



# VMWare View 5.1 and SendQuick ConeXa One-time-Password (OTP) Configuration Guide

Prepared by

#### TalariaX Pte Ltd

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

# VMWARE VIEW 5.1 AND SENDQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

## **1.0 INTRODUCTION**

This document is prepared as a guide to configure VMWare View 5.1 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 CONEXA CONFIGURATION

### 2.1 Client Configuration

To create a new client, Go to Configuration -> Client Configuration -> New Client

### 2.1.1 Add New Client

			send UICK® Conexa
Server Log		User Management	[Configuration]
[ Client Configuration ] New Client	VPN Configuration	Remote DB Configuration	LDAP Server Configuration
No		Name	
			Client list is empty

1.100

Radius Server IP	IP address of the View Connection Server.	
Name	Short name of the radius client.	
Secret	Shared secret of the radius client.	



## 2.2 VPN Configuration

To create a new VPN, Go to Configuration -> VPN Configuration -> New VPN

				sendQuick® Conexa
	Server Log		User Management	[Configuration]
Client (	Configuration	[ VPN Configuration ]	Remote DB Configuration	LDAP Server Configuration
New V	/PN			
	Name	NAS IP	Description	Authentication Type
				VPN list is empty

### 2.2.1 Add New VPN

NAS-IP	192.168.1.234		
Name	Unique name of this VPN.		
Description	Description of this VPN. For reference only.		
Authentication Type	Two Factor Access Challenge		
Authentication Server	LDAP LDAP $\rightarrow$ Authentication through LDAP server such as Active Directory or OpenLDAP. Select LDAP server from list, which are predefined in LDAP Server Configuration page.		
User Contact List	Check on 'Same as authentication server' to use the same user list in authentication server. LDAP $\rightarrow$ Select from a list of predefined LDAP servers. Mobile and email attributes are required.		

	Add New VPN			
NAS-IP	192.168.1.234			
Name	VMView			
Description	VMWare View 5.1			
Authentication Type	Two Factor Access Challenge			
Authentication Server	LDAP ‡			
LDAP Server	Configuration (Au	ithentication)		
Return Option	Return LDAP gro	oup as Filter-Id (11) oup as Class (25)		
Server	ldap101 🛟			
OTP Prompt Message (Access Challenge)	Enter OTP: ^M = Mobile numb	er , ^E = Email address		
ОТР Туре	One Time PIN (OTP)			
OTP Method	SMS 💲			
OTP Length	4 🛟 🖲 Numeric Only 🔾 Alphanumeric			
One Time PIN Validity Period	2 minutes			
Message Template	sendQuick Conexa ^P = OTP token , ^	One Time password: ^P Expire in: ^E mins E = Validity period (in minutes) , ^D = Date , ^T = Time		
Message Mode	Normal Text	0		
User Contact List Same as authentication server				
LDAP Serve	er Configuration (C	Contact List)		
Attribute Name	Mobile	(Mobile)		
	Email (Email)			
	Submit Reset			

### 2.3 LDAP Server Configuration

Configuration -> LDAP Server Configuration -> New LDAP Server



### 2.3.1 Add New LDAP Server

Name	Unique name for LDAP server, which will be used as identifier in VPN configuration .		
Description	For reference only.		
Server 1 & Port	LDAP Server IP and port number. LDAP default port : 389		
Server 2 & Port	DAP Server IP (Backup/Secondary) and port number. DAP default port : 389		
Service Account Name & Password	Valid login name & password, which will be used for binding and searching.		
Login Mode	[Display Name   Login ID   Email] Type of login ID for this LDAP server.		
Base DN	Base DN of the location of user list in LDAP.		
Domain	Windows login domain for the user, apply to AD only.		

	Edit LDAP Server
Name	Idap101
Description	
Server 1	192.168.1.101 Port 389
Server 2	192.168.1.102 Port 389
Туре	Active Directory
Service Account Bind DN	conexaadmin Test Service Account
Service Account Password	
Login Mode	Login ID
Base DN	dc=mail,dc=sendquickasp,dc=com
Domain	mail
	Submit Reset

## 3.0 Configuring VMWare View 5.1

To configure for the RADIUS authentication protocol, you modify the View Connection Server settings in View Administrator.

In View Administrator, to set the type of authentication, select:

#### View Configuration > Servers and select a Connection Server.

Select **Details** and then the **Authentication** tab. In the Advanced Authentication area, for the 2-factor authentication field, select **RADIUS** from the drop-down menu.

두 🗞 192.168.1.234 https	://192.168.1.234/admin/#/serv	ег			🕆 🐨 🚱 🚼 🕶 Google	۹ 🏠 👁
VMware View Admi	nistrator	_		_		About   Help   Logout (administrator)
Updated 07/10/2012 04:49:03 PM 2 Remote Sessions 0 Local Sessions 0 Problem Desktops 0 Events 0 0 0 0 0	Servers vCenter Servers Security Enable Disable Edit.	Servers Connection Server	s Transf	er Servers		a <i>e</i>
System Health	Connection Server	Version PCoIP Secure	State	Settings		Last Backup
	VMVIEW	5.1.0-704644 Installed	Enabled	Smart card authentication: Optiona 🛩	07/10/2012 03:00:10 PM	
Source Additional  Source Addit						
Servers						
Froduct Licensing and Usage Global Settings Registered Desktop Sources Administrators ThinApp Configuration Event Configuration						

The diagram below shows Advanced Authentication > Select Radius.

VMware View Adm	nistrator	
Updated 07/10/2012 04:49:03 PM 💭 Remote Sessions 0 Local Sessions 0	Servers           Venter Servers         Connection Servers         Transfer Servers	
Problem Desktops 0 Events 0 1 0	Enable Disable Edit Backup Now     More Commands	<b>a a</b>
System Health I 1 1 0	Connection Server Version PCoIP Secure State Settings VMVIEW 5.1.0-704642 Installard Enabled Smart card authentication 0	Last Backup
Dashboard     Users and Groups     Inventory     Inventory     Dosktops     Desktops     Persistent Disks     ThinApps     Monitoring     Policies     View Configuration     Servers     Product Licensing and Usage     Global Settings     Registered Desktop Sources     Administrators     ThinApp Configuration     Event Configuration	Edit View Connection Server Settings	OK Cancel

Then, at the bottom of the page, select **Authenticator** and select **Create New Authenticator**. This is shown in the diagram below.

VMware View Administ	trator	About   Help   Logout (administrator)
Updated 07/10/2012 04:49:03 PM 😂 S Remote Sessions 0 Local Sessions 0	Servers VCenter Servers Security Servers Connection Servers Transfer Servers	
Problem Desktops 0 Events 0 (A) 0	Enable Disable Edit Backup Now    More Commands	8
System Health	Connection Server Version PCoIP Secure State Settings MMEW 5.1.0-200504 Installed Exabled Smart card exthemication: Online: ef 07(10/2012.03)00:10	Last Backup PM
Deshboard Deshb	Edit View Connection Server Settings	

After selecting a new authenticator, a new screen to Add RADIUS Authenticator as shown below. Follow the explanation in the table below to complete the form.

VMware View Admir						About   Help   Logout (administrator)
Updated 07/19/2012 04 49 03 PM 💩 Remote Sessions 0	Servers vCenter Servers	Security Se Add RADIUS Authenticato	r			
Local Sessions 0 Problem Desktops 0 Events 0 (A) 0 System Health 1 (B)	Enable Di Edit V Connectio G	ew Connect A RADIUS authenticator	is available to all Connecti	on Servers in this View environment.	0	E 2
1 1 1 0	VMVIEW	Label: anges to au	MyToken	Enter a label that will be shown to clients	PM	
▼ Inventory Pools Desktons	Sn [	nart card au Description: Disconne Primary Authenticatio	MyToken RADIUS Au	thenticator		
Persistent Disks ThinApps Monitoring	Ad 2-f	wanced Au actor authe Hostname/Address:	192.168.1.42		8	
► Policies ▼ View Configuration Servers		Use the	PAP V	g port: 1813		
Product Licensing and Usage Global Settings Registered Desktop Sources Administrators		Authenticato Sinai eu seu e. Server timeout Max retries:	3 seconds			
ThinApp Configuration Event Configuration		Realm prefix: Realm suffix:			C Cancel	
			_	Next > Cancel		

HostName/Address	IP address of sendQuick Conexa
Port	1812
Shared Secret	Shared secret of the sendQuick Conexa

Select on **Finish**, when completed (as shown below). This will complete the Radius server configuration on VM Ware View 5.1 for integrating to sendQuick Conexa.

-					where I mater I manage to destruct and
VMware View Admir	listrator				About [ Help ] Cogsuc (administrator)
Updated 07/10/2012 04:49:03 PM	Servers				
Remote Sessions 0	vCenter Servers Security	Add RADIUS Authenticato			
Local Sessions 0		Correction Authorities	tion Conver		
Events 0 0 0 0	Enable Disable Edit	Secondary Authentica			🖬 🤤
System Health 🔳 🗐 💽	Connection Server	Use a secondary server if primary is unavailable		Lac	t Backup
1 1 1 0	And the connection server	1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.		67/10/2012 02:00:10 DM	Саскар
Cashboard	Edit View Connection	Hostname/Address:		0	
👸 Users and Groups		Authentication port	1812 Accounting port 1813	and the second se	
▼ Inventory	General Loca	Authentication type:	PAP		
Pools		Sharad carrat			
🗇 Desktops	Changes to auther	Shared Secree			
ThinApps	Smart card auther	Server timeout:	3 seconds		
<ul> <li>Monitoring</li> </ul>	Disconnect u	Max retries:	5	8	
► Policies		Realm prefix:			
View Configuration	Advanced Authe				
Servers	2-factor authentica	Realm suffix:			
Product Licensing and Usage	Enforce 2-fa				
Registered Desktop Sources					
Administrators					
ThinApp Configuration	Authenticator:				
Event Configuration					
			< Back Finish C	Cancel	
			24	OK Cancel	

## 4.0 Testing the 2FA Integration

First, start the VMWare View Client and enter the information of the server that you wish to connect to. The server information is entered in the **Connection Server** field as shown below. Select **Connect** when ready.

NMware View Clier	ıt	
Vmwar VMw	e	
Enter the host name o	f the View Connection Server.	
Connection Server:	192, 168, 1, 234	•
Connect	Exit Help	Options >>

Then, enter **User Name** and **Passcode (password)** when prompted as shown below. This is the the AD username and password, if using AD.

VMware Vie	w Client	_ <b>_ X</b>
VII VII	Nware: ⊡Pcolle:	
	Mware View <sup>™</sup>	
https://192	. 168. 1. 234	
Enter your My	oken user name and passcode.	
User name:	thet	
Passcode:		
Support Inform	ation	

You will receive the SMS OTP message as shown below (left). At the same time, the Enter OTP page will be shown as seen on diagram below (right). Enter the OTP received via SMS in the space provided.



	/are' ⊡rco⊪ ware Vie	9* ?₩™	
<b>10 https://1</b> 92.16	8.1.234		
Enter your next M	yToken response in t	he field below.	
Next response:			
Support Information	<u>on</u>		
	ОК	Cancel	Help

Once successful, you will login to the application.