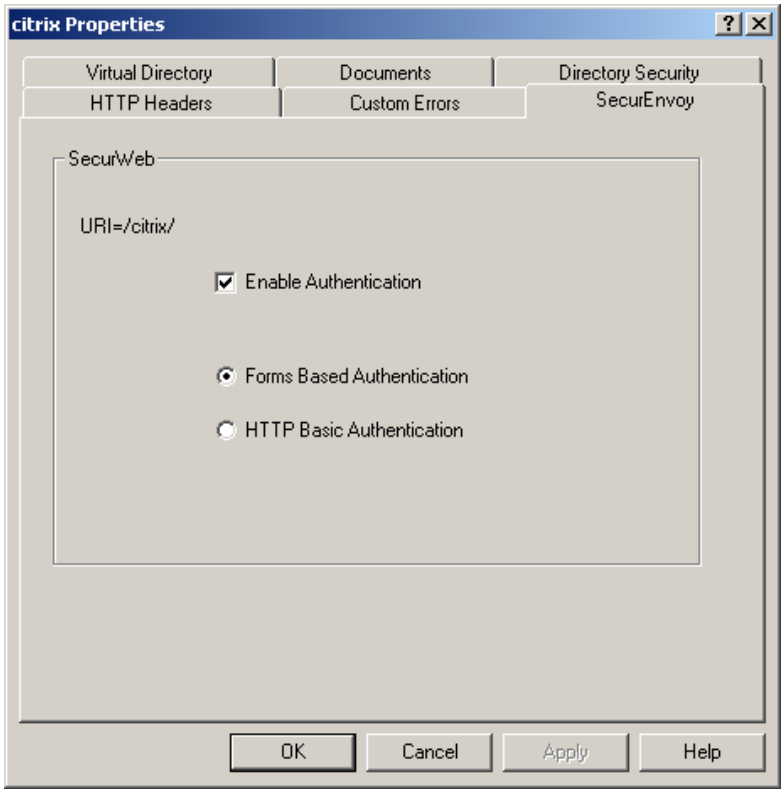


© 2005 SecurEnvoy Ltd. All rights reserved



Select the "Enable SecurAccess Authentication On This Server" check box to enable the IIS agent on this server. Note the "Allow Non Secure Connections" must NOT be checked as Citrix redirects all communication via https.

To enable protection of the Citrix server, navigate the web site tree within the IIS snap-in, select the Citrix folder and go to the properties of this web folder. Select the SecurEnvoy tab and click enable then select "Forms Based Authentication".



Once completed click OK and then click the restart Web.

© 2005 SecurEnvoy Ltd. All rights reserved

2.2 Additional Configuration of SecurEnvoy - Microsoft IIS Web Agent

Edit the file c:\WINDOWS\seiis.ini
Locate “HTTP_HOST=” and add just the server part of the URL you are trying to connect to. In this example we are trying to connect to https://secauth.securenvoy.com/citrix so the value HTTP_HOST=secauth.securenvoy.com
Restart the world wide web service

3.0 Configuration of SecurEnvoy Admin

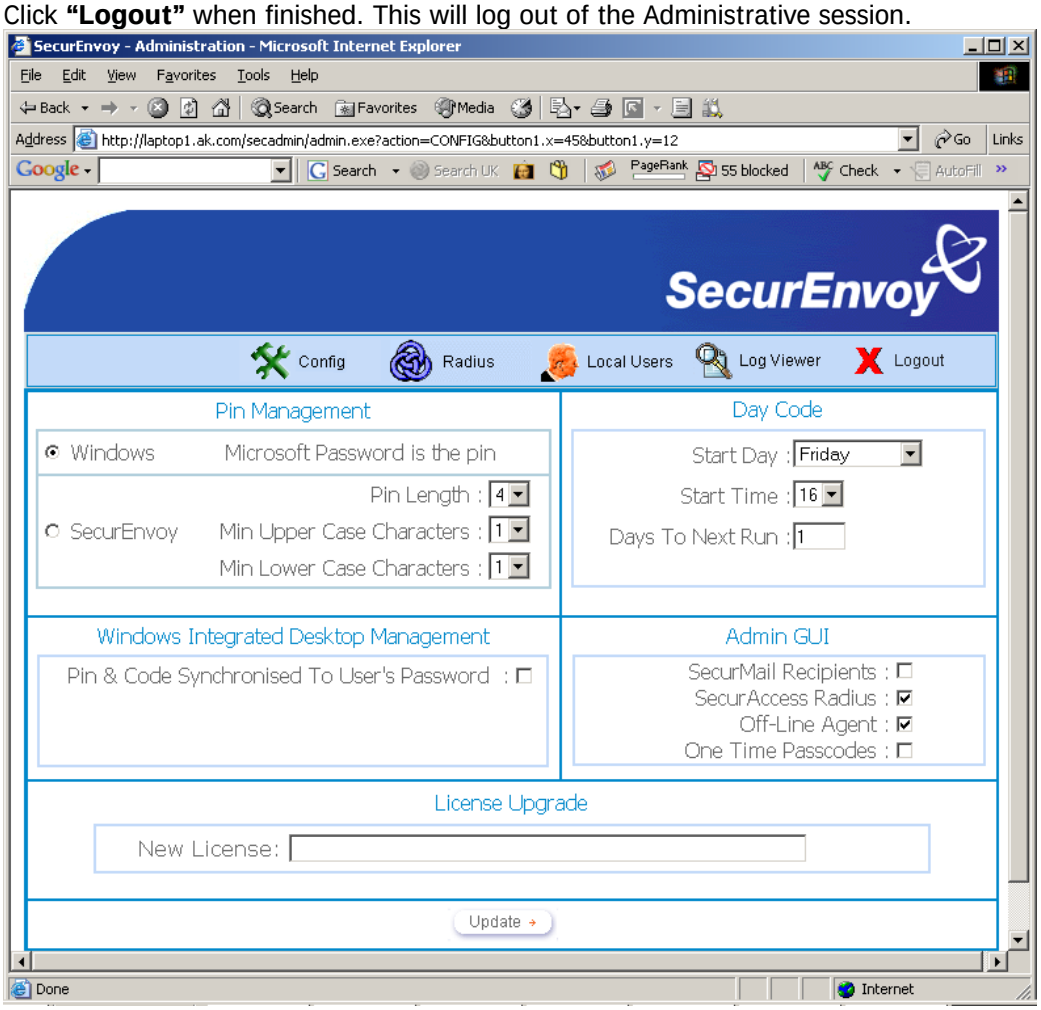
Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click **“Config”**

Select **Windows** – Microsoft Password is the PIN under PIN Management
This will now use the users existing password as the PIN (this is the default setting).

Click **“Update”** to confirm the changes

Click **“Logout”** when finished. This will log out of the Administrative session.



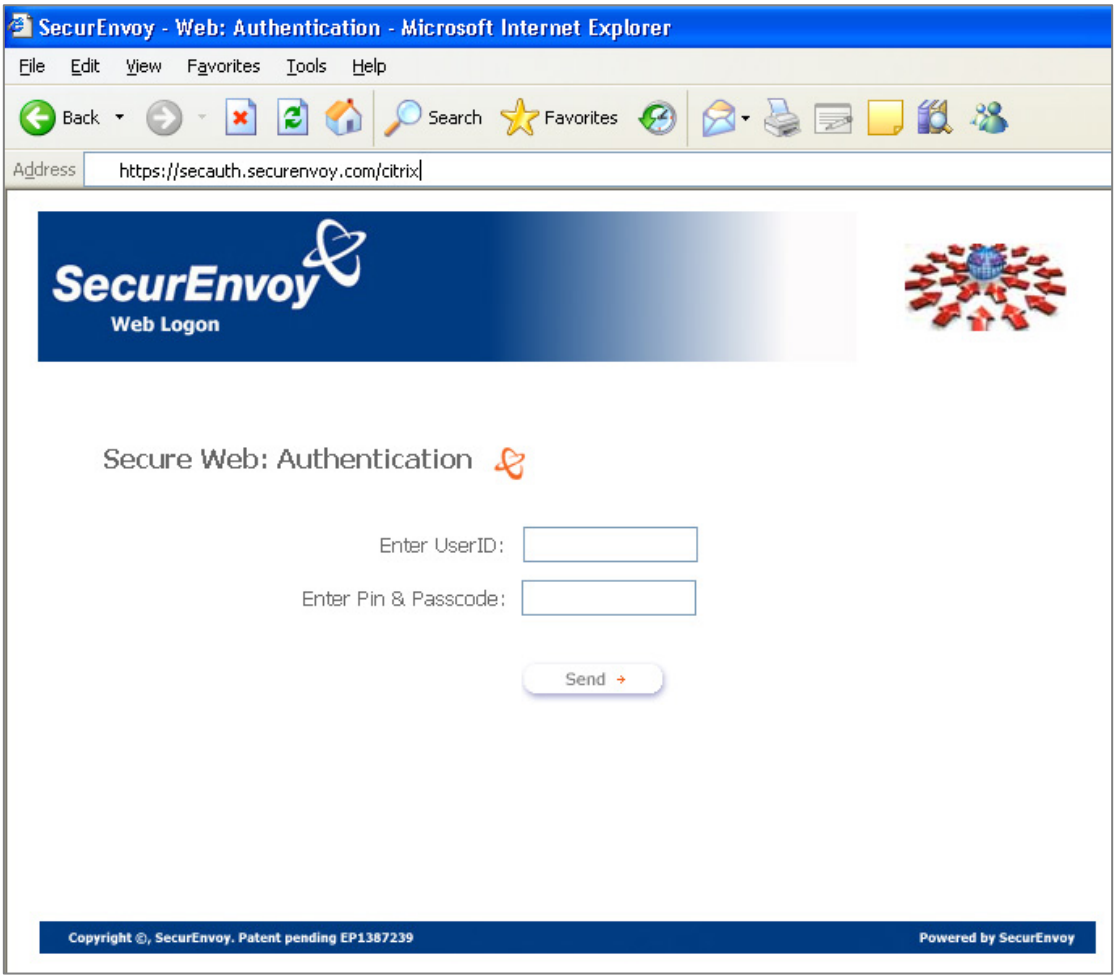
4.0 Test Logon

To access the protected Citrix environment go to:

https://secauth.securenvoy.com/citrix

The following page will be displayed; this is the SecurEnvoy Two-Factor Web authentication page. All users will be stopped from proceeding to any protected resource, until Two-Factor authentication has been completed. The user carries out the following:

1.0 Enter Domain Username
2.0 Enter Domain password (This is the PIN)
3.0 Enter the One Time Passcode (OTP) received on their mobile phone

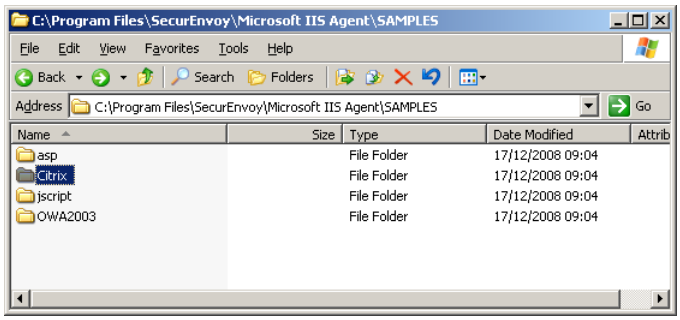


When all details have been entered click **"Send"**.
The user now has access to the Citrix front page.

5.0 Single sign on Solution

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

Navigate to **\Program Files\SecurEnvoy\Microsoft IIS Agent\Samples\Citrix** directory, there will be a number of Citrix versions.



Select the version that is correct for your environment.

Following the instructions in the readme.txt file.

© 2005 SecurEnvoy Ltd. All rights reserved