External Authentication with Citrix Access Gateway Advanced Edition

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Andy Kemshall Martin Blackburn	akemshall@securenvoy.com M.Blackburn@esteem.co.uk	

Citrix Access Gateway Advanced Edition Integration Guide

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

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

Citrix Access Gateway™ Advanced Edition extends access to more devices and users, including browser-only kiosk access and mobile devices. Extensive SmartAccess capabilities provide flexible, highly granular policy based access control, including tight integration with Citrix Presentation Server™.

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. 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 v4.5.8
- Citrix Advanced Access Control v4.5 Hotfix AAC450W004

SecurEnvoy

- Windows 2003 server SP2
- IIS installed
- Active Directory installed or connection to Active Directory via LDAP protocol.
- SecurAccess software release v4.1.504

Contents

Pre Requisites

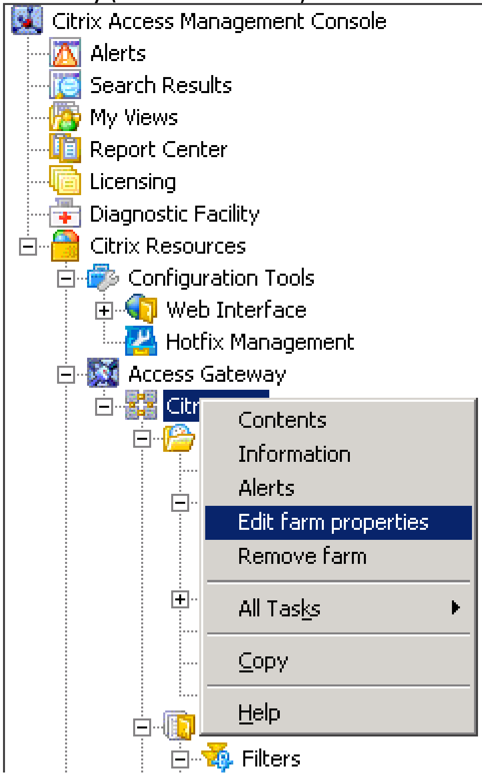
It is assumed that the Citrix Access Gateway hardware and Advanced Access Control has been installed and is authenticating with a username and password.

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.

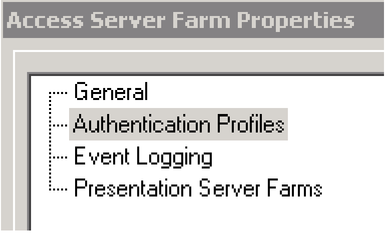
Add radius profiles for each Advanced Access Control Server that requires Two-Factor Authentication.

Configuration of the Advanced Access Control Server

1. Start > Programs > Citrix > Management Consoles > Citrix Access Management Console
2. Right click the Citrix Access Management Console\Citrix Resources\Access Gateway*AAC farm name*, and choose "Edit Farm Properties"



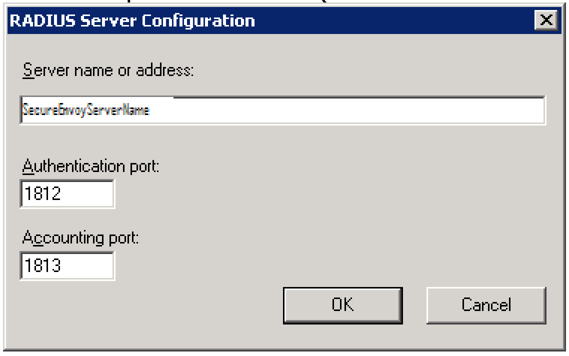
3. Within the Access server farm properties choose "Authentication Profiles"



Access Server Farm Properties

- General
- Authentication Profiles
- Event Logging
- Presentation Server Farms

4. Under the RADIUS profiles, click "New…"
5. Enter a profile name and description, then click "New.." under the server section
6. Enter the SecurEnvoy server name or IP address
7. Leave the ports as default (authentication = 1812, accounting = 1813)



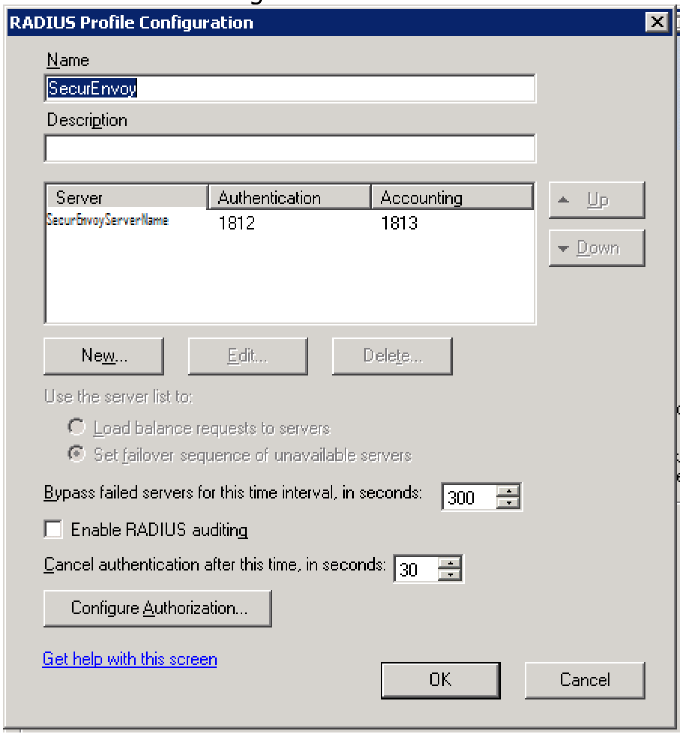
RADIUS Server Configuration

Server name or address: SecureEnvoyServerName

Authentication port: 1812

Accounting port: 1813

8. Click OK
9. Leave all other settings as default



RADIUS Profile Configuration

Name: SecurEnvoy

Description:

Server	Authentication	Accounting
SecurEnvoyServerName	1812	1813

Use the server list to:

○ Load balance requests to servers

● Set failover sequence of unavailable servers

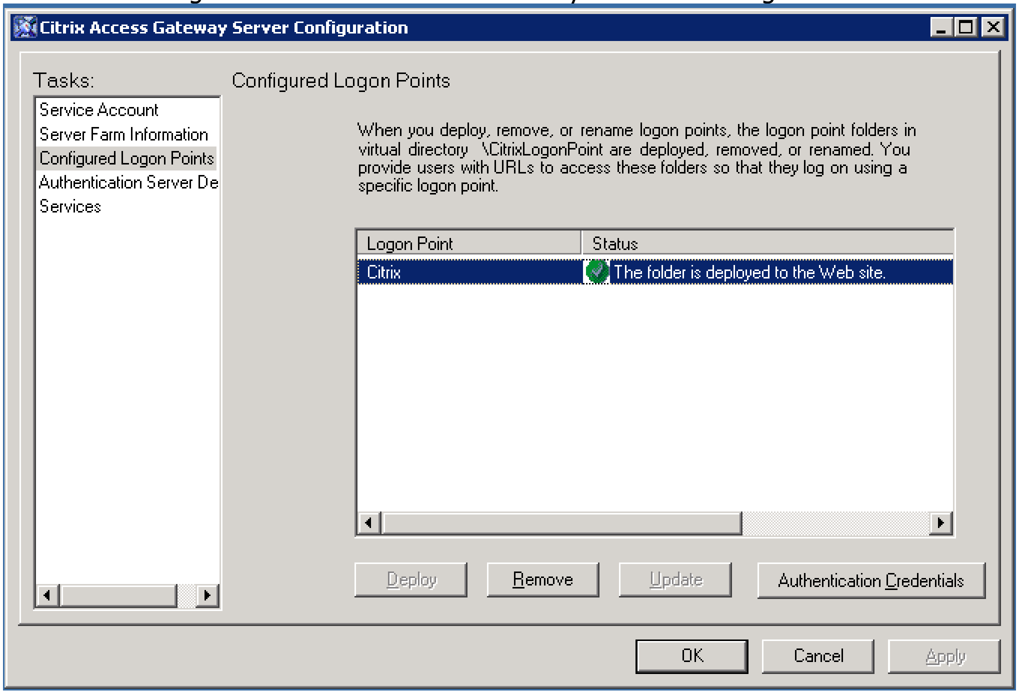
Bypass failed servers for this time interval, in seconds: 300

□ Enable RADIUS auditing

Cancel authentication after this time, in seconds: 30

10. Click OK on the RADIUS profile Configuration dialogue box
11. Click OK on the Access Server Farm Properties dialogue box

12. Run Start > Programs > Citrix > Access Gateway > Server Configuration



Citrix Access Gateway Server Configuration

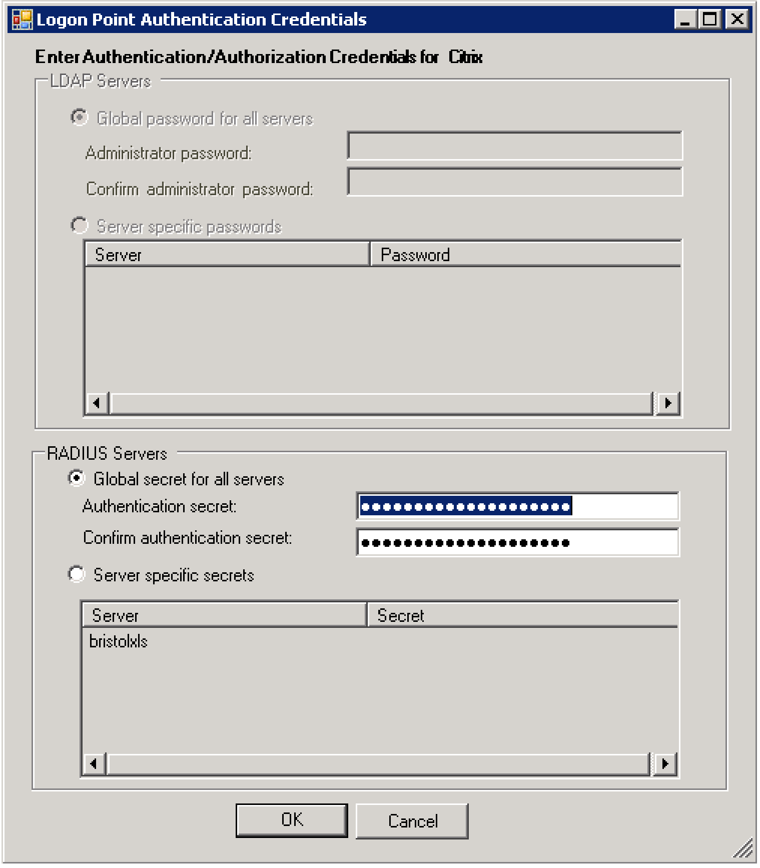
Tasks:
- Service Account
- Server Farm Information
- Configured Logon Points
- Authentication Server De
- Services

Configured Logon Points

When you deploy, remove, or rename logon points, the logon point folders in virtual directory \CitrixLogonPoint are deployed, removed, or renamed. You provide users with URLs to access these folders so that they log on using a specific logon point.

Logon Point	Status
Citrix	✓ The folder is deployed to the Web site.

13. Highlight the logon point name and click on Authentication Credentials



Logon Point Authentication Credentials

Enter Authentication/Authorization Credentials for Citrix

LDAP Servers

○ Global password for all servers

Administrator password:

Confirm administrator password:

○ Server specific passwords

Server	Password

RADIUS Servers

● Global secret for all servers

Authentication secret: ••••••••••••••••••••

Confirm authentication secret: ••••••••••••••••••••

○ Server specific secrets

Server	Secret
bristolxls	

14. Enter a Global secret for all servers (ensuring to use only numbers or upper and lower case letters in the password)
15. Click OK to close the Logon Point Authentication Credentials dialogue box
16. Click OK to close the Access Gateway Server Configuration dialogue box

Modifying the Logon Page Secondary Authentication Text

In order to modify the secondary authentication prompt from reading “RADIUS Password” to a more user friendly piece of text like “PIN” or “SMS Passcode” modify the following:

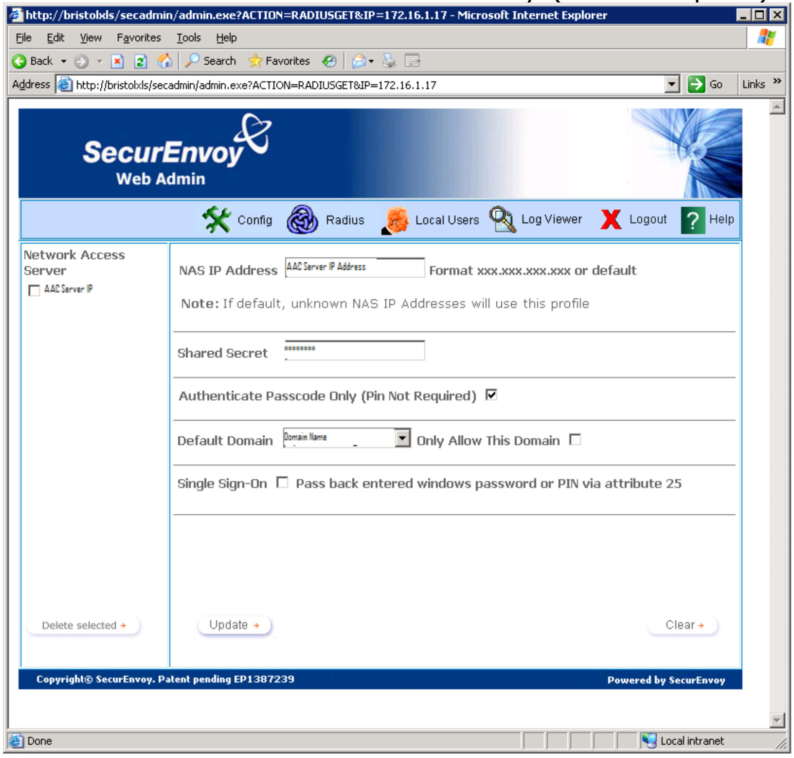
1. In Windows Explorer, navigate to the logon point’s virtual directory. For example, C:\inetpub\wwwroot\CitrixLogonPoint\logonpointname, where logonpointname is the name of the logon point.
2. Open the web.config file in a text editor and add the following line to the appSettings section:
   <add key="SecondaryAuthenticationPromptOverride" value="PIN:" />
3. Repeat steps 1-2 for all logon points you want to modify

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.

1. Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.
2. Click the **“Radius”** Button
3. Enter IP address and Shared secret for each Advanced Access Control server that wishes to use **SecurEnvoy** Two-Factor authentication. (Note this is not the Citrix Access Gateway Appliance IP address)
4. Make sure the “Authenticate Passcode Only (Pin not required) checkbox is ticked.



http://bristolxls/secadmin/admin.exe?ACTION=RADIUSGET&IP=172.16.1.17 - Microsoft Internet Explorer

Address http://bristolxls/secadmin/admin.exe?ACTION=RADIUSGET&IP=172.16.1.17

Network Access Server
□ AAC Server IP

NAS IP Address AAC Server IP Address Format xxx.xxx.xxx.xxx or default

Note: If default, unknown NAS IP Addresses will use this profile

Shared Secret ********

Authenticate Passcode Only (Pin Not Required) ☑

Default Domain Domain Name Only Allow This Domain □

Single Sign-On □ Pass back entered windows password or PIN via attribute 25

Copyright© SecurEnvoy. Patent pending EP1387239

Powered by SecurEnvoy

5. Press Update
6. Now Logout

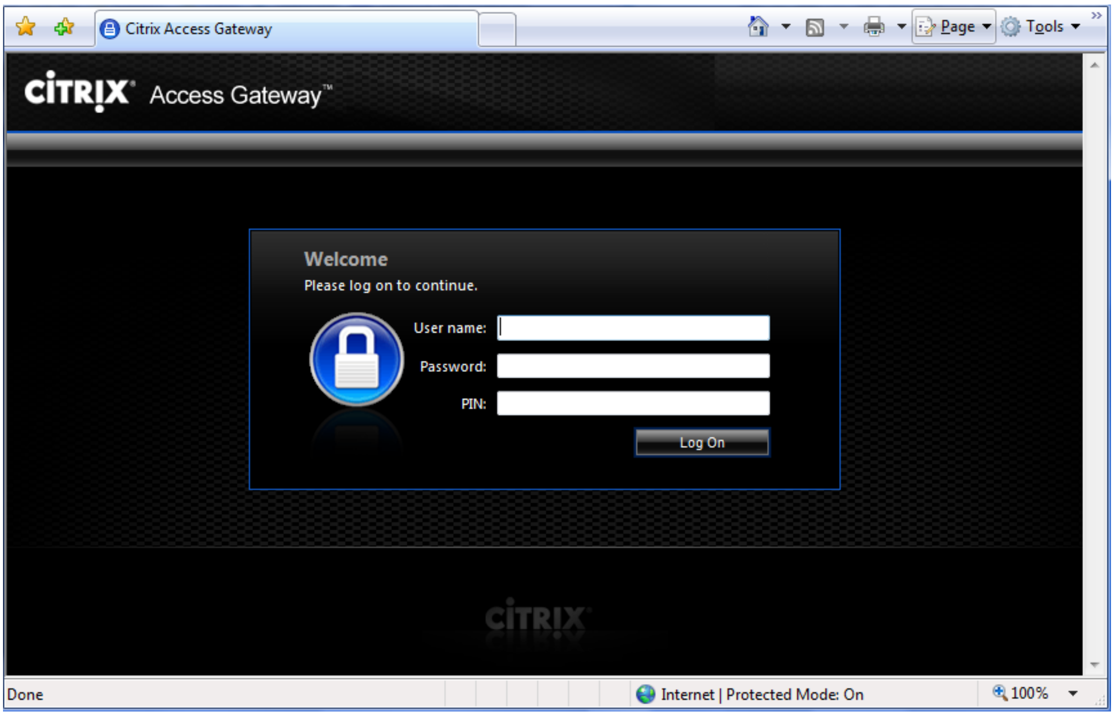
Test Logon

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 PIN box



Citrix Access Gateway

CITRIX Access Gateway™

Welcome

Please log on to continue.

User name:

Password:

PIN:

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.