External Authentication with Citrix Access Gateway

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 Access Gateway Integration Guide

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

Citrix Access Gateway provides - Secure Remote Access to the internal corporate network.

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 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. SecurEnvoy utilises a web GUI for configuration, as does the Citrix Access Gateway. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Citrix

Citrix Access Gateway v4.2.2 Build 80.3

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

SecurAccess software release v3.01.0200

© 2005 SecurEnvoy Ltd. All rights reserved

Index

1.0 Pre Requisites..... 3
1.1 Configuration of Citrix Access Gateway..... 4
2.0 Configuration of SecurEnvoy..... 5
3.0 Test Logon..... 6

1.0 Pre Requisites

It is assumed that the Citrix Access Gateway has been installed and is authenticating with a username and password.

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 Citrix Access Gateway appliance(s), additional open ports will be required.

NOTE: *Add radius profiles for each Citrix Access Gateway that requires Two-Factor Authentication.*

© 2005 SecurEnvoy Ltd. All rights reserved

1.1 Configuration of Citrix Access Gateway

To enable a Two-Factor logon to the Citrix Access Gateway appliance, login to the administration interface. Select authentication and delete the existing "Default" profile.

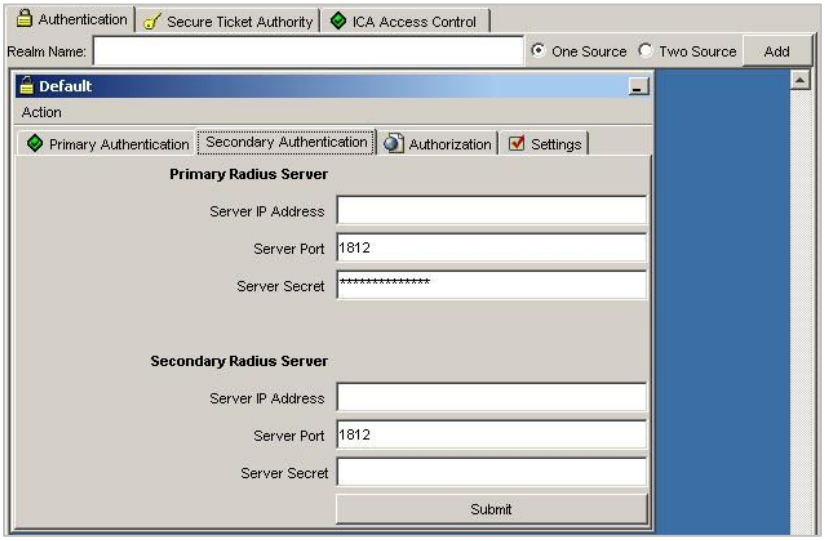
Create a new profile named "Default" and select it to be a "two source" click "add".

Select the Authentication drop down menu for the primary authentication, select LDAP. Select the Authentication drop down menu for the secondary authentication, select Radius. Click OK when complete.

Populate information for primary authentication to designate what IP address, port etc is to be used for LDAP authentication. Populate information for secondary authentication to designate what IP address, port and pre shared key is to be used for SecurEnvoy Radius authentication.
The SecurEnvoy Radius server is using UDP port 1812. (This is the default).
Finally enter details for Authorisation.

See diagrams below





© 2005 SecurEnvoy Ltd. All rights reserved

This is the only configuration required on the Citrix appliance.

NOTE:

The profile must be entered and saved as "Default" to Two-Factor Authenticate all users.

2.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can be set up to only authenticate the passcode component as both authentication servers that are required to authenticate a remote user.

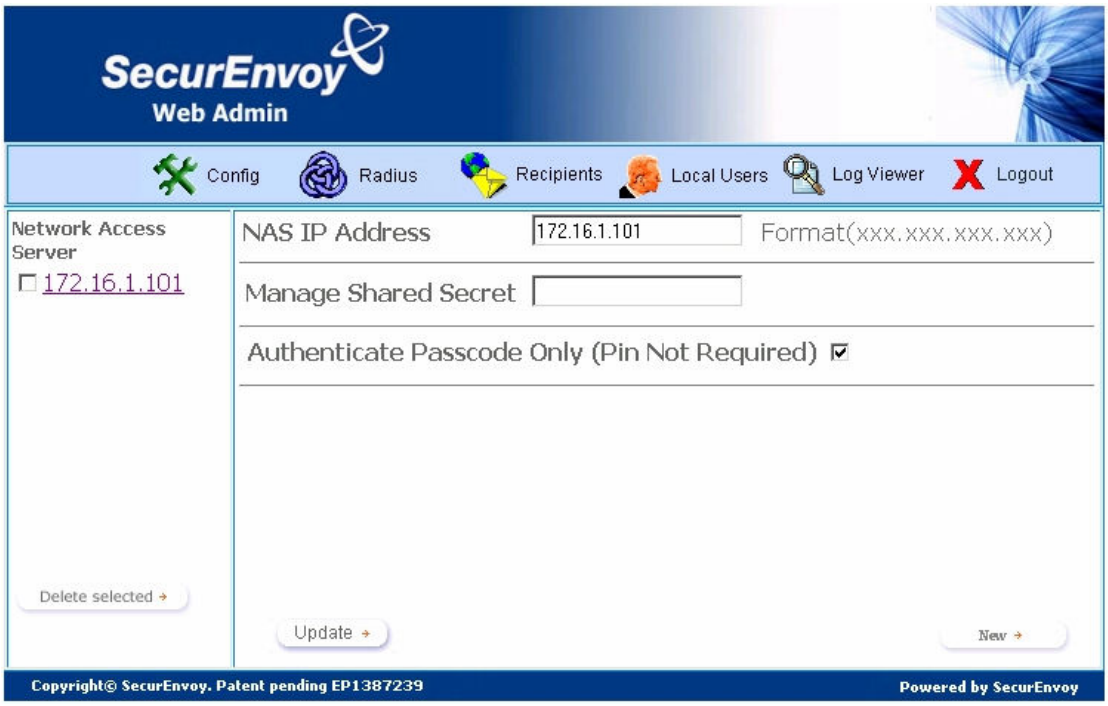
SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

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

Click the **"Radius"** Button

Enter IP address and Shared secret for each Citrix Access Gateway that wishes to use **SecurEnvoy** Two-Factor authentication.

Make sure the "Authenticate Passcode Only (Pin not required) checkbox is ticked.



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

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

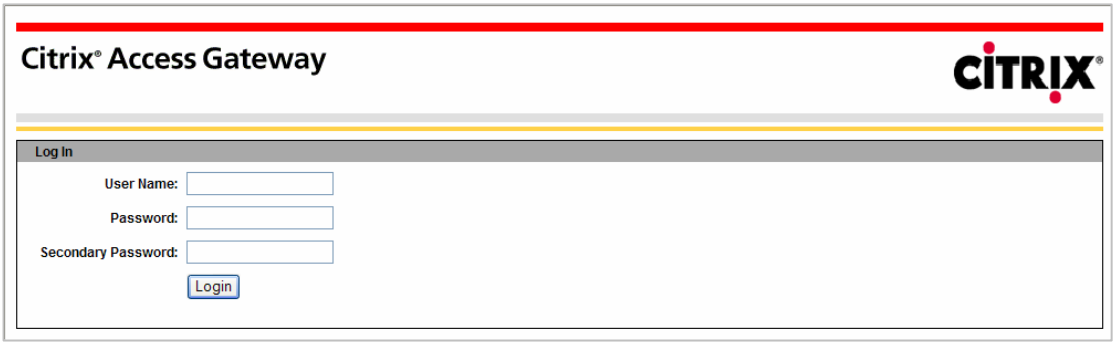
© 2005 SecurEnvoy Ltd. All rights reserved

3.0 Test Logon

Browse to the web location of the Citrix Access Gateway

https://remote.securenvoy.com

Three input dialogue boxes will be displayed.
User will enter: UserID in the User name box
Domain password in password box
Passcode (via SMS) in Secondary box



Click logon to complete the process.

Once authenticated a new SMS passcode will be sent to the user's mobile phone, ready for the next authentication.

© 2005 SecurEnvoy Ltd. All rights reserved