



SonicWall SSL VPN and SendQuick for 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

JUNIPER SA SSL VPN & SENQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

1.0 INTRODUCTION

This document is prepared as a guide to configure Juniper SA SSL VPN 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.

It is recommended that the Juniper SSL VPN to be running firmware 6.5R5 (15991)

2.0 CONFIGURE JUNIPER SSLVPN

In the Juniper SSL VPN configuration, selection **Authentication > Authentication Servers** and configure **NEW RADIUS Authentication Server** as shown below.

The screenshot displays the Juniper Administrator Console interface. The left sidebar shows a navigation menu with categories: System, Authentication, Administrators, Users, and Maintenance. The main content area is titled 'Auth Servers > sendQuick' and contains a 'Settings' tab. The configuration fields are as follows:

Name:	sendQuick	Label to reference this server.
NAS-Identifier:	192.168.1.144	Name of the device as known to Radius server
Primary Server		
Radius Server:	192.168.1.144	Name or IP address
Authentication Port:	1812	
Shared Secret:	*****	
Accounting Port:	1813	Port used for Radius accounting, if applicable
NAS-IP-Address:	192.168.1.144	IP address
Timeout:	30	seconds
Retries:	0	
<input type="checkbox"/> Users authenticate using tokens or one-time passwords		
<small>Note: If you select this, the device will send the user's authentication method as "token" if you use SAML, and this credential will not be used in automatic SSO to backend applications.</small>		

Figure 1: Authentication Server Configuration

You will need to configure the following as shown above:

- Name (of the authentication server)
- NAS Identifier (include a name)
- Radius Server (IP address of sendQuick Conexa)
- Authentication Port (for Radius): 1812 (this must be 1812 as this is the port used in Conexa)
- Shared secret (the same secret need to be included in Conexa)
- Accounting port and others are optional

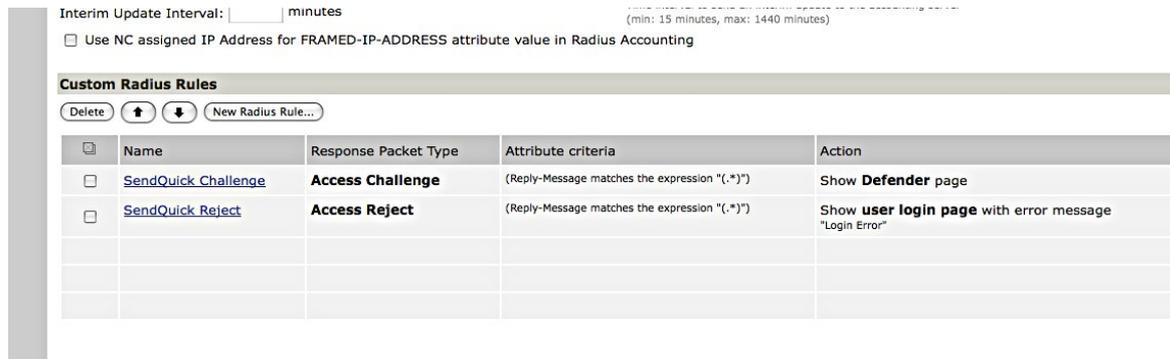


Figure 2: Custom Radius Rule

Then, configure the Custom Radius Rules as shown above to allow Juniper to show the right page for Access Challenge and Error page respectively.

Note:

“Access Challenge” has to be added where the “Reply-Message” matches the expression “(.*)” and in that case shows “show GENERIC LOGIN page”. This will present the OTP field for the user.

Edit the Custom Radius Rule as shown in Figure 3 and 4 below. The final result should be as shown in Figure 2.

Figure 3 is the Custom Rule for Access Challenge while Figure 4 is the Custom Rule for Access Reject.

Status > Configuration > Network > IF-MAP Federation > Log/Monitoring > **Authentication** > Signing In > Endpoint Security > Auth. Servers

Auth Servers > sendQuick > **Edit Custom Radius Rule**

Name:

If received Radius Response Packet ...

Response Packet Type:

Attribute criteria:

Radius Attribute	Operand	Value	
<input type="text" value="Reply-Message (18)"/>	<input type="text" value="matches the expression"/>	<input type="text"/>	<input type="button" value="Add"/>
Reply-Message	matches the expression	(.*)	<input type="button" value="X"/>

Then take action ...

show **New Pin** page

show **Next Token** page

show **Generic Login** page

show **user login page** with error message

show **Reply-Message** attribute from the Radius server to the user

Figure 3: Custom Radius Rule Editing

Status > Configuration > Network > IF-MAP Federation > Log/Monitoring > **Authentication** > Signing In > Endpoint Security > Auth. Servers

Auth Servers > sendQuick > **Edit Custom Radius Rule**

Name:

If received Radius Response Packet ...

Response Packet Type:

Attribute criteria:

Radius Attribute	Operand	Value	
<input type="text" value="Reply-Message (18)"/>	<input type="text" value="matches the expression"/>	<input type="text"/>	<input type="button" value="Add"/>
Reply-Message	matches the expression	(.*)	<input type="button" value="X"/>

Then take action ...

show **New Pin** page

show **Next Token** page

show **Generic Login** page

show **user login page** with error message

show **Reply-Message** attribute from the Radius server to the user

Figure 4: Custom Radius Rule Editing (Access Reject)

3.0 CREATE USER REALM

Create User Realm that use the Authentication Server created in Section 2.0 above for authentication and configure the connection to sendQuick Conexa.

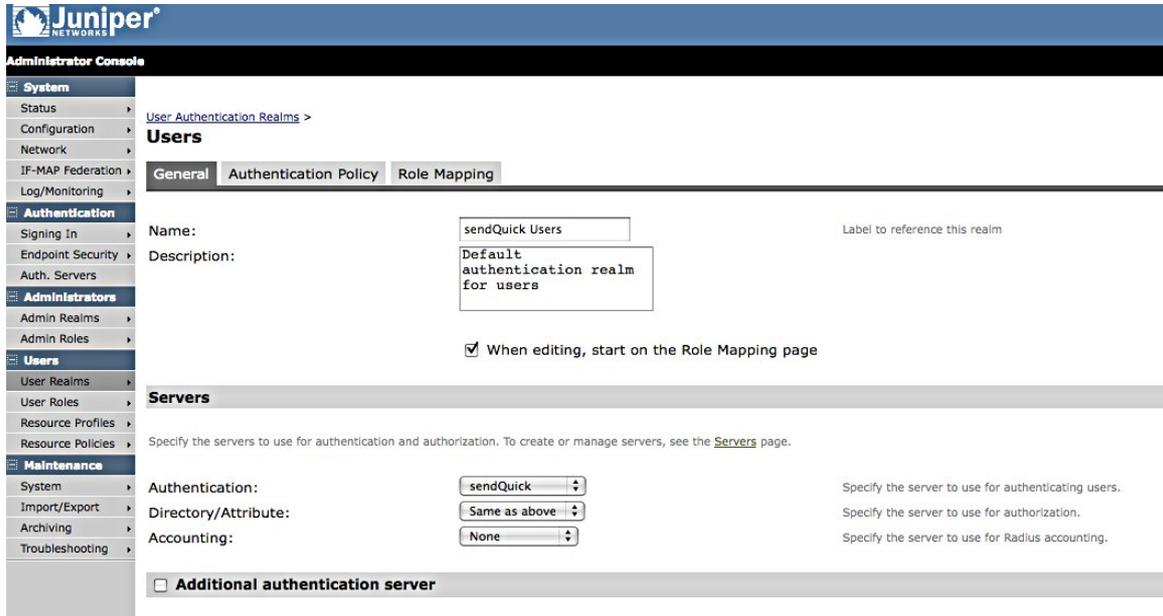


Figure 5: User Realm Configuration

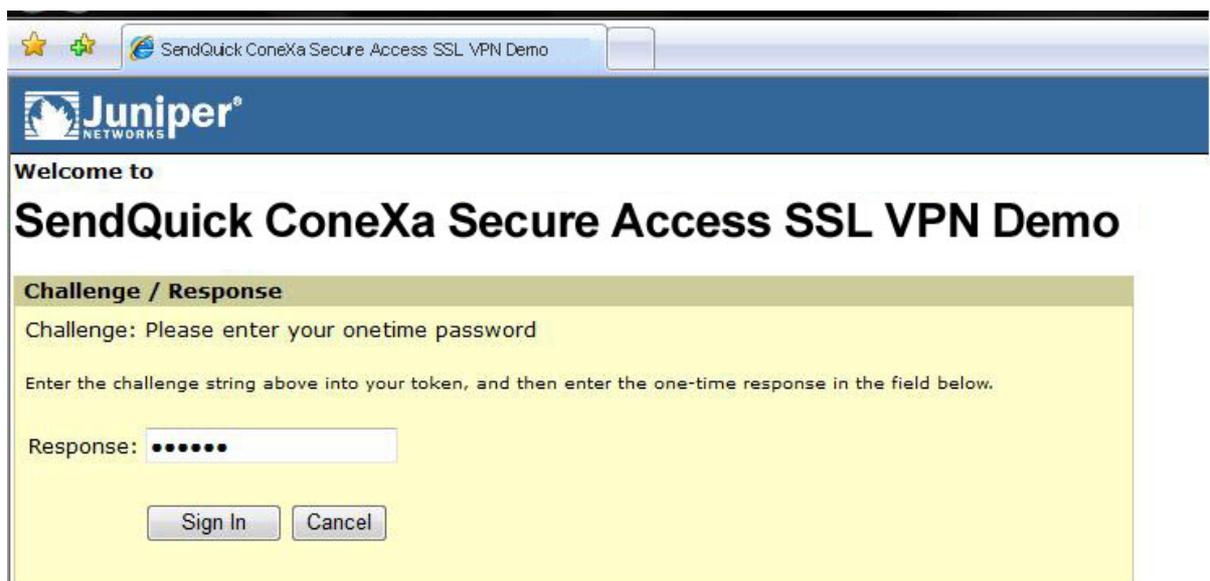
4.0 CREATE SIGN-IN POLICY

Create a Sign-In Policy that uses the Sign In Page from 2.0 and User Realm from 3.0. The login pages can be customized with text and logos of your choice for your users to view.



The screenshot shows a web browser window with the address bar displaying "SendQuick ConeXa Secure Access SSL VPN Demo". The page features the Juniper Networks logo in the top left corner. Below the logo, the text "Welcome to" is followed by the main heading "SendQuick ConeXa Secure Access SSL VPN Demo". There are two input fields: "Username" with a placeholder "<username>" and "Password" with a masked field of seven dots. To the right of the password field, the text "Please sign in to begin your secure session." is displayed. A "Sign In" button is located below the password field.

Figure 6: First Login Page



The screenshot shows the same web browser window as Figure 6. The page content has changed to a challenge-response screen. It features the Juniper Networks logo and the heading "Welcome to SendQuick ConeXa Secure Access SSL VPN Demo". Below this, a yellow box contains the text "Challenge / Response". The challenge text reads: "Challenge: Please enter your onetime password" and "Enter the challenge string above into your token, and then enter the one-time response in the field below." There is a "Response:" label followed by a masked input field with seven dots. At the bottom of the yellow box, there are two buttons: "Sign In" and "Cancel".

Figure 7: OTP Challenge-Response Page