Citrix NetScaler 11 and SendQuick ConeXa One-time-Password Configuration Guide

Prepared by

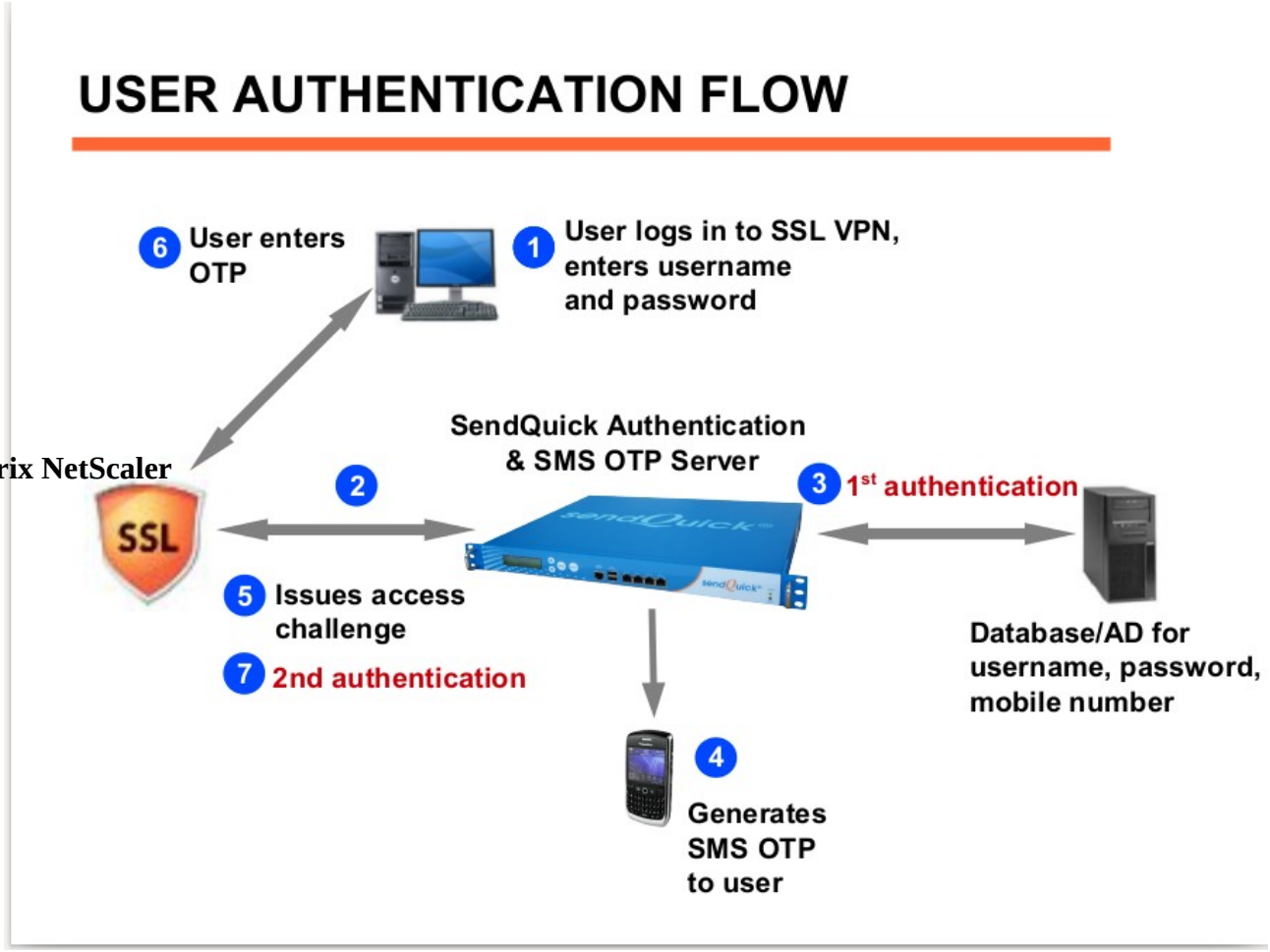
TalariaX Pte Ltd
76 Playfair Road
#08-01 LHK2
Singapore 367996
Tel: 65-62802881
Fax: 65-62806882

Citrix NetScaler 11
&
SENDQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

1.0 INTRODUCTION

This document is prepared as a guide to configure Citrix NetScaler 11 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.



2.0 CONFIGURE On sendQuick coneXa

Access with http://<sendQuick IP>/

Figure 1 : Radius Client Page

To add new radius client, goto Authentication Configuration > Radius Client Configuration

Radius Client IP : <Ciritx NetScaler IP>
Shared Secret : <Shared secret of the radius client>

Figure 2 : Add New Radius Client

We will use the user name and password in the AD server to login to SSL VPN.

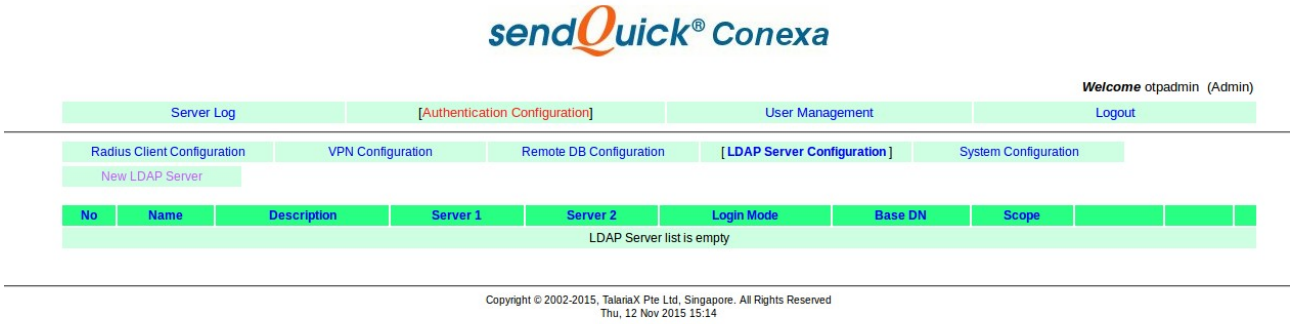


Figure 3 : LDAP Server Configuration Page

Add the AD server under Authenication Configuration > LDAP Server Configuration

IP address of AD server, Server 1 : 192.168.1.213, Port 389
Type : Active Directory
Service Account Bind DN : < need an AD account>
Login Mode : Login ID
Base DN : <Base DN of the location of user list in LDAP >

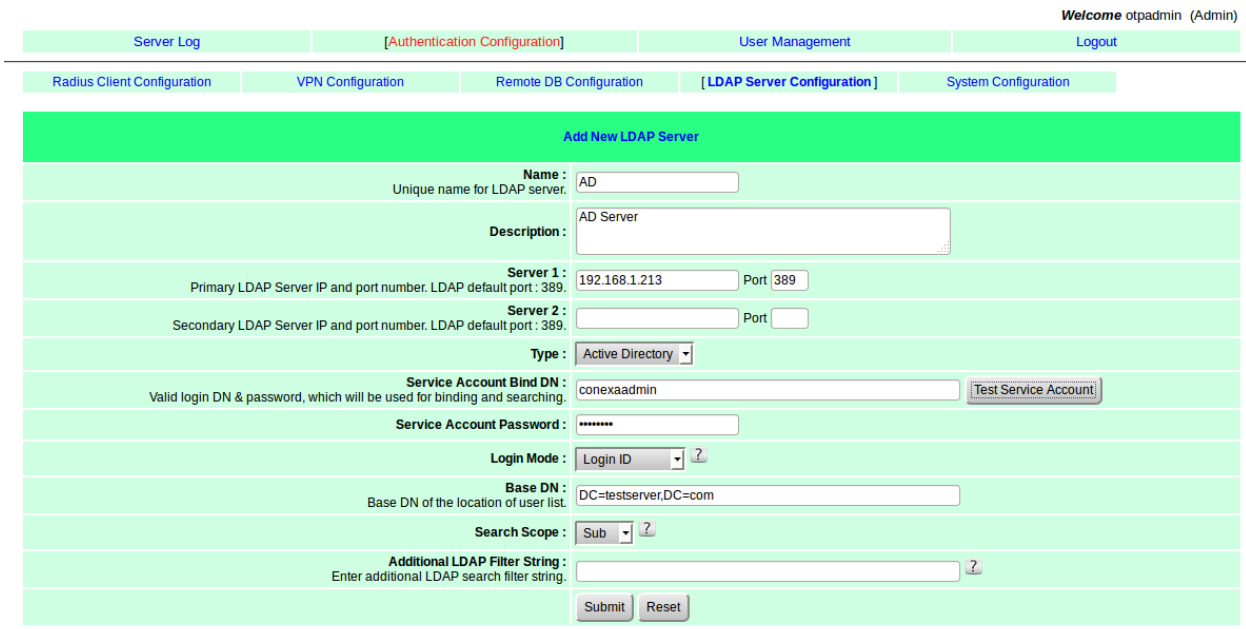


Figure 4 : Add New AD Server

Check the connection between your AD and sendQuick coneXa by clicking on “Test Service Account”

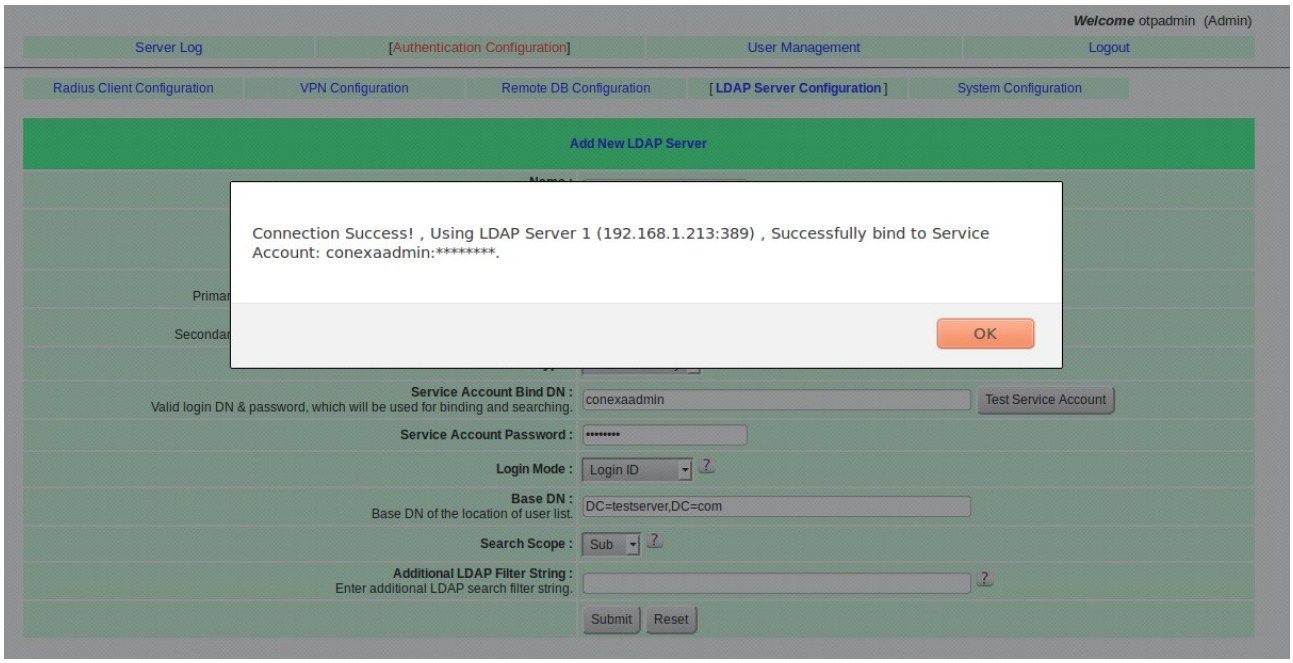


Figure 5 : Test Service Account

Configuraiton VPN configuration

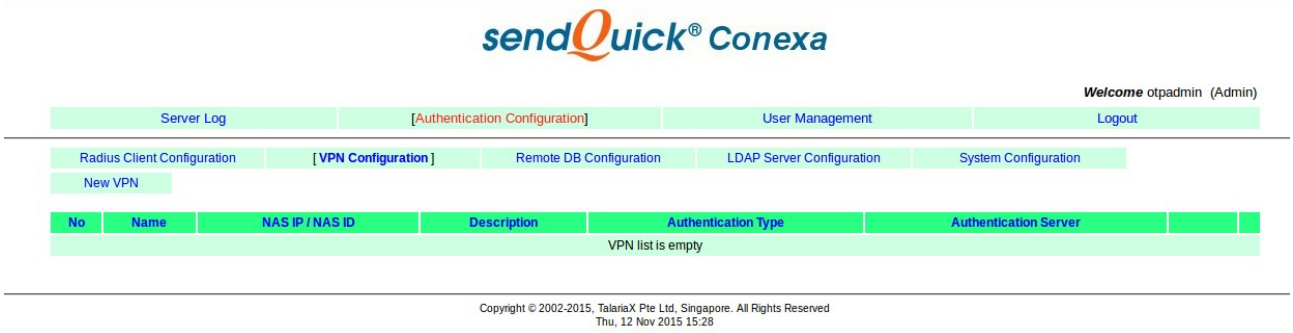


Figure 6 : VPN Configuration Page

NAS IP Address : <Ciritx NetScaler IP>
Authentication Type : Two Factor Access Challenge
Authentication Server : LDAP
LDAP Server : AD
OTP Deliver Method : SMS

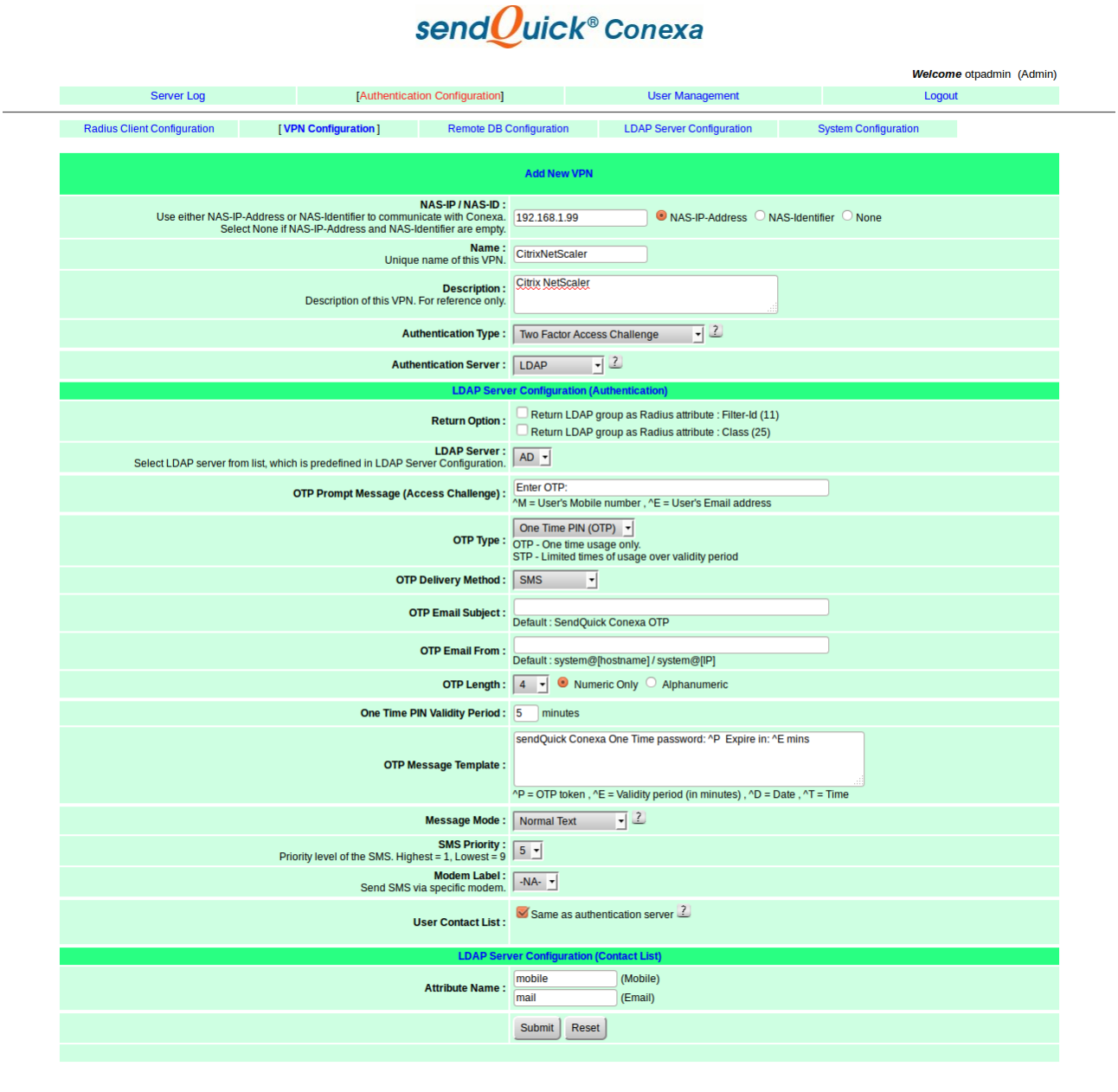


Figure 7 : Add New VPN

3.0 CONFIGURE On Citrix NetScaler

Login to Citrix Netscaler

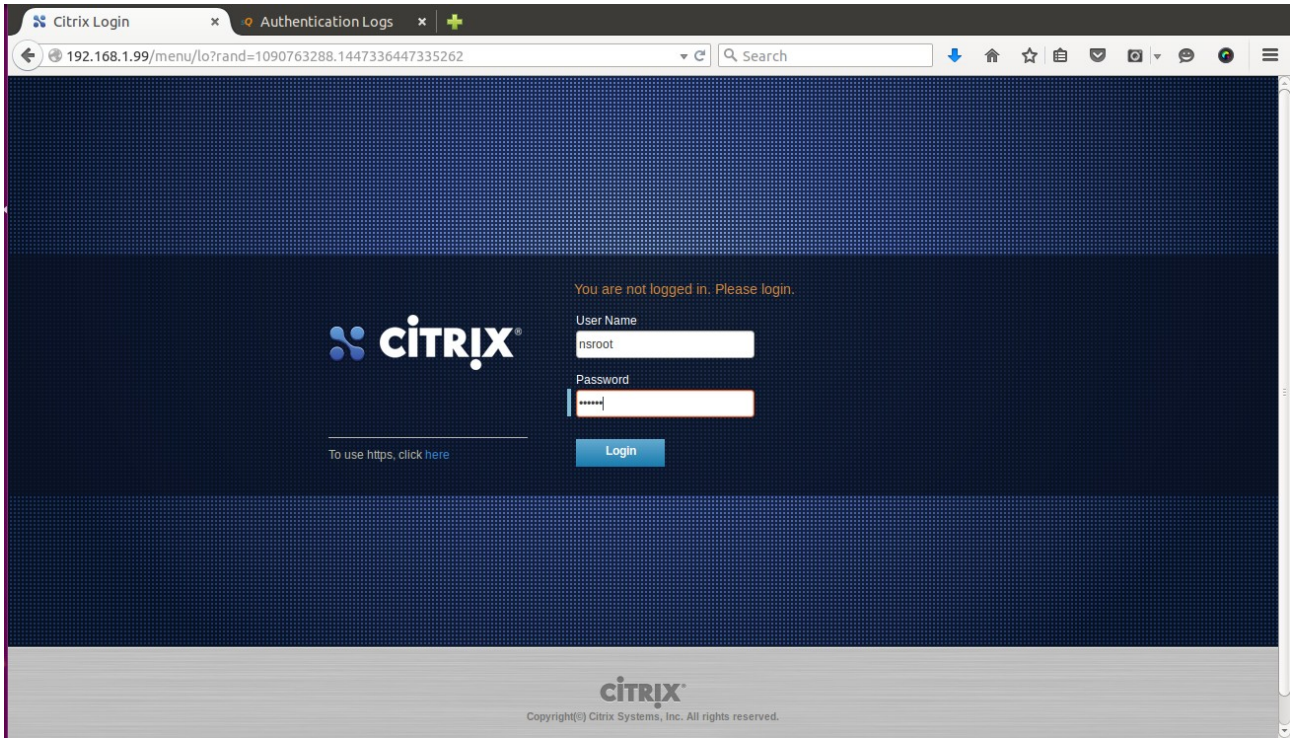


Figure 8 :

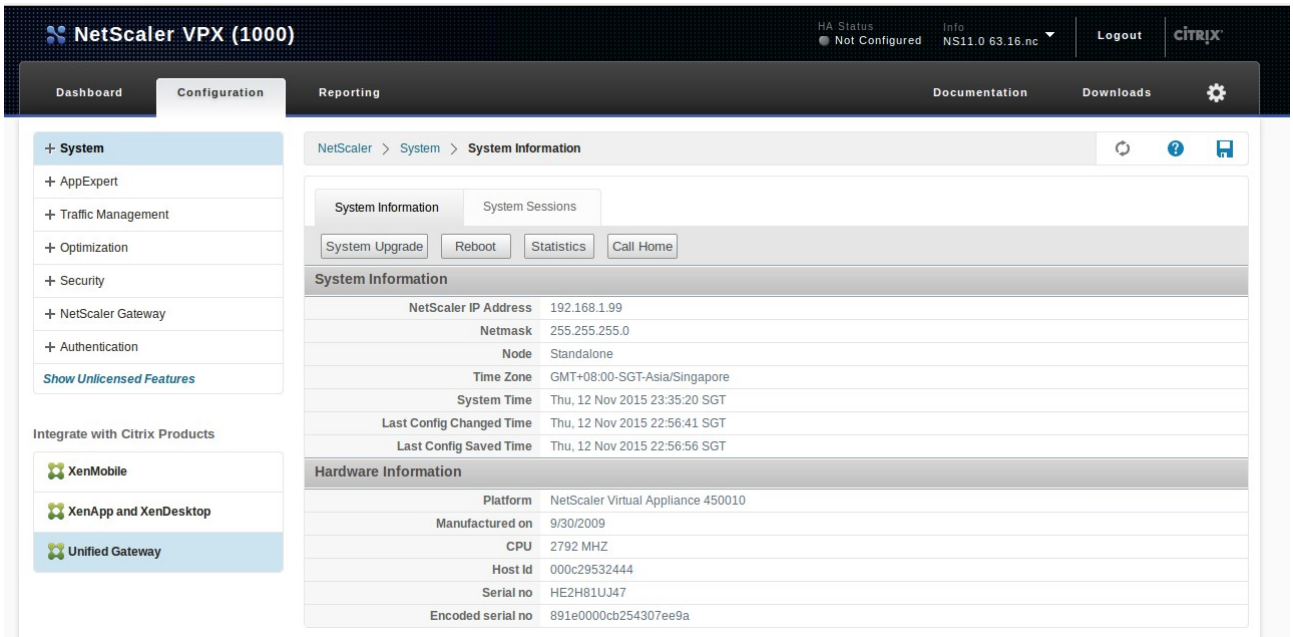


Figure 9 : Configuration Page

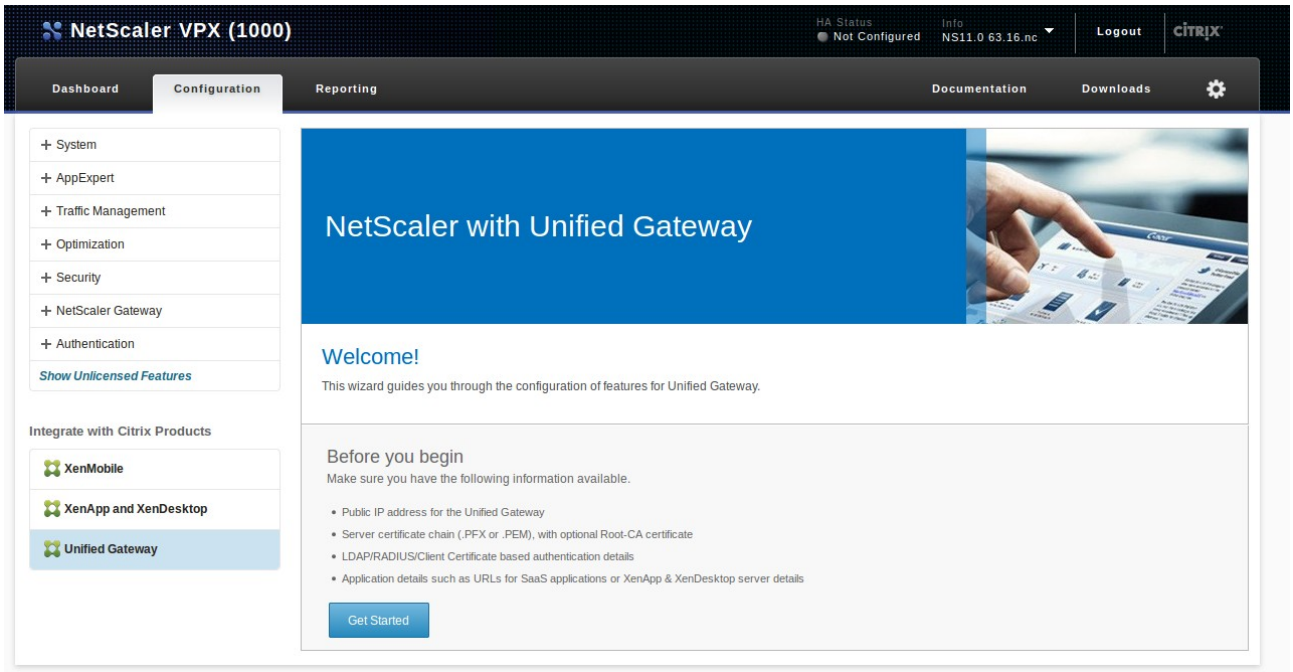


Figure 9 : Unified Gateway wizard

Add Authentication

Primary Authentication Method : Radius
IP Address : < sendQuick coneXa IP>
Port : 1812
Secret Key : <Shared secret of sendQuick coneXa>

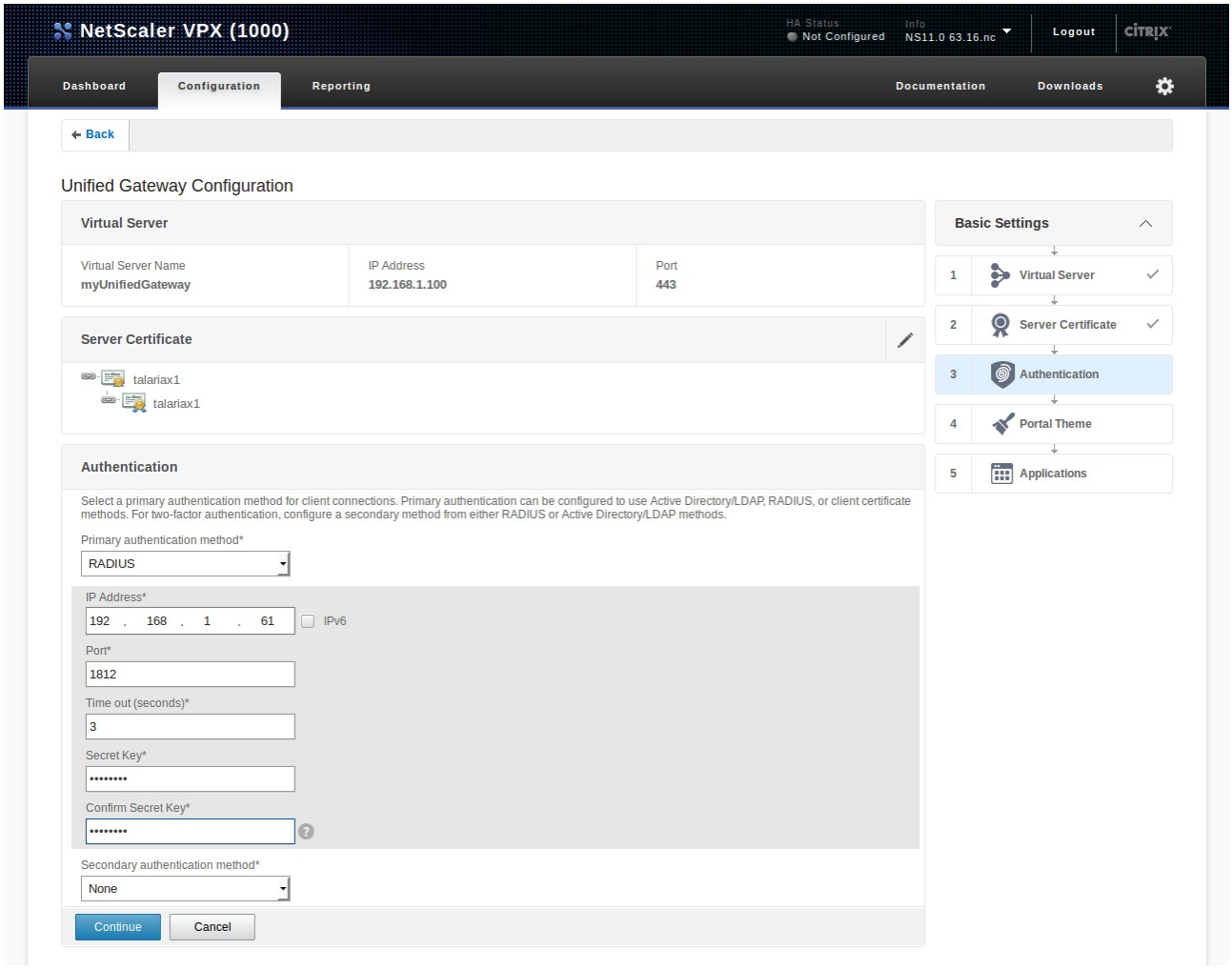


Figure 10 : Unified Gateway wizard

4.0 REMOTE ACCESS WITH TWO FACTOR AUTHENTICATION

Enter user name and password which is stored in your AD server to login VPN for the 1st authentication. Once the first authentication is successful, the Enter OTP page will appear as shown in Figure 12 below. The OTP will be sent to the mobile phone. Enter the OTP in the space provided and click Submit.

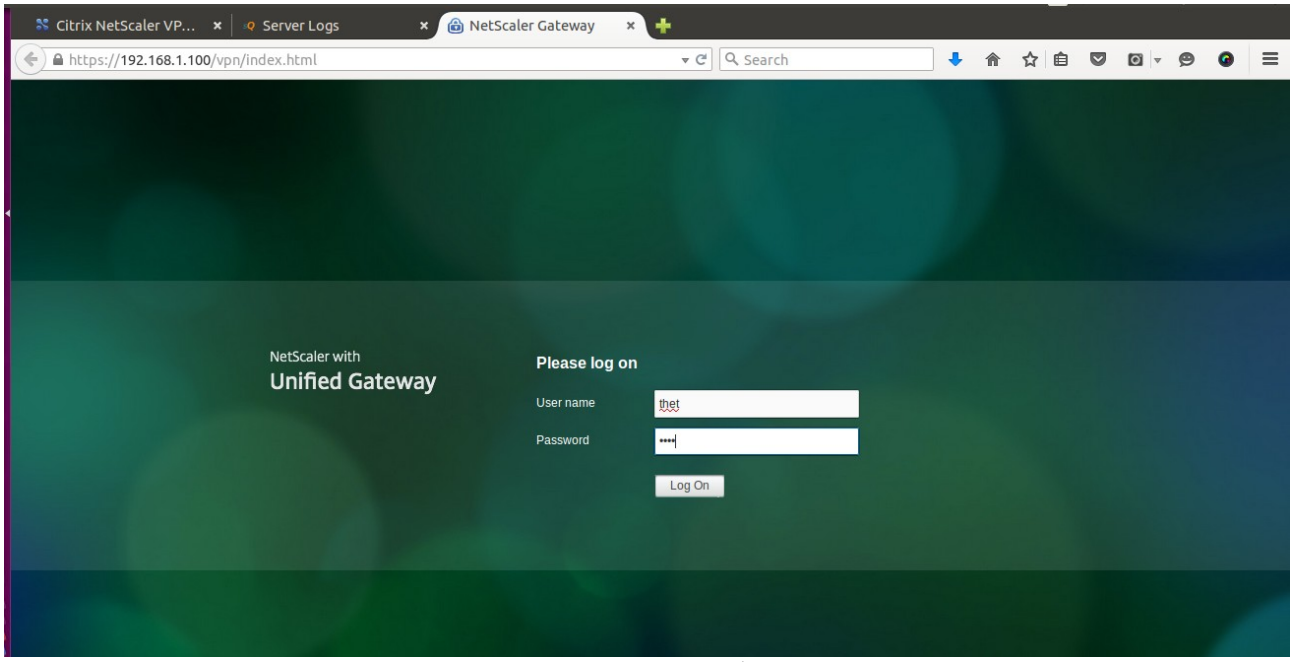


Figure 11 : Login page of 1st Authentication

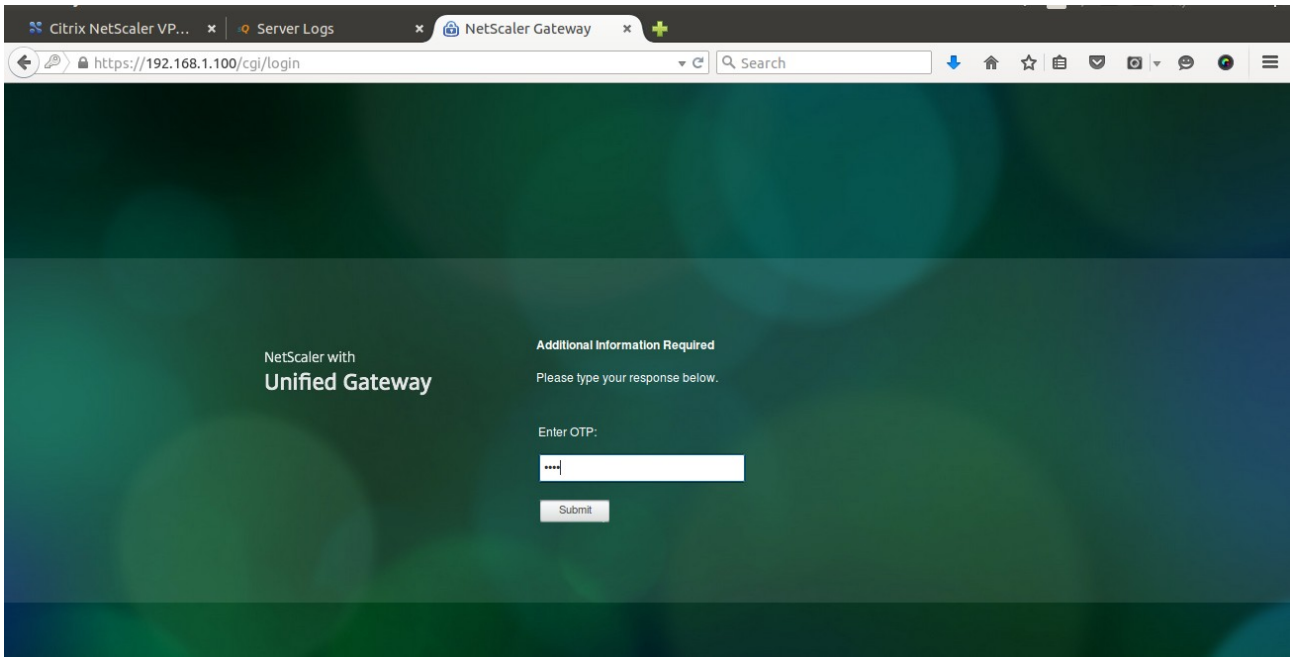


Figure 12 : OTP Login Page

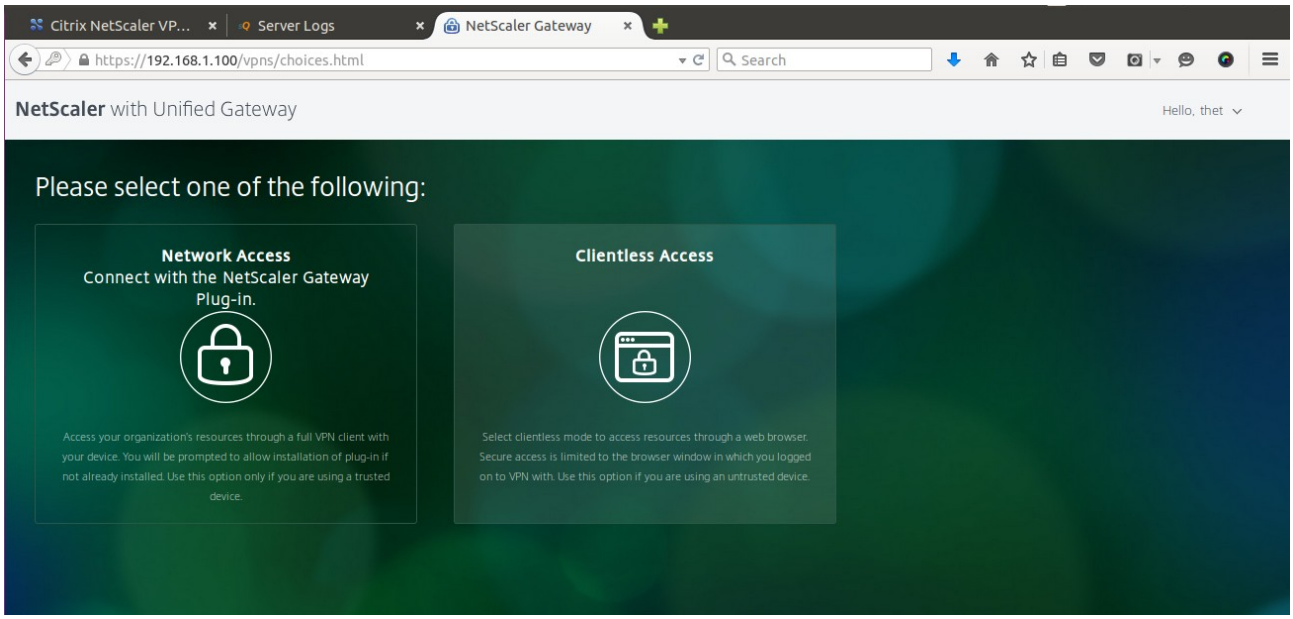


Figure 13 : Successful Access with SSL VPN

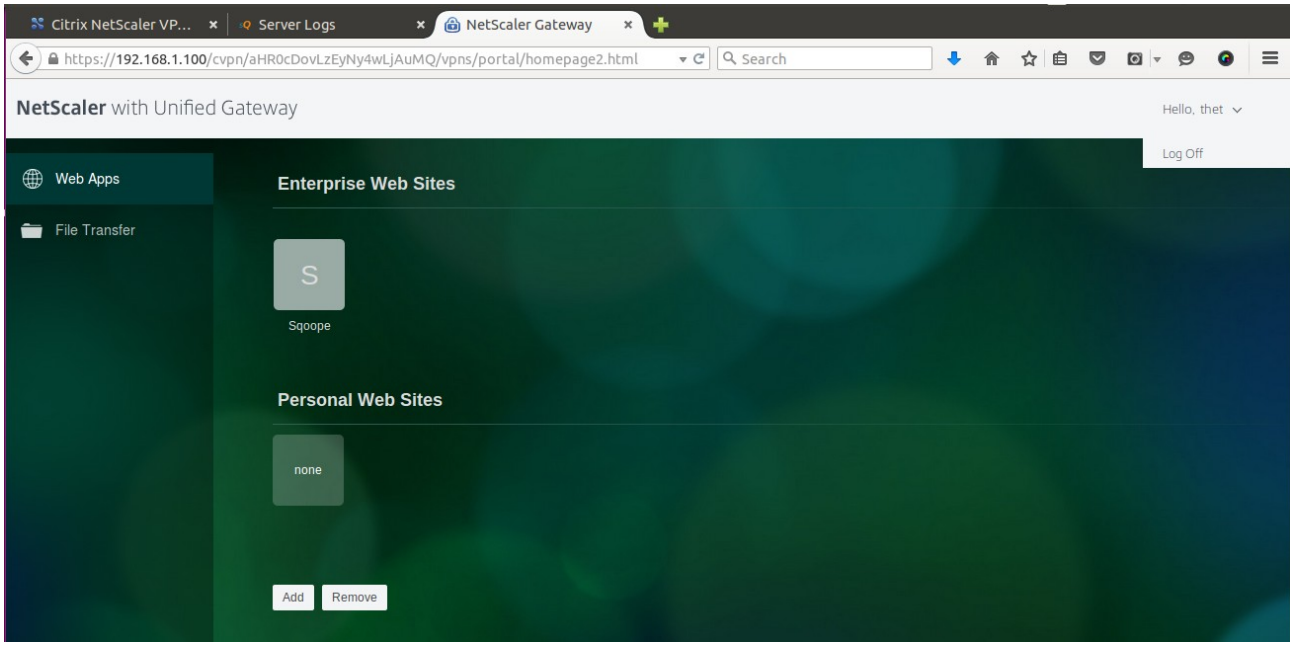


Figure 14 : Successful Access

ConeXa Server Log

sendQuick® Conexa

Welcome otpadmin (Admin)

[Server Log] | Authentication Configuration | User Management | Logout

[**Server Log**] | Authentication Log

Server Log

```
2015-11-12 15:56:49 Radius[10544] (OTPapi) Send SMS (otp:1899) to thet (91072730)
2015-11-12 15:56:49 Radius[10544] (OTPapi) Request from thet (192.168.1.99). 2FC CHALLENGE
2015-11-12 15:57:04 Radius[10544] (OTPapi) *****Request from NAS-IP-Address:192.168.1.99 NAS-Identifier:- (thet)*****
2015-11-12 15:57:04 Radius[10544] (OTPapi) 2-Factor AC authentication success (thet OTP:1899)
2015-11-12 15:57:04 Radius[10544] (OTPapi) Request from thet (192.168.1.99). 2FC ACCEPT
2015-11-12 16:38:37 smsConexa[15996] (OTPapi) Received SMS From:Singtel Keyword:We are delighted to inform you that unlimited Singtel WiFi usage has been extended to 29 Feb'16. Enjoy seamless surfing at over 600 hotspots as part of your mobile plan. Monitoring of your Singtel WiFi usage will be made available via MySingtel app soon. T&Cs apply. www.singtel.com/singtelwifi
2015-11-12 16:38:37 smsConexa[15996] Cannot find VPN with keyword:We
2015-11-12 16:45:58 smsConexa[15996] (OTPapi) Received SMS From:+6591072730 Keyword:Test reply
2015-11-12 16:45:58 smsConexa[15996] Cannot find VPN with keyword:Test
2015-11-12 16:48:55 Radius[10544] (OTPapi) *****Request from NAS-IP-Address:192.168.1.99 NAS-Identifier:- (thet)*****
2015-11-12 16:48:55 Radius[10544] (OTPapi) Using LDAP (AD) Server 1 (192.168.1.213:389)
2015-11-12 16:48:55 Radius[10544] (OTPapi) CheckValidLdapUser (AD) for thet, Mode:loginid, Server(192.168.1.213:389) success
2015-11-12 16:48:55 Radius[10544] (OTPapi) 2-FA AC 1st authentication success (thet)
2015-11-12 16:48:55 Radius[10544] (OTPapi) Using LDAP (AD) Server 1 (192.168.1.213:389)
2015-11-12 16:48:55 Radius[10544] (OTPapi) GetLdapUserInfo (AD) for thet, Mode:loginid, Server(192.168.1.213:389) : (mobile:91096771 , email:thet@talariax.com)
2015-11-12 16:48:55 Radius[10544] (OTPapi) Send SMS (otp:8775) to thet (91096771)
2015-11-12 16:48:55 Radius[10544] (OTPapi) Request from thet (192.168.1.99). 2FC CHALLENGE
2015-11-12 16:49:43 Radius[10544] (OTPapi) *****Request from NAS-IP-Address:192.168.1.99 NAS-Identifier:- (thet)*****
2015-11-12 16:49:43 Radius[10544] (OTPapi) 2-Factor AC authentication success (thet OTP:8775)
2015-11-12 16:49:43 Radius[10544] (OTPapi) Request from thet (192.168.1.99). 2FC ACCEPT
```

Refresh

Download Log files : current log | log 1 | log 2 | log 3 | log 4 | log 5 | log 6

Figure 15 : Server Logs of sendQuick coneXa

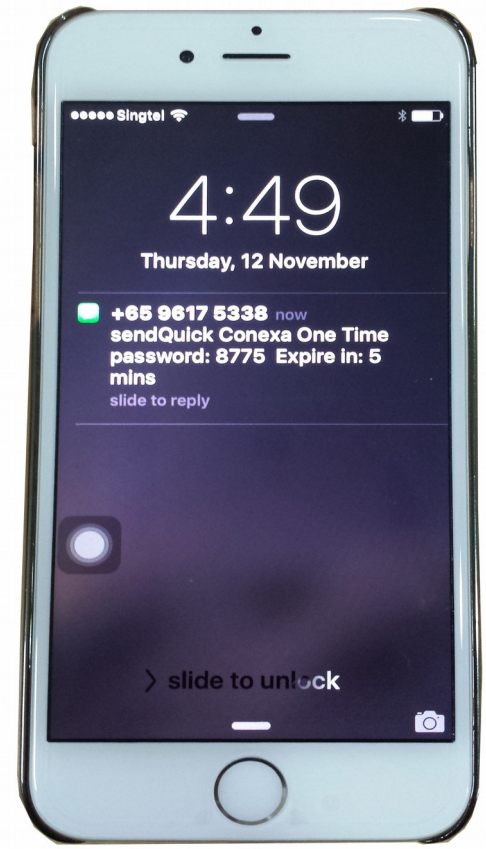


Figure 16 : Received OTP