SecurEnvoy

External Authentication with CiscoSecure ACS

Authenticating Users Using

SecurAccess Server

by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Andy Kemshall	akemshall@securenvoy.com	

CiscoSecure ACS Integration Guide

This document describes how to integrate a Cisco ACS Radius Server with SecurEnvoys two-factor authentication solution called 'SecurAccess'.

Cisco ACS provides a central RADIUS authentication gateway that can be configured for multiple back-end two-factor authentication servers and is ideal for use when migrating from an existing token based system to SecurEnvoy.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Cisco), 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.

SecurEnvoys 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, as does the Cisco VPN Concentrator. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Cisco
Cisco ACS Version 3.0.2 installed on a server that's IP Address is 192.168.99.11

SecurEnvoy
Windows 2003 server SP1 (IP Address 192.168.99.10)
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 v3.1

Index

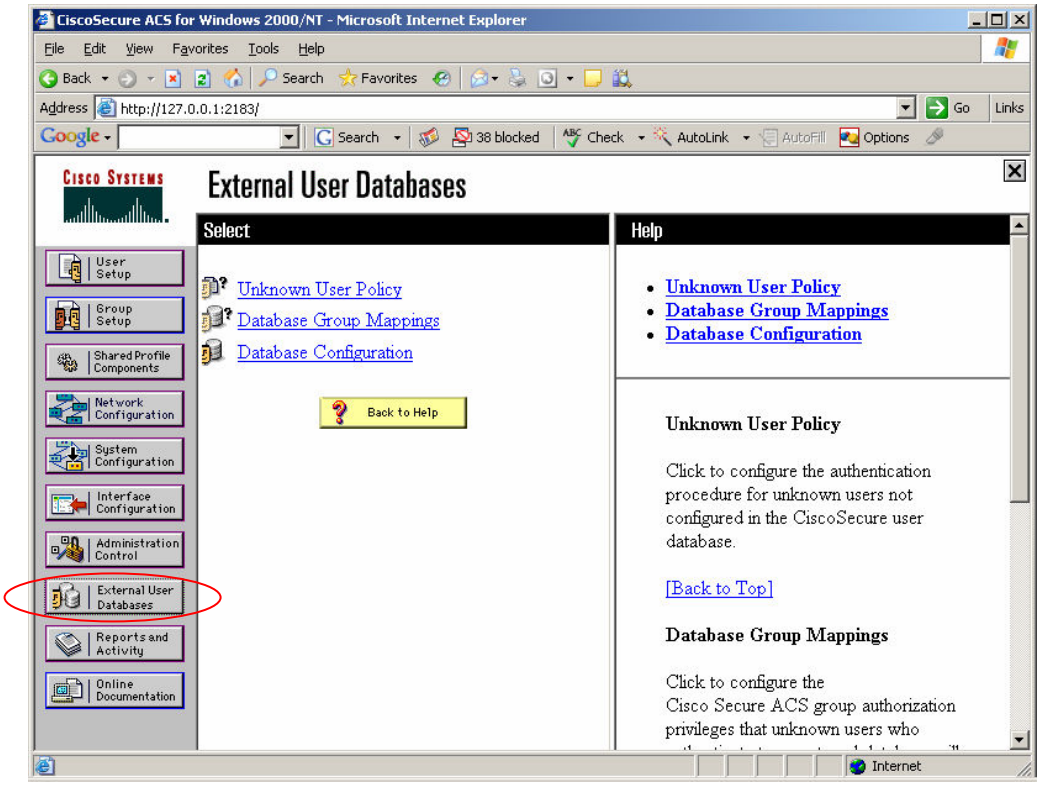
1.0 Pre Requisites

It is assumed that Cisco ACS has been installed and is authenticating with a username and password or other third party token system.

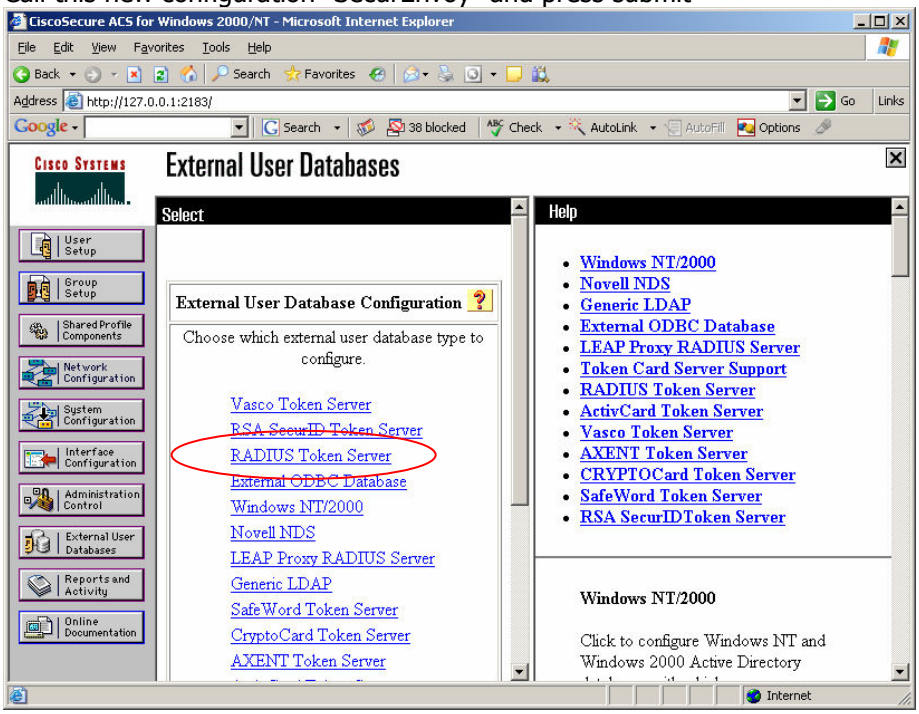
The SecurEnvoy Security Server has been installed with the Radius service and has a suitable account with read and write privileges to the Active Directory. If firewalls are between the SecurEnvoy Security server and CiscoSecure ACS, additional open ports will be required, by default UDP 1812 is used.

2.0 Configuration of Cisco ACS

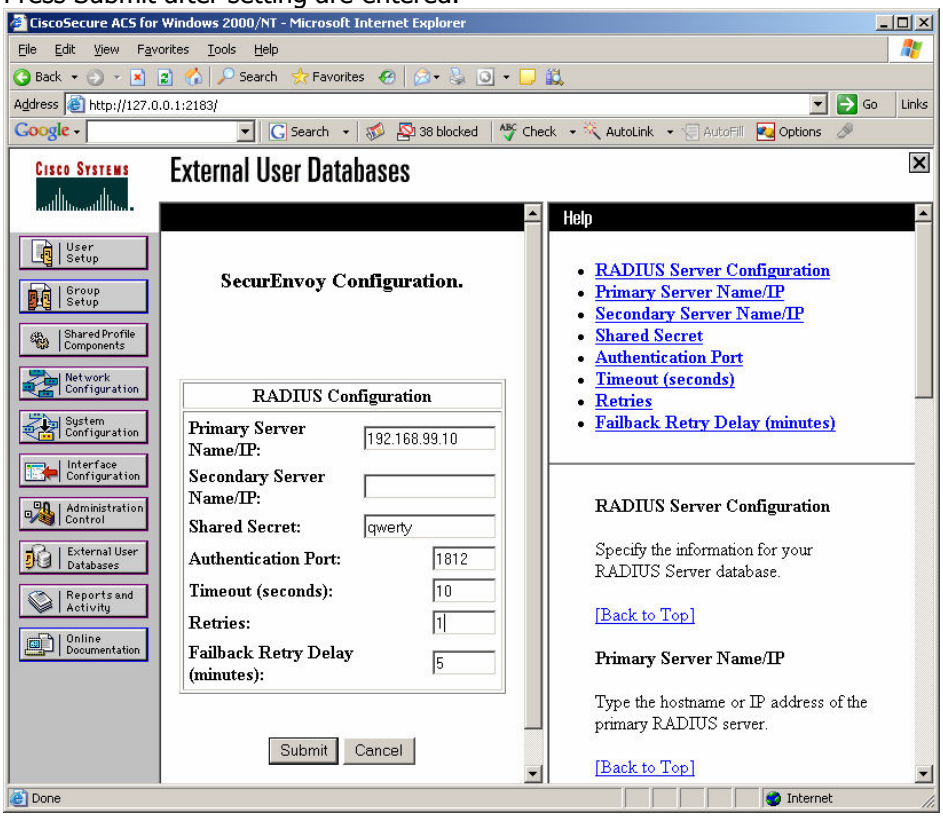
Login to the Cisco Secure Web Interface, select the left button **"External User Database"** Select the link "**Database Configuration**"



Select the link "**RADIUS Token Server**" and press the button "**Create New Configuration**"
Call this new configuration "SecurEnvoy" and press submit



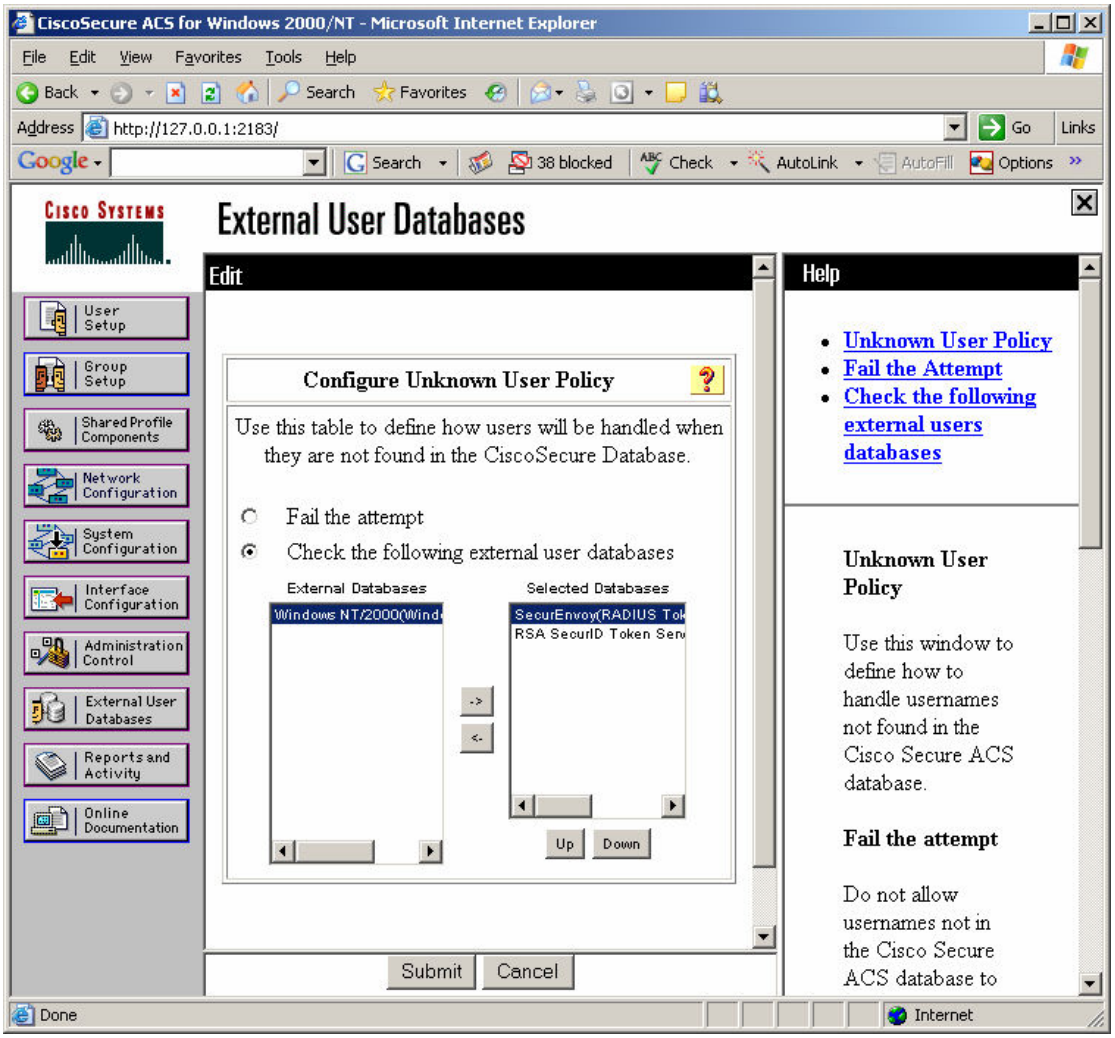
Next press the "Configure" button to setup SecurEnvoy's Radius settings and enter the SecurEnvoy server IP Address, Radius Port (default is 1812) and shared secret.
In this case the IP Address of the SecurEnvoy server is 192.168.99.10, the Radius port is the default (1812) and the shared secret is qwerty.
It is recommended that a retry of 1 and timeout of 10 seconds is used.
Press Submit after setting are entered.



After the SecurEnvoy server has been defined it must be added as one of the active servers. If no local users or groups are used then setup the following:-

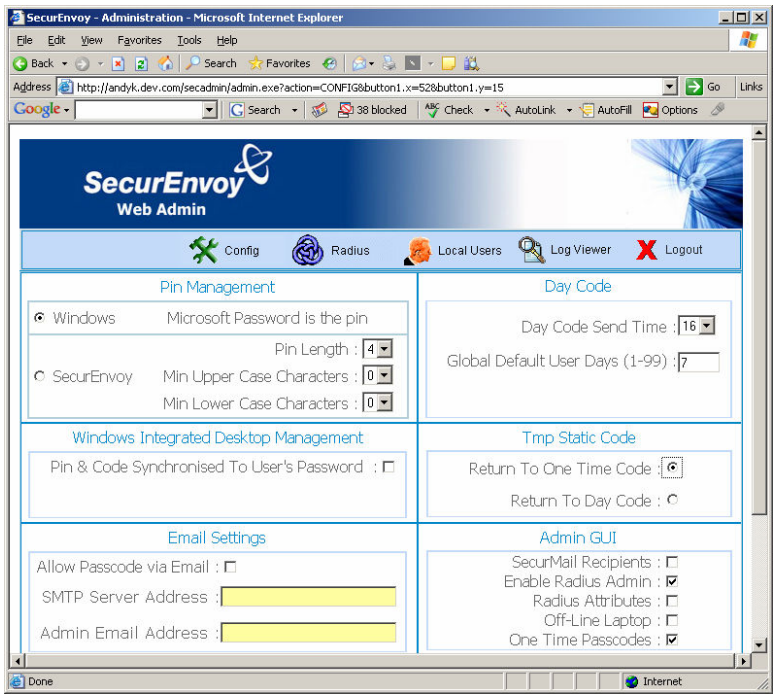
Re-select the left button "External User Databases" and select the link "Unknown User Policy" Add "SecurEnvoy" to the selected database list and press submit.

If SecurEnvoy is set to the top of the list it will be authenticated first, this is recommended as SecurEnvoy has a very fast authentication time.
If the user is not setup in SecurEnvoy then an access denied is received which will cause ACS to try authenticating the next server in the list thus multiple token types can co-exist.



3.0 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 the IP address and Shared secret of the Cisco ACS server, in this example: 192.168.99.11 qwerty

Click **"Update"** to confirm settings.

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