



**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	
Andy Kemshall	akemshall@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 seamless 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 v8.1

Index

1.0 Prerequisites	3
1.1 Configuration of Citrix using RADIUS	4
1.2 Configuration of SecurEnvoy.....	6
2.0 Test OneSwipe Logon.....	7
3.0 Notes	9

1.0 Prerequisites

It is assumed that the Citrix Net Scaler 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.

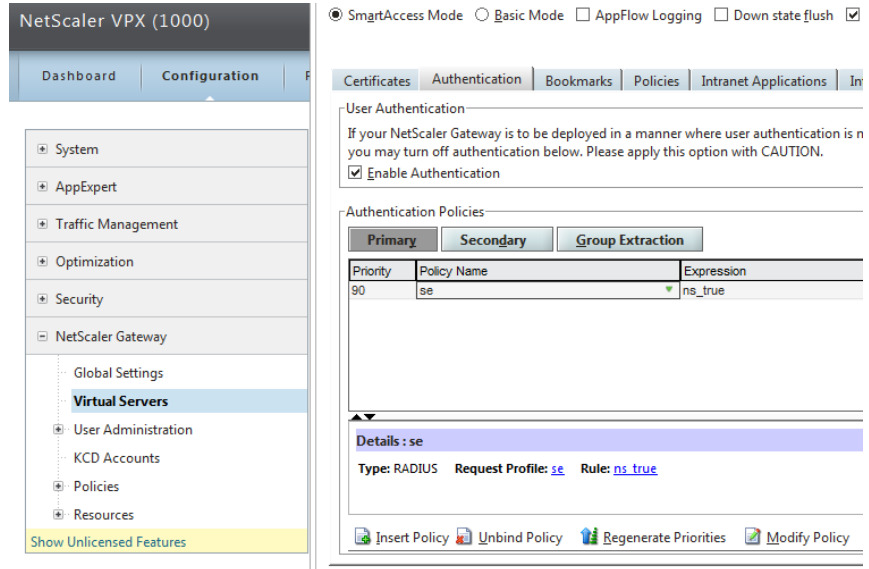
NOTE: Add radius profiles for each Citrix server that requires Two-Factor Authentication.

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 Push	✓
One Swipe QRCode	X

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



NetScaler VPX (1000)

Dashboard Configuration

- System
- AppExpert
- Traffic Management
- Optimization
- Security
- NetScaler Gateway
 - Global Settings
 - Virtual Servers**
 - User Administration
 - KCD Accounts
 - Policies
 - Resources

Show Unlicensed Features

SmartAccess Mode Basic Mode AppFlow Logging Down state flush

Certificates Authentication **Bookmarks** Policies Intranet Applications In

User Authentication

If your NetScaler Gateway is to be deployed in a manner where user authentication is you may turn off authentication below. Please apply this option with CAUTION.

Enable Authentication

Authentication Policies

Primary Secondary **Group Extraction**

Priority	Policy Name	Expression
90	se	ns_true

Details : se

Type: RADIUS Request Profile: se Rule: ns_true

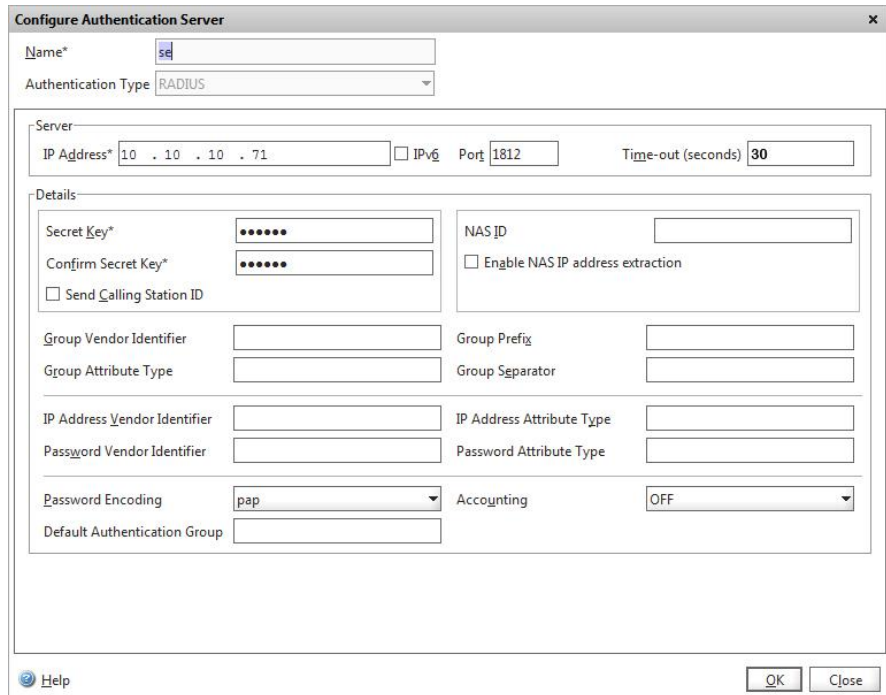
Insert Policy Unbind Policy Regenerate Priorities Modify Policy

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 Time-out to 30 seconds.

Set the "Password encoding" to PAP.

Click OK when complete.



Configure Authentication Server

Name* se

Authentication Type RADIUS

Server

IP Address* 10 . 10 . 10 . 71 IPv6 Port 1812 Time-out (seconds) 30

Details

Secret Key* NAS ID

Confirm Secret Key* Enable NAS IP address extraction

Send Calling Station ID

Group Vendor Identifier Group Prefix

Group Attribute Type Group Separator

IP Address Vendor Identifier IP Address Attribute Type

Password Vendor Identifier Password Attribute Type

Password Encoding pap Accounting OFF

Default Authentication Group

Help OK Close

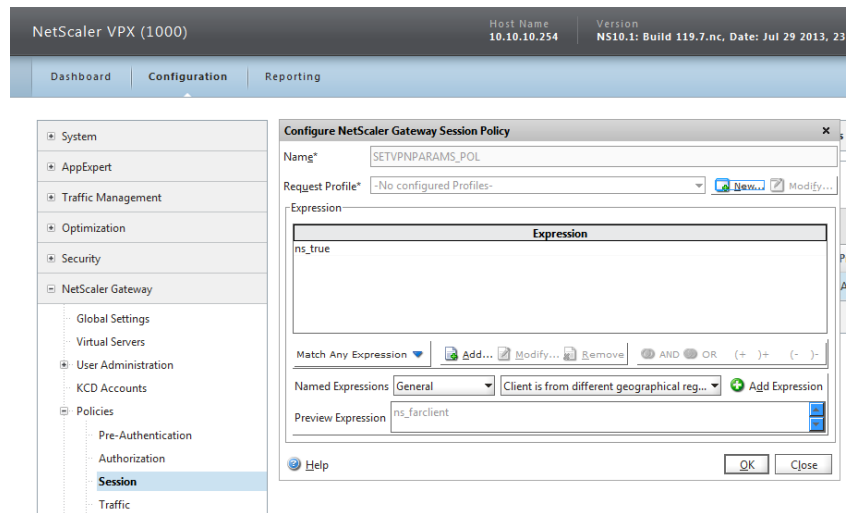
Once completed, a session policy must be created.

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 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.

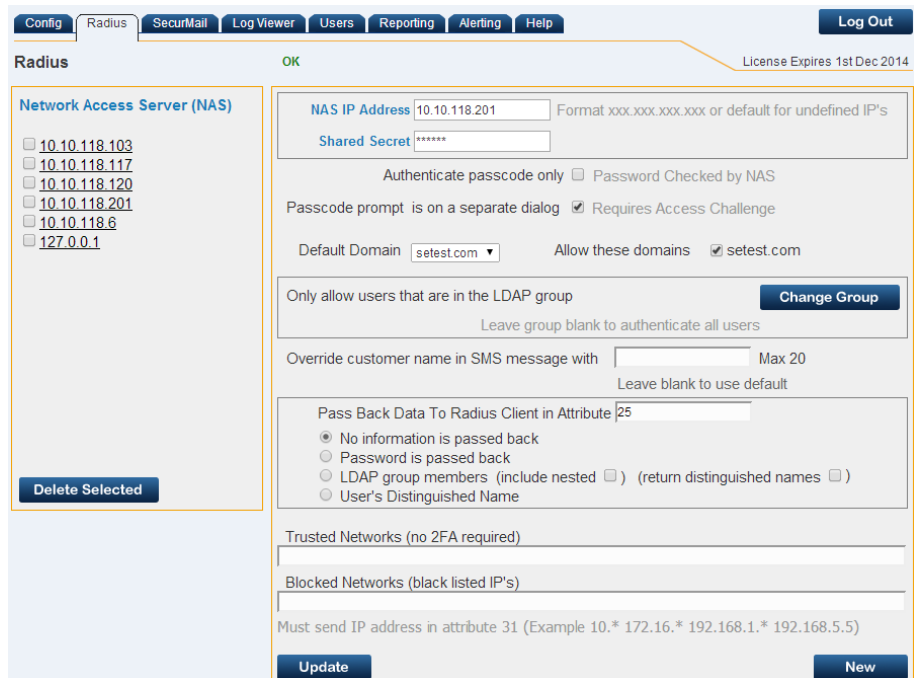
Click the **"Radius"** tab

Enter IP address and Shared secret for each Juniper SA 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.



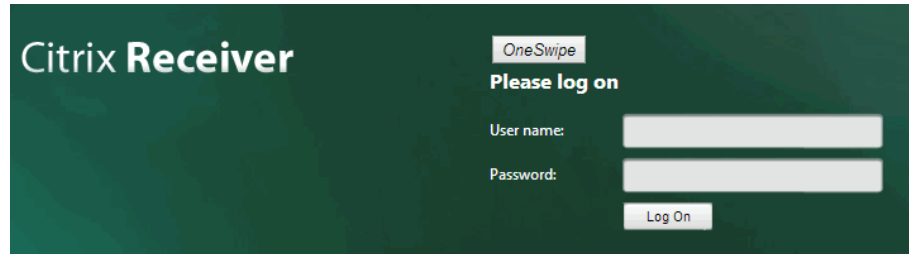
The screenshot shows the SecurEnvoy administration interface for configuring Radius. The 'Radius' tab is active. On the left, under 'Network Access Server (NAS)', there is a list of IP addresses with checkboxes: 10.10.118.103, 10.10.118.117, 10.10.118.120, 10.10.118.201, 10.10.118.6, and 127.0.0.1. A 'Delete Selected' button is below the list. The main configuration area on the right includes:

- NAS IP Address: 10.10.118.201 (Format: xxx.xxx.xxx.xxx or default for undefined IP's)
- Shared Secret: *****
- Authentication options: Authenticate passcode only, Password Checked by NAS
- Passcode prompt: is on a separate dialog, Requires Access Challenge
- Default Domain: setest.com (dropdown), Allow these domains: setest.com
- Only allow users that are in the LDAP group (Change Group button), Leave group blank to authenticate all users
- Override customer name in SMS message with: [] Max 20, Leave blank to use default
- Pass Back Data To Radius Client in Attribute: 25
- Options for data passing back:
 - No information is passed back
 - Password is passed back
 - LDAP group members (include nested) (return distinguished names)
 - User's Distinguished Name
- Trusted Networks (no 2FA required): []
- Blocked Networks (black listed IP's): []
- Must send IP address in attribute 31 (Example 10.* 172.16.* 192.168.1.* 192.168.5.5)
- Buttons: Update, New

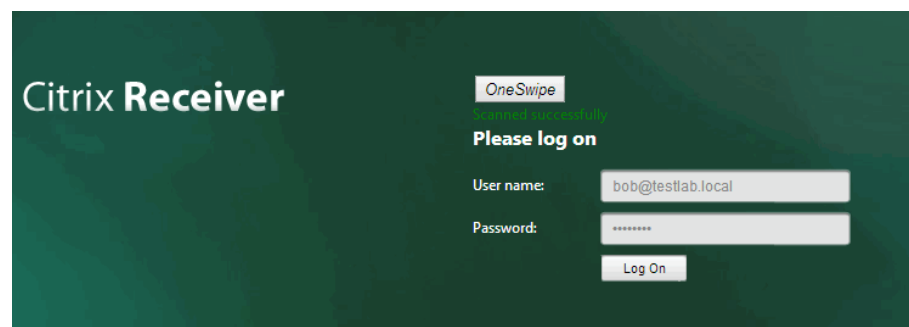
2.0 Test Logon

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

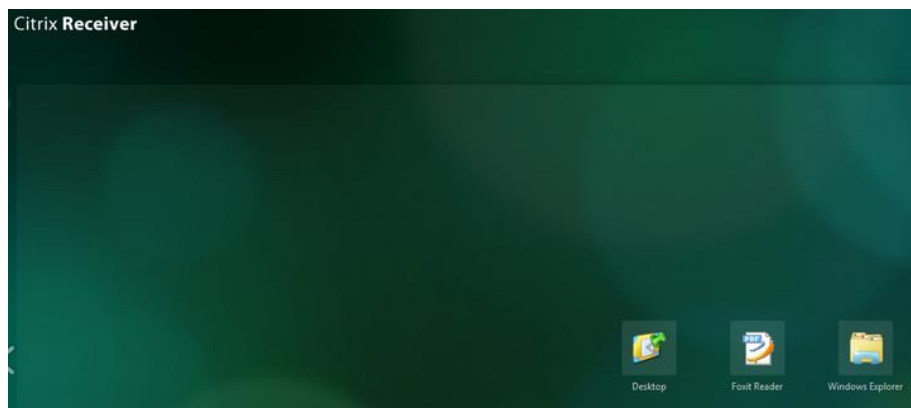
Click the OneSwipe button



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



User is presented with Citrix Web Interface



3.0 Notes