SecurEnvoy

External Authentication with Windows 2003 Server with Routing and Remote Access service

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	

Windows 2003 Server with Routing and Remote Access service
Integration Guide

This document describes how to integrate a Windows 2003 Server with Routing and remote Access service installed with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Microsoft Windows 2003 Routing and Remote Access provides - Secure Remote Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Microsoft), 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 it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. It provides a seemless login into the Windows Server environment by entering three pieces of information. SecurEnvoy utilises a web GUI for configuration, whereas the Microsoft Windows Server environment uses a GUI application. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Microsoft Server

Any compatible Server to support Windows 2003 server.
See (http://www.microsoft.com/windowsserver2003/evaluation/sysreqs/default.mspx) for more information.
In this integration guide all tests were completed with Microsoft Windows 2003 server (SP1)

Microsoft Client

In this integration guide all tests were completed with Microsoft Windows XP (SP2)

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 v3.0.010

© 2005 SecurEnvoy Ltd. All rights reserved

Index

1.0 Pre Requisites..... 3
1.1 Configuration of Routing and Remote Access - RRAS..... 3
2.0 Configuration of SecurEnvoy 4
3.0 Test Logon 5

1.0 Pre Requisites

It is assumed that Routing and Remote access service has been installed upon the relevant server(s).
Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Routing and Remote Access server(s), additional open ports will be required.
***NOTE:** Add radius profiles for Windows server with the Routing and Remote access server(s) that requires Two-Factor Authentication.*

1.1 Configuration of Routing and Remote Access - RRAS

Windows 2003 server SP1 - IPSec VPN

1. Install Routing and remote access service if not already installed
2. Launch Routing and remote access MMC, select server and click "configure and enable Routing and remote access"
3. Follow wizard and setup for VPN access, set up for IPSec VPN. Start RRAS service
4. Select the server within RRAS MMC, go to properties
5. Select Security, select Radius for Authentication provider, select configure. Populate with Radius information. Timeout should at least be 10 seconds.
6. Select Authentication methods, deselect all, and only enable PAP protocol.
7. Restart RRAS service.

Client Windows XP SP2

1. Create new network connection wizard, select VPN
2. Go to properties, select Security tab, select Advanced, and go to settings.
3. Change Data encryption to "Optional encryption", and only select PAP for protocols.
4. Enter Pre shared key for IPSec settings.

© 2005 SecurEnvoy Ltd. All rights reserved

2.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can utilise the existing Microsoft password as the PIN. This allows the users to only remember their Domain password. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

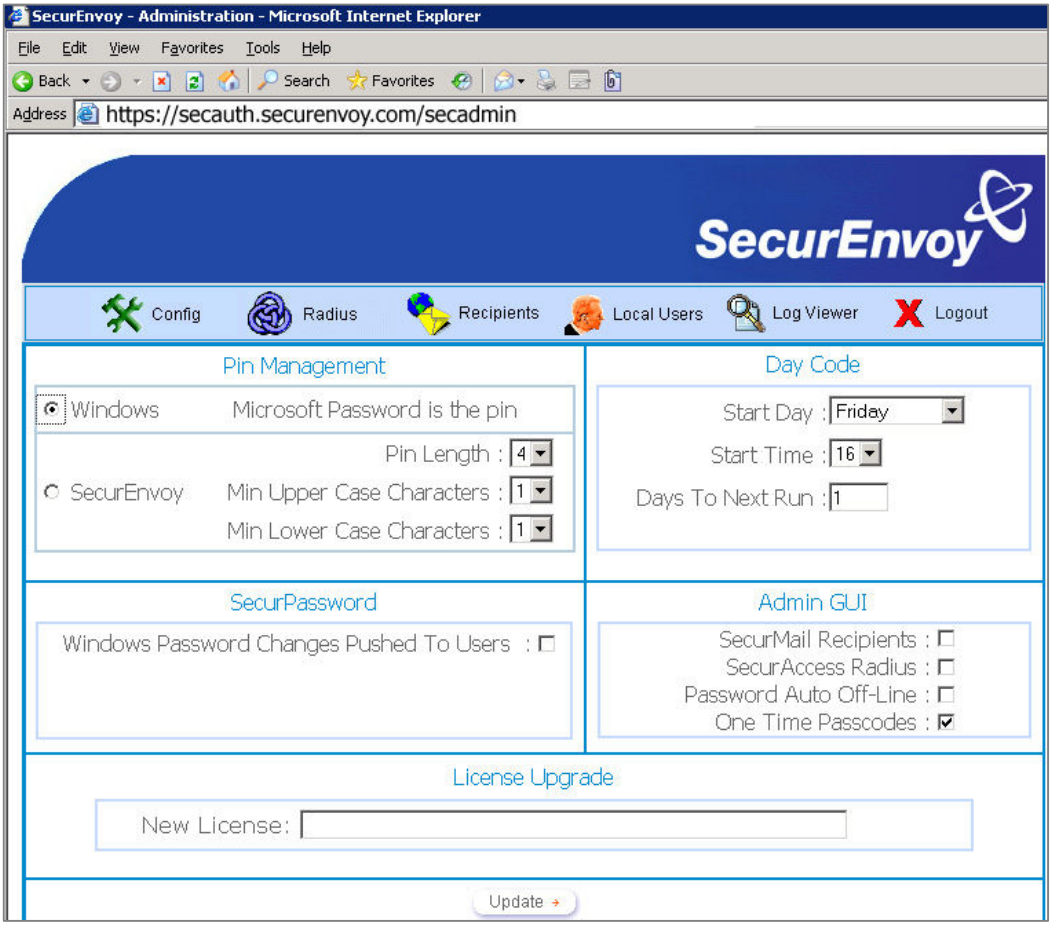
Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click **"Config"**

Select **Windows** – Microsoft Password is the PIN under PIN Management

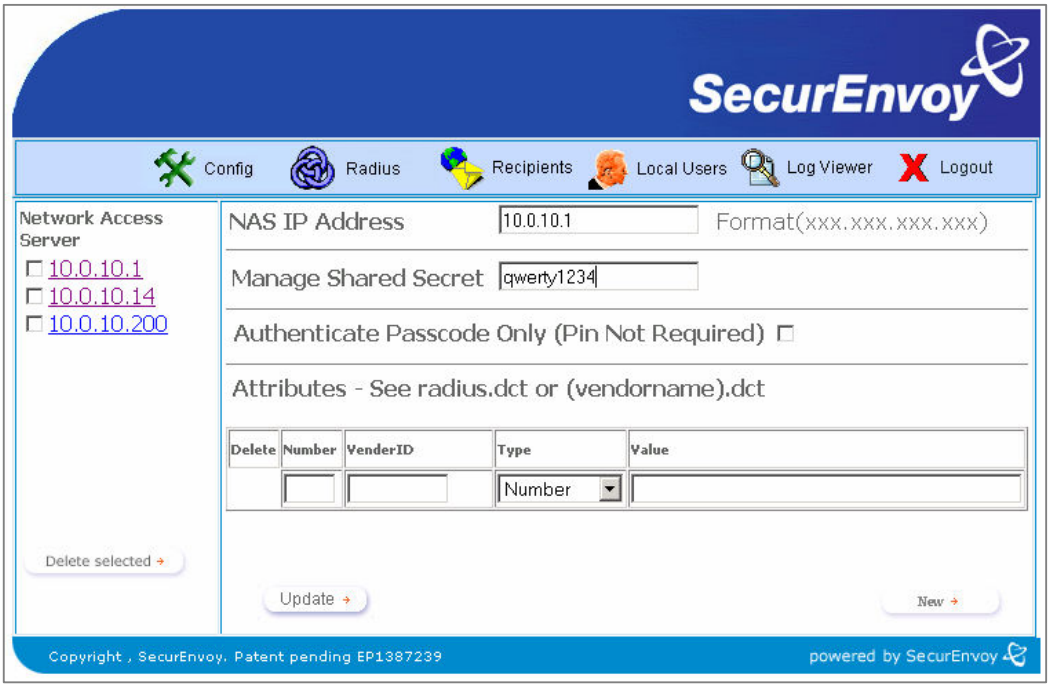
This will now use the users existing password as the PIN.

Click **"Update"** to confirm the changes



Click the "Radius" Button

Enter IP address and Shared secret for each Server that has Routing and Remote Access installed and wishes to use SecurEnvoy Two-Factor authentication.



Click "Update" to confirm settings.

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

3.0 Test Logon

Enter the UserID in the Username field

Enter password and passcode in the password field.

E.g. *P4ssw0rd*678123

