Citrix Netscaler 9.x VPX and SendQuick ConeXa One-Time Password Configuration Guide

Prepared by

TalariaX Pte Ltd
76 Playfair Road #08-00, LHK2
Singapore 367996

Tel: +65 62802881
Fax: +65 62806882

E-mail: info@talariax.com
Web: www.talariax.com

1.0 INTRODUCTION

This document is prepared as a guide to configure Citrix VPX to run with SendQuick Conexa for One-time-password via SMS.

The pre-requisite is that SendQuick Conexa OTP server is configured with RADIUS on port 1812. Ensure that both applications are using the same port for radius.

The software version for Citrix Netscaler is 9.0x (VPX).

2.0 CONFIGURE CITRIX NETSCALER

First login into Citrix. Go to **Configure Authentication Server** as shown below (Fig 1).

Provide a server name for the sendQuick ConeXa (eg sendQuickSMS). Make sure **Radius** is selected as the Authentication Type.

Configure the following items as below:

- Server IP Address – IP address of sendQuick ConeXa server
- Port – Specify **1812** (this must be 1812 as this is the radius port of communication used in ConeXa)
- Timeout – Configure a value of between 40-60 seconds (value need to be 25 seconds and higher for the system to perform well)
- Secret Key - This is a shared secret key (case-sensitive) text string that will be used to validate Radius communication between sendQuick ConeXa and Citrix Netscaler. Use the same secret on ConeXa.
- NAS IP address extraction – select Enable

Once completed, select **OK** and the server is configured.

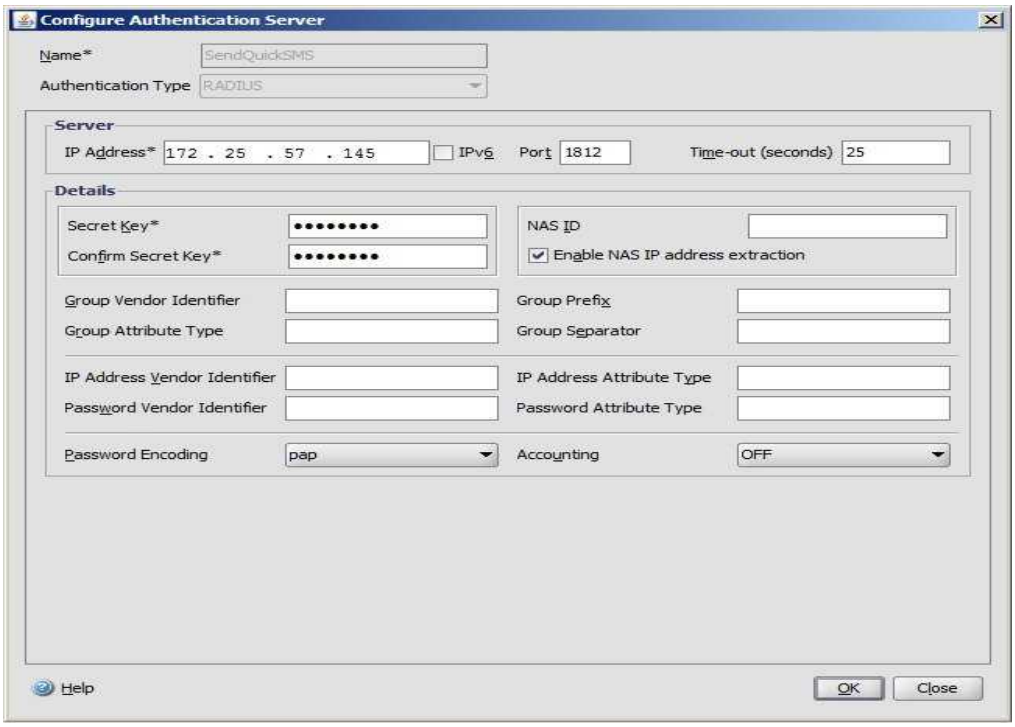

Figure 1: Authentication Server Configuration

Next, go to Citrix Access Gateway Virtual Server to enable sendQuick as Authentication Server. See Fig 2.

Configure the following items as below:

- URL IP address
- Port – 443 is the default SSL port
- Max Users – select "0" to refer to unlimited
- Select Basic Mode
- Click on the **Authentication** tab. sendQuick ConeXa should show up as one of the authentication policy. Select sendQuick as the primary Authentication (Radius) Server

Select **OK** once completed.

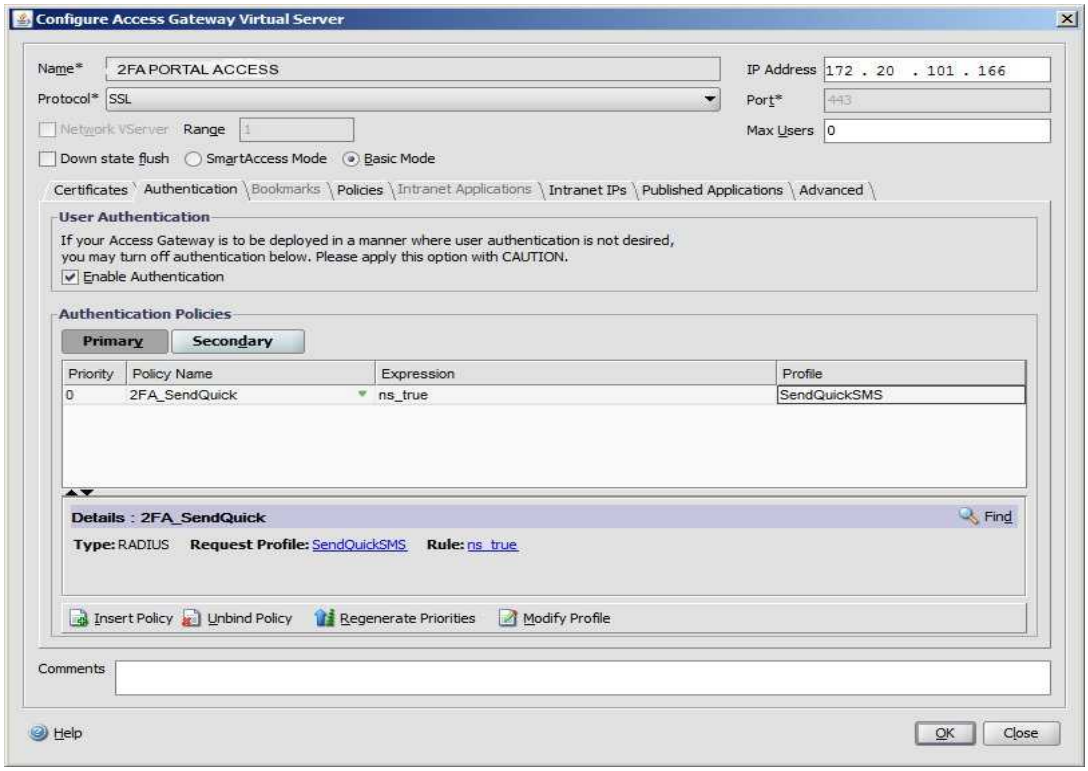

Figure 2: Enable Authentication Server

3.0 CONFIGURE SENQUICK CONEXA

Log in to sendQuick ConeXa **Admin** Page (Fig 3). Select **New Radius Configuration**.

Configure the following items as below

- IP address and description – IP address and description for Netscaler
- Radius status - Enable
- Radius Secret – Use the same shared secret text string that was earlier configured on Netscaler

Click **Submit** when completed

Figure 3: Radius configuration on sendQuick

Next, go to **Configuration** tab and select **New OTP Configuration.** See Figure 4 below.

Configure the following items as below:

- NAS IP and VPN description – Netscaler NAS IP and desc
- Authentication Type – Select desired authentication type

If LDAP is used, configure the following:

- LDAP Login Mode and IP address – LDAP server login details and IP address
- LDAP Query Attribute - LDAP Query Attribute for sendQuick to access. For example, "mobile" for the mobile number used by sendQuick to deliver OTP by SMS
- LDAP Base DN
- LDAP Domain

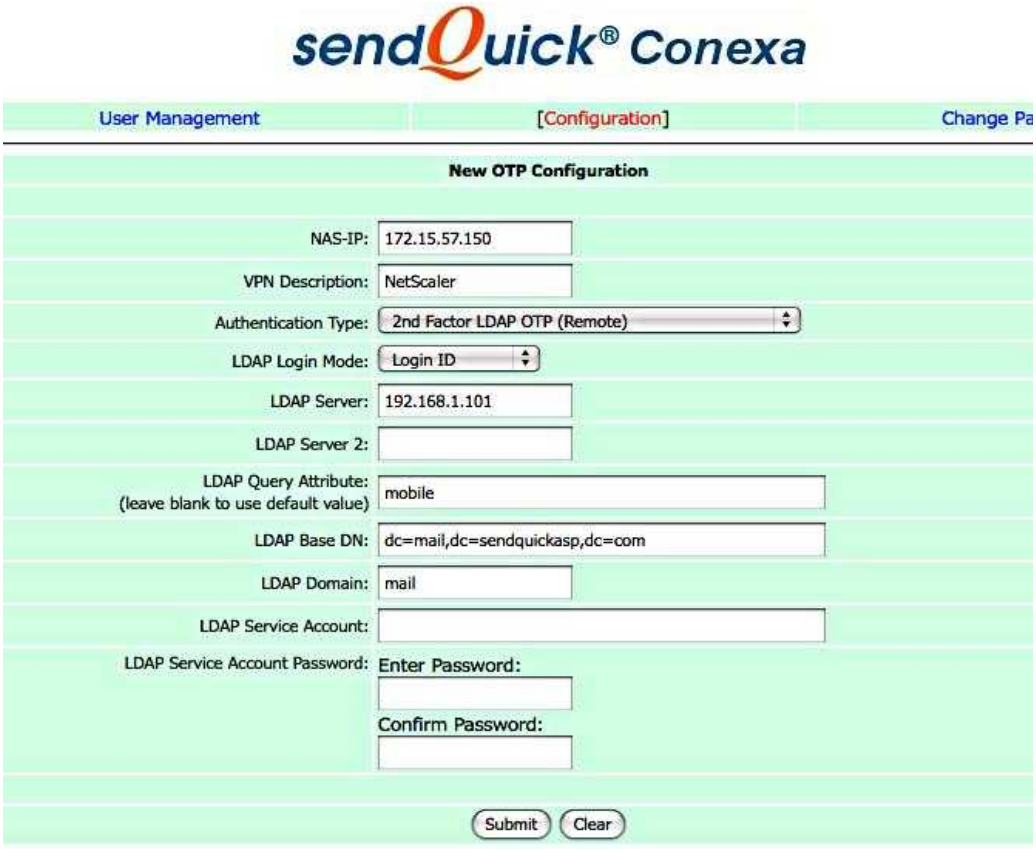

Figure 4: 2 Factor Authentication configuration on sendQuick

4.0 REMOTE ACCESS WITH TWO FACTOR AUTHENTICATION

When accessing using SSL VPN, open a web browser and access the Internet address (URL) for SSL VPN access. The Username and Password will appear as shown in Figure 5 below.

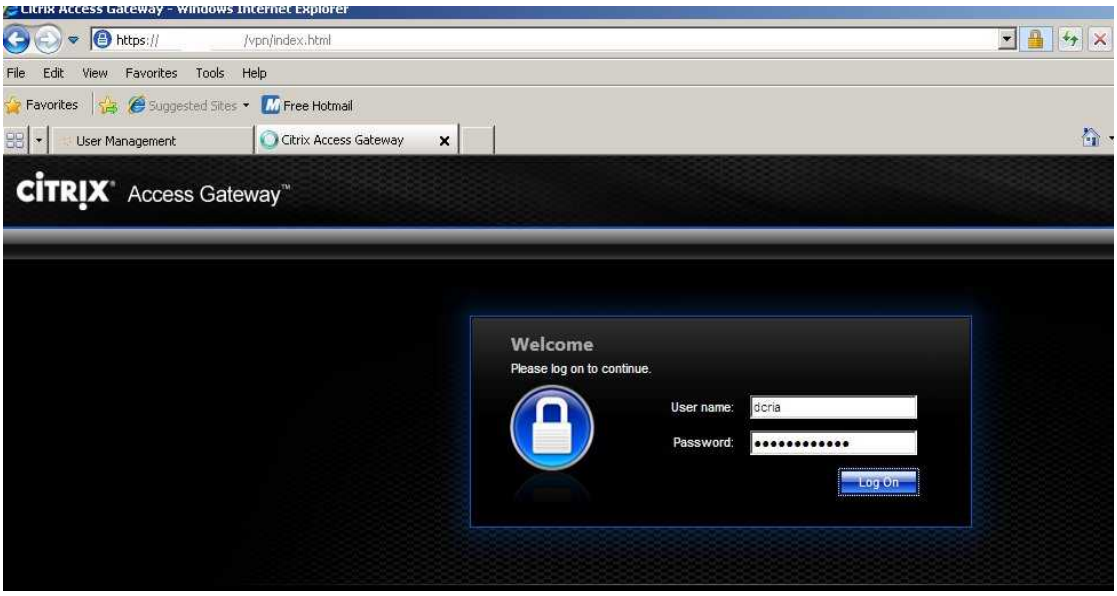

Figure 5: SSLVPN Login with Username and Password

Enter the **Username** and **Password** and select **Log On**. (If Active Directory is used, it should be a valid username and password). Once the first authentication is completed, an Enter OTP page will appear on the web page. The SMS will be sent to the mobile phone.

Enter the OTP in the **Response** space provided and select **Submit**, as shown in Figure 6 below. Once the second factor authentication is approved, the success page or user access realm will be shown as in Figure 7 below.

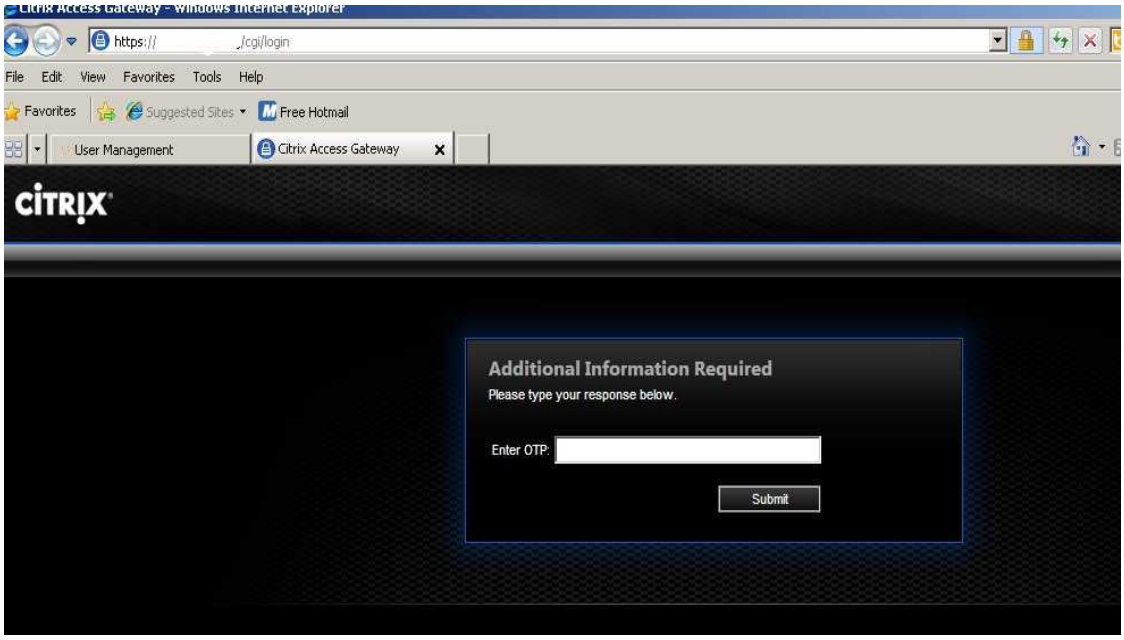

Figure 6: Enter OTP for SSL VPN Authentication

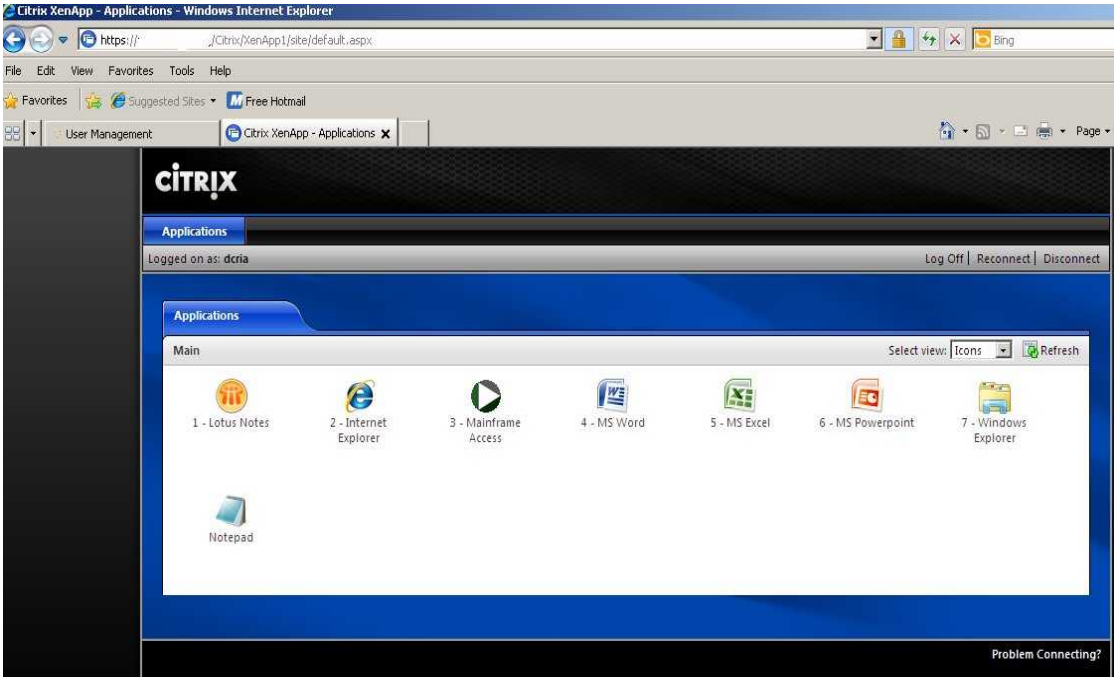

Figure 7: Successful Access with SSL VPN