External authentication with Citrix Net Scaler (Access Gateway Enterprise) using iPad 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	

© 2011 SecurEnvoy Ltd. All rights reserved Confidential

Citrix Net Scaler (Radius) Integration Guide

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

The Citrix Net Scaler provides - Secure Remote Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Citrix Net Scale series), 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 onetime 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 Net Scaler (Access Gateway Enterprise) ver. 9.x

SecurEnvoy
Windows 2008 server R2 64bit
IIS installed with SSL certificate (required for remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v5.3.501

© 2011 SecurEnvoy Ltd. All rights reserved

Index

1.0 Pre Requisites 3
2.0 Configuration of Citrix using RADIUS 4
3.0 Configuration of SecurEnvoy 6
4.0 Configuration of Citrix Receiver 7
5.0 Test Logon – iPhone User Experience 8
6.0 Support for Web based and iPhone users on same Citrix Server 9

1.0 Pre Requisites

It is assumed that the Citrix Net Scaler *is setup and operational. An existing Domain user can authenticate using a Domain password and access applications, your users can access through SSL using Domain accounts.*

Securenvoy Security Server has a suitable account created that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Citrix server, additional open ports will be required.
NOTE: *SecurEnvoy requires LDAP connectivity either over port 389 or 636 to the Active Directory servers and port 1645 or 1812 for RADIUS communication from the Citrix® Net Scaler (Access Gateway).*

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

© 2011 SecurEnvoy Ltd. All rights reserved

2.0 Configuration of Citrix using RADIUS

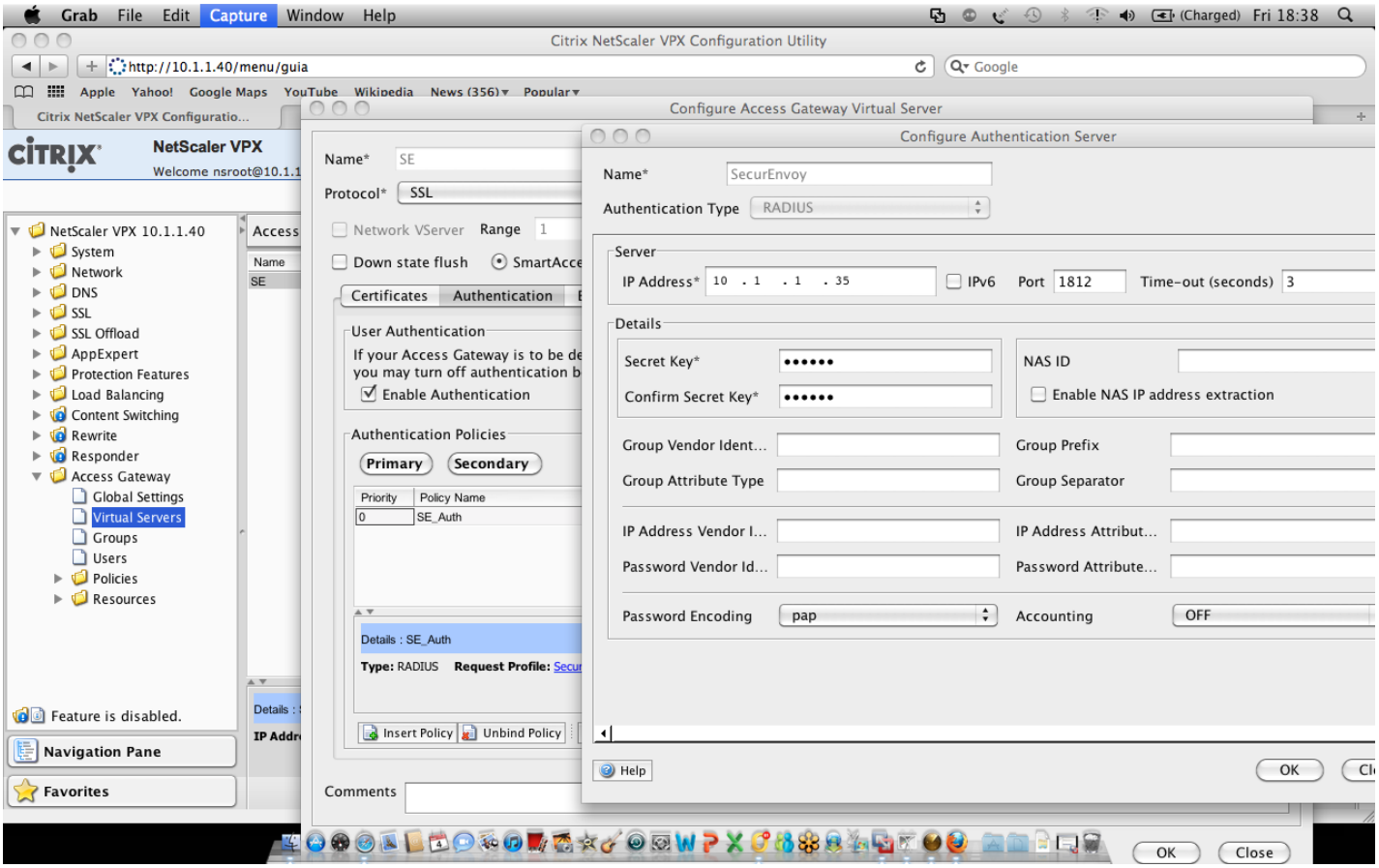
This document describes how to configure Access Gateway Enterprise to use RADIUS authentication as the secondary authentication, and LDAP as primary for the iPhone, iPad, and Android devices.

In the **Access Gateway Configuration Utility**, navigate to **Access Gateway, Virtual Servers and then select the Authentication tab**

1. Locate your existing LDAP policy for Microsoft Domain authentication and then select the "Secondary" button under authentication policies.

2. Create an authentication policy for SecurEnvoy and then select "Configure Authentication server" and set up for authentication type "RADIUS", assign the IP address for the SecurEnvoy server and enter the "pre shared secret".
3. Set the "Password encoding" to PAP.

Click OK when complete.

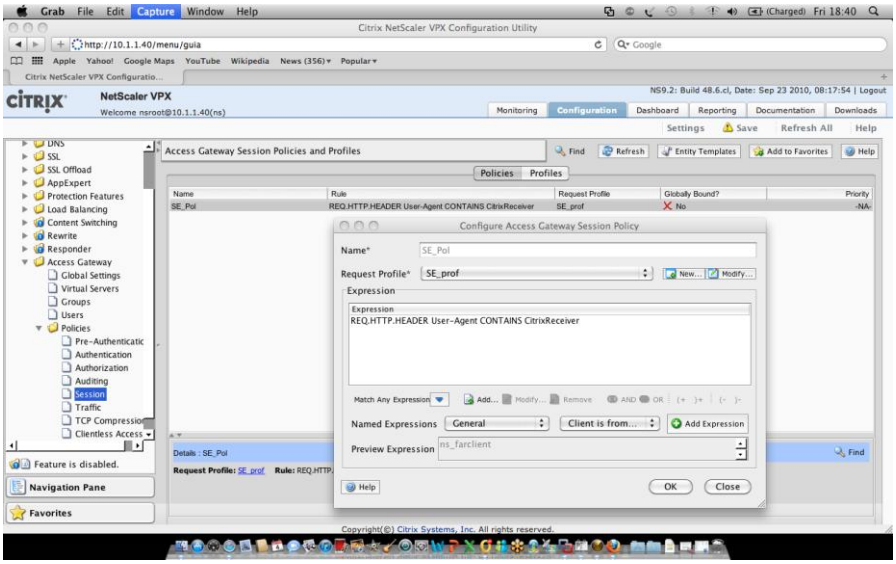


Once completed a session policy must be created.

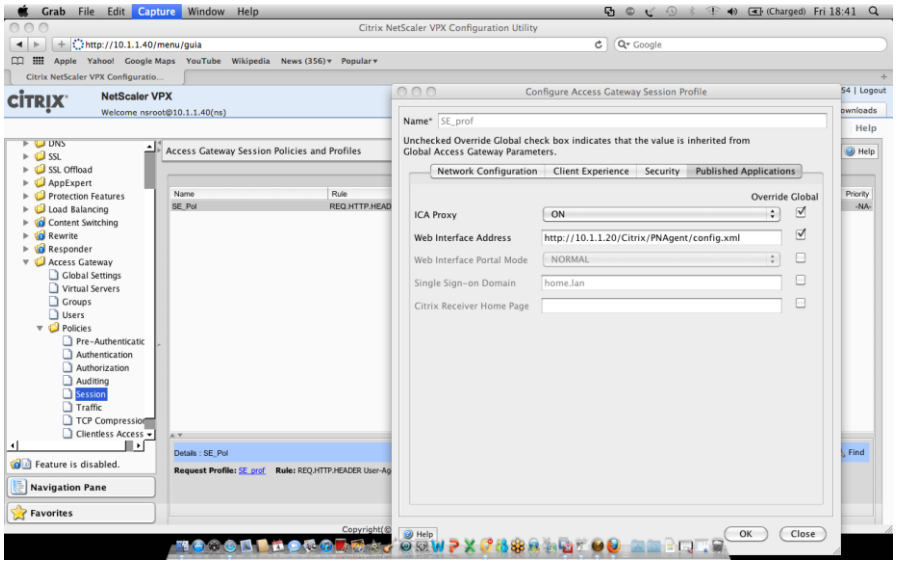
In the **Access Gateway Configuration Utility**, navigate to **Access Gateway, Policies, session.**

Create a session policy for the Mobile Devices. To bind this policy to only mobile devices, use the following expression: REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver

Point this session policy to use the SecurEnvoy radius profile (Previously created)



Once completed, navigate to "session profile", populate "Published applications" and enter the path for PNAgent directory.



Click Ok when complete

© 2011 SecurEnvoy Ltd. All rights reserved

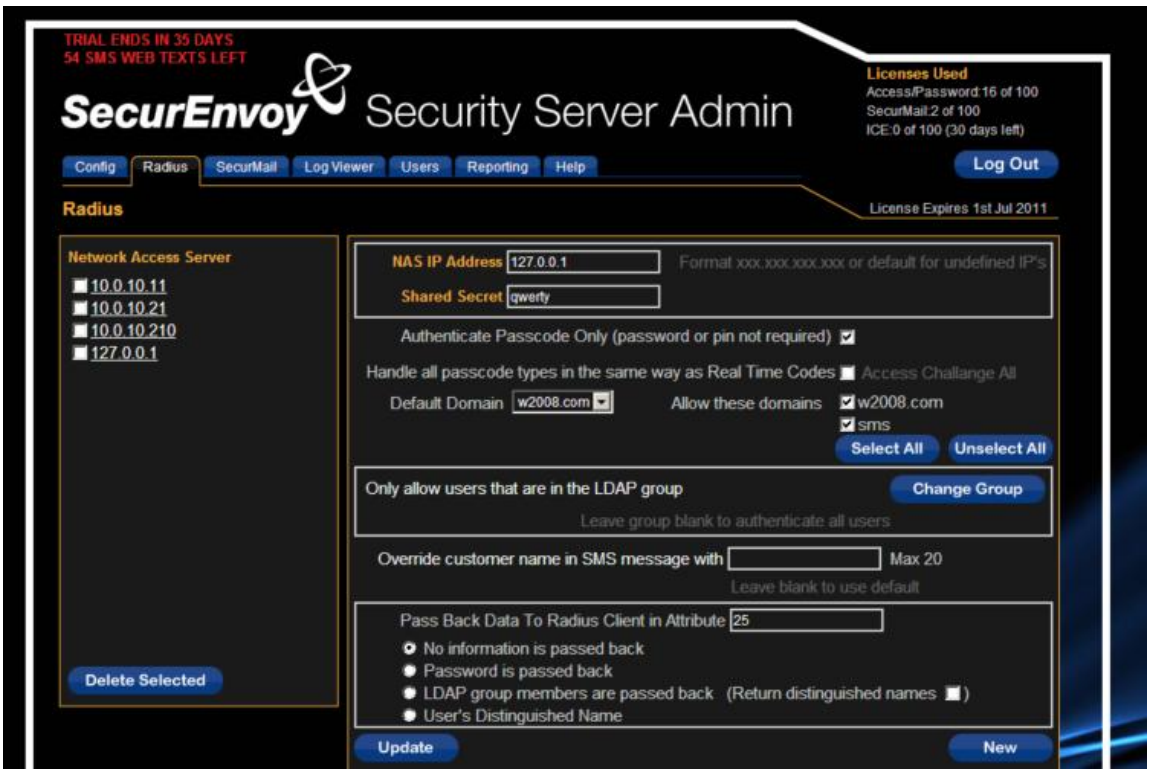
3.0 Configuration of SecurEnvoy

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.

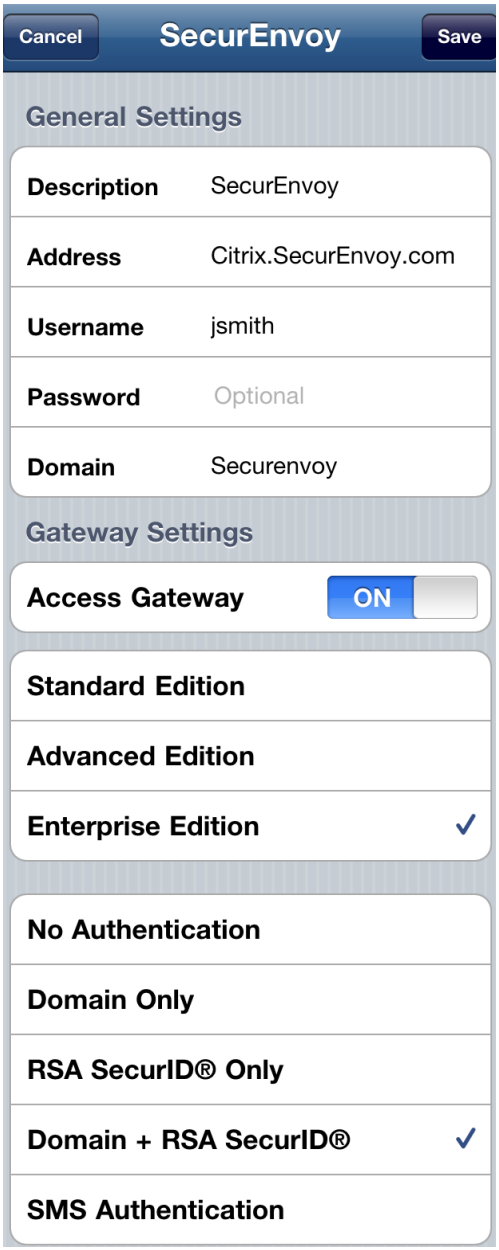
1. Click the **"Radius"** Button
2. Enter IP address and Shared secret for each Citrix Web Interface server that wishes to use **SecurEnvoy** Two-Factor authentication.
3. Make sure the "Authenticate Passcode Only (Pin not required) checkbox is ticked.



4. Select the domains that can authenticate from this Radius profile
5. Press Update
6. Now Logout

© 2011 SecurEnvoy Ltd. All rights reserved

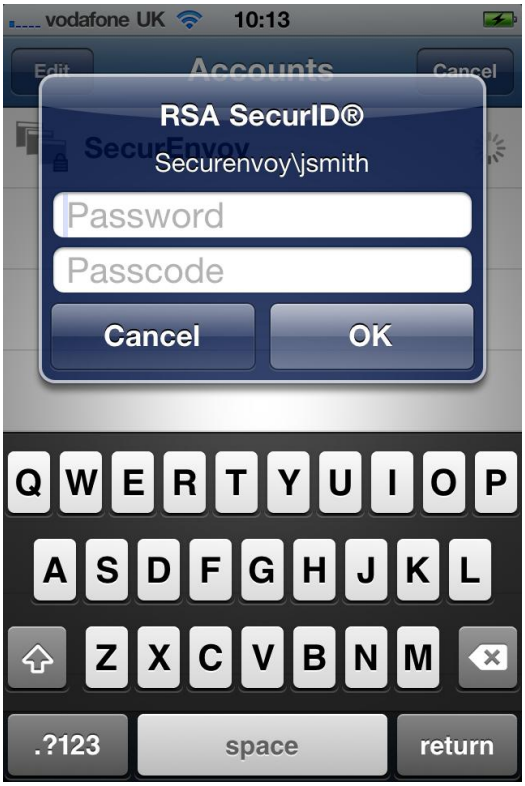
4.0 Configuration of Citrix Receiver



1. Download and install the Citrix receiver application from Apples App Store.
2. Add a new entry
3. Create a description for this entry
4. Add the web address of the Citrix server (WI)
5. Enter UserID
6. Enter Domain
7. Select Access Gateway ON
8. Select Enterprise Edition
9. Select Domain + RSA
10. Save settings

© 2011 SecurEnvoy Ltd. All rights reserved

5.0 Test Logon – iPhone User Experience



Launch Citrix Receiver application.

Select previously created entry.

User is then prompted for their Domain password and Passcode

Click Ok when complete.

User is then presented with their applications.

© 2011 SecurEnvoy Ltd. All rights reserved

6.0 Support for Web based and iPhone users on same Citrix Server

Additional configuration steps:

To facilitate supporting both PC browser based web sessions and iPhone user, the following configuration steps are required. This will allow the Netscaler to detect the presence of the Citrix receiver in the Host Header request and then direct the web request to either the Citrix Web Interface (WI) or the PNAgent virtual directory.

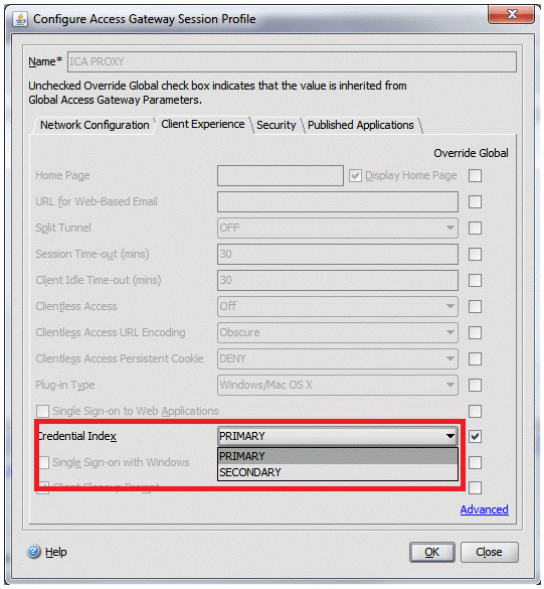
Please see Citrix support document http://support.citrix.com/article/CTX125364 for more information.

1. In the **Access Gateway Configuration Utility**, go to **Access Gateway, Policies, Authentication** and create an authentication policy for LDAP and SecurEnvoy RADIUS for mobile devices and non-mobile devices. This is necessary to avoid a logic condition that could allow users to bypass the RADIUS Authentication.
2. Create an LDAP policy for the **Mobile Devices**. To bind this policy to only mobile devices, use the following expression:
   REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver:
3. Create a SecurEnvoy RADIUS Mobile policy for the **Mobile Devices**. To bind this policy to only mobile devices, use the expression below:
   REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver:

4. Create an LDAP policy for **Non-Mobile devices**. To bind this policy to only non-mobile devices, use the expression that follows:
   REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver:
5. Create a SecurEnvoy RADIUS Non-Mobile policy for **Non-Mobile devices**. To bind this policy to only non-mobile devices, use the following expression:
   REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver

6. Go to the properties of your Access Gateway Virtual Server and go to the **Authentication** tab. On the **Primary** Authentication Policies, add the SecurEnvoy RADIUS policy as top priority and the LDAP_NonMobile policy as secondary priority:

7. On the **Secondary** Authentication Policies, add the LDAP_Mobile Policy as top priority, followed by the SecurEnvoy Radius Non-Mobile Policy.



Important: The session policy given must have the correct single sign-on credential index, meaning, it must be the LDAP credentials. Because of this, you might use the same policy expression on the session policy associated with non-mobile devices (REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver).

© 2011 SecurEnvoy Ltd. All rights reserved

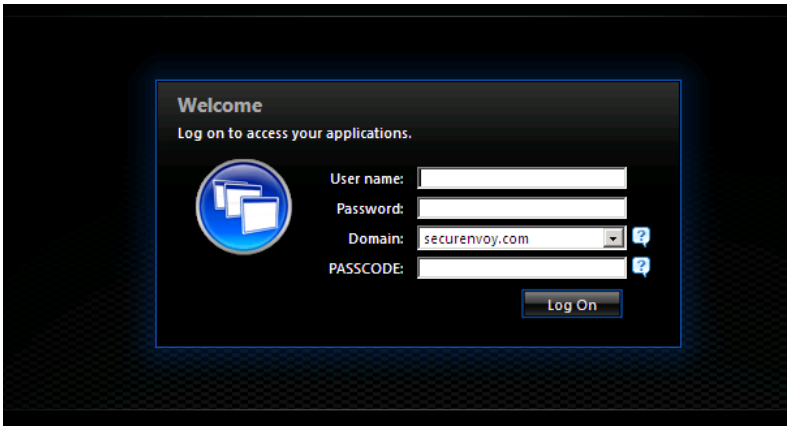
Navigate to the Citrix Logon page.

Default will be https://ls1.securenvoy.com/Citrix/Xenapp , where ls1.securenvoy.com is the server used for this guide.

Three or four input boxes will be displayed; this is a Citrix configuration setting.

User will enter: UserID in the User name box
Domain password in Password box
Select Domain
Enter 6 digit Passcode received via SMS in Passcode box

Click logon to complete the process.
If using SMS, a new SMS passcode will be sent to the user's mobile phone, ready for the next authentication.
If using the SecurEnvoy or Google soft token, the passcode is automatically refreshed every 30 seconds.



© 2011 SecurEnvoy Ltd. All rights reserved