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.

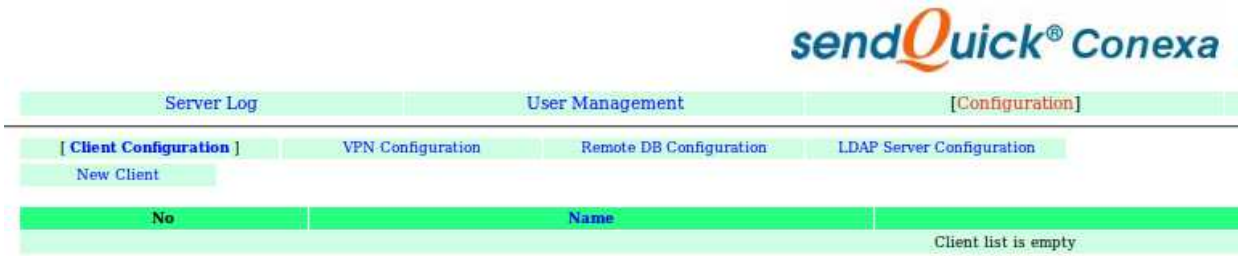
The pre-requisite is that SendQuick Conexa OTP server is configured with RADIUS on port 1812. Ensure that both applications are using the same port for radius.

2.0 CONEXA CONFIGURATION

2.1 Client Configuration

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

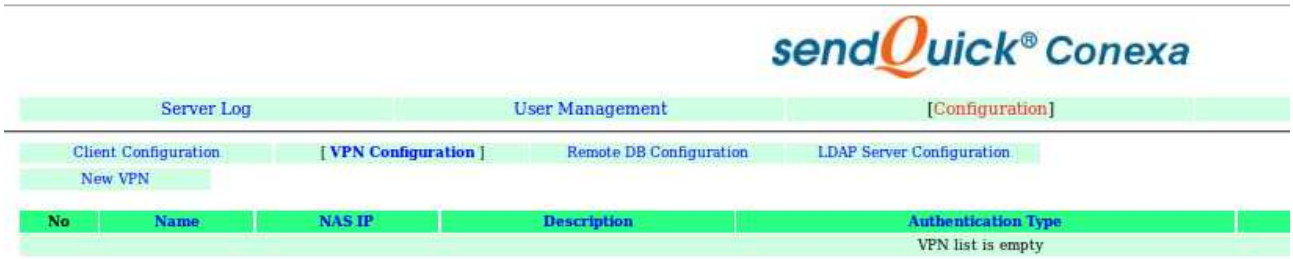
2.1.1 Add New Client



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



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 → 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 → Select from a list of predefined LDAP servers. Mobile and email attributes are required.

Add New VPN

NAS-IP	192.168.1.234 (•) NAS-IP-Address ( ) NAS-Identifier
Name	VMView
Description	VMWare View 5.1
Authentication Type	Two Factor Access Challenge
Authentication Server	LDAP
LDAP Server Configuration (Authentication)	
Return Option	[ ] Return LDAP group as Filter-Id (11) [ ] Return LDAP group as Class (25)
Server	ldap101
OTP Prompt Message (Access Challenge)	Enter OTP: ^M = Mobile number , ^E = Email address
OTP Type	One Time PIN (OTP)
OTP Method	SMS
OTP Length	4 (•) Numeric Only ( ) Alphanumeric
One Time PIN Validity Period	2 minutes
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
User Contact List	[x] Same as authentication server
LDAP Server Configuration (Contact List)	
Attribute Name	Mobile (Mobile) Email (Email)
	Submit Reset

2.3 LDAP Server Configuration

Configuration -> LDAP Server Configuration -> New LDAP Server

sendQuick® Conexa

Server Log | User Management | [Configuration]

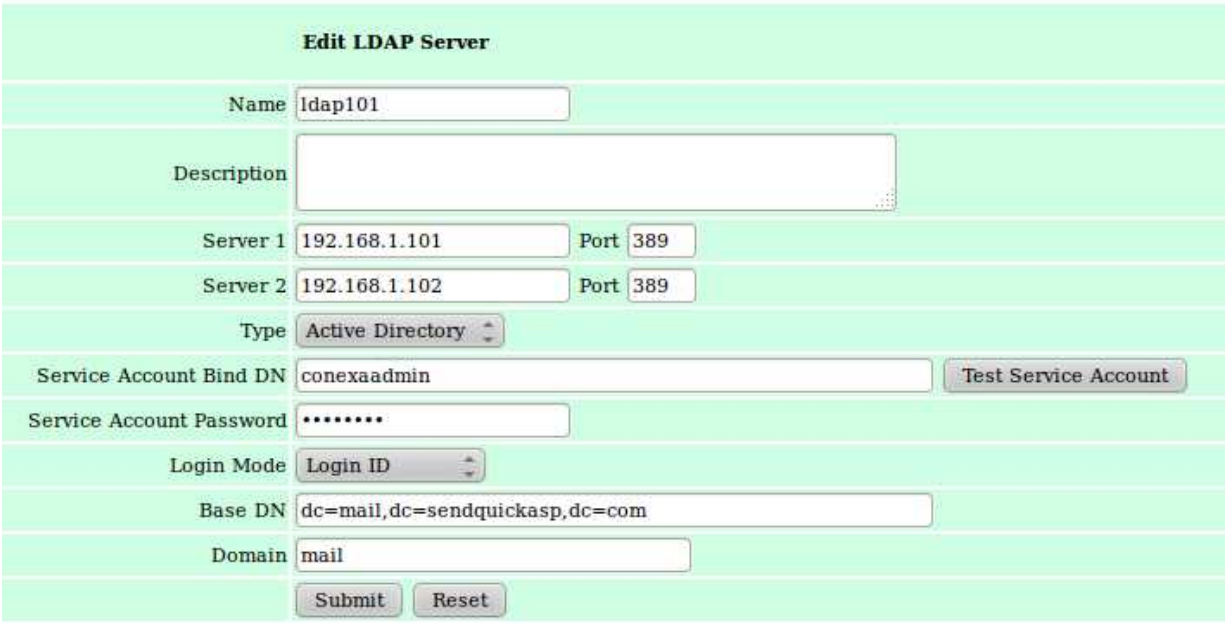
Client Configuration | VPN Configuration | Remote DB Configuration | [LDAP Server Configuration]

New LDAP Server

No	Name	Description	IP 1	IP 2	Login Mode
LDAP Server list is empty					

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	LDAP Server IP (Backup/Secondary) and port number. LDAP 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.



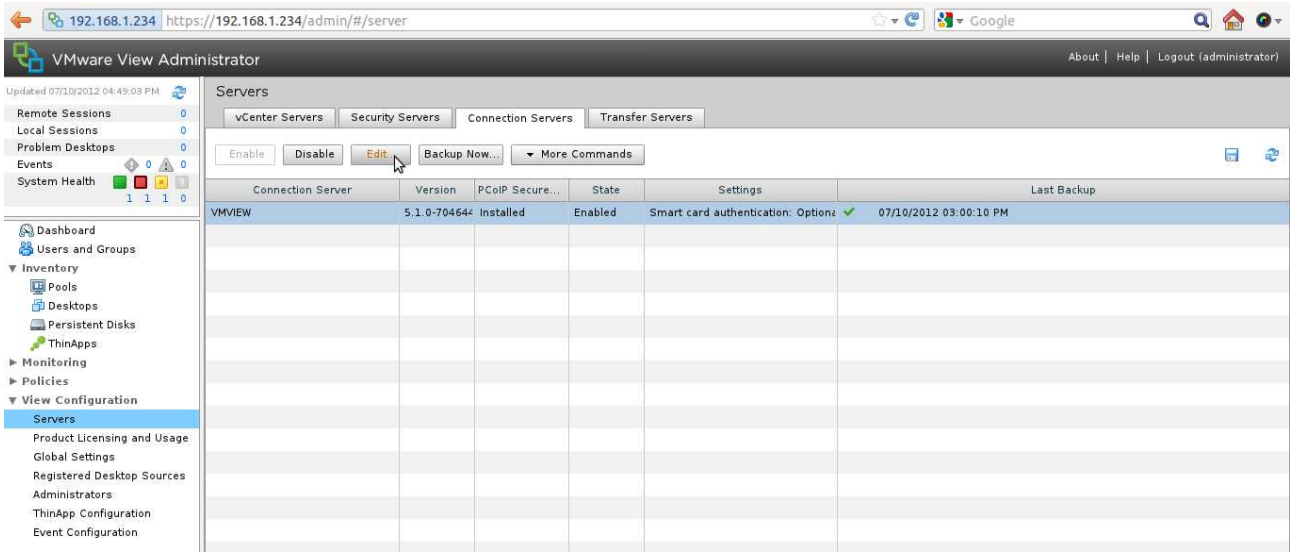
3.0 Configuring VMWare View 5.1

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

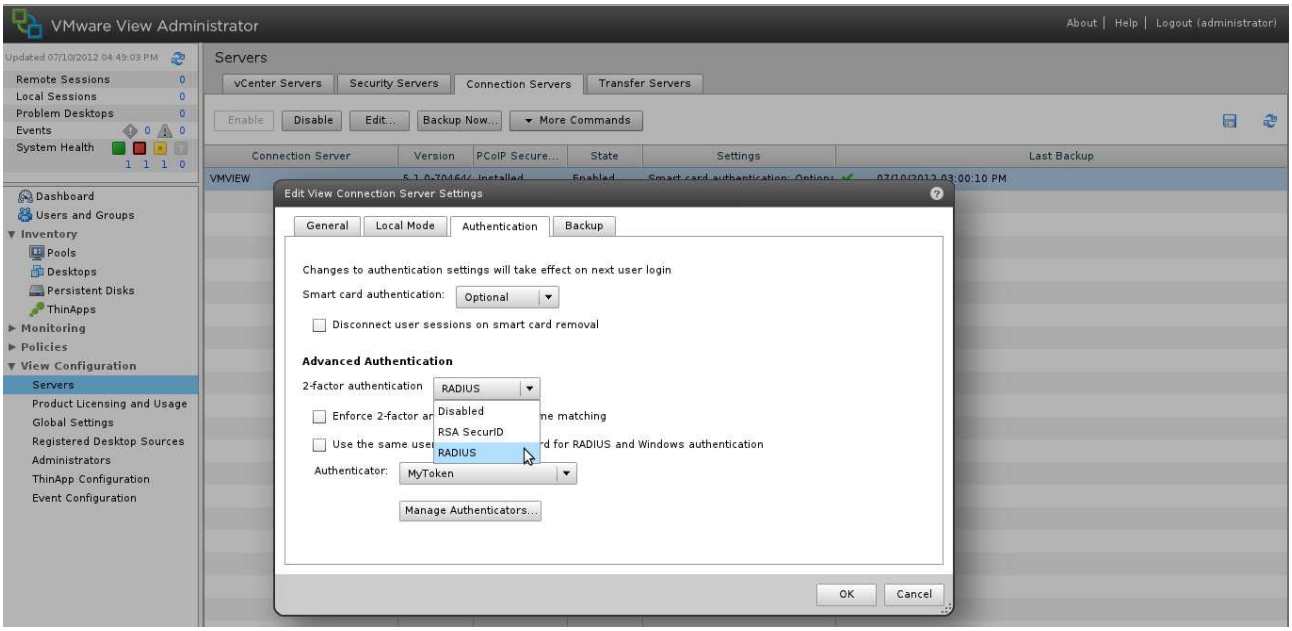
In View Administrator, to set the type of authentication, select:

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

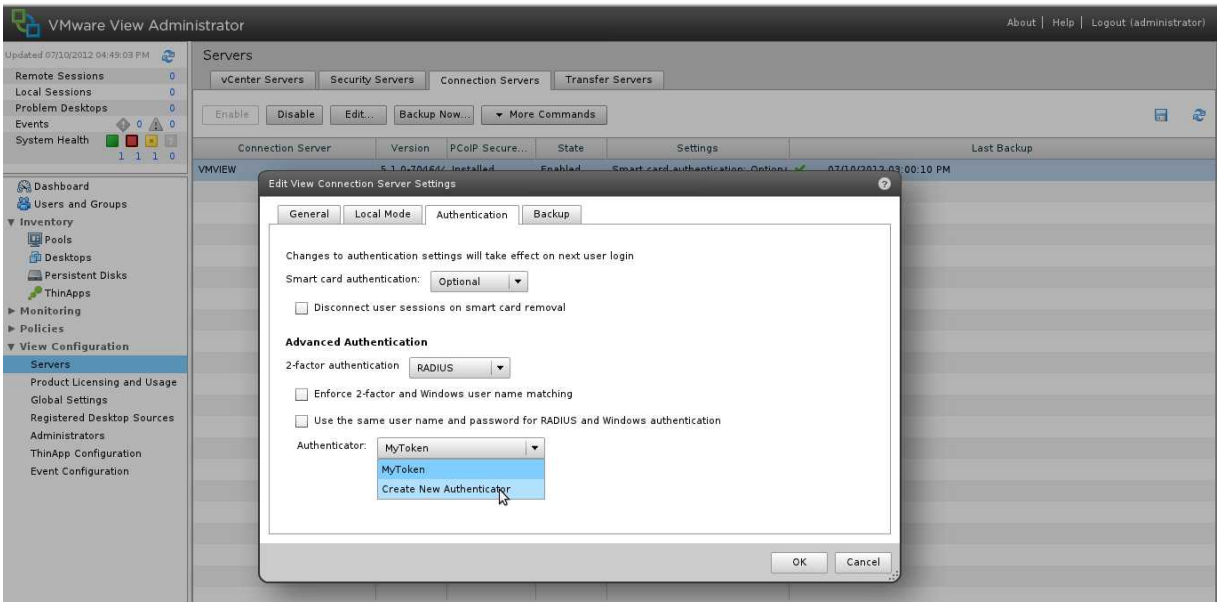
Select **Details** and then the **Authentication** tab. In the Advanced Authentication area, for the 2-factor authentication field, select **RADIUS** from the drop-down menu.



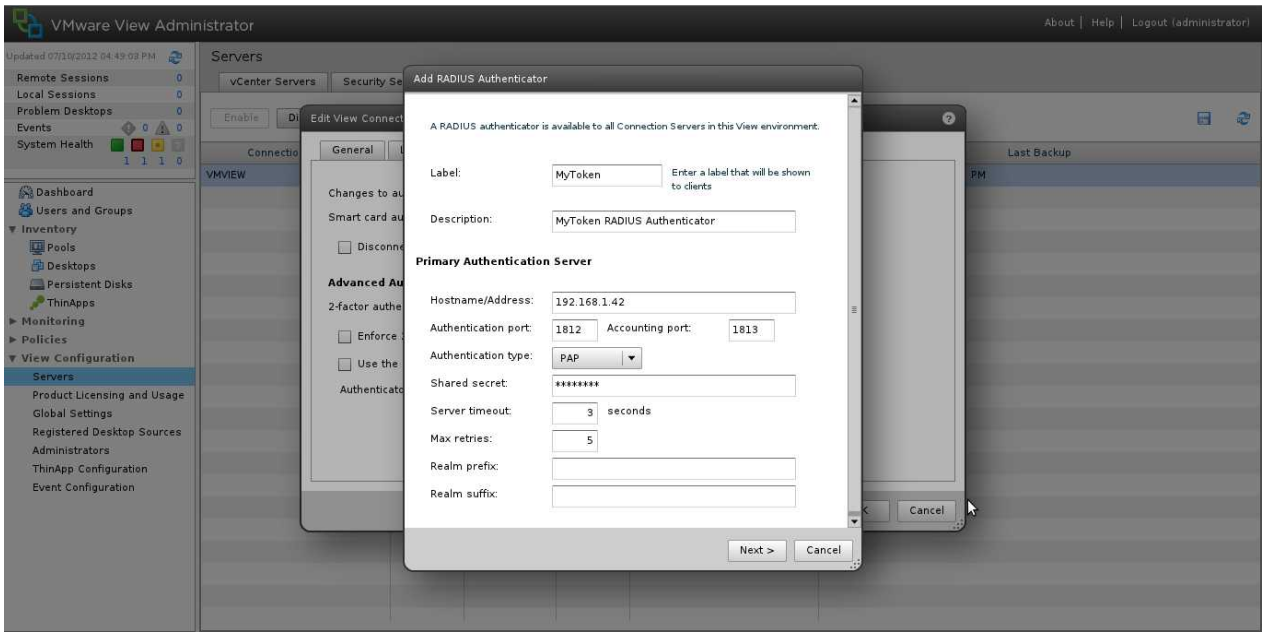
The diagram below shows Advanced Authentication > Select Radius.



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

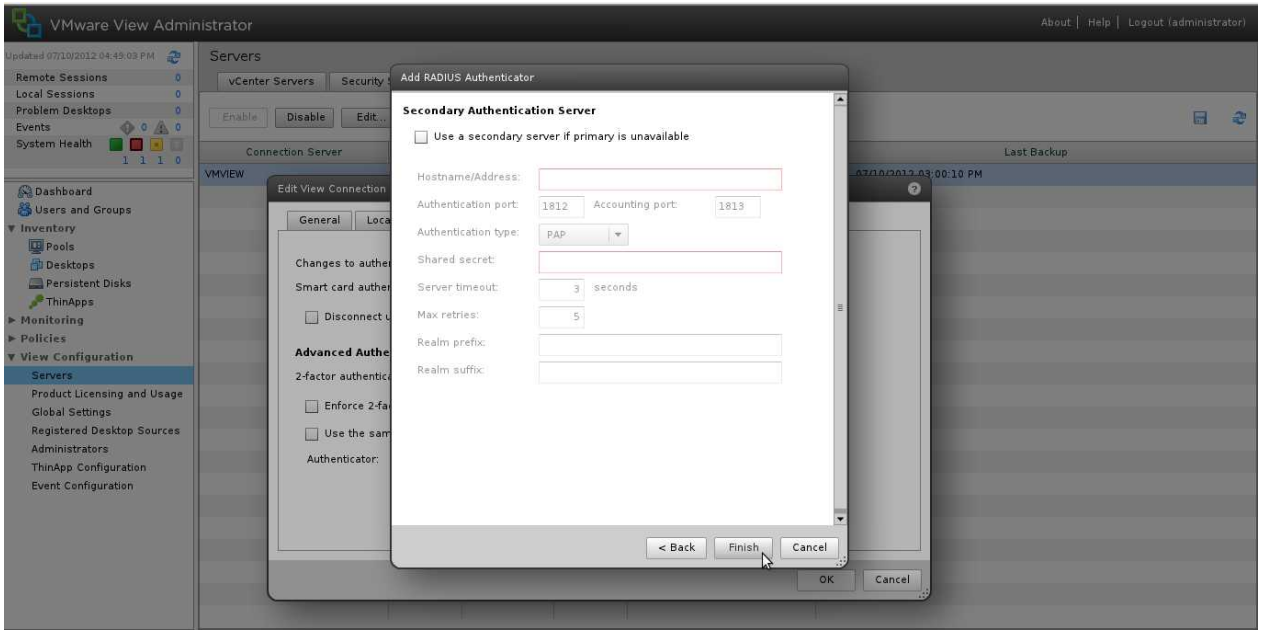


After selecting a new authenticator, a new screen to Add RADIUS Authenticator as shown below. Follow the explanation in the table below to complete the form.



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

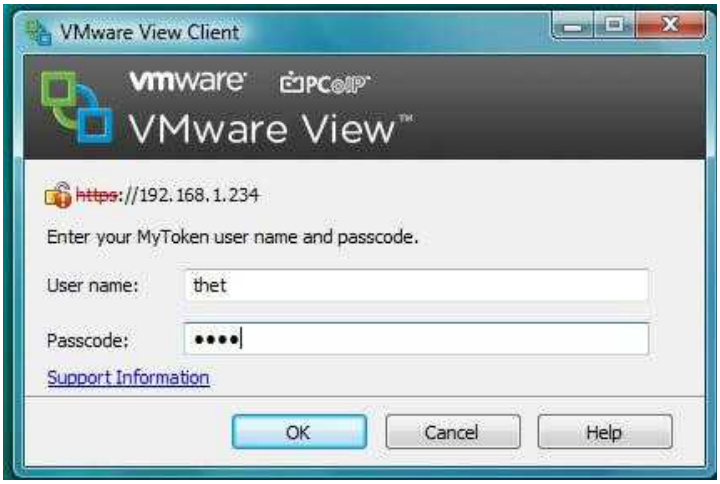
Select on **Finish**, when completed (as shown below). This will complete the Radius server configuration on VM Ware View 5.1 for integrating to sendQuick Conexa.



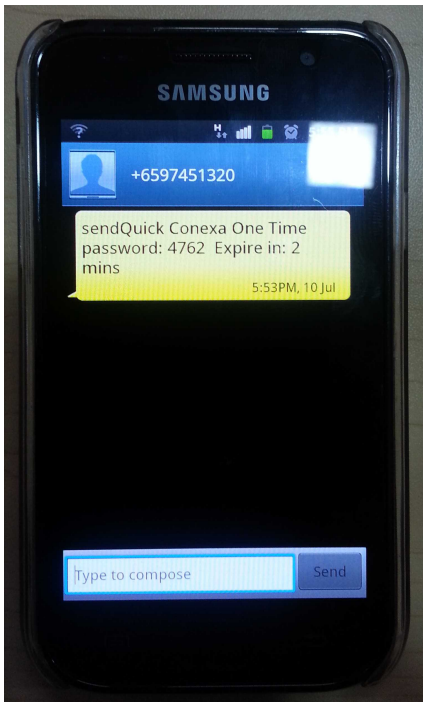
4.0 Testing the 2FA Integration

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.

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



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.



Once successful, you will login to the application.

