



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>/

		sendQuick	[®] Conexa						
						Wel	come ot	padmin	(Admin)
Server Log	[Authenti	cation Configuration]	User Management			Lo	gout		
[Radius Client Configuration]	VPN Configuration	Remote DB Configuration	LDAP Server Configuration	Sy	stem Confi	guration			
New Radius Client									
No	Name		Radius Client IP						
		Client list is en	ipty						

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>

sendQuick[®] Conexa

Server Log	[Authentica	tion Configuration]		User Management		Welcome otpadmin (Admin) Logout
[Radius Client Configuration]	VPN Configuration	Remote DB Config	iguration	LDAP Server Configuration	System Configura	tion
		Add	New Radius Clie	ent		
	IP address of the	Radius Client IP : 19 origin Radius client.	92.168.1.99			
	Short name	Name : Cr	itrix NetScaler			
	Shared secret between Radius	Shared Secret : et and Conexa.	•••••			
		S	Submit Reset	J		

Figure 2 : Add New Radius Client

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

sendQuick[®] Conexa

Server Log [Authentication Configuration] User Management Logout Radius Client Configuration VPN Configuration Remote DB Configuration [LDAP Server Configuration] System Configuration New LDAP Server New Logout Remote DB Configuration [LDAP Server Configuration] System Configuration										
Radius Client Configuration VPN Configuration Remote DB Configuration [LDAP Server Configuration] System Configuration New LDAP Server Server										
New LDAP Server										
No Name Description Server 1 Server 2 Login Mode Base DN Scope										
LDAP Server list is empty										

Copyright © 2002-2015, TalariaX Pte Ltd, Singapore. All Rights Reserved Thu, 12 Nov 2015 15:14

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 >

						Welcome	otpadmin (Admin)
Server Log	[Authenticatio	n Configuration]		User Management		Logout	
Radius Client Configuration	VPN Configuration	Remote DB Configura	tion [LC	OAP Server Configuration]	Sys	em Configuration	
		Add New	LDAP Server				
	Unique name	Name : AD					
		Description :	ver				
Primary L	DAP Server IP and port number. LDAP	Server 1: default port : 389.	8.1.213	Port 389			
Secondary L	DAP Server IP and port number. LDAP	Server 2 : default port : 389.		Port			
		Type : Active	Directory 🚽				
Valid login DN &	Service Ac password, which will be used for bindin	g and searching.	admin			Test Service Account	
	Service Acc	ount Password :					
		Login Mode : Login	D <u>-</u> ?				
	Base DN of the lo	Base DN : DC=te	tserver,DC=com				
		Search Scope : Sub	• ?				
	Additional LD Enter additional LDAP s	AP Filter String :			i	?	
		Subm	Reset				

Figure 4 : Add New AD Server

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

				Welcome otpadmin (Admin)
Server Log	[Authentication Configuration]	User Mar	lagement	Logout
Radius Client Configuration	VPN Configuration Remote DB 0	Configuration [LDAP Server C	configuration] S	System Configuration
	4	dd New LDAP Server		
Primar Secondar	onnection Success! , Using LDAP Server	1 (192.168.1.213:389) , Succ	essfully bind to Serv	vice
Valid login DN & pas	Service Account Bind DN : ssword, which will be used for binding and searching.	conexaadmin		Test Service Account
	Service Account Password :	•••••		
	Login Mode :	Login ID - ?		
	Base DN of the location of user list.	DC=testserver,DC=com		
	Search Scope :	Sub - ?		
	Additional LDAP Filter String : Enter additional LDAP search filter string.]2
		Submit Reset		

Figure 5 : Test Service Account

Configuration VPN configuration

				Welcome of	padmin (Admi
Server Log	[A	uthentication Configuration	User Management	Logout	
Radius Client Configuration	[VPN Configuration	n] Remote DB Configura	tion LDAP Server Configuration	System Configuration	
New VPN					
No Name	NAS IP / NAS ID	Description	Authentication Type	Authentication Server	
		VPN			

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

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

sendQuick® Conexa

						Welcome otpadr	nin <mark>(Admin)</mark>
Server Log	[Authentication Confi	guration]		User Management		Logout	
Radius Client Configuration [V	PN Configuration] Re	mote DB C	Configuration	LDAP Server Configuration	System	Configuration	
			Add Now VDN				
			Add New VPN				
Use either NAS-IP-Address of Select None if	NAS-IP / or NAS-Identifier to communicate with NAS-IP-Address and NAS-Identifier a	NAS-ID : Conexa. are empty.	192.168.1.99	NAS-IP-Address	NAS-Identifier	None	
	Unique name of	Name : this VPN.	CitrixNetScaler				
	Des Description of this VPN. For refere	cription : ence only.	Citrix NetScaler				
	Authenticati	on Type :	Two Factor Access	Challenge 🛃			
	Authentication	Server :	LDAP -	?			
	u	DAP Serve	er Configuration (Au	thentication)			
	Return	n Option :	Return LDAP gro	oup as Radius attribute : Filter-Id (1 oup as Radius attribute : Class (25	11))		
Select LDAP server from list, which	LDAF h is predefined in LDAP Server Conf	Server : iguration.	AD 💌				
	OTP Prompt Message (Access Ch	allenge) :	Enter OTP: ^M = User's Mobile r	number , ^E = User's Email addres	S		
	o	ТР Туре :	One Time PIN (OTP OTP - One time usag STP - Limited times	P) • ge only. of usage over validity period			
	OTP Delivery	Method :	SMS -				
	OTP Email	Subject :	Default : SendQuick	Conexa OTP			
	OTP Ema	ail From :	Default : system@[he	ostname] / system@[IP]			
	OTF	Length :	4 • Numer	ic Only O Alphanumeric			
	One Time PIN Validity	y Period :	5 minutes				
			sendQuick Conexa	One Time password: ^P Expire in	: ^E mins		
	OTP Message T	emplate :					
			^P = OTP token , ^E	= Validity period (in minutes) , ^D =	= Date , ^T = Time		
	Messag	ge Mode :	Normal Text	• ?			
Pr	sms iority level of the SMS. Highest = 1, L	Priority : owest = 9	5 -				
	Mode Send SMS via specifi	m Label : c modem.	-NA- 🔻				
	User Con	tact List :	Same as authen	tication server <mark>?</mark>			
	1	DAP Serv	ver Configuration (C	ontact List)			
	Attribut	e Name :	mobile mail	(Mobile) (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 :

💦 NetScaler VPX (1000)		HA Status Not Configured	Info NS11.0 63.16.nc 🔻	Logout	CİTR	X.
Dashboard Configuration	Reporting		3	Documentation	Downloads		\$
+ System	NetScaler > System > System Info	rmation			¢	0	
+ AppExpert							
+ Traffic Management	System Information System Se	essions					
+ Optimization	System Upgrade Reboot Statistics Call Home						
+ Security	System Information						
+ NetScaler Gateway	NetScaler IP Address	192.168.1.99					
	Netmask	255.255.255.0					
+ Authentication	Node	Standalone					
Show Unlicensed Features	Time Zone	GMT+08:00-SGT-Asia/Singapore					
	System Time	Thu, 12 Nov 2015 23:35:20 SGT					
tegrate with Citrix Products	Last Config Changed Time	Thu, 12 Nov 2015 22:56:41 SGT					
	Last Config Saved Time	Thu, 12 Nov 2015 22:56:56 SGT					
🞇 XenMobile	Hardware Information						
	Platform	NetScaler Virtual Appliance 450010					
XenApp and XenDesktop	Manufactured on	9/30/2009					
T Unified Gateway	CPU	2792 MHZ					
	Host Id	000c29532444					
	Serial no	HE2H81UJ47					
	Encoded serial no	891e0000cb254307ee9a					





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>

Dashboard Configuration Re	eporting		Docum	nentation	Downloads	
← Back						
Unified Gateway Configuration						
Virtual Server				Basic	c Settings	^
Virtual Server Name	IP Address	Port			+	
myUnifiedGateway	192.168.1.100	443		1	Virtual Server	~
				2	Server Certificate	
Server Certificate			/		∧ ↓	
📟 🧱 talariax1				3	Authentication	
📼 🕎 talariax1					+	
				4	Portal Theme	
Authentication				5	Applications	
Primary authentication method* RADIUS IP Address* 192 168 197 1812 Time out (seconds)* 3 Secret Key* ••••••• Confirm Secret Key*	IPv6					
Secondary authentication method*						

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.

💲 Citrix NetScaler VP 🗴 🕫	Server Logs × 🙆 NetS	caler Gateway ×	+					iki		
← A https://192.168.1.100/vpn/in	ndex.html		▼ C ^e] Q Search	÷	⋒	☆ 自	•	9	0	Ξ
	NetScaler with	Please log on								
	onined Gateway	User name	thet							
		Password								
			Log On							

Figure 11 : Login page of 1st Authentication

Scitrix NetScaler VP 🗴 🔍 Server Logs 🛛 🗴 🕲 NetSca	ler Gateway × 🕂							
() @ https://192.168.1.100/cgi/login	▼ C Q Search	٠	⋒	☆自	•	ø	0	≡
NetScaler with Unified Gateway	Additional Information Required Please type your response below. Enter OTP: *** Submit							

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]	Server end SMS (op:1899) to thet (91072730) equest from thet (1921681.99) 2FC CHALLENGE equest from thet (1921681.99) 2FC CHALLENGE equest from thet (1921681.99) 2FC ACCEPT p) Received SMS From:Singlel Keyword:We are delighted Monitoring of your Single Wiff I usage will be made availab tf ind VPN with keyword:We p) Received SMS From:+6591072730 Keyword:Test reply th dn VPN with keyword:We sing LDAP (AD) Server 1 (1921681.213:389) heckValidLdapUser (AD) for thet, ModeIoginid, Server(192 FA C 151 authentication success (thet OP- sing LDAP (AD) Server 1 (1921681.213:389) heckValidLdapUser (AD) for thet, ModeIoginid, Server(192 FA C 151 authentication success (thet OP- sing LDAP (AD) Server 1 (1921681.213:389) med SMS (op 8775) to thet (91096771) equest from hAS-P.Address.192.1681.99 NAS-Identif sing LDAP (AD) Server 1 (1921681.213:389) med SMS (op 8775) to thet (91096771) equest from hAS-P.Address.192.1681.99 NAS-Identif Sing LDAP (AD) Server 1 (1921681.99).27C CHALLENGE ****Request from NAS-P.Address.192.1681.99 NAS-Identif sing LDAP (AD) Server 1 (1921681.99).27C MALLENGE ****Request from NAS-P.Address.192.1681.99 NAS-Identif Server(192751) equest from the (1921681.99).27C CHALLENGE *****Request from NAS-P.Address.192.1681.99 NAS-Identif ************************************	rr Log http://www.involutionality.com/involutionality.com/ fierr- (thet)***** to inform you that unlimited Singtel WiFi usage has beer le via MySingtel app soon. T&Cs apply. www.singtel.com fierr- (thet)***** .168.1.213:389) success .1.213:389) : (mobile:91096771, email:thet@talariax.co fierr- (thet)*****	n extended to 29 Feb'16. Enjoy seamless surfing Visingtelwifi						
Refresh Download Log files : current log log 2 log 3 log 4 log 5 log 6									

Figure 15 : Server Logs of sendQuick coneXa



Figure 16 : Received OTP