External Authentication with Citrix NetScaler

(Access Gateway Enterprise)

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House Brunel Road Theale Reading RG7 4AB	
Tony Davis	tdavis@securenvoy.com	
Nick Walter	nick.walter@topologyconsulting.com	

Citrix NetScaler (Radius) Integration Guide

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

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

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Citrix NetScaler 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 one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into any LDAP server 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 in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing LDAP password. Utilising the LDAP password as the PIN, allows the User to enter their UserID, Domain 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 Juniper SA. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Citrix
Citrix NetScaler (Access Gateway Enterprise) ver. 10.x

SecurEnvoy

Windows 2012 R2 Server
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 v7.2.505

© 2014 SecurEnvoy Ltd. All rights reserved

Index

1.0 Prerequisites 3
1.1 Configuration of Citrix using RADIUS 4
1.2 Configuration of OneSwipe (optional) 5
1.3 Configuration of SecurEnvoy 6
2.0 Test Logon 8
2.1 Test OneSwipe Logon 8
3.0 Notes 10

1.0 Prerequisites

It is assumed that the Citrix NetScaler has been installed and is authenticating users 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 Routing and Remote Access server(s), additional open ports will be required.

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

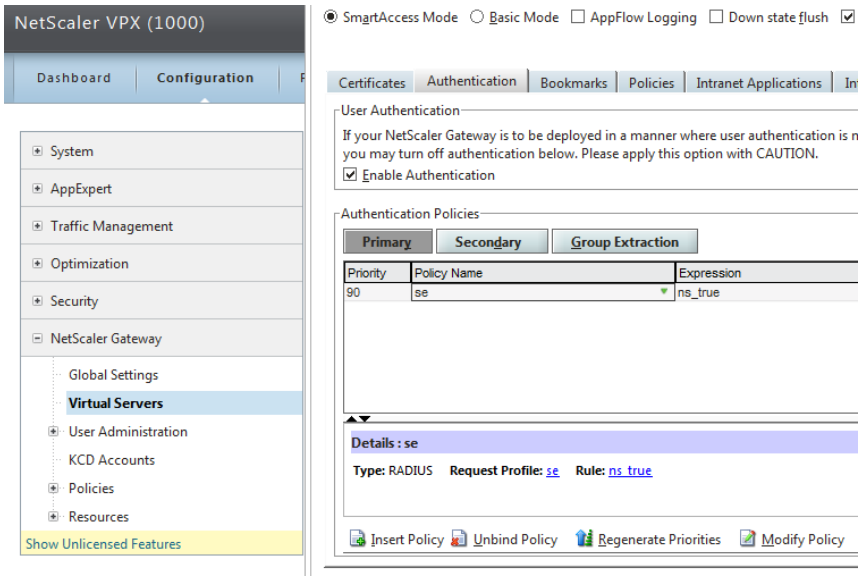
The following table shows what token types are supported.

Token Type Supported	
Real Time SMS or Email	✓
Preload SMS or Email	✓
Soft Token Code	✓
Soft Token Next Code	✓
Voice Call	✓
One Swipe	✓

© 2014 SecurEnvoy Ltd. All rights reserved

1.1 Configuration of Citrix using RADIUS

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

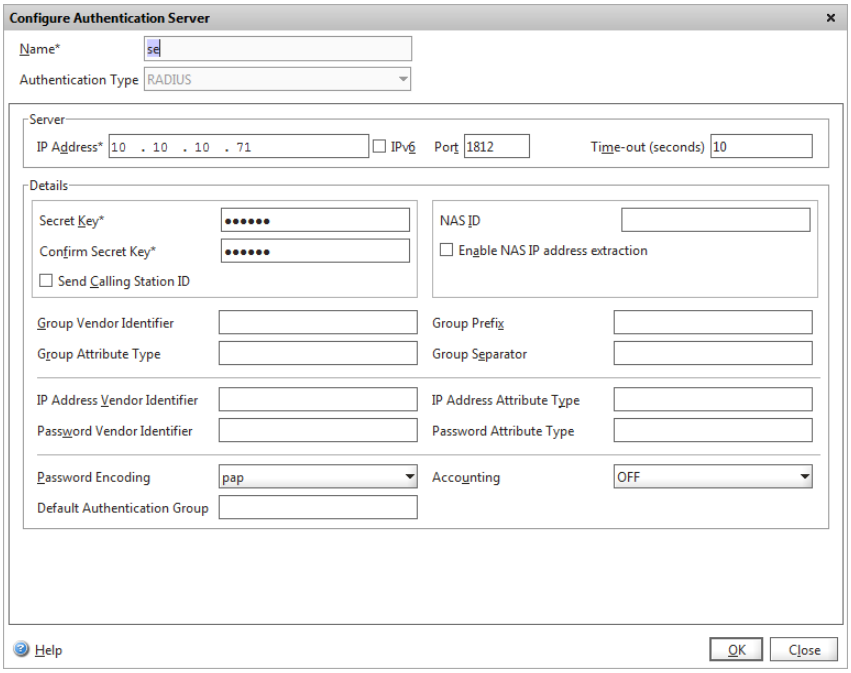


Locate your existing policy and disable it.

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".

Set the "Password encoding" to PAP.

Click OK when complete.



© 2014 SecurEnvoy Ltd. All rights reserved

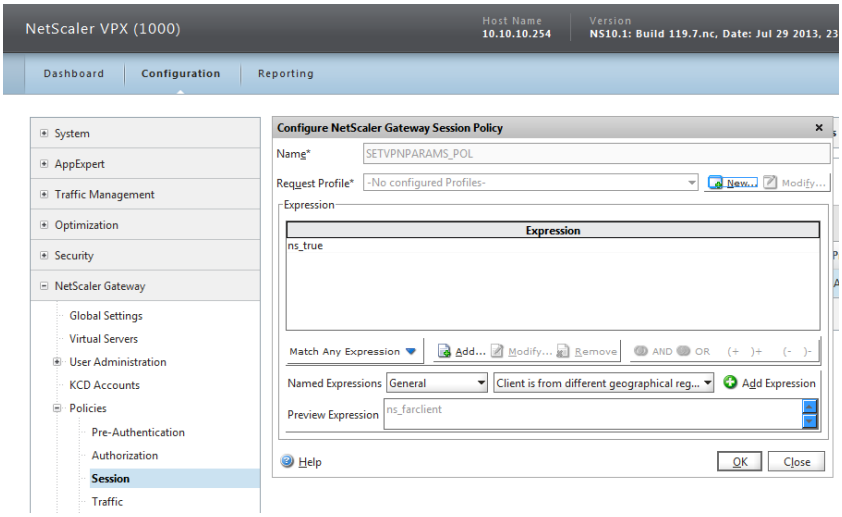
Once completed, a session policy must be created.

In the "Netscaler Gateway" Configuration Utility, navigate to "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



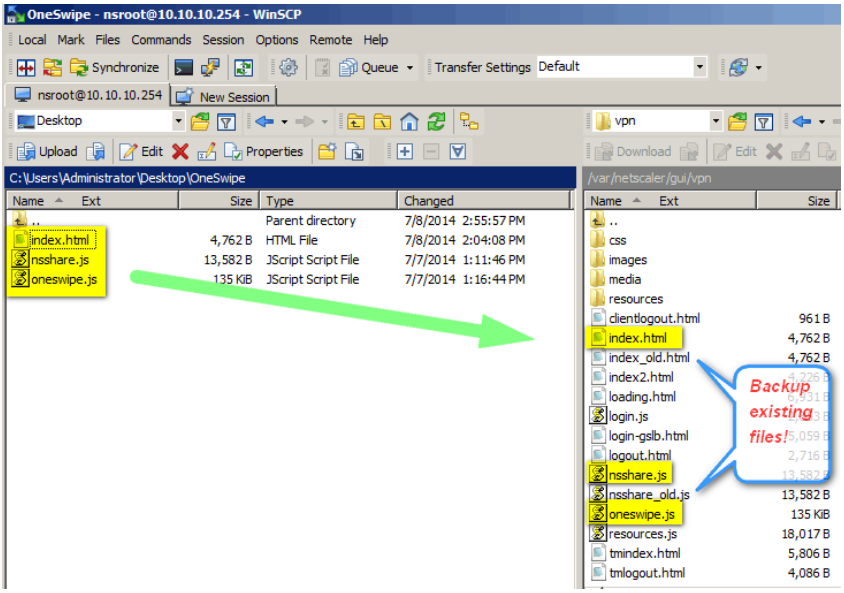
1.2 Configuration of OneSwipe (optional)

Using an SSH client, log into the NetScaler. In this example I have used WinSCP.

Download OneSwipe.zip: https://www.dropbox.com/s/bah8c8avamgb6at/OneSwipe.zip

Unpack and copy files across to the NetScaler "/var/netscaler/gui/vpn" directory.

Ensure you backup index.html and nsshare.js



Note

To prevent customizations to the Citrix NetScaler from being lost after a reboot, the following guide will help retain the changes made http://support.citrix.com/article/CTX122271

© 2014 SecurEnvoy Ltd. All rights reserved

1.3 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can be set up to use the existing Windows password as the PIN component. 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.

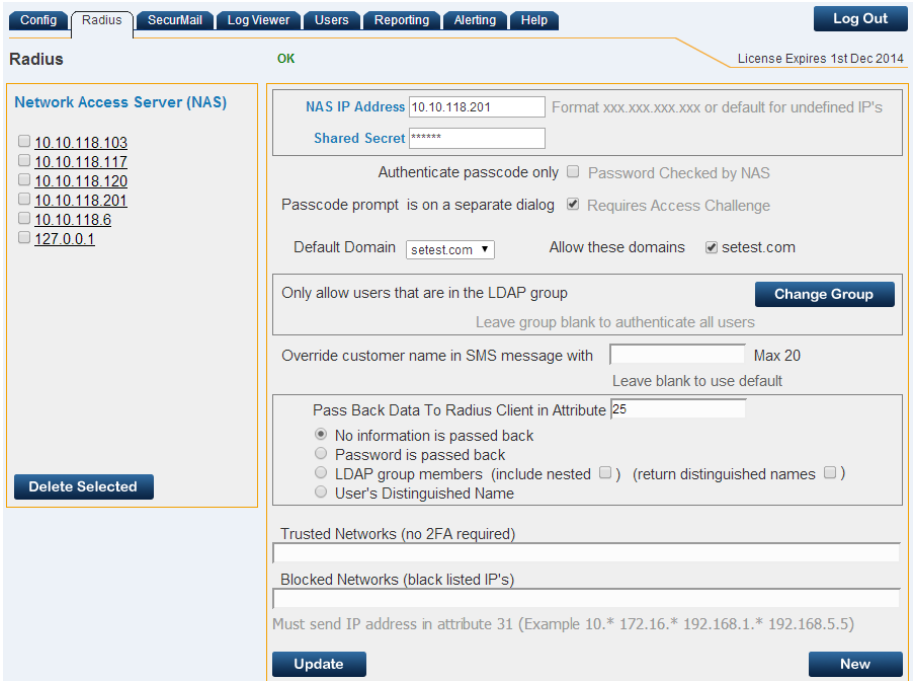
Click the **"Radius"** tab

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

Click checkbox "Passcode prompt is on a separate dialog".

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

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

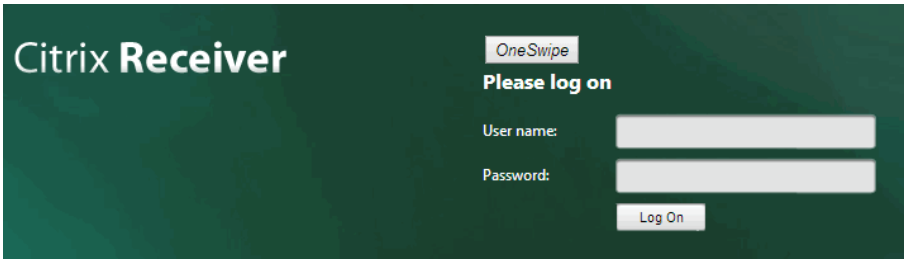


© 2014 SecurEnvoy Ltd. All rights reserved

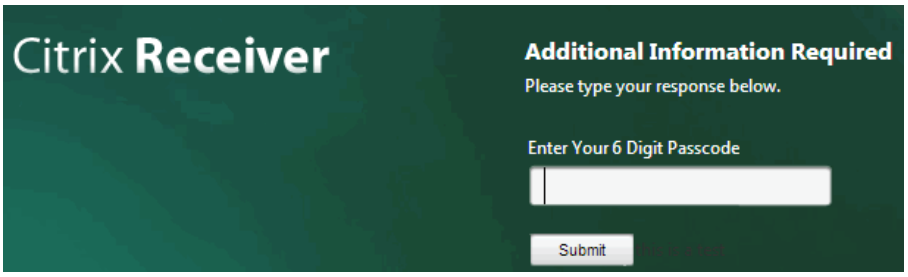
2.0 Test Logon

Browse to the web URL address of the Citrix NetScaler appliance.

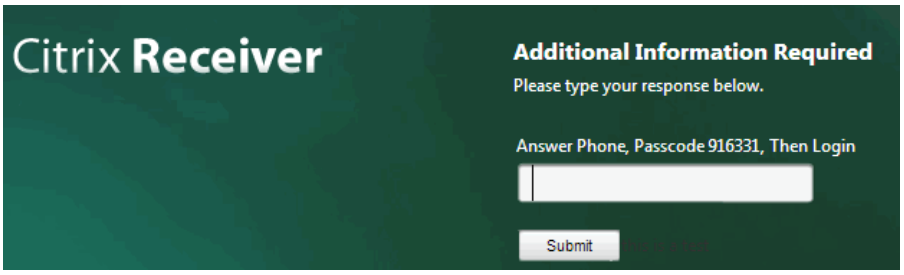
Enter UserID and password:



Pre load, Realtime and Soft tokens:

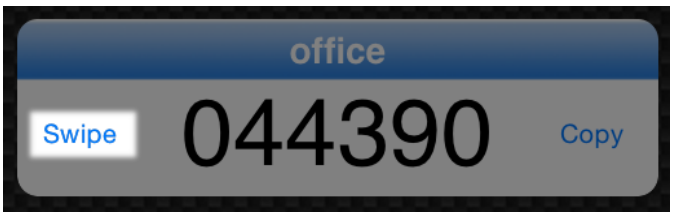


VOICE tokens:

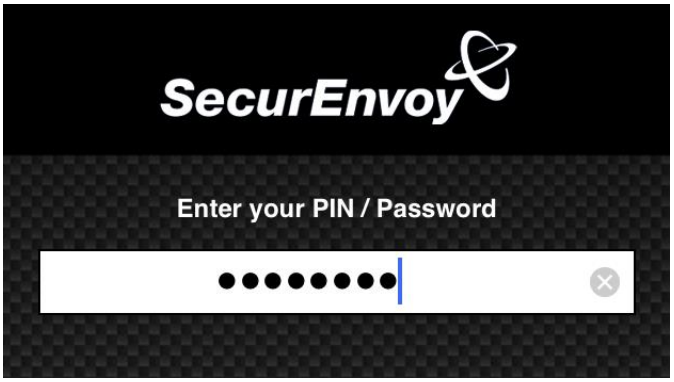


2.1 Test OneSwipe Logon

Select 'Swipe' from the phone Soft Token

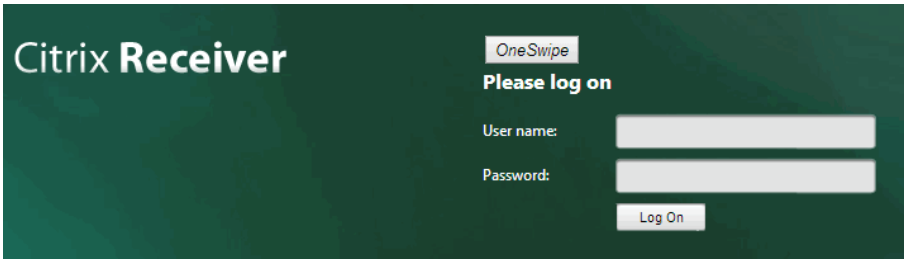


Enter your PIN / Password into the PIN / Password field and click 'Done'.

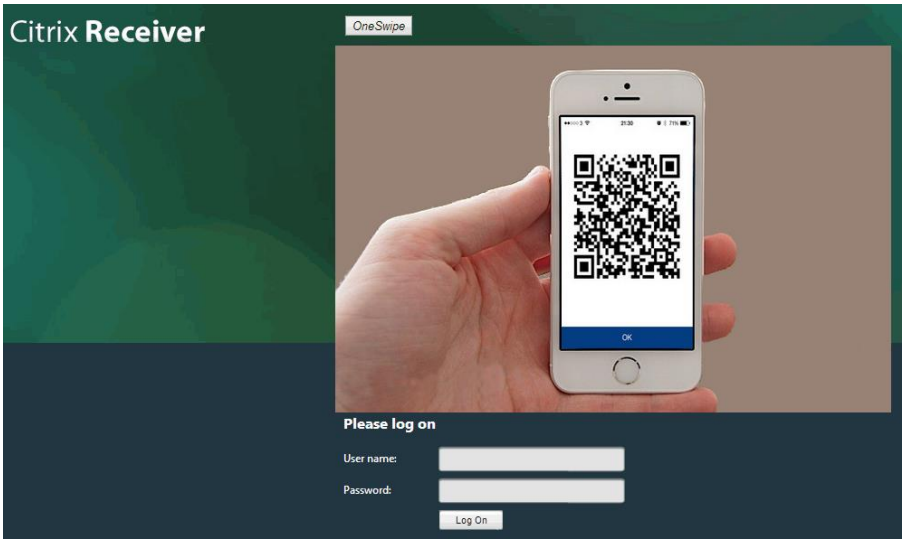


© 2014 SecurEnvoy Ltd. All rights reserved

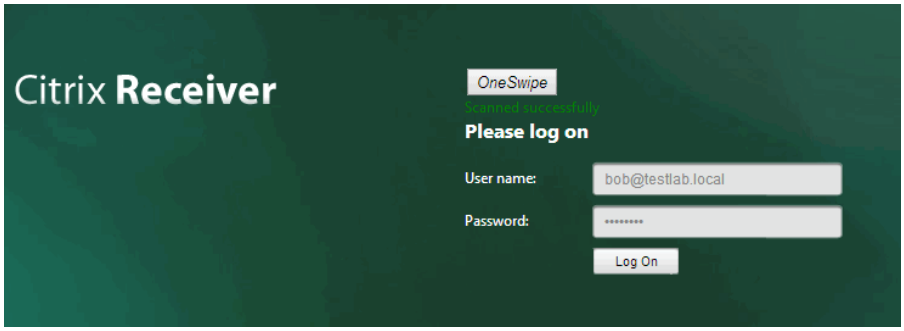
Click the OneSwipe button



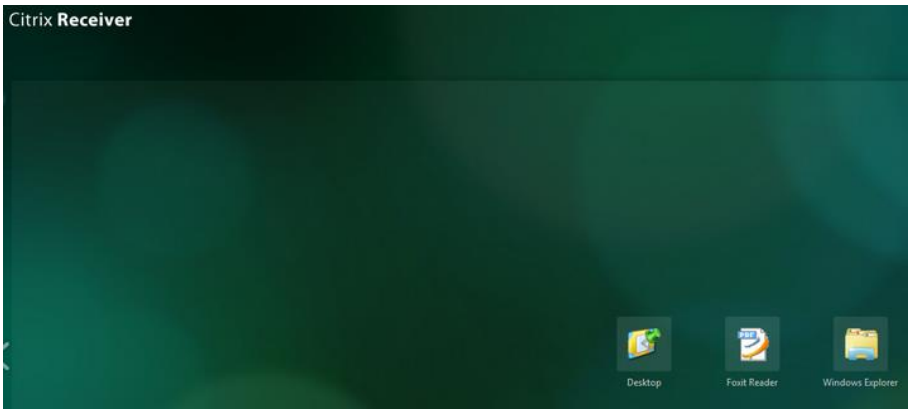
Your webcam is now activated & you will be able to present the QRCode on your phone.



UserID, password and passcode are passed to the Citrix NetScaler authentication page and user successfully logs in.



User is presented with Citrix Web Interface



© 2014 SecurEnvoy Ltd. All rights reserved

3.0 Notes

© 2014 SecurEnvoy Ltd. All rights reserved