External Authentication with Citrix Net Scaler (Access Gateway Enterprise)

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House Brunel Road Theale Berkshire United Kingdom RG7 4AB	

Citrix Net Scaler (Radius) Integration Guide

© 2011 SecurEnvoy Ltd. All rights reserved

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 Test Login 7

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

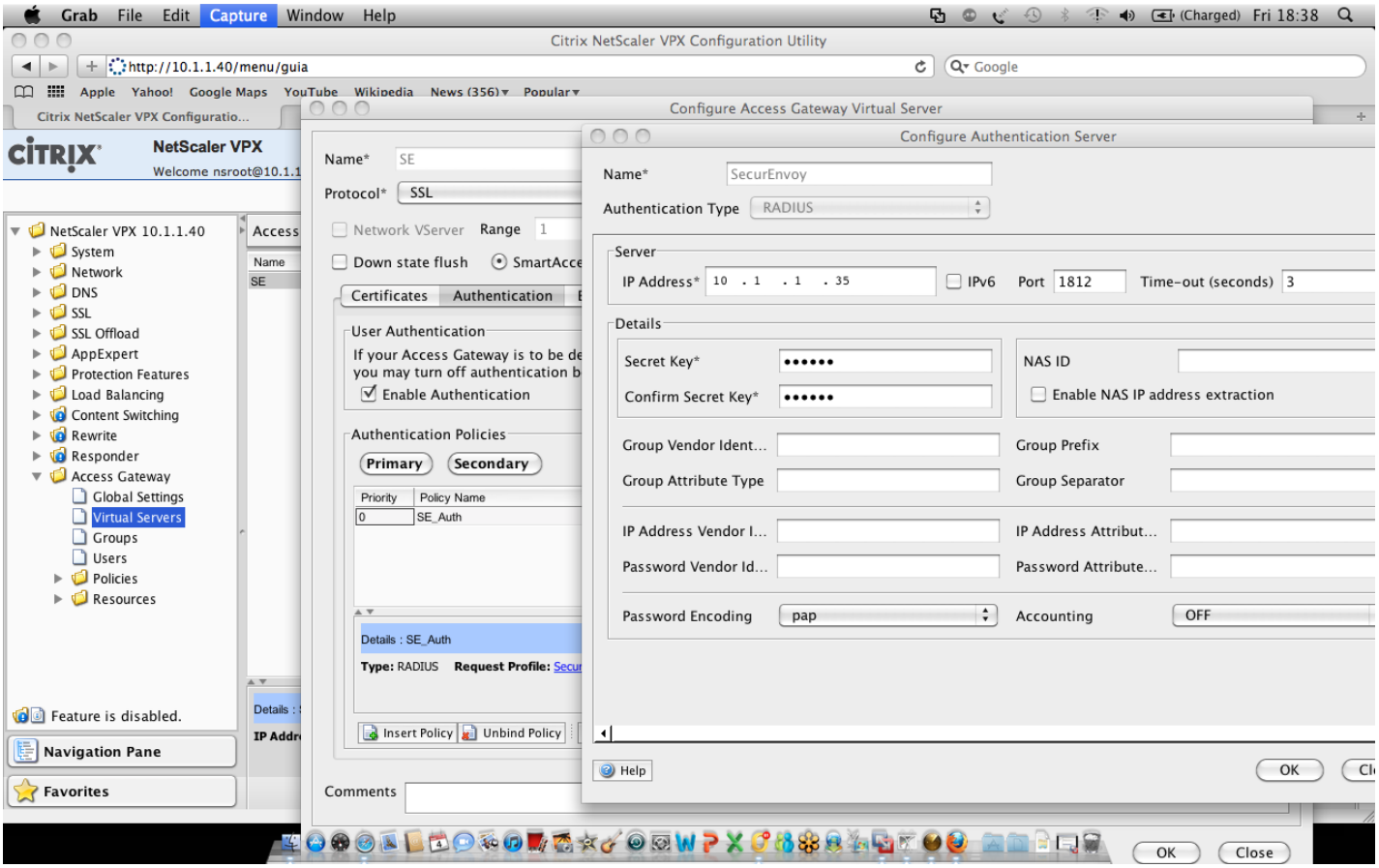
This document describes how to configure Access Gateway Enterprise to use RADIUS authentication as the secondary authentication, and LDAP as primary for the iPhone, iPad, and Android devices.

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

1. Locate your existing policy and disable it.

2. Create a new 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.

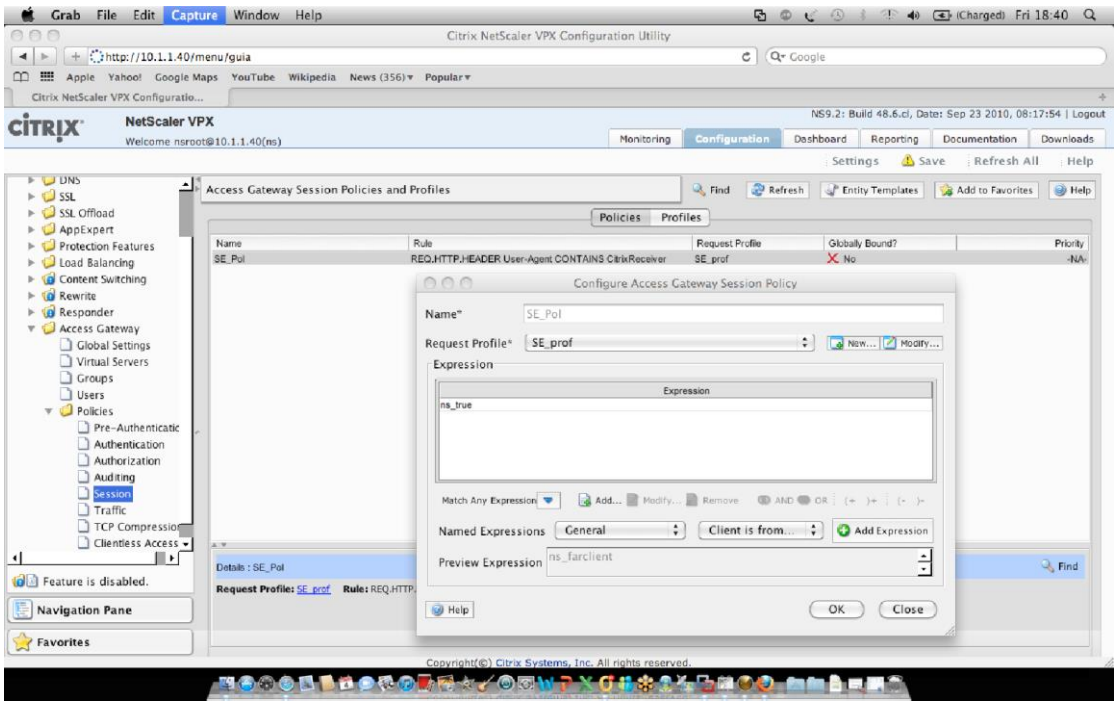


Once completed a session policy must be created.

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

Create a session policy. To bind this policy to all devices use the following expression: ns_true

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



Click Ok when complete

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 Netscaler that wishes to use **SecurEnvoy** Two-Factor authentication.
3. Make sure the "Authenticate Passcode Only (Pin not required) checkbox is NOT checked.
4. Check the box "Handle all passcode types in the same way as Real Time Codes" (If you are using SecurEnvoy PIN's and require users to enter their PIN+6 digit code then uncheck this box)



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

© 2011 SecurEnvoy Ltd. All rights reserved

4.0 Test Login

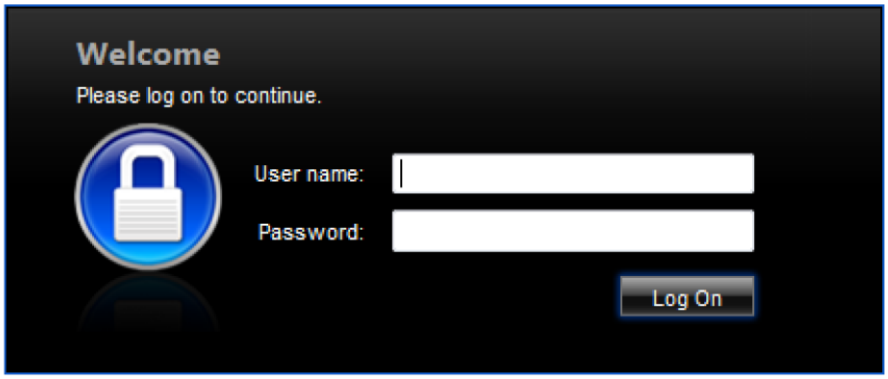
Navigate to the Citrix Logon page.

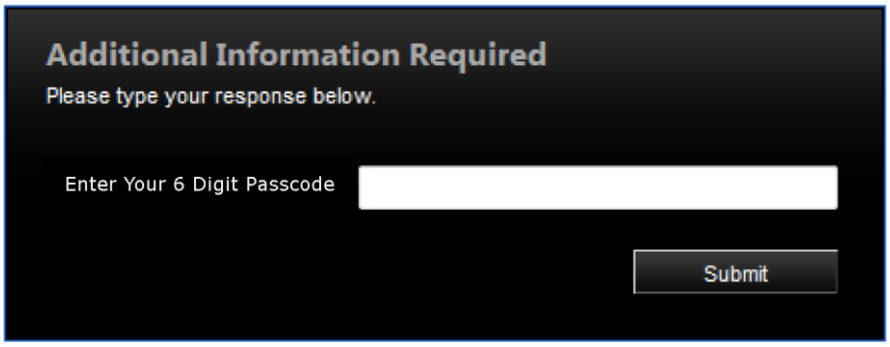
Default will be https://ls1.securenvoy.com/Citrix/Xenapp , where ls1.securenvoy.com is the server used for this guide.

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 (or PIN if SecurEnvoy PIN's are configured on the server)

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





© 2011 SecurEnvoy Ltd. All rights reserved