



F5 SSL VPN 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

F5 SSL VPN & SENDQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

1.0 INTRODUCTION

This document is prepared as a guide to configure F5 SSL VPN to run with SendQuick Conexa for One-time-password via SMS.

TESTING ENVIRONMENT			
Product Name			
SendQuick Conexa	F5 Big IP Access Policy Manager		

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 SSLVPN

Open a web browser and access the Internet address (URL) for F5 access. To create an AAA server

- On the Main tab, expand Access Policy, and then click AAA servers.
- Click the Create button.
- In the Name box, provide a name for the sendQuick Conexa (eg, Conexa).
- From the Type list, select the RADIUS protocol.
- Mode : Auth
- Auth Host : IP address of sendQuick Conexa
- Auth Service Port : 1812 (this must be 1812 as this is the port used in Conexa)
- Shared secret (the same secret need to be included in Conexa)
- NAS IP Address : IP address of F5
- Timeout configure a value of between 40-60 seconds (value need to be higher than 25 seconds for the system to perform well)

• Click Finished.

BIG-	IP® - bigip1 (192.168.1	L.239)	-		
Main Help About Acce			Access Policy	ers 💀 New Server	
	Overview Access statistics, performance graphs, and links to helpful too	ils.	General Properties		
Ê	Templates and Wizards Greate common application tra and system configurations.	affic	Туре	RADIUS	
			Configuration		
0:0	Local Traffic Control the delivery of applicat	ion	Mode	Auth Accounting Auth & Accounting	LT.
	traffic for a local area network		Auth Host	< SendQuick OTP Server IP >	
	Access Policy		Auth Service Port	1812	
00	Access Profiles	18	Secret		
	AAA Servers	\oplus			
	ACLs	\odot	Confirm Secret		
	SSO Configurations	\odot	NAS IP Address	< F5 IP >	
	Webtops	\odot	Timeout	30 seconds	
	Network Access	- 90	Retries	3	
	Web Applications	E	0		
	Connectivity Profiles	\odot	Service Type	Default	
	Rewrite Profiles	•	Cancel Finished		
	Reports	×			
Done					

Figure 1: New AAA server configuration

To Edit the Access Profile

1. On the Main tab, expand Access Policy, and then click Access Profiles.



Figure 2 : Access Profiles List

2. Locate the Access Profile you created, and in the Access Policy column, click Edit. The Visual Policy Editor opens. (See Figure 3)

3. Click the + symbol between Logon Page and Deny.

4. In the Authentication section, click the RADIUS Auth option button, and then click the Add Item button.



Figure 3 : RADIUS Authentication box on the Visual Policy Editor

5. From the Server list, select the AAA Source you created in Creating an AAA resource, (see Figure 4).

Strictly Private and Confidential

🕞 BIG-IP® - bigip1 (192.168 🗱 🌀 BIG-IP®	- VPE - vpn-access 🗱 🚽	F	¥
f5		<u></u>	Close
Access Policy: vpn-access-policy	Properties Branch Rules	N	
	Name: RADIUS Auth		
Start fallback + Logon Page fallback	RADIUS		
RADIUS AU	AAA Server	Conexa 💌]
	Show Extended Error	Enabled 💽	1
	Max Logon Attempts Allowed	3 💌].
Add New Macro			
An access policy consists of a start point, actions, and a inside the box. To delete an action, click on the x on th items, to simplify access policy creation. You can get started with <u>Device Wizards</u> . On the main r wizard, to create a simple access policy that you can in access policy. Please see the <u>Online Help</u> for more Visual Policy Edit	Cancei	Heip	the link folicy on ling an

Figure 4 : RADIUS Authentication box on the Visual Policy Editor

6. Click the Save button. You now see two paths, Successful and Fall Back. (See Figure 5)

🚯 BIG-IP® - bigip1 (192.168 💥	🚯 BIG-IP® - VPE - vpn-access 💥	
6		
Access Policy: vpn-access-	policy Edit Endings (Endings: Allow	, Deny [default])
fallback	× Successful	
Start + Logon Page	RADIUS Auth	Allow
	/+	Denv
Add New Macro		

Figure 5 : Final result of our Access Policy example

Once the configuration is completed, select Apply Access Policy as shown in Figure 6 below.

Strictly Private and Confidential

Mair	h Help About	Access Po	licy » Access	Profiles : Access Profiles List					
	Overview Access statistics, performance graphs, and links to helpful tools.	🕸 👻 Prot	file List	Windows Group Policy List					
Ê	Templates and Wizards Create common application traffic	* ✓ ▼ Sta	atus 🔺 Name	Search	Partition	Access Policy	Export	Copy	Virtual Servers
	and system configurations.		access vpn-acces	ss-policy	Common	(none)	(none) Export	(none) Copy	conexa_sslvpn
	Control the delivery of application traffic for a local area network.	Delete,	Apply Access P	olicy					

Figure 6 : Apply Access Policy

To select the name of the policy, On the Main tab, expand Local Traffic, click Virtual Servers and then select virtual server you created.

In the Access Policy section, from the Access Profile list, select the name of the policy you created in an Access Profile List.

Access Profile	vpn-access-policy -
Connectivity Profile	vpn-connectivity -
Rewrite Profile	None •

Figure 7 : Access Policy section of the virtual server configuration

3.0 CONFIGURE SENDQUICK CONEXA

Log in to sendQuick ConeXa Admin Page (Fig 8). Select New Radius Configuration.

Configure the following items as below

- IP address and description IP address and description for F5
- Radius status Enable
- Radius Secret Use the same shared secret text string that was earlier configured on F5

Click Submit when completed

Management		Configuration
	New Radius	s Configuration
Radius IP:	192.168.6.239	
Radius Description:	F5	
Radius Status:	Enable 🛟	
Radius Secret:		
Verify Secret:		

Figure 8: Radius configuration on sendQuick

Next, go to **Configuration** tab and select **New OTP Configuration**. See Figure 9 below.

Configure the following items as below:

- NAS IP and VPN description F5 NAS IP and desc
- Authentication Type Select desired authentication type

If LDAP is used, configure the following:

- LDAP Login Mode and IP address LDAP server login details and IP address
- LDAP Query Attribute LDAP Query Attribute for sendQuick to access. For example, "mobile" for the mobile number used by sendQuick to deliver OTP by SMS
- LDAP Base DN
- LDAP Domain

User Management	[Configuration]	
	New OTP Configuration	
NAS-IP:	192.168.1.239	
VPN Description:	F5	
Authentication Type:	2nd Factor LDAP OTP (Remote)	۵
LDAP Login Mode:	Login ID 🛟	
LDAP Server:	192.168.1.101	
LDAP Server 2:		
LDAP Query Attribute: (leave blank to use default value)	mobile	
LDAP Base DN:	dc=mail,dc=sendquickasp,dc=com	
LDAP Domain:	mail	
LDAP Service Account:		
LDAP Service Account Password:	Enter Password:	
	Confirm Password:	

Figure 9: 2 Factor Authentication configuration on sendQuick

4.0 REMOTE ACCESS WITH TWO FACTOR AUTHENTICATION

I. Using F5 Edge Client

Establish a SSL VPN connection using the F5 Edge Client. After click connection, the page for Username and Password will appear as shown in Figure 10 below.

	https://20.1.1.8 - BIG-IP Edge Client**	
BIG-IP Edge Cliv	6	
Conr Server	SendQuick ConeXa Secure Access SSL VPN Demo	
Course divers	Username	
Connection	useraccount	
🥘 Auto-Con	Password	
Establish a conne		
'Disconnect' but	Logon	
Change Server		
Service States		~
		Cancel

Figure 10 : F5 Login with Username and Password

Enter the Username and Password and click Logon. Once the first authentication is successful, the Enter OTP page will appear as shown in Figure 9 below. The OTP will be sent to the mobile phone. Enter the OTP in the space provided and click Logon.

	https://20.1.1.8 - BIG-IP Edge Client**
BIG-IP Edge Clip	6
Conr Server:	Enter OTP:
Connection	Logon
Establish a conne 'Disconnect' but	
Change Server	

Figure 11 : OTP Prompt

Once successfully connected, the client will display a Connected message and the Inbound and Outbound Traffic byte per second (b/s) will start increasing.

IG-IP Edge Client*		
Server: https	ed ://20.1.1.8/	Inbound Traffic 68 b/s Outbound Traffic 165 b/s
onnection		
Auto-Connect	Connect	0 Disconnect
affic Inbound: 4.8 Ki Inbound: 4.8 Ki Inbound: 4.8 Ki	B total (0% compression)	Throughput: 68 b/s
10K 1K 100		*
1 minute ago	30 seconds ago	Carren
10%		
	A	And the second division of the second divisio
• Outbound: 14.0	5 KB total (0% compression)	Throughput: 165 b/s
100 Outbound: 14.4	5 KB total (0% compression)	Throughput: 165 b/s

Figure 13 : Successful Connection for F5 Edge Client

II. Using SSL VPN

When accessing using SSL VPN, open a web browser and access the Internet address (URL) for SSL VPN access. The Username and Password will appear as shown in Figure 14 below.

🕘 20.1.1.8 - Mozilla Firefox	
<u>File Edit View History Bookmarks Tools H</u> elp	
E 20.1.1.8	*
20.1.1.8 https://20.1.1.8/my.policy	🏫 🛪 😋 🚮 🛪 Google 🖉 🎓
(5)	
SendQuick ConeXa Secure Access SSL VPN Demo	
Username	
<username></username>	
Password	

Logon	

Figure 14 : SSLVPN Login with Username and Password

Enter the Username and Password and select Logon. Once the first authentication is completed, an Enter OTP page will appear. The SMS will be sent to the mobile phone. Enter the OTP in the Response space provided and select Continue, as shown in Figure 15 below. Once the second factor authentication is approved, the success page will be shown as in Figure 16 below.

Strictly Private and Confidential

🕹 20.1.1.8 - Mozilla Firefox	
Eile Edit View History Bookmarks Tools Help	
1 20.1.1.8	*
◆ 20.1.1.8 https://20.1.1.8/my.policy	🟫 🛪 🗷 🚷 🛪 Google 🔎 🍙
6	
Enter OTP:	
Logon	

Figure 15 : Enter OTP for SSL VPN Authentication

letwork Access	×	🧔 Server Logs	×	4	Ν	
5					43	
Status: Connect	ted					Logout
Activity [Hide]						
Data						
Received:						1.02 KB
Sent:						2.25 KB
Compression						
Received:						0%
						0%

Figure 16 : Successful Access with SSL VPN