



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

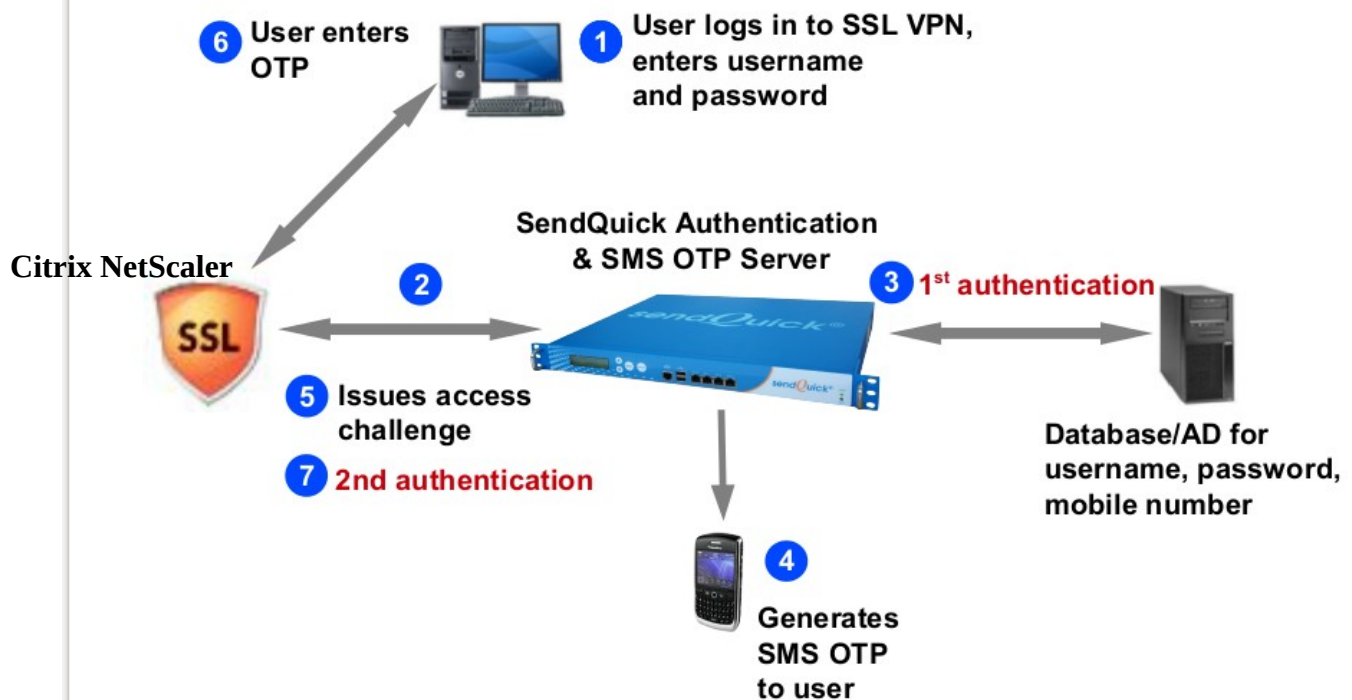
Citrix NetScaler 11 & SENDQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

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.

USER AUTHENTICATION FLOW



2.0 CONFIGURE On sendQuick coneXa

Access with http://<sendQuick IP>/

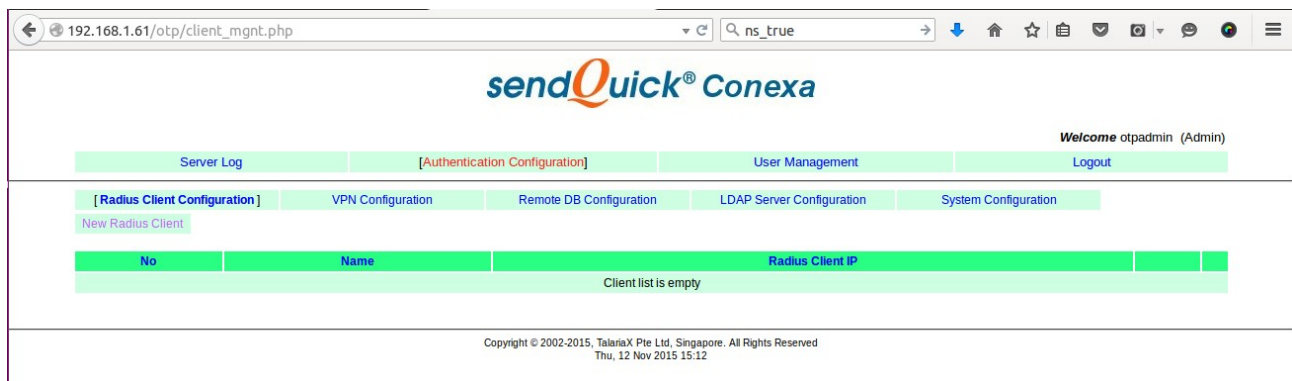


Figure 1 : Radius Client Page

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

Radius Client IP : <Citrix NetScaler IP>

Shared Secret : <Shared secret of the radius client>

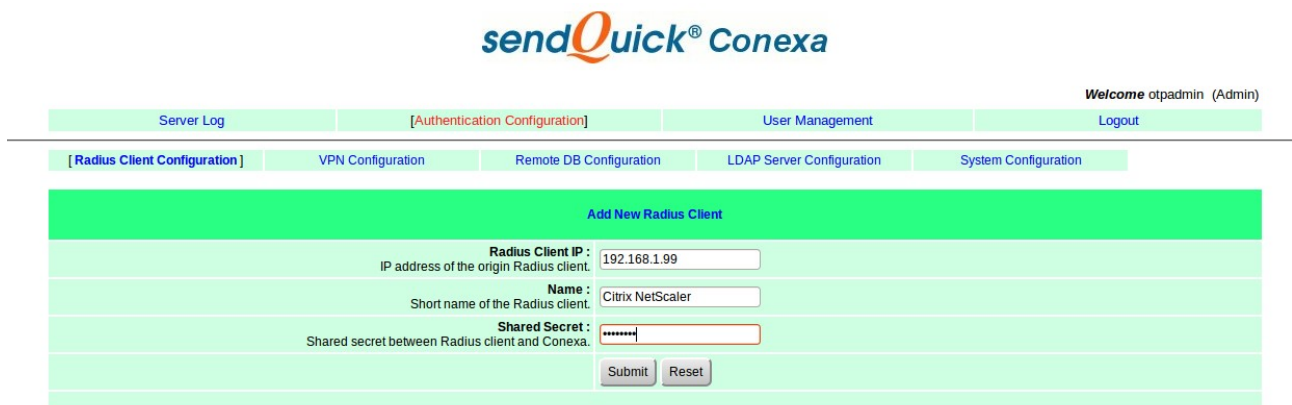


Figure 2 : Add New Radius Client

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

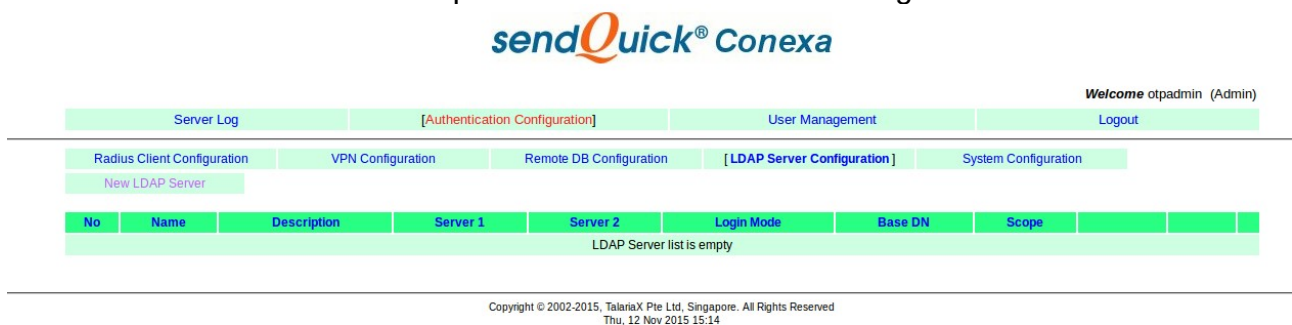


Figure 3 : LDAP Server Configuration Page

Add the AD server under Authentication 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 >

Welcome otpadmin (Admin)

Server Log	[Authentication Configuration]	User Management	Logout
Radius Client Configuration	VPN Configuration	Remote DB Configuration	[LDAP Server Configuration]
System Configuration			

Add New LDAP Server

Name : <small>Unique name for LDAP server.</small>	<input type="text" value="AD"/>
Description :	<input type="text" value="AD Server"/>
Server 1 : <small>Primary LDAP Server IP and port number. LDAP default port : 389.</small>	<input type="text" value="192.168.1.213"/> Port <input type="text" value="389"/>
Server 2 : <small>Secondary LDAP Server IP and port number. LDAP default port : 389.</small>	<input type="text"/> Port <input type="text"/>
Type :	Active Directory ▾
Service Account Bind DN : <small>Valid login DN & password, which will be used for binding and searching.</small>	<input type="text" value="conexaadmin"/> <input type="button" value="Test Service Account"/>
Service Account Password :	<input type="password" value="*****"/>
Login Mode :	Login ID ▾ ?
Base DN : <small>Base DN of the location of user list.</small>	<input type="text" value="DC=testserver,DC=com"/>
Search Scope :	Sub ▾ ?
Additional LDAP Filter String : <small>Enter additional LDAP search filter string.</small>	<input type="text"/> ?
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Figure 4 : Add New AD Server

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

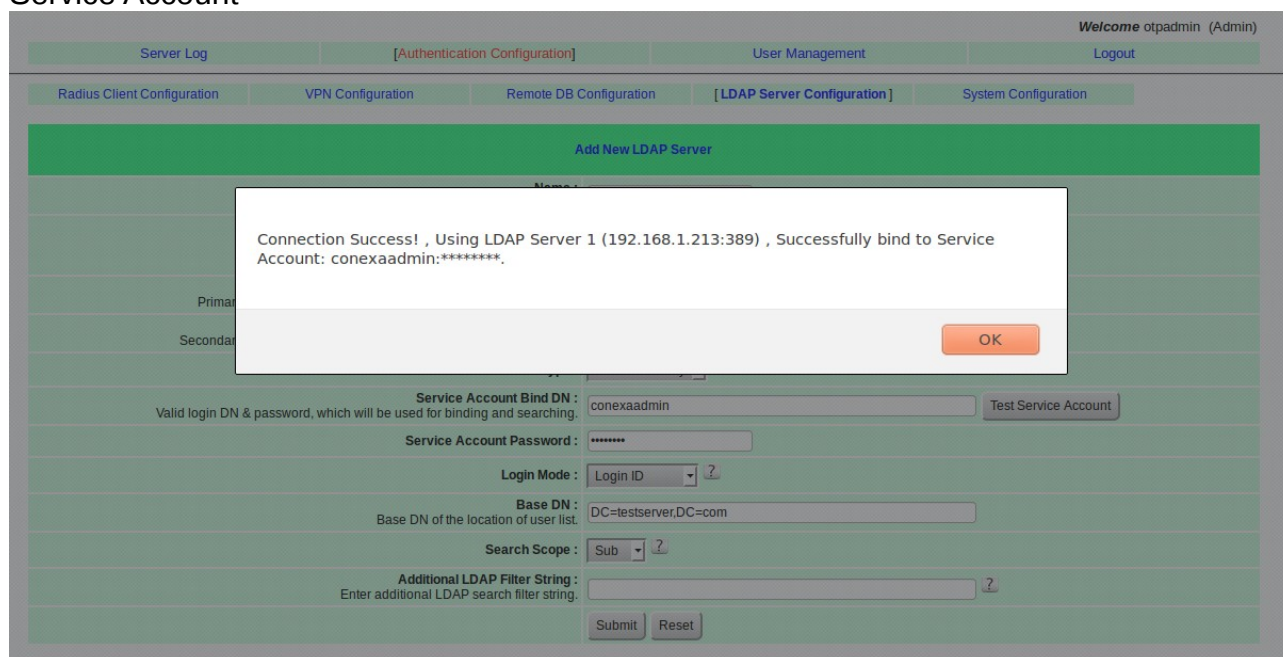


Figure 5 : Test Service Account

Configuraiton VPN configuration

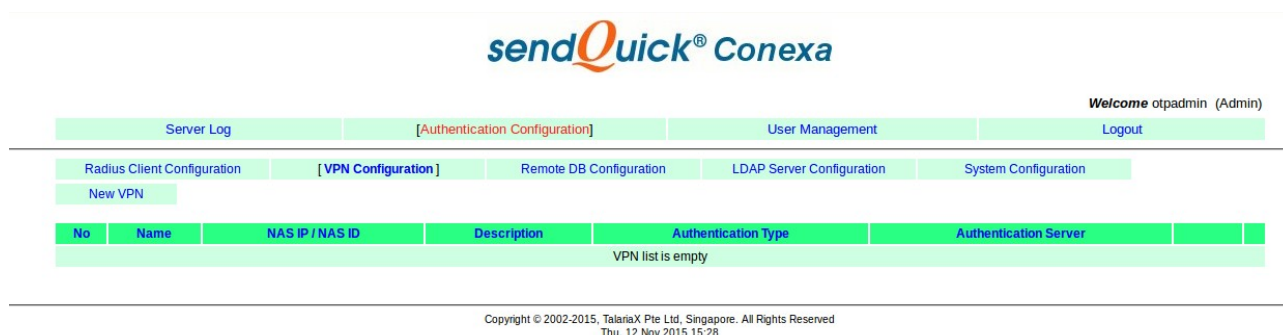


Figure 6 : VPN Configuration Page

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



Welcome otpadmin (Admin)

Server Log	[Authentication Configuration]	User Management	Logout
Radius Client Configuration	[VPN Configuration]	Remote DB Configuration	LDAP Server Configuration
System Configuration			

Add New VPN

Use either NAS-IP-Address or NAS-Identifier to communicate with Conexa. Select None if NAS-IP-Address and NAS-Identifier are empty.

NAS-IP / NAS-ID : 192.168.1.99 ☒ NAS-IP-Address ☐ NAS-Identifier ☐ None

Name : Unique name of this VPN: CitrixNetScaler

Description : Description of this VPN. For reference only: Citrix NetScaler

Authentication Type : Two Factor Access Challenge ?

Authentication Server : LDAP ?

LDAP Server Configuration (Authentication)

Return Option : ☐ Return LDAP group as Radius attribute : Filter-Id (11)
☐ Return LDAP group as Radius attribute : Class (25)

LDAP Server : Select LDAP server from list, which is predefined in LDAP Server Configuration: AD

OTP Prompt Message (Access Challenge) : Enter OTP:
^M = User's Mobile number , ^E = User's Email address

OTP Type : One Time PIN (OTP) ?
OTP - One time usage only.
STP - Limited times of usage over validity period

OTP Delivery Method : SMS

OTP Email Subject : Default : SendQuick Conexa OTP

OTP Email From : Default : system@[hostname] / system@[IP]

OTP Length : 4 ☒ Numeric Only ☐ Alphanumeric

One Time PIN Validity Period : 5 minutes

OTP Message Template : sendQuick Conexa One Time password: ^P Expire in: ^E mins
^P = OTP token , ^E = Validity period (in minutes) , ^D = Date , ^T = Time

Message Mode : Normal Text ?

SMS Priority : 5
Priority level of the SMS. Highest = 1, Lowest = 9

Modem Label : -NA-
Send SMS via specific modem.

User Contact List : ☒ Same as authentication server ?

LDAP Server Configuration (Contact List)

Attribute Name : mobile (Mobile)
mail (Email)

Submit Reset

Copyright © 2002-2015, TalariaX Pte Ltd, Singapore. All Rights Reserved
Thu, 12 Nov 2015 15:28

Figure 7 : Add New VPN

3.0 CONFIGURE On Citrix NetScaler

Login to Citrix Netscaler

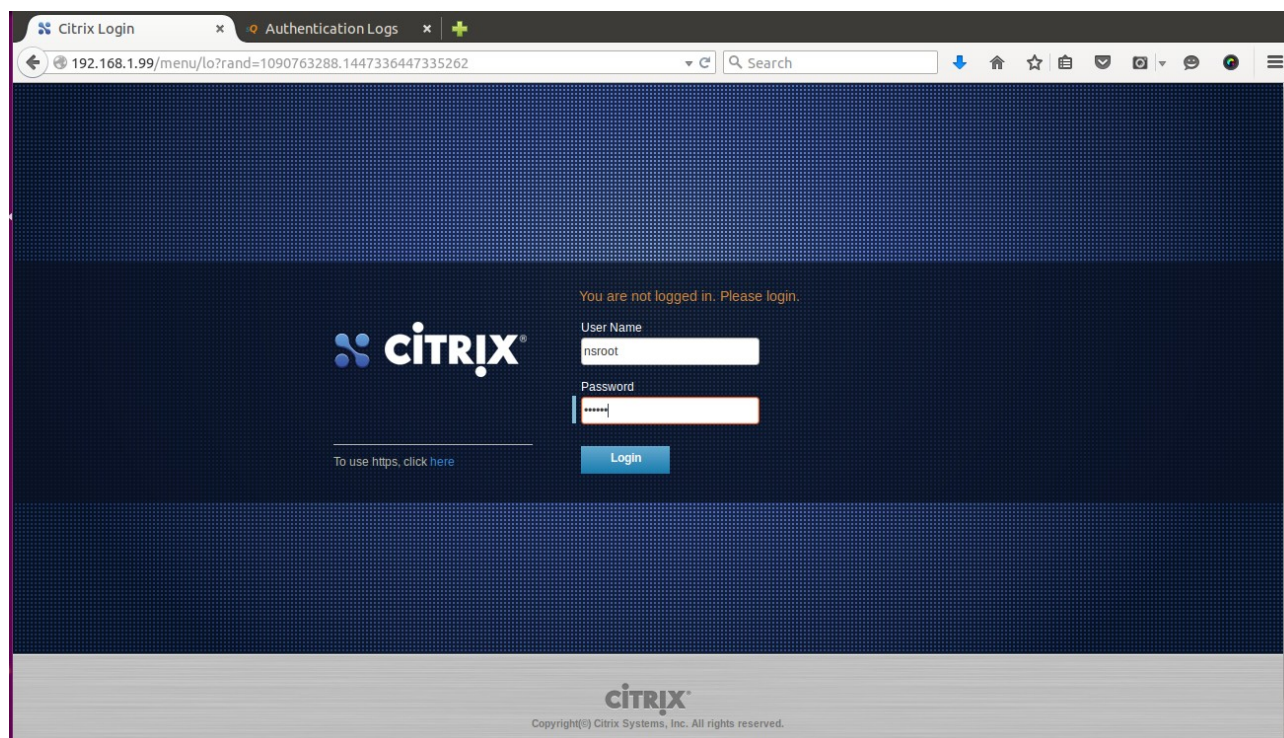


Figure 8 :

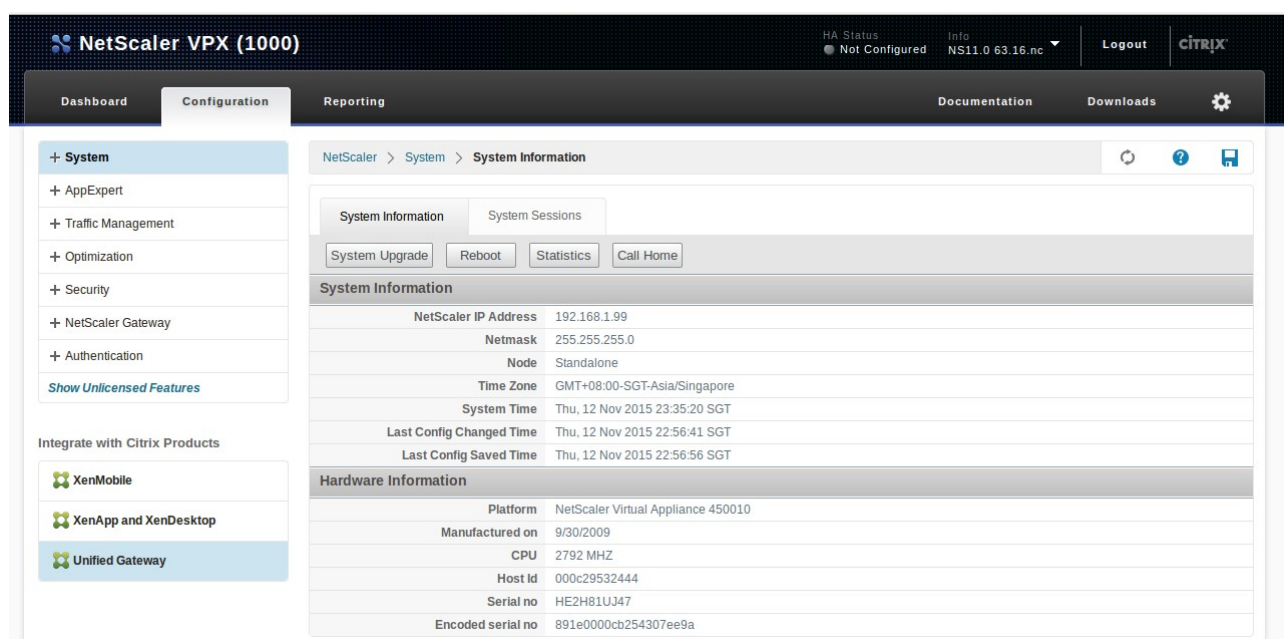


Figure 9 : Configuration Page

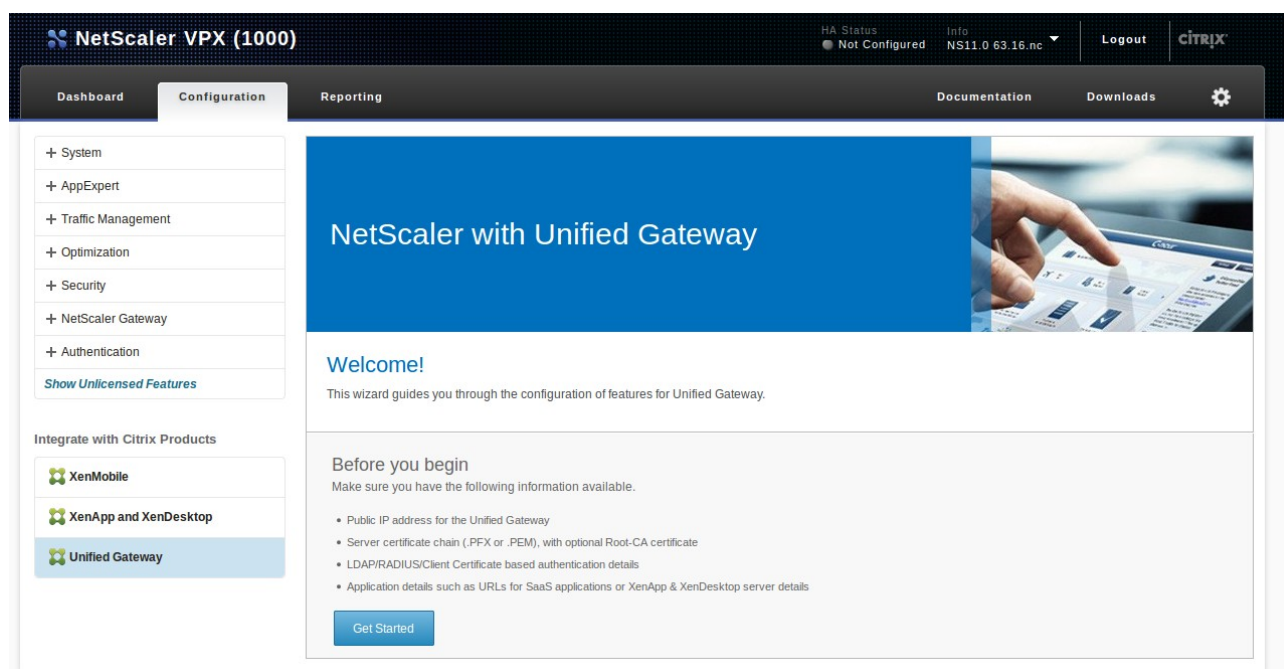


Figure 9 : Unified Gateway wizard

Add Authentication

Primary Authentication Method : Radius

IP Address : < sendQuick coneXa IP>

Port : 1812

Secret Key : <Shared secret of sendQuick coneXa>

NetScaler VPX (1000)

HA Status: Not Configured | Info: NS11.0 63.16.nc | Logout | Citrix

Dashboard | Configuration | Reporting | Documentation | Downloads

Unified Gateway Configuration

Virtual Server

Virtual Server Name	IP Address	Port
myUnifiedGateway	192.168.1.100	443

Server Certificate

talariax1

Authentication

Select a primary authentication method for client connections. Primary authentication can be configured to use Active Directory/LDAP, RADIUS, or client certificate methods. For two-factor authentication, configure a secondary method from either RADIUS or Active Directory/LDAP methods.

Primary authentication method*
RADIUS

IP Address*
192 . 168 . 1 . 61 ☐ IPv6

Port*
1812

Time out (seconds)*
3

Secret Key*

Confirm Secret Key*

Secondary authentication method*
None

Continue Cancel

Basic Settings

- 1 Virtual Server ✓
- 2 Server Certificate ✓
- 3 Authentication
- 4 Portal Theme
- 5 Applications

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.

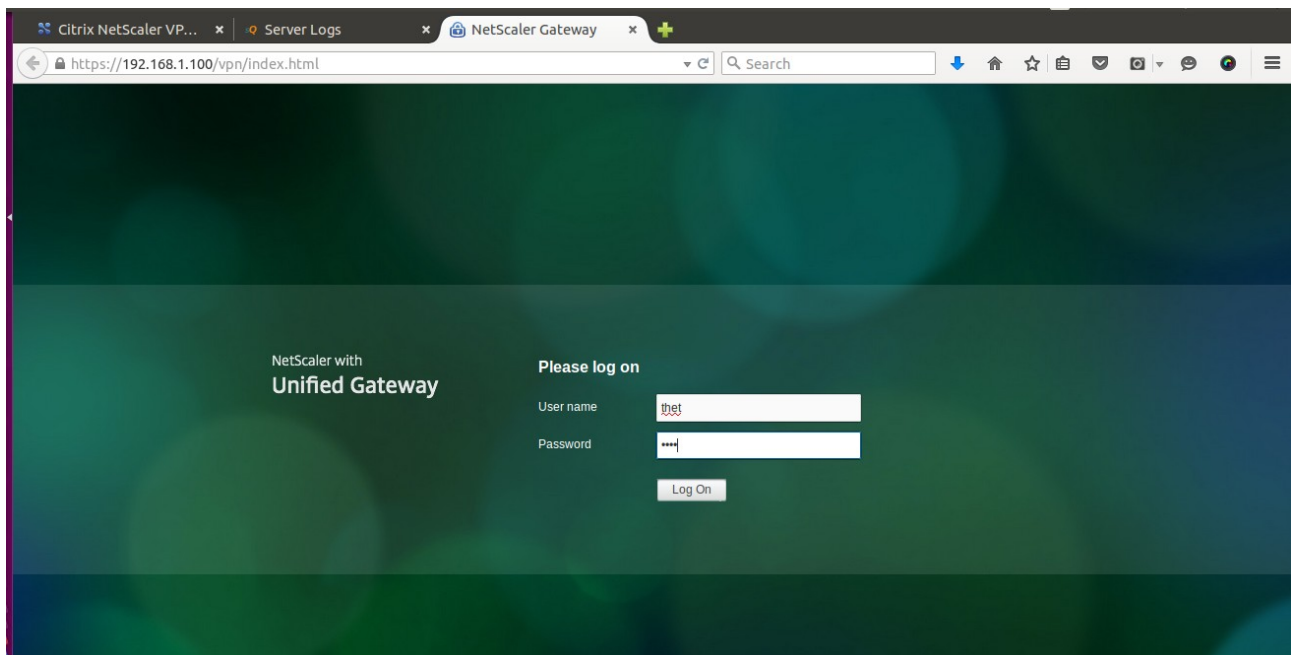


Figure 11 : Login page of 1st Authentication

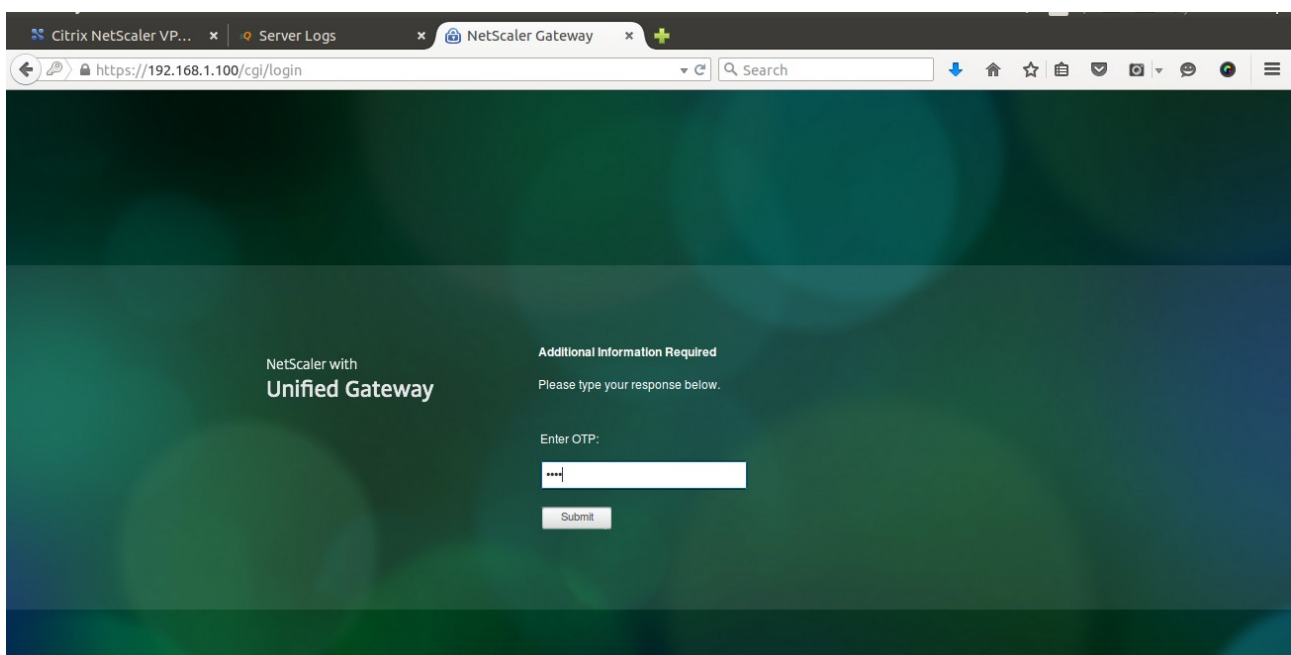


Figure 12 : OTP Login Page

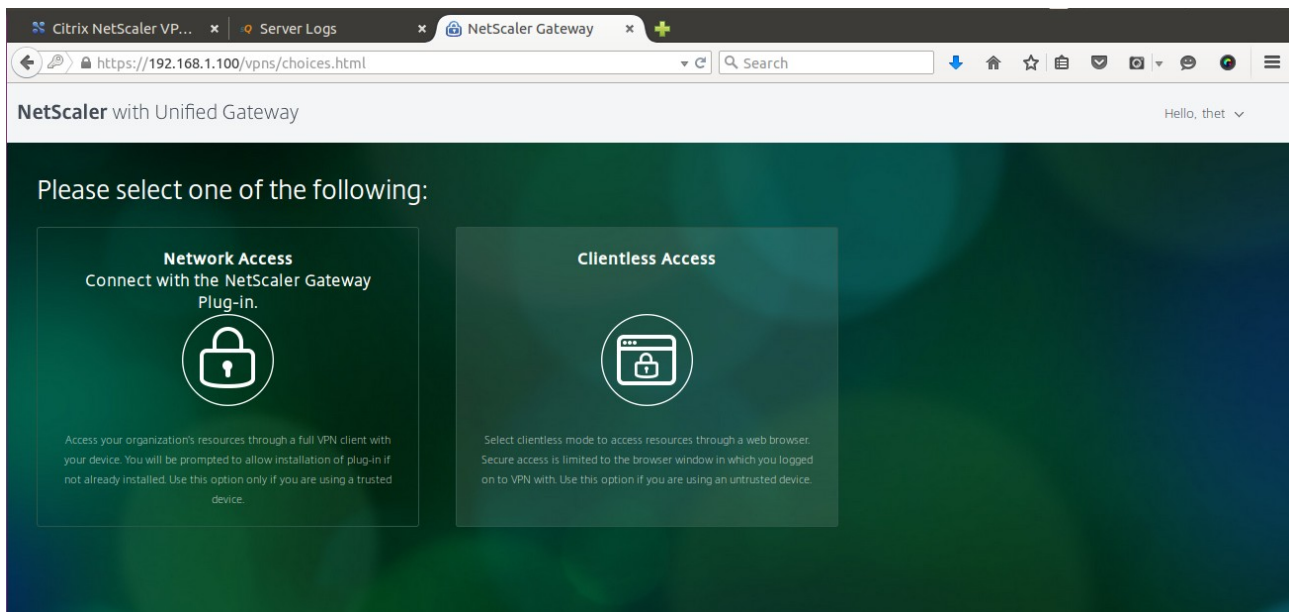


Figure 13 : Successful Access with SSL VPN

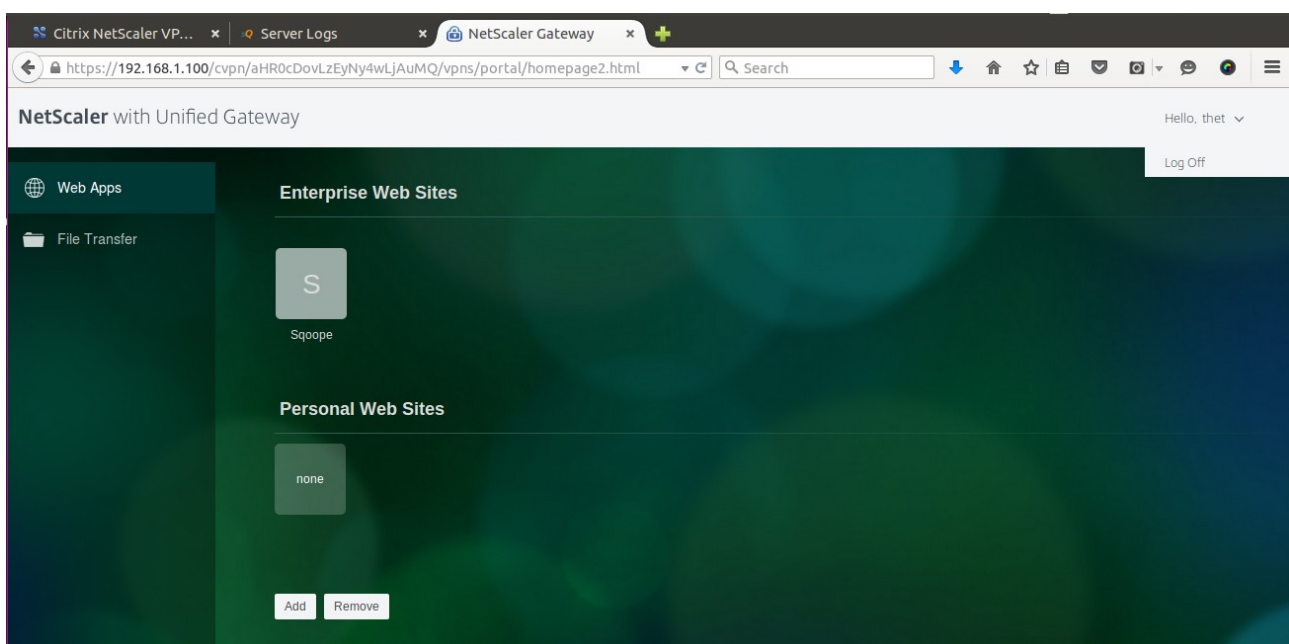


Figure 14 : Successful Access

ConeXa Server Log

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 16:45:58 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 16:49:43 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

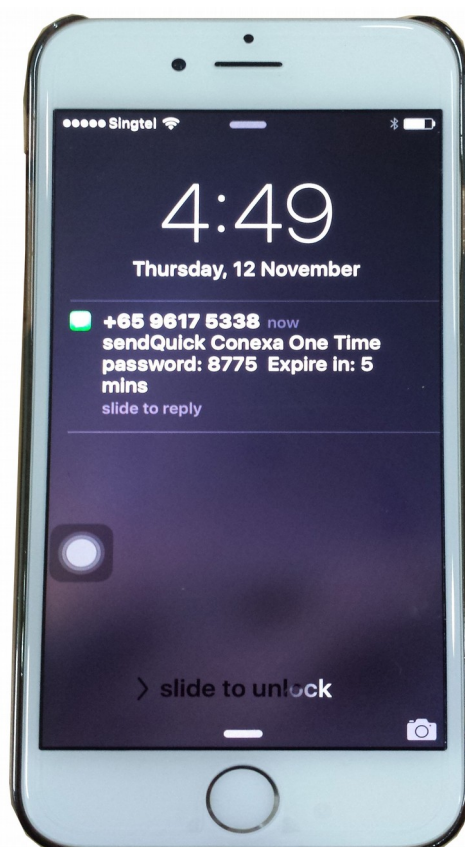


Figure 16 : Received OTP