F5 Firepass SSLVPN 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

E-mail: info@talariax.com
Web: www.talariax.com

F5 FIREPASS SSL VPN & SENQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

1.0 INTRODUCTION

This document is prepared as a guide to configure F5 Firepass SSL VPN to integrate 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 F5 FIREPASS

In the F5 Firepass configuration, select **Users > Groups > Master Groups,** and then select the **Create New Group** button.

Then, Create New Group and provide a **Name** for the group.

In the **Users in Group** list, select the **External** setting. From the **Authentication method** list, select **RADIUS**.as shown below.

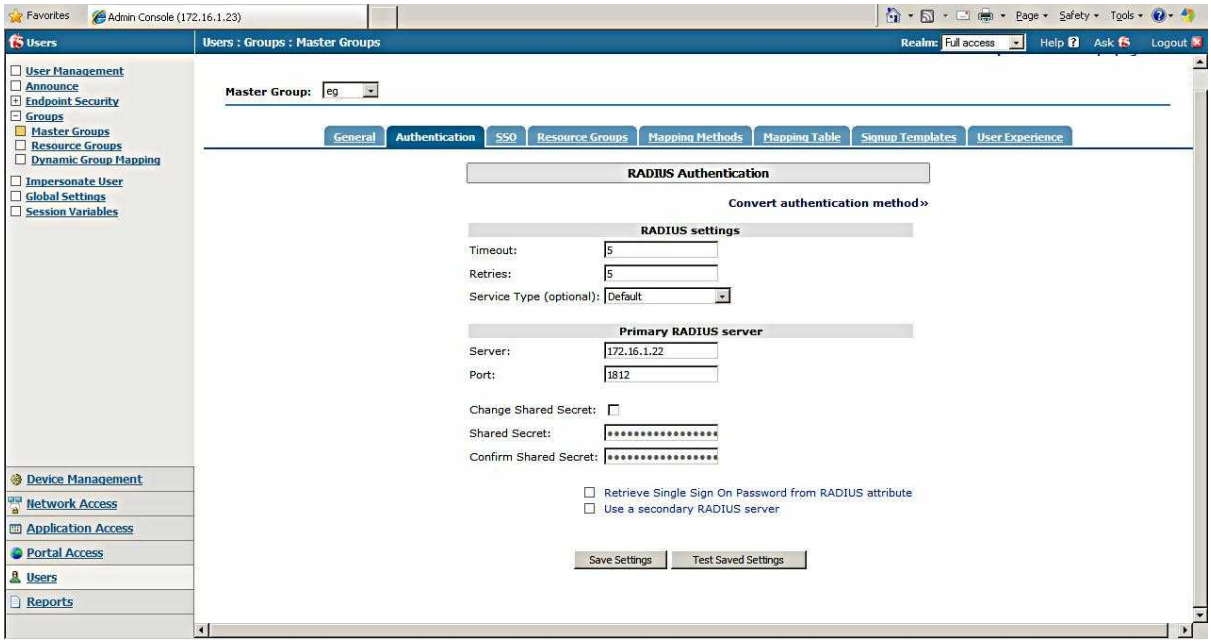

Figure 1: Authentication Server Configuration

You will need to configure the following as shown above:

Items	**Description**
Timeout	The time lapse before it is a timeout for the authentication process. Configure a higher value, between 10-20 seconds
Retries	Number of radius retries.
Service Type	Keep as default
Server	This is the IP of radius server. Put sendQuick Conexa IP in this field
Port	Radius port, set to **1812**
Shared Secret	The share secret for radius authentication, which is the same secret to be configured in sendQuick Conexa
Confirm Shared Secret	Repeat the secret in this field for confirmation

Once the configuration is completed, select the **Save Settings** button.

Once you have configured the Radius server integration on sendQuick Conexa, you can select the Test Saved Settings button to test the radius integration between F5 and sendQuick Conexa.

Once this is completed, you are ready to configure sendQuick Conexa to complete the 2-factor authentication integration.