SendQuick®

Palo Alto Networks - SendQuick Conexa

One-Time-Password Configuration Guide

Version 1.0

SendQuick Pte Ltd

76 Playfair Road

#08-01 LHK2 Building

Singapore 367996

Tel : +65 6280 2881   Fax : +65 6280 6882

Email : info@sendquick.com

www.SendQuick.com

REVISION SHEET

Release No.	Date	Description
1.0	*16/01/2023*	*First Published Version*

Table of Contents

1.0 Introduction

1.1 About SendQuick

SendQuick™ develops and offers **enterprise mobile messaging solutions** to facilitate and improve business workflow and communication. Our solutions are widely used in areas such as IT alerts & notifications, secure remote access via 2-Factor Authentication, emergency & broadcast messaging, business process automation and system availability monitoring.

In addition to functionality, SendQuick's messaging solutions have also been developed with other key features in mind. These include **security** and **confidentiality** of company information, and **ease in mitigating disruption** during unplanned system downtime such as that arising from cyberattacks. Our solutions are available in the form of server-grade hardware Appliance, Virtual Machine or Cloud-based.

SendQuick is your Innovative Partner for future-proof enterprise mobility solutions — used by over 1,500 corporations, with over 2,000 installations, including many Fortune Global 500 companies, in over 40 countries across the banking, finance, insurance, manufacturing, retail, government, education, and healthcare sectors.

1.2 About SendQuick Conexa

SendQuick Conexa is the ideal solution for companies seeking low-cost and seamless MFA implementation.

It has a built-in SMS OTP, Soft Token and Email OTP with Authentication and Authorisation (AA) capability, Radius server and an SMS transmission engine, all in a single appliance. SendQuick Conexa fulfils all the MFA requirements of organisations and easily integrates with your Active Directory or RADIUS and can support multiple SSL VPN sessions as required.

1.3 Purpose of Document

This document is prepared as a guide to configure Palo Alto Networks to integrate with SendQuick Conexa for multi factor authentication. Palo Alto can use either RADIUS or SAML to connect with SendQuick Conexa.

For **RADIUS** connection, ensure that both applications are using the same port for Radius. SendQuick Conexa OTP server is configured with RADIUS on **port 1812**.

For **SAML** connection, SendQuick Conexa need to be accessible from the Internet to host the SAML login portal for user login.

This integration was tested on **Palo Alto Networks version 10.1.6-h3** and **SendQuick Conexa version 20150611-10HF4**

2.0 Create User on SendQuick Conexa

Prior to configuring the connection via RADIUS or SAML, we must first create the user in SendQuick Conexa.

2.1 Creating user on SendQuick Conexa (Local User authentication)

SendQuick Conexa can authenticate user by authenticating against local user database, Active Directory/LDAP, external Radius server and remote database server.

For this guide, we will create a local user as an example.

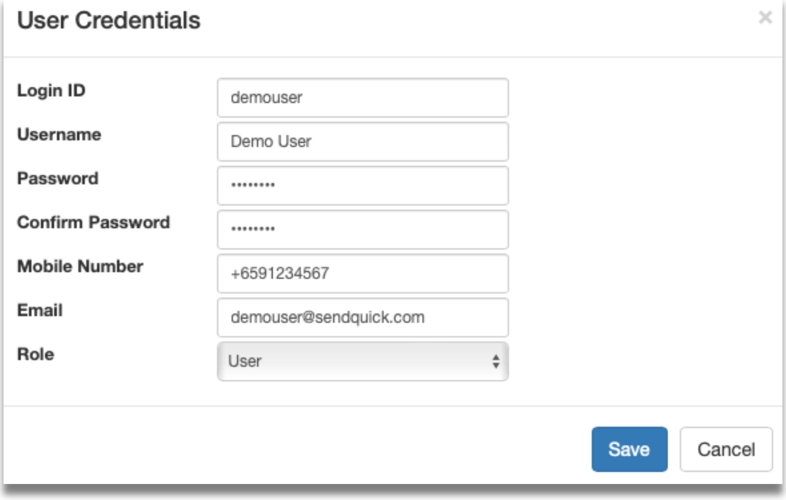
Step 1: On the SendQuick Conexa dashboard, navigate to

User Management > All Users

Step 2: Click on **New User**

Step 3: Fill in the following fields:

- **Login ID**
- **Username**
- **Password**
- **Confirm Password**
- **Mobile Number**
- **Email**
- **Role**



User Credentials

Login ID	demouser
Username	Demo User
Password	••••••••
Confirm Password	••••••••
Mobile Number	+6591234567
Email	demouser@sendquick.com
Role	User

Figure 1 Creating "User" under Local User

2.2 Create Soft Token user (SendQuick OTP)

This is to create a user to be able to login using soft token. We will be using SendQuick OTP app as the soft token.

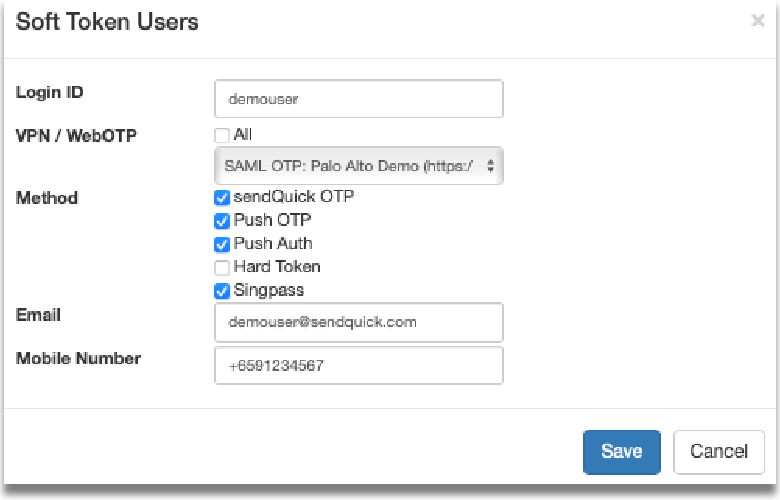
Step 1: On the SendQuick Conexa dashboard, navigate to

Soft Token Management > Soft Token Users

Step 2: Click on **New User**

Step 3: Fill in the following fields:

- **Login ID**
- **VPN / WebOTP** -Allow this soft token user to login to All or single VPN profile by selecting from the dropdown list.
- **Method -** Check SendQuick OTP and/or Singpass (Singpass is only available for SAML profile)
- **Email -** After activated, user will receive soft token QR and/or Singpass registration link to this email.
- **Mobile Number -** After activated, user will receive SMS notification to this number.



Soft Token Users

Login ID: demouser
VPN / WebOTP: □ All
SAML OTP: Palo Alto Demo (https:/
Method: ☑ sendQuick OTP ☑ Push OTP ☑ Push Auth □ Hard Token ☑ Singpass
Email: demouser@sendquick.com
Mobile Number: +6591234567

Figure 2 Add Soft Token User

3.0 Configuring Radius for OTP

To use Radius method, we first configure SendQuick Conexa as the Radius server and Palo Alto as the Radius Client. Before the configuration, you will need to know the IP address/hostname for both systems.

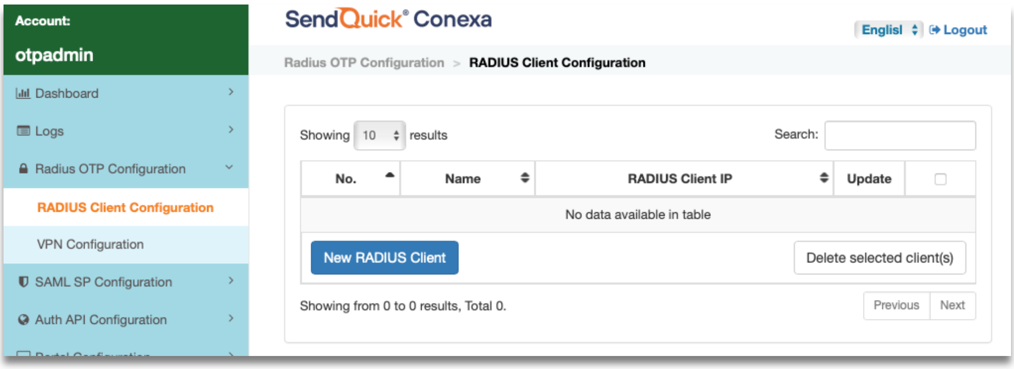
3.1 Configure Radius Client on SendQuick Conexa

On SendQuick Conexa, configure Palo Alto Networks as the Radius Client.

Step 1: At the SendQuick Conexa dashboard, navigate to the following:

Radius OTP Configuration > Radius Client Configuration

Step 2: Click on **New Radius Client**



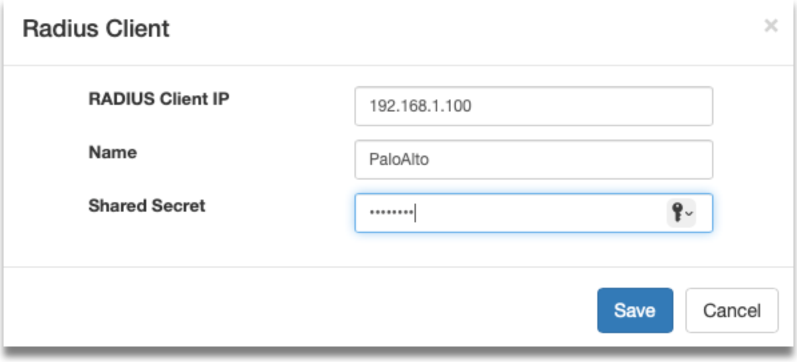
No.	Name	RADIUS Client IP	Update	□
No data available in table				

Showing from 0 to 0 results, Total 0.

Figure 3 Add New Radius Client

Step 3: Fill up the following fields:

- **Radius Client IP** - This is the IP Address of Palo Alto Networks system.
- **Name** – Create a unique name to identify this Radius Client.
- **Shared secret** - Define a shared secret key that needs to be configured later in the Palo Alto system.



RADIUS Client IP	192.168.1.100
Name	PaloAlto
Shared Secret	••••••••

Figure 4 Configure Radius Client

3.2 Configure Radius Server on Palo Alto Networks

On Palo Alto Networks, configure SendQuick Conexa as the Radius Server.

Step 1: At the Palo Alto Networks dashboard, navigate to the following:

Device > Server Profiles > RADIUS

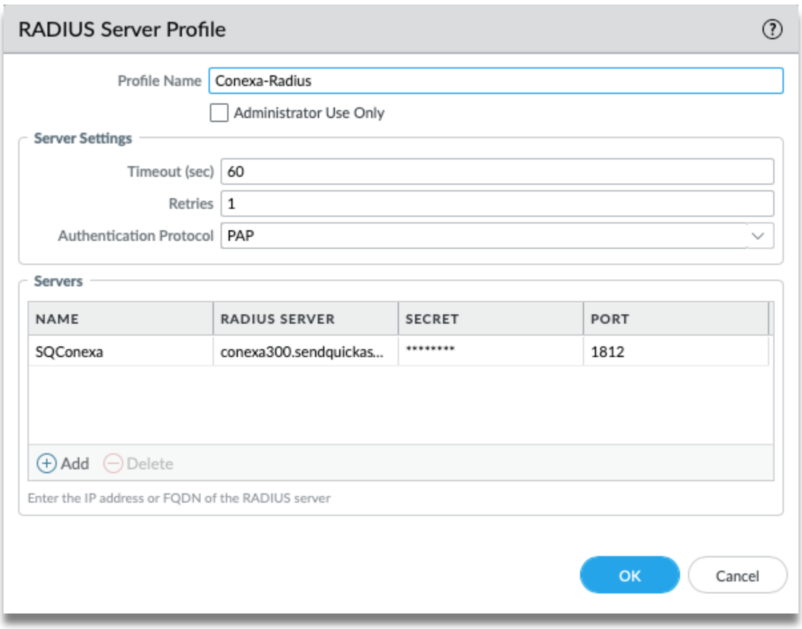
Step 2: Click ⊕ Add at the bottom of the screen to add a new Radius Server Profile.

Step 3: Fill up the following fields:

- **Profile Name** - Create a name to identify this Radius Server Profile.
- **Timeout (sec) -** Set a timeout duration either 60s to 180s for user to enter OTP.
- **Retries** - Set the number of retries.
- **Authentication Protocol** - Select "PAP" from the dropdown list.

Step 4: Click ⊕ Add to add new Server and key in the following:

- **Name:** Create a unique name to identify this Radius Server.
- **RADIUS Server:** Enter your SendQuick Conexa IP or hostname.
- **Secret:** Same secret as configured in Conexa Radius Client Configuration in the previous section.
- **Port:** 1812.



RADIUS Server Profile

Profile Name: Conexa-Radius

□ Administrator Use Only

Server Settings

Timeout (sec): 60

Retries: 1

Authentication Protocol: PAP

Servers

NAME	RADIUS SERVER	SECRET	PORT
SQConexa	conexa300.sendquickas...	********	1812

Enter the IP address or FQDN of the RADIUS server

Figure 5 Configure Radius Server Profile

3.3 Add Authentication Profile on Palo Alto Networks

Add an authentication profile on Palo Alto Networks that later needs to be linked to SendQuick Conexa VPN configuration.

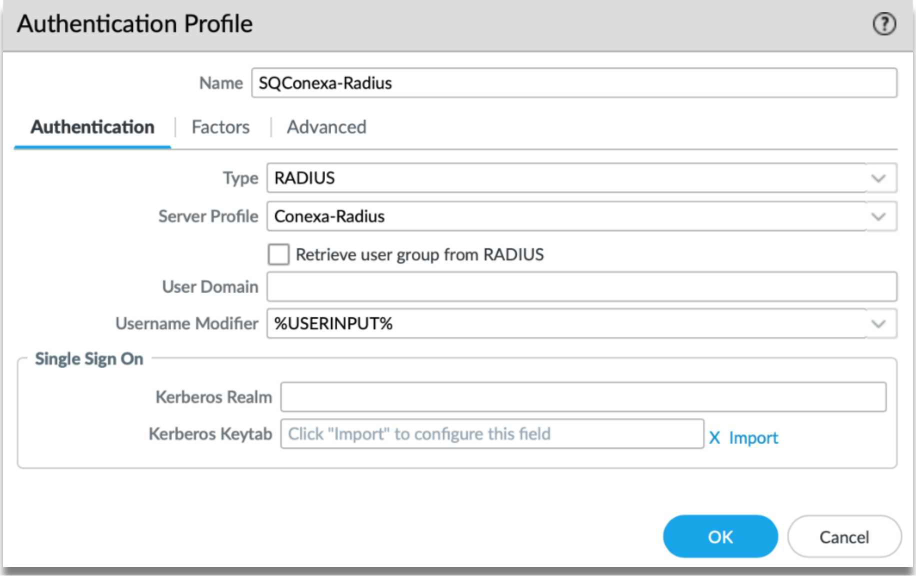
Step 1: At the Palo Alto Networks dashboard, navigate to the following:

Device > Authentication Profile

Step 2: Click ⊕ Add at the bottom of the screen to add a new Authentication Profile.

Step 3: Under "Authentication" tab, fill up the following fields:

- **Name** – Create a unique name to identify this Authentication Profile.
- **Type** – Select "RADIUS" from the dropdown list.
- **Server Profile** – Select the Radius Server Profile that was created earlier from the dropdown list.



Authentication Profile

Name: SQConexa-Radius

Authentication | Factors | Advanced

Type: RADIUS

Server Profile: Conexa-Radius

□ Retrieve user group from RADIUS

User Domain:

Username Modifier: %USERINPUT%

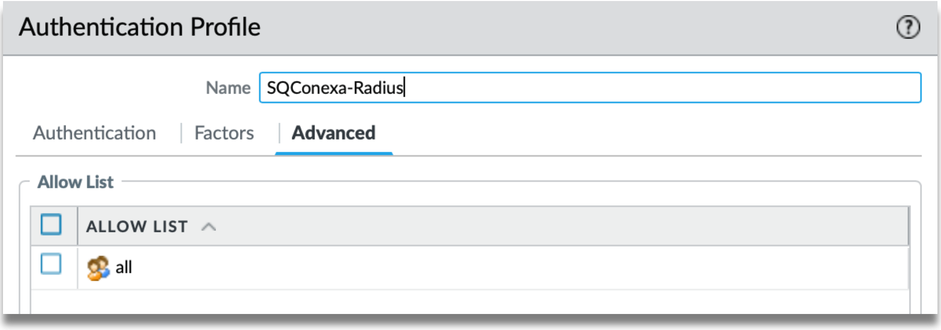
Single Sign On

Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field

Figure 6 Configure Authentication Profile for RADIUS

Step 4: Under "Advanced" tab, add user or user group in the Allow List to use this profile.



Authentication Profile

Name: SQConexa-Radius

Authentication | Factors | Advanced

Allow List

□	ALLOW LIST
□	all

Figure 7 Configure Authentication - Allow Users

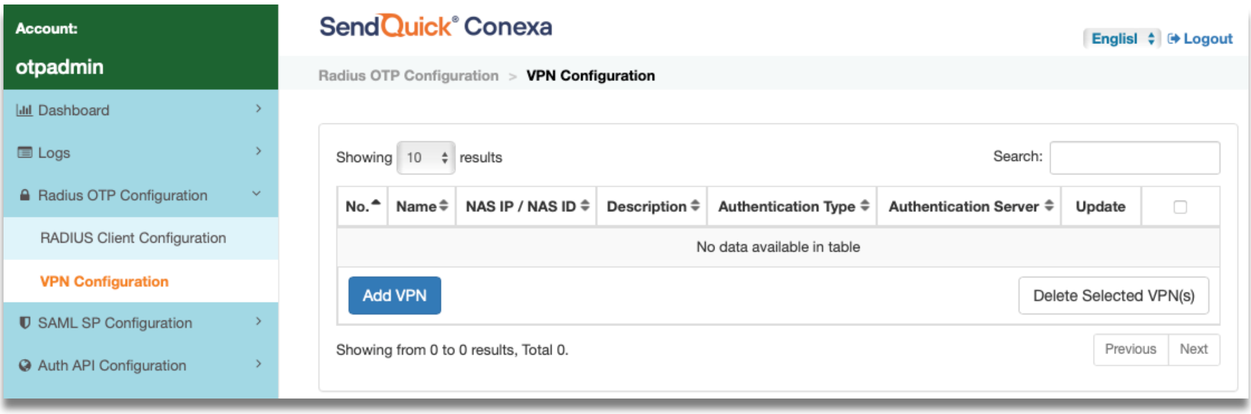
3.4 Add VPN Configuration on SendQuick Conexa

Configure VPN profile on SendQuick Conexa to link to the Palo Alto Networks Authentication Profile.

Step 1: At the SendQuick Conexa dashboard, navigate to the following:

Radius OTP Configuration > VPN Configuration

Step 2: Click on **Add VPN.**



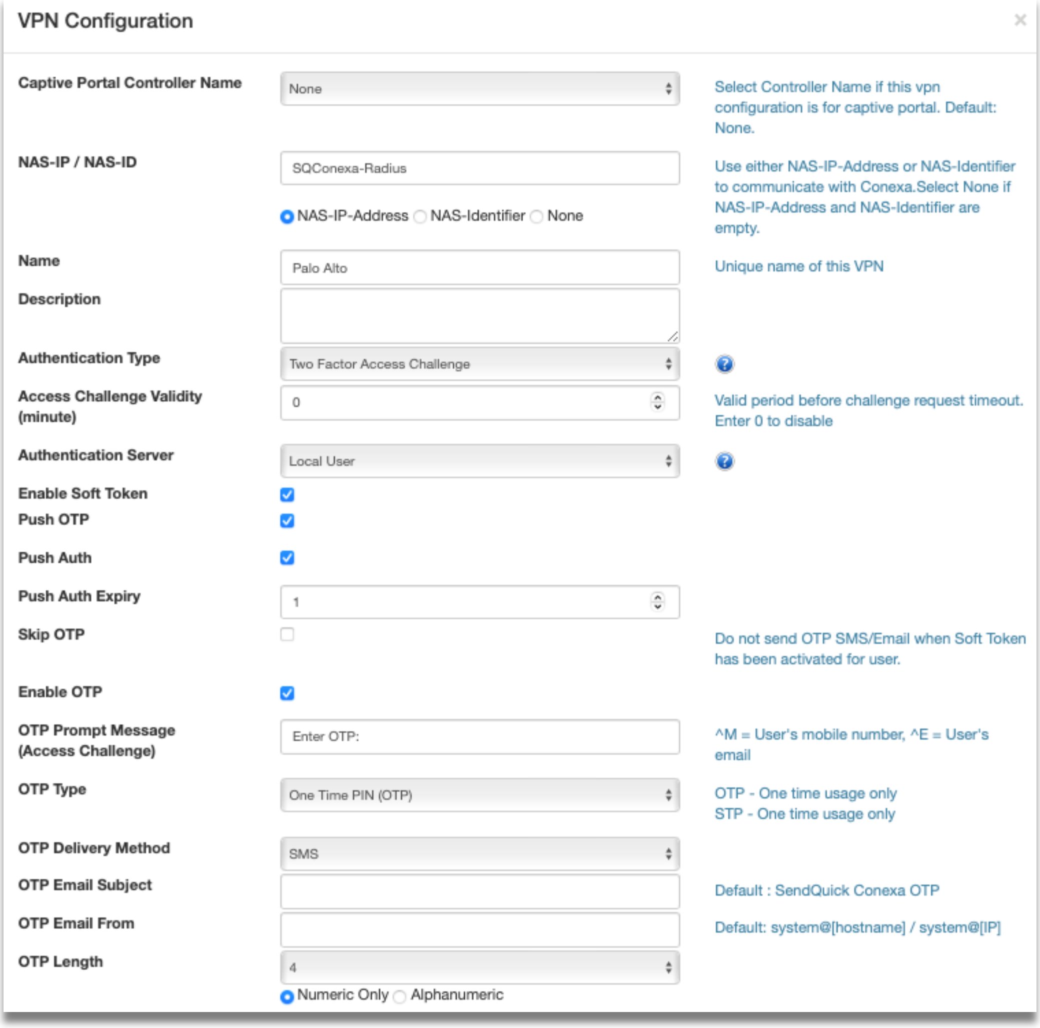
No.	Name	NAS IP / NAS ID	Description	Authentication Type	Authentication Server	Update	□
No data available in table							

Showing from 0 to 0 results, Total 0.

Figure 8 Add new VPN

Step 3: Fill up the following fields:

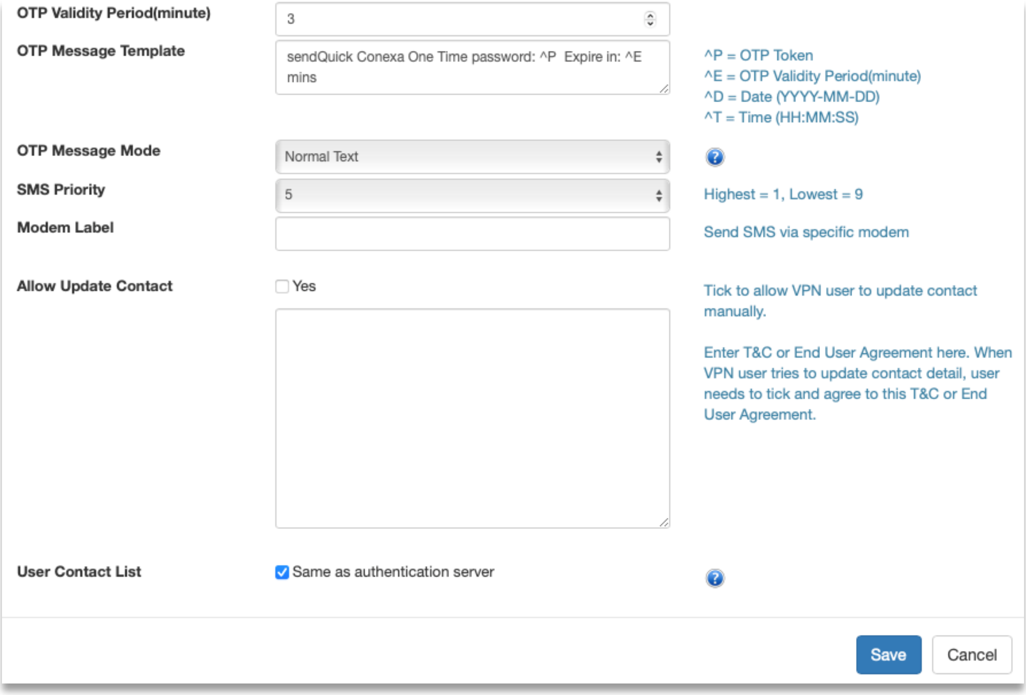
- **NAS-IP/NAS-ID -** NAS-IP-Address or NAS-Identifier used in the Radius request. It is usually the Palo Alto Networks interface IP or the Radius authentication profile name that was created earlier.
- **Name** – Create a unique name to identify this VPN configuration.
- **Authentication Type -** Select **Two Factor Access Challenge** from the dropdown list.
- **Check the following boxes** - **Enable Soft Token** & **Enable OTP.**
- **OTP Delivery Method -** Select **SMS & Email.**
- **User Contact List -** Check **Same as Authentication Server.**



VPN Configuration

Captive Portal Controller Name	None	Select Controller Name if this vpn configuration is for captive portal. Default: None.
NAS-IP / NAS-ID	SQConexa-Radius ● NAS-IP-Address ○ NAS-Identifier ○ None	Use either NAS-IP-Address or NAS-Identifier to communicate with Conexa.Select None if NAS-IP-Address and NAS-Identifier are empty.
Name	Palo Alto	Unique name of this VPN
Description		
Authentication Type	Two Factor Access Challenge	?
Access Challenge Validity (minute)	0	Valid period before challenge request timeout. Enter 0 to disable
Authentication Server	Local User	?
Enable Soft Token	☑	
Push OTP	☑	
Push Auth	☑	
Push Auth Expiry	1	
Skip OTP	□	Do not send OTP SMS/Email when Soft Token has been activated for user.
Enable OTP	☑	
OTP Prompt Message (Access Challenge)	Enter OTP:	^M = User's mobile number, ^E = User's email
OTP Type	One Time PIN (OTP)	OTP - One time usage only STP - One time usage only
OTP Delivery Method	SMS	
OTP Email Subject		Default : SendQuick Conexa OTP
OTP Email From		Default: system@[hostname] / system@[IP]
OTP Length	4 ● Numeric Only ○ Alphanumeric	

Figure 9 VPN Configuration



OTP Validity Period(minute)	3	
OTP Message Template	sendQuick Conexa One Time password: ^P Expire in: ^E mins	^P = OTP Token ^E = OTP Validity Period(minute) ^D = Date (YYYY-MM-DD) ^T = Time (HH:MM:SS)
OTP Message Mode	Normal Text	?
SMS Priority	5	Highest = 1, Lowest = 9
Modem Label		Send SMS via specific modem
Allow Update Contact	□ Yes	Tick to allow VPN user to update contact manually.
		Enter T&C or End User Agreement here. When VPN user tries to update contact detail, user needs to tick and agree to this T&C or End User Agreement.
User Contact List	☑ Same as authentication server	?

Figure 10 VPN Configuration (continue)

3.5 Configure GlobalProtect on Palo Alto Networks to use RADIUS

GlobalProtect is Palo Alto Networks' VPN solution.

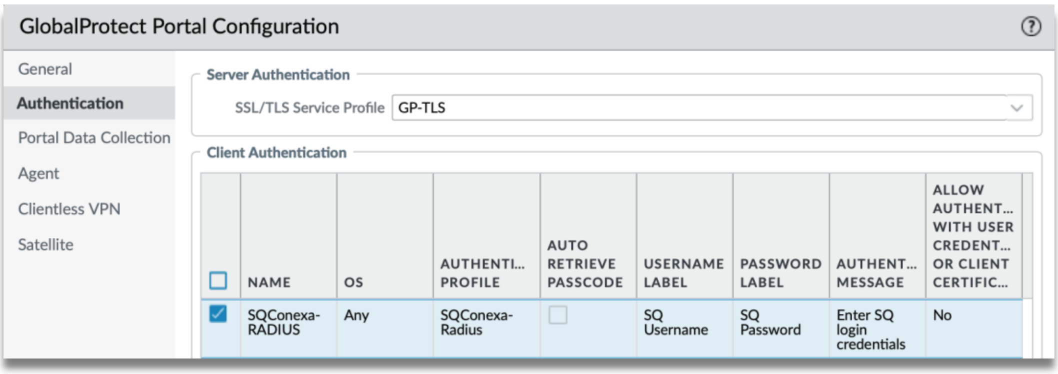
Step 1: At the Palo Alto Networks dashboard, navigate to the following:

Network > GlobalProtect > Portals

Step 2: Add or Edit an existing Portal Configuration.

Step 3: Click on Authentication and add a new Client Authentication and set it to Radius authentication profile we created for SendQuick Conexa.

Move this up and set it as the first client authentication profile if you have multiple entries in the list.



Server Authentication

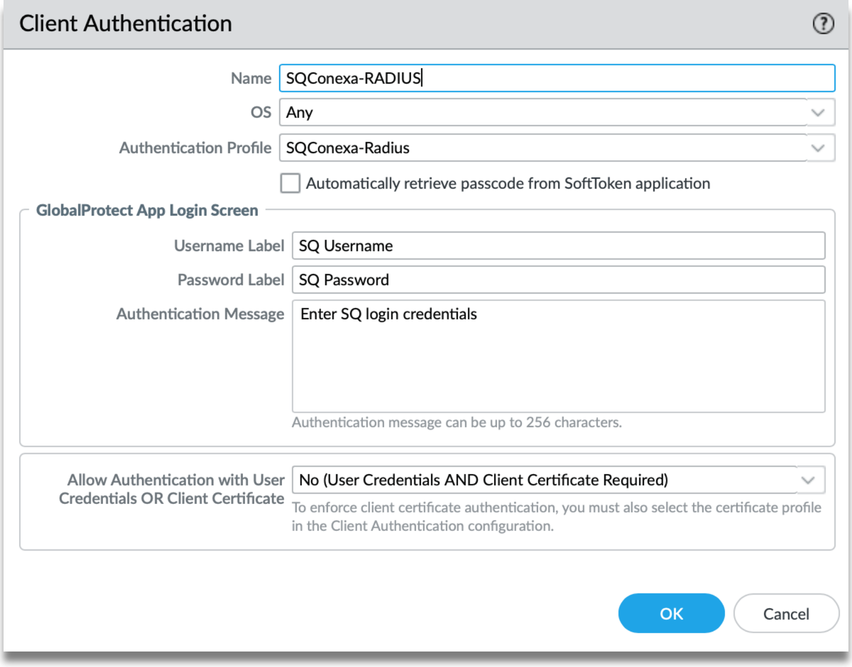
SSL/TLS Service Profile: GP-TLS

Client Authentication

☐	NAME	OS	AUTHENTI... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENT... MESSAGE	ALLOW AUTHENT... WITH USER CREDENT... OR CLIENT CERTIFIC...
☑	SQConexa-RADIUS	Any	SQConexa-Radius	☐	SQ Username	SQ Password	Enter SQ login credentials	No

Figure 11 Link GlobalProtect Portal to RADIUS Authentication Profile

Click on the name of the Client Authentication and provide the labels for the login screen. See example below:



Name: SQConexa-RADIUS

OS: Any

Authentication Profile: SQConexa-Radius

☐ Automatically retrieve passcode from SoftToken application

GlobalProtect App Login Screen

Username Label: SQ Username

Password Label: SQ Password

Authentication Message: Enter SQ login credentials

Authentication message can be up to 256 characters.

Allow Authentication with User Credentials OR Client Certificate: No (User Credentials AND Client Certificate Required)

To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

Figure 12 Client Authentication Set Up for RADIUS

3.6 Accessing GlobalProtect Web Portal using RADIUS

Logging in via your organisation's GlobalProtect web portal will now have an additional step to authenticate via OTP using RADIUS.

Step 1: Browse to GlobalProtect portal public IP address that has been configured for your organisation.

Step 2: Enter valid Username and Password. In this example, we use the Local User account we created earlier.

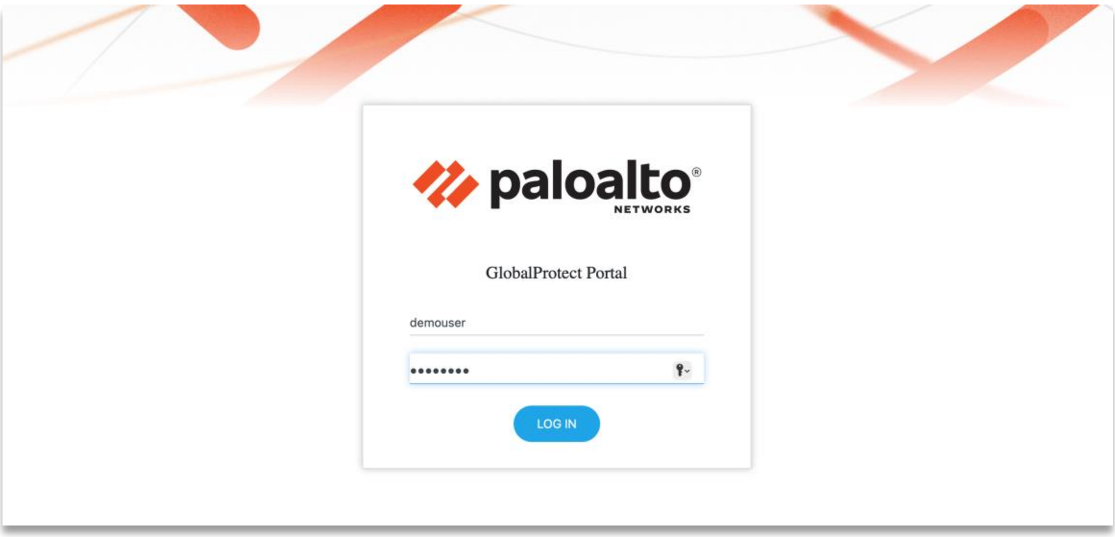


Figure 13 Enter username and password to login to the portal

Step 3: Received the OTP via SMS, Email or Push message.

Step 4: Enter OTP from SMS/Email or Soft Token app if activated.

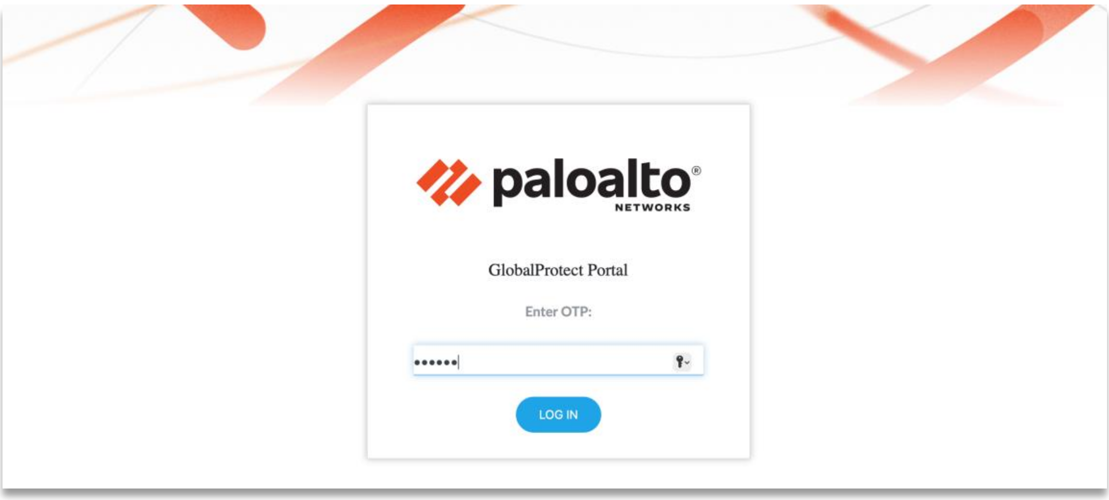
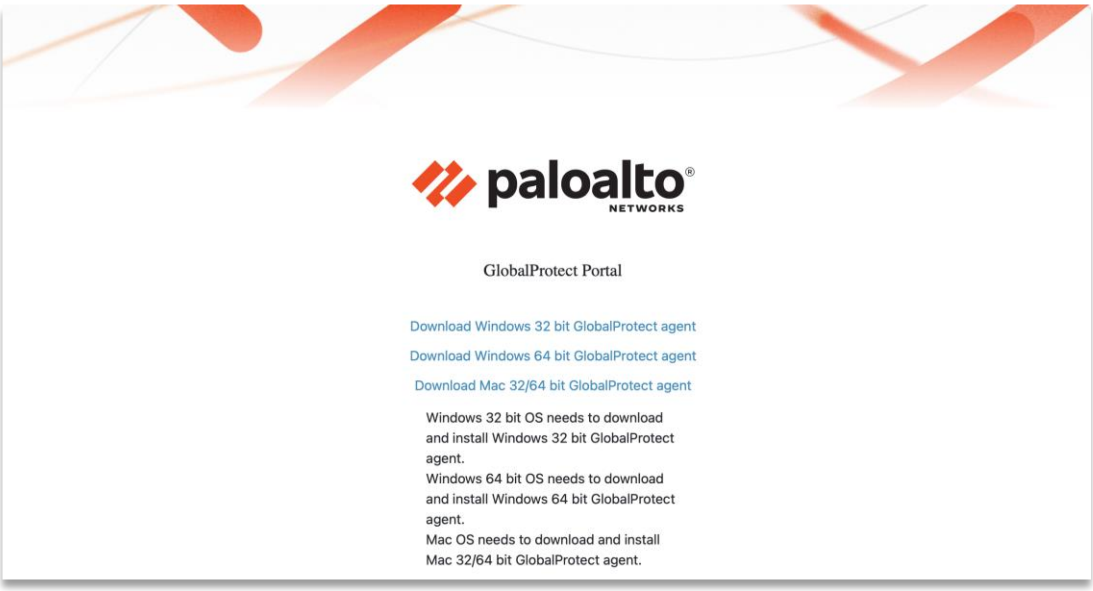


Figure 14 Enter the OTP received on your mobile device

Step 5: If the OTP entered tallies, you will successfully log in to the portal.



GlobalProtect Portal

Download Windows 32 bit GlobalProtect agent
Download Windows 64 bit GlobalProtect agent
Download Mac 32/64 bit GlobalProtect agent

Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.
Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.
Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.

Figure 15 Log in Successful

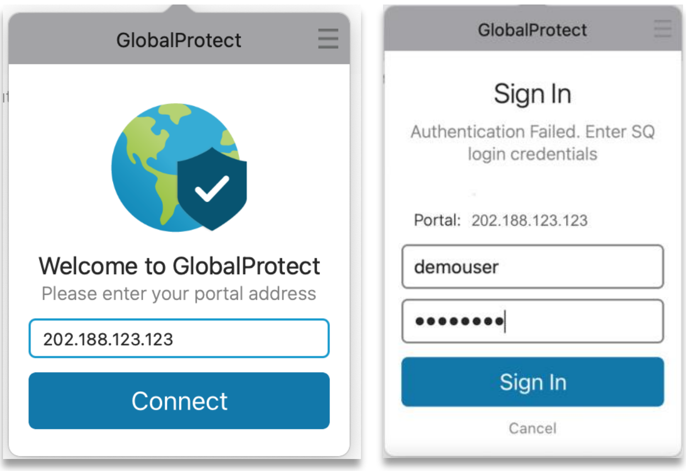
3.7 Access via GlobalProtect agent using RADIUS

You can also access the portal via GlobalProtect Agent.

Step 1: Download GlobalProtect agent from web portal.

Step 2: Enter your public portal address and click on Connect.

Step 3: Enter your local user ID and password, click Sign In.



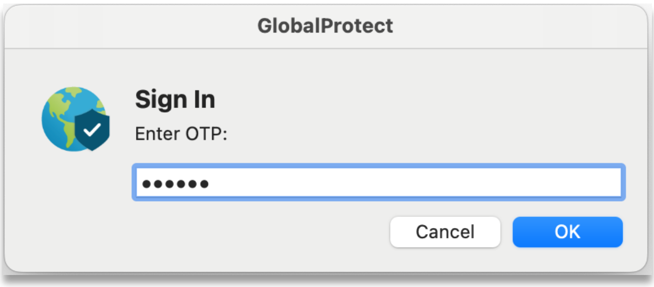
Welcome to GlobalProtect
Please enter your portal address
202.188.123.123

Sign In
Authentication Failed. Enter SQ login credentials
Portal: 202.188.123.123
demouser
••••••••

Figure 16 Login via GlobalProtect Agent

Step 4: Receive the OTP via SMS, Email or Push message.

Step 5: Enter OTP from SMS/Email or Soft Token app if activated.


GlobalProtect

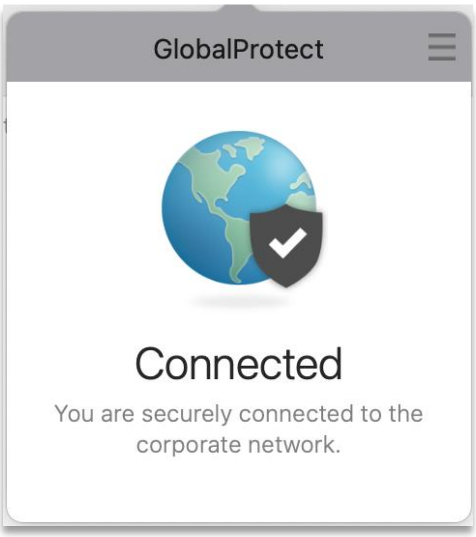
Sign In

Enter OTP:

••••••

Figure 17 Enter the OTP received on your mobile device

Step 6: Successfully connect to GlobalProtect.


GlobalProtect

Connected

You are securely connected to the corporate network.

Figure 18 Successfully Connect via GlobalProtect Agent

4.0 Configuring SAML for OTP

You can also use SAML method for sending OTP. Configure Palo Alto Networks as the Service Provider in SendQuick Conexa and SendQuick Conexa as the Identity Provider in Palo Alto Networks.

4.1 Configure SAML Service Provider on SendQuick Conexa

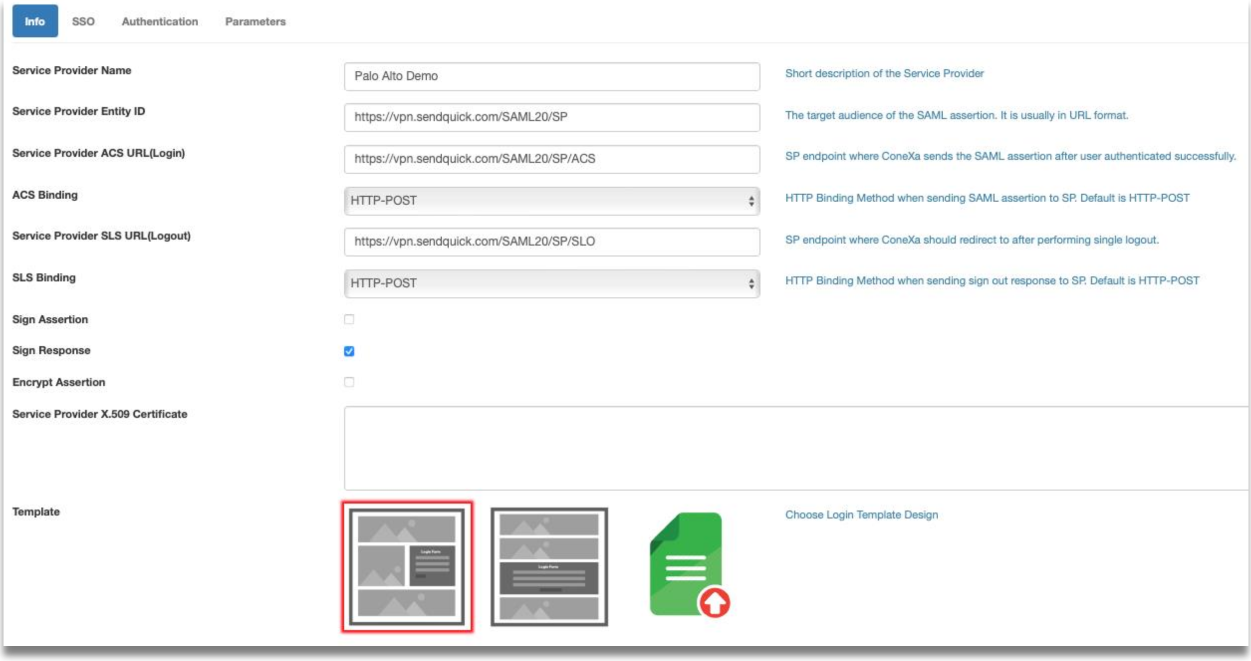
Step 1: On the SendQuick Conexa dashboard, navigate to

SAML SP Configuration > SP Configuration

Step 2: Click on **Add New SP.**

Step 3: Fill in the following fields:

- **Service Provider Name**
- **Service Provider Entity ID:** Enter dummy data first if unsure
- **Service Provider ACS URL(Login):** Leave it blank first if unsure
- **ACS Binding**
- **Service Provider SLS URL(Logout):** Leave it blank first if unsure
- **SLS Binding**
- **Sign Assertion:** Default is disabled
- **Sign Response:** Default is enabled
- **Encrypt Assertion:** Default is disabled
- **Template:** Choose from predefined template or upload own portal login UI.



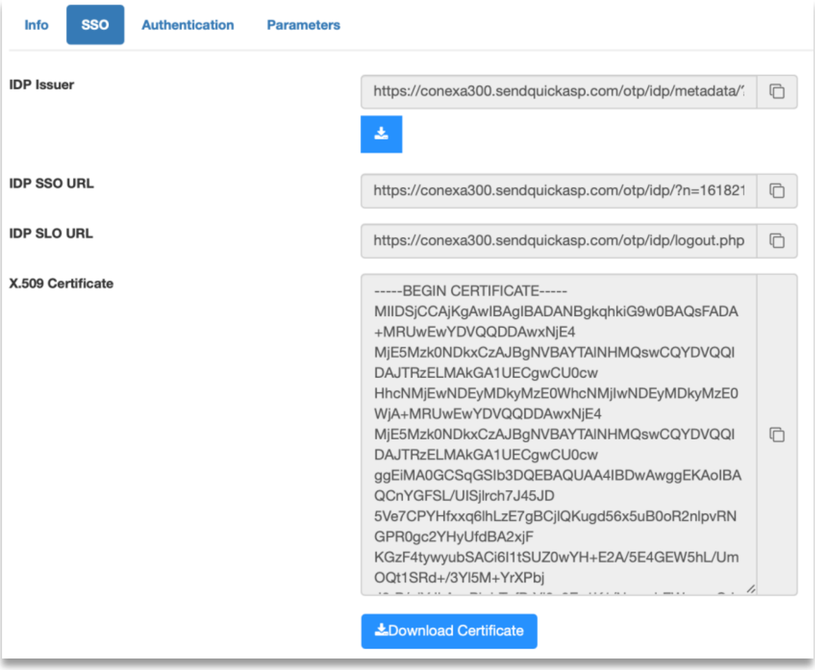
Service Provider Name	Palo Alto Demo	Short description of the Service Provider
Service Provider Entity ID	https://vpn.sendquick.com/SAML20/SP	The target audience of the SAML assertion. It is usually in URL format.
Service Provider ACS URL(Login)	https://vpn.sendquick.com/SAML20/SP/ACS	SP endpoint where ConeXa sends the SAML assertion after user authenticated successfully.
ACS Binding	HTTP-POST	HTTP Binding Method when sending SAML assertion to SP. Default is HTTP-POST
Service Provider SLS URL(Logout)	https://vpn.sendquick.com/SAML20/SP/SLO	SP endpoint where ConeXa should redirect to after performing single logout.
SLS Binding	HTTP-POST	HTTP Binding Method when sending sign out response to SP. Default is HTTP-POST
Sign Assertion	☐	
Sign Response	☑	
Encrypt Assertion	☐	
Service Provider X.509 Certificate		
Template		Choose Login Template Design

Figure 19 Add New Service Provider

Step 4: Click Save and then click on "**SSO**" tab. Copy IDP details or download metadata. These are required to create SAML profile at Palo Alto.

Download metadata or gather the following details from SendQuick Conexa.

- Service Provider Entity ID
- Service Provider ACS URL(Login)
- Service Provider SLS URL(Logout)
- IDP Issuer
- IDP SSO URL
- IDP SLO URL
- X.509 Certificate



IDP Issuer: https://conexa300.sendquickasp.com/otp/idp/metadata/'

IDP SSO URL: https://conexa300.sendquickasp.com/otp/idp/?n=161821

IDP SLO URL: https://conexa300.sendquickasp.com/otp/idp/logout.php

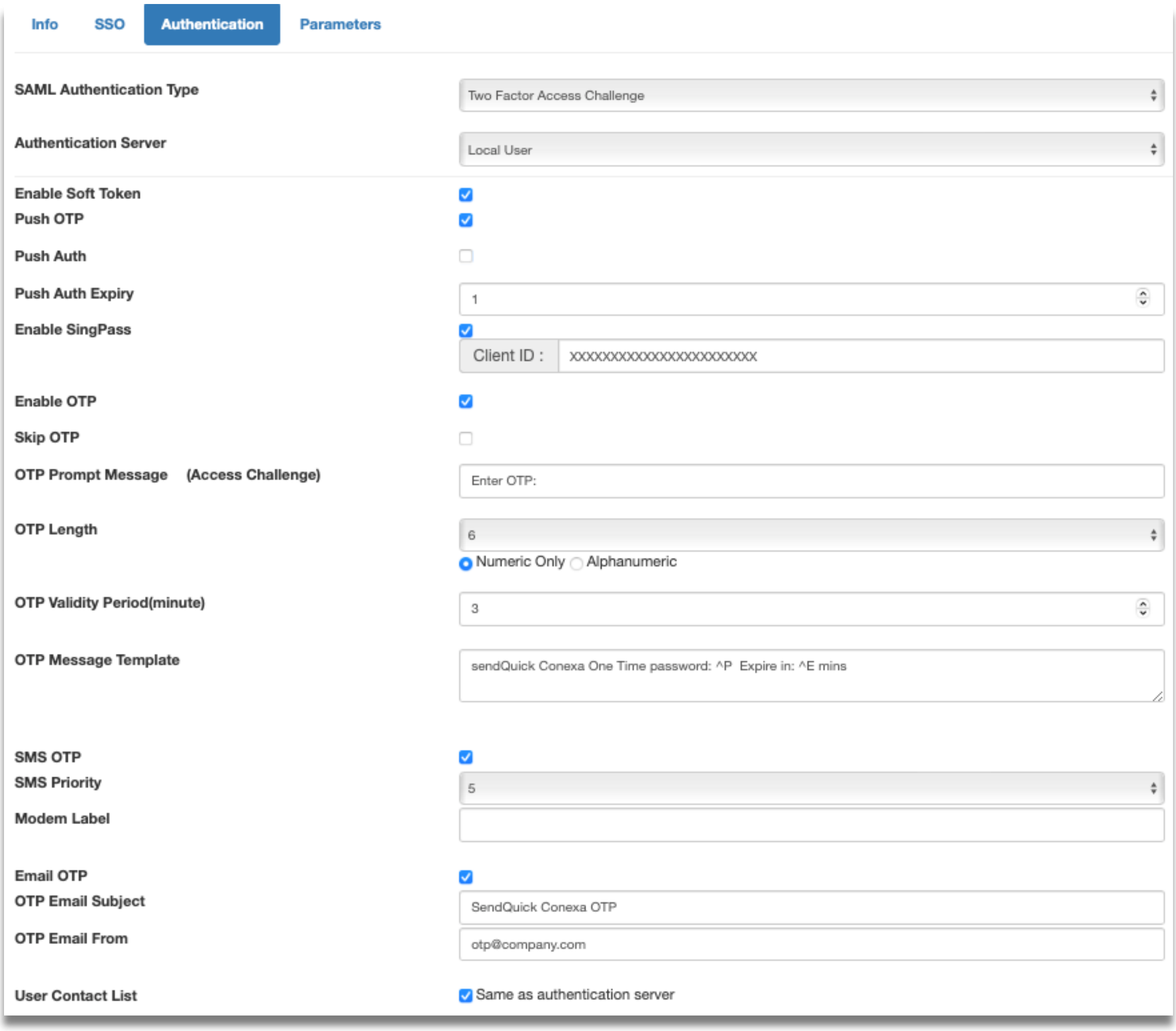
X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIBADANBgkqhkiG9w0BAQsFADA
+MRUwEwYDVQQDDAwxNjE4
MjE5Mzk0NDkxCzAJBgNVBAYTAlNHMQswCQYDVQQI
DAJTRzELMAkGA1UECgwCU0cw
HhcNMjEwNDEyMDkyMzE0WhcNMjIwNDEyMDkyMzE0
WjA+MRUwEwYDVQQDDAwxNjE4
MjE5Mzk0NDkxCzAJBgNVBAYTAlNHMQswCQYDVQQI
DAJTRzELMAkGA1UECgwCU0cw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBA
QCnYGFSL/UISjlrch7J45JD
5Ve7CPYHfxxq6lhLzE7gBCjlQKugd56x5uB0oR2nlpvRN
GPR0gc2YHyUfdBA2xjF
KGzF4tywyubSACi6l1tSUZ0wYH+E2A/5E4GEW5hL/Um
OQt1SRd+/3YI5M+YrXPbj
```

Figure 20 Download the Metadata to be entered into Palo Alto Networks

Step 5: Go to "**Authentication**" tab. Fill up the following fields:

- **SAML Authentication Type -** Select "Two Factor Access Challenge"
- **Authentication Server -** Select where the Authentication server is. In this example we will use Local User
- **Check the following boxes** -**Enable Soft Token**, **Enable SingPass (optional)** and enter SingPass Client ID, **Enable OTP**
- **OTP Delivery Method** - Enable **SMS OTP** and/or **Email OTP**
- **User Contact List -** Select where your user contact is. In this example we use Local User

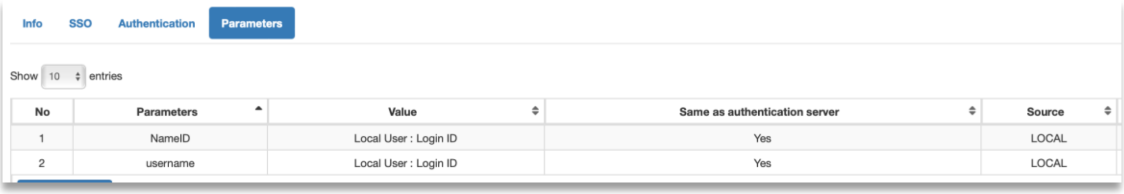


SAML Authentication Type	Two Factor Access Challenge
Authentication Server	Local User
Enable Soft Token	☑
Push OTP	☑
Push Auth	□
Push Auth Expiry	1
Enable SingPass	☑ Client ID : xxxxxxxxxxxxxxxxxxxxxxxx
Enable OTP	☑
Skip OTP	□
OTP Prompt Message (Access Challenge)	Enter OTP:
OTP Length	6 ● Numeric Only ○ Alphanumeric
OTP Validity Period(minute)	3
OTP Message Template	sendQuick Conexa One Time password: ^P Expire in: ^E mins
SMS OTP	☑
SMS Priority	5
Modem Label	
Email OTP	☑
OTP Email Subject	SendQuick Conexa OTP
OTP Email From	otp@company.com
User Contact List	☑ Same as authentication server

Figure 21 Configure SAML Authentication

Step 6: Click Save and then click on “**Parameters**” tab. Check the source of **NameID** attribute. Check “Same as authentication server” and set Parameter Value to “Login ID”.

Step 7: Add new parameter “username” and set the source to retrieve it. This will be the username sent to PaloAlto.



No	Parameters	Value	Same as authentication server	Source
1	NameID	Local User : Login ID	Yes	LOCAL
2	username	Local User : Login ID	Yes	LOCAL

Figure 22 Parameters for Login

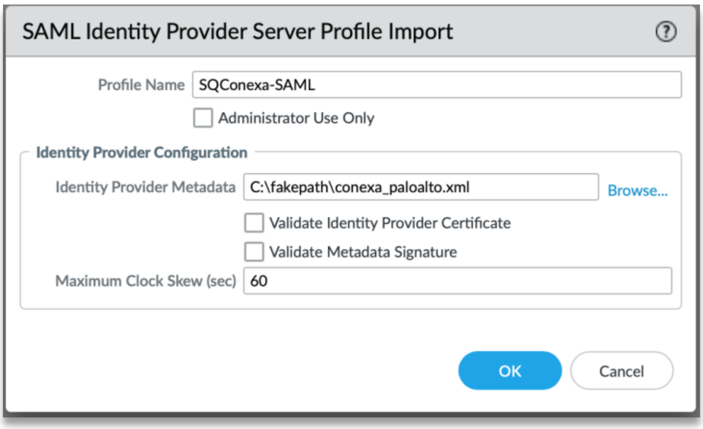
4.2 Configure Identity Provider on Palo Alto Networks

Next, we configure SendQuick Conexa as the Identity Provider on Palo Alto Networks.

Step 1: At the Palo Alto Networks dashboard, navigate to the following:

Device > Server Profiles > SAML Identity Provider

Step 2: Click "Import" and upload the metadata(.xml) that was downloaded earlier.



SAML Identity Provider Server Profile Import

Profile Name: SQConexa-SAML

□ Administrator Use Only

Identity Provider Configuration

Identity Provider Metadata: C:\fakepath\conexa_paloalto.xml Browse...

□ Validate Identity Provider Certificate

□ Validate Metadata Signature

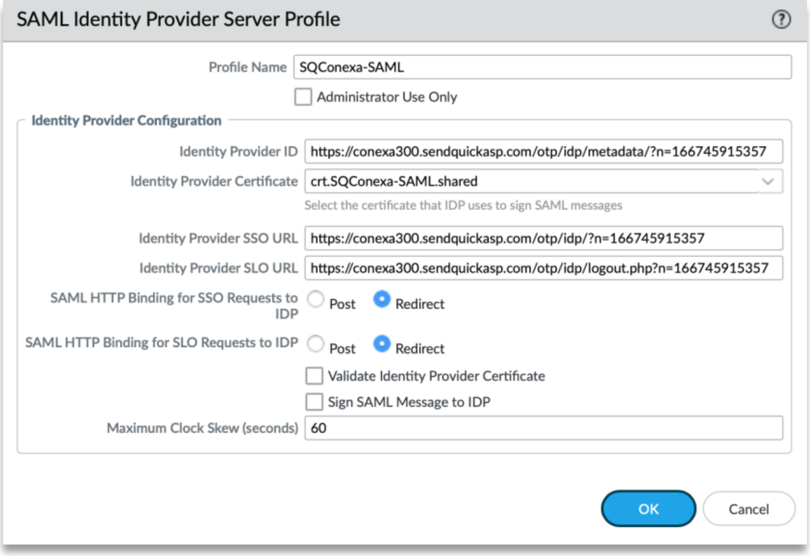
Maximum Clock Skew (sec): 60

OK Cancel

Figure 23 Import SAML IDP Server Profile

Step 3: Alternatively, you can also add the profile manually. Fill up the following fields:

- **Profile Name**
- **Identity Provider ID:** IDP Issuer from SendQuick Conexa
- **Identity Provider Certificate:** Upload new cert from X.509 Certificate from SendQuick Conexa
- **Identity Provider SSO URL:** IDP SSO URL from SendQuick Conexa
- **Identity Provider SLO URL:** IDP SLO URL from SendQuick Conexa
- **SAML HTTP Binding for SSO Requests to IDP:** Select "Redirect"
- **SAML HTTP Binding for SLO Requests to IDP:** Select "Redirect"



SAML Identity Provider Server Profile

Profile Name: SQConexa-SAML

□ Administrator Use Only

Identity Provider Configuration

Identity Provider ID: https://conexa300.sendquickasp.com/otp/idp/metadata/?n=166745915357

Identity Provider Certificate: crt.SQConexa-SAML.shared

Select the certificate that IDP uses to sign SAML messages

Identity Provider SSO URL: https://conexa300.sendquickasp.com/otp/idp/?n=166745915357

Identity Provider SLO URL: https://conexa300.sendquickasp.com/otp/idp/logout.php?n=166745915357

SAML HTTP Binding for SSO Requests to IDP: ○ Post ● Redirect

SAML HTTP Binding for SLO Requests to IDP: ○ Post ● Redirect

□ Validate Identity Provider Certificate

□ Sign SAML Message to IDP

Maximum Clock Skew (seconds): 60

OK Cancel

Figure 24 Fill in SAML IDP Server Profile

4.3 Configure Authentication Profile on Palo Alto Networks

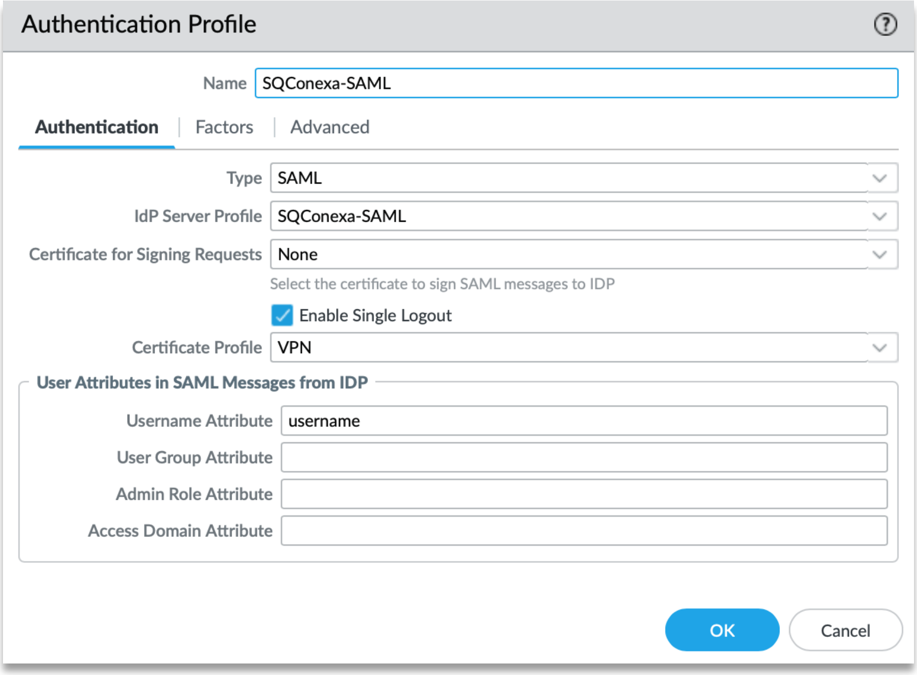
Step 1: At the Palo Alto Networks dashboard, navigate to the following:

Device > Authentication Profile

Step 2: Add a New Authentication Profile

Step 3: At "Authentication" tab, fill up the following fields:

- **Name** – Create a unique name for this Authentication Profile
- **Type** – Select "SAML" from the dropdown list
- **IdP Server Profile:** Select SendQuick Conexa IdP profile



Authentication Profile

Name: SQConexa-SAML

Type: SAML

IdP Server Profile: SQConexa-SAML

Certificate for Signing Requests: None

Select the certificate to sign SAML messages to IDP

☑ Enable Single Logout

Certificate Profile: VPN

User Attributes in SAML Messages from IDP

Username Attribute: username

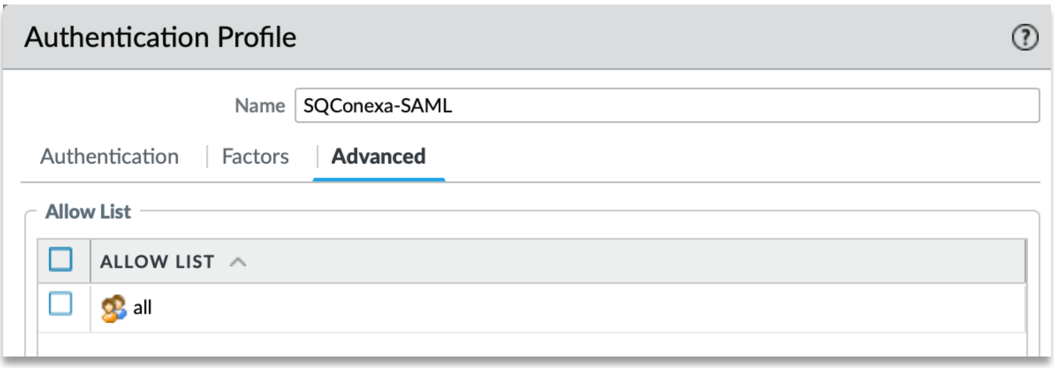
User Group Attribute:

Admin Role Attribute:

Access Domain Attribute:

Figure 25 Create Authentication Profile for SAML

Step 4: Under "Advanced" tab, add user or user group in the Allow List to use this profile.



Authentication Profile

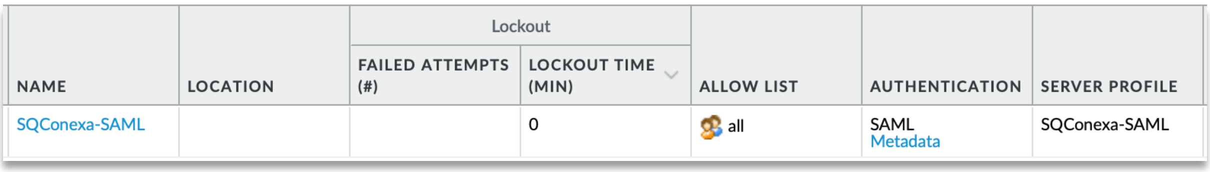
Name: SQConexa-SAML

Allow List

□	ALLOW LIST
□	all

Figure 26 Configure Authentication - Allow Users

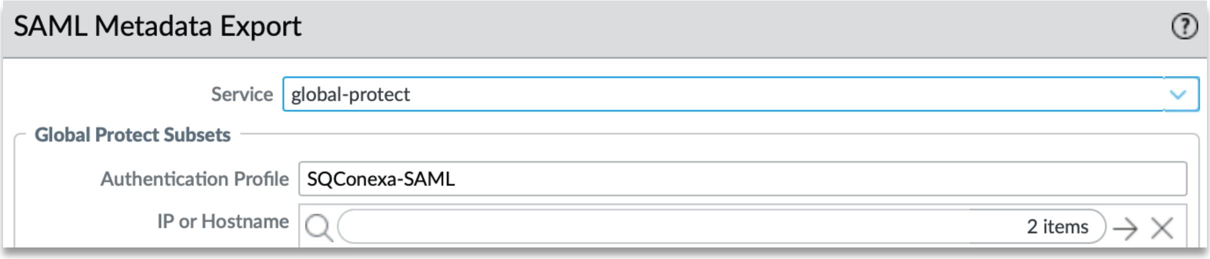
Step 5: Once created, click on the Metadata link and export the SAML metadata.



NAME	LOCATION	Lockout		ALLOW LIST	AUTHENTICATION	SERVER PROFILE
		FAILED ATTEMPTS (#)	LOCKOUT TIME (MIN)			
SQConexa-SAML			0	all	SAML Metadata	SQConexa-SAML

Figure 27 List of Authentication Profile – Select “Metadata” to export

Step 6: Select “global-protect” service and your public IP or Hostname. Click OK and save the metadata.



SAML Metadata Export

Service: global-protect

Global Protect Subsets

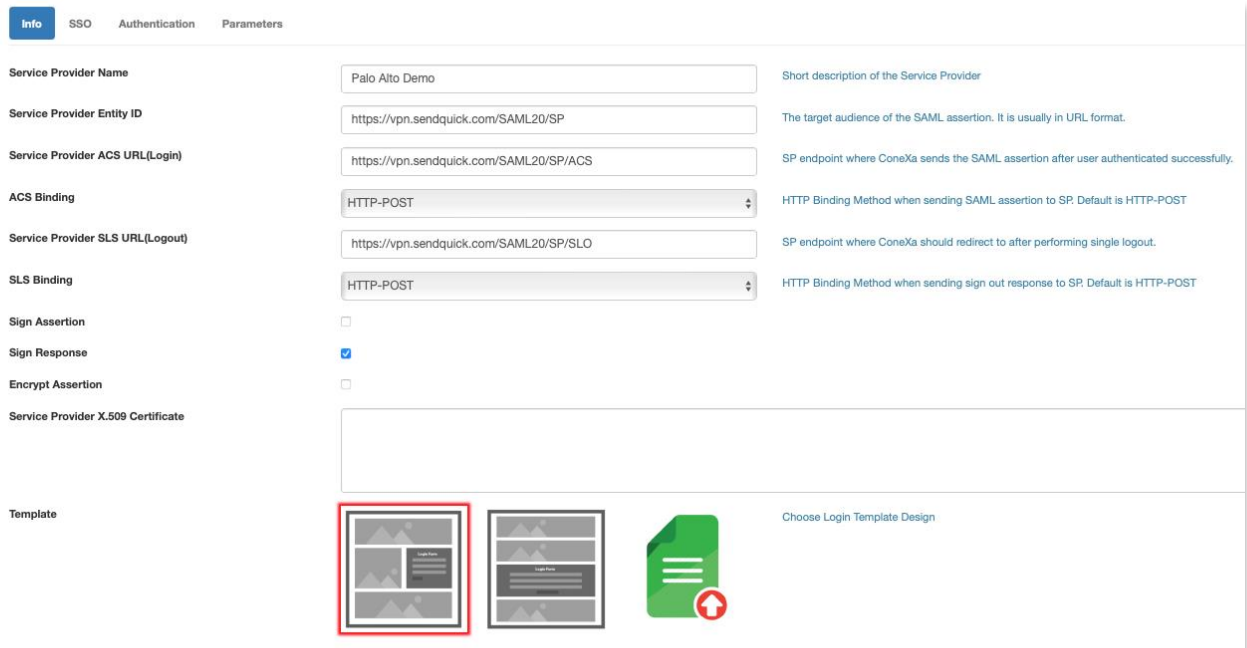
Authentication Profile: SQConexa-SAML

IP or Hostname: 2 items

Figure 28 Export SAML Metadata

Step 7: Open the metadata(.xml) file and copy the details and update to SendQuick Conexa. Navigate on SendQuick Conexa dashboard to SAML Service Provider, info tab.

- **EntityID -** Update Service Provider Entity ID in SendQuick Conexa
- **AssertionConsumerService Location** - Update Service Provider ACS URL(Login) in SendQuick Conexa
- **SingleLogoutService Location -** Update Service Provider SLS URL(Logout) in SendQuick Conexa



Service Provider Name	Palo Alto Demo	Short description of the Service Provider
Service Provider Entity ID	https://vpn.sendquick.com/SAML20/SP	The target audience of the SAML assertion. It is usually in URL format.
Service Provider ACS URL(Login)	https://vpn.sendquick.com/SAML20/SP/ACS	SP endpoint where ConeXa sends the SAML assertion after user authenticated successfully.
ACS Binding	HTTP-POST	HTTP Binding Method when sending SAML assertion to SP. Default is HTTP-POST
Service Provider SLS URL(Logout)	https://vpn.sendquick.com/SAML20/SP/SLO	SP endpoint where ConeXa should redirect to after performing single logout.
SLS Binding	HTTP-POST	HTTP Binding Method when sending sign out response to SP. Default is HTTP-POST
Sign Assertion	☐	
Sign Response	☑	
Encrypt Assertion	☐	
Service Provider X.509 Certificate		
Template		Choose Login Template Design

Figure 29 Update Metadata on SendQuick Conexa SAML config

4.4 Configure GlobalProtect on Palo Alto Networks to use SAML

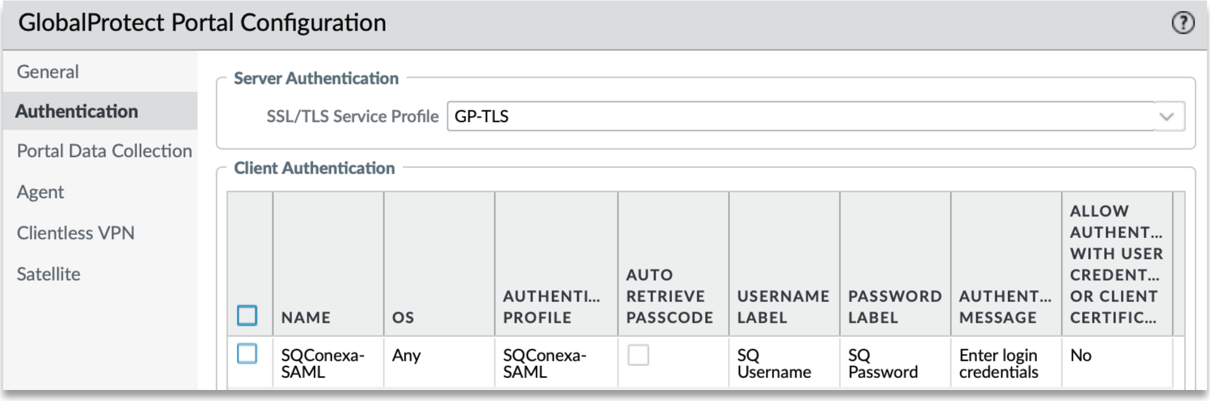
GlobalProtect is Palo Alto Networks' VPN solution.

Step 1: At the Palo Alto Networks dashboard, navigate to the following:

Network > GlobalProtect > Portals

Step 2: Add or Edit an existing Portal Configuration.

Step 3: Click on Authentication and add a new Client Authentication and set it to SAML authentication profile we created for SendQuick Conexa. Move this up and set it as the first client authentication profile if you have multiple entries in the list.



Server Authentication

SSL/TLS Service Profile: GP-TLS

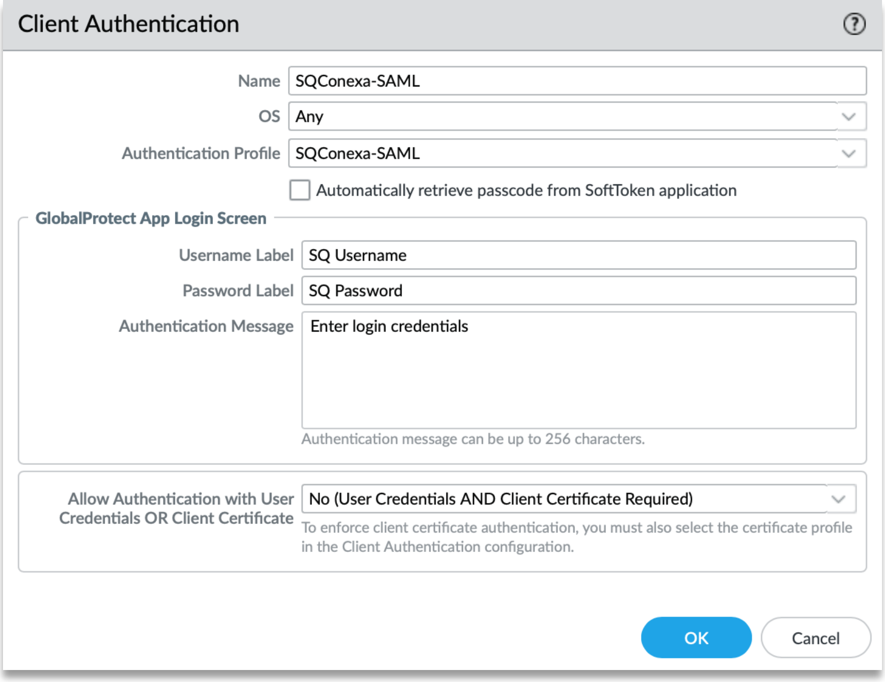
Client Authentication

☐	NAME	OS	AUTHENTI... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENT... MESSAGE	ALLOW AUTHENT... WITH USER CREDENT... OR CLIENT CERTIFIC...
☐	SQConexa-SAML	Any	SQConexa-SAML	☐	SQ Username	SQ Password	Enter login credentials	No

Figure 30 Link GlobalProtect Portal to SAML Authentication Profile

Click on the name of the Client Authentication and provide the labels for the login screen.

See example below:



Client Authentication

Name: SQConexa-SAML

OS: Any

Authentication Profile: SQConexa-SAML

□ Automatically retrieve passcode from SoftToken application

GlobalProtect App Login Screen

Username Label: SQ Username

Password Label: SQ Password

Authentication Message: Enter login credentials

Authentication message can be up to 256 characters.

Allow Authentication with User Credentials OR Client Certificate: No (User Credentials AND Client Certificate Required)

To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

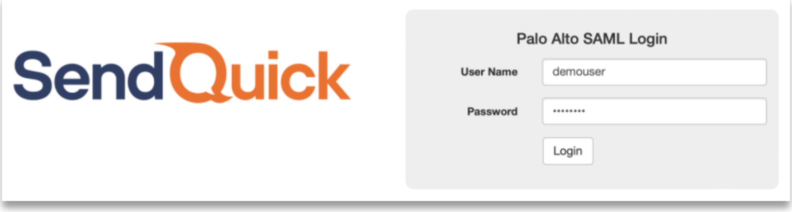
Figure 31 Client Authentication Set Up for SAML

4.5 Accessing GlobalProtect Web Portal using SAML

Logging in via your organisation's GlobalProtect web portal will now have an additional step to authenticate via OTP using SAML.

Step 1: Browse to GlobalProtect portal public IP address that has been configured for your organisation. You will be redirected to SendQuick Conexa SAML login page.

Step 2: Enter valid Username and Password. In this example, we use the Local User account we created earlier.



Palo Alto SAML Login

User Name: demouser

Password: ••••••••

Figure 32 SAML login page

Step 3: Receive the OTP via SMS, Email or Push message.

Step 4: Enter OTP from SMS/Email or Soft Token app (if activated.)

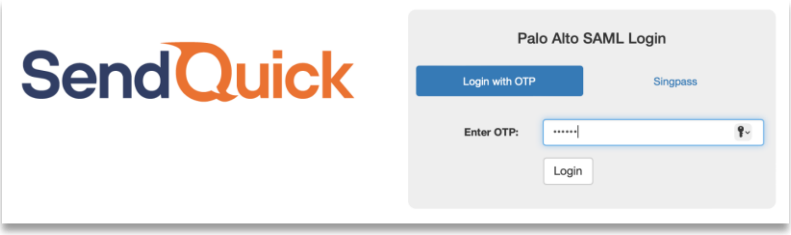
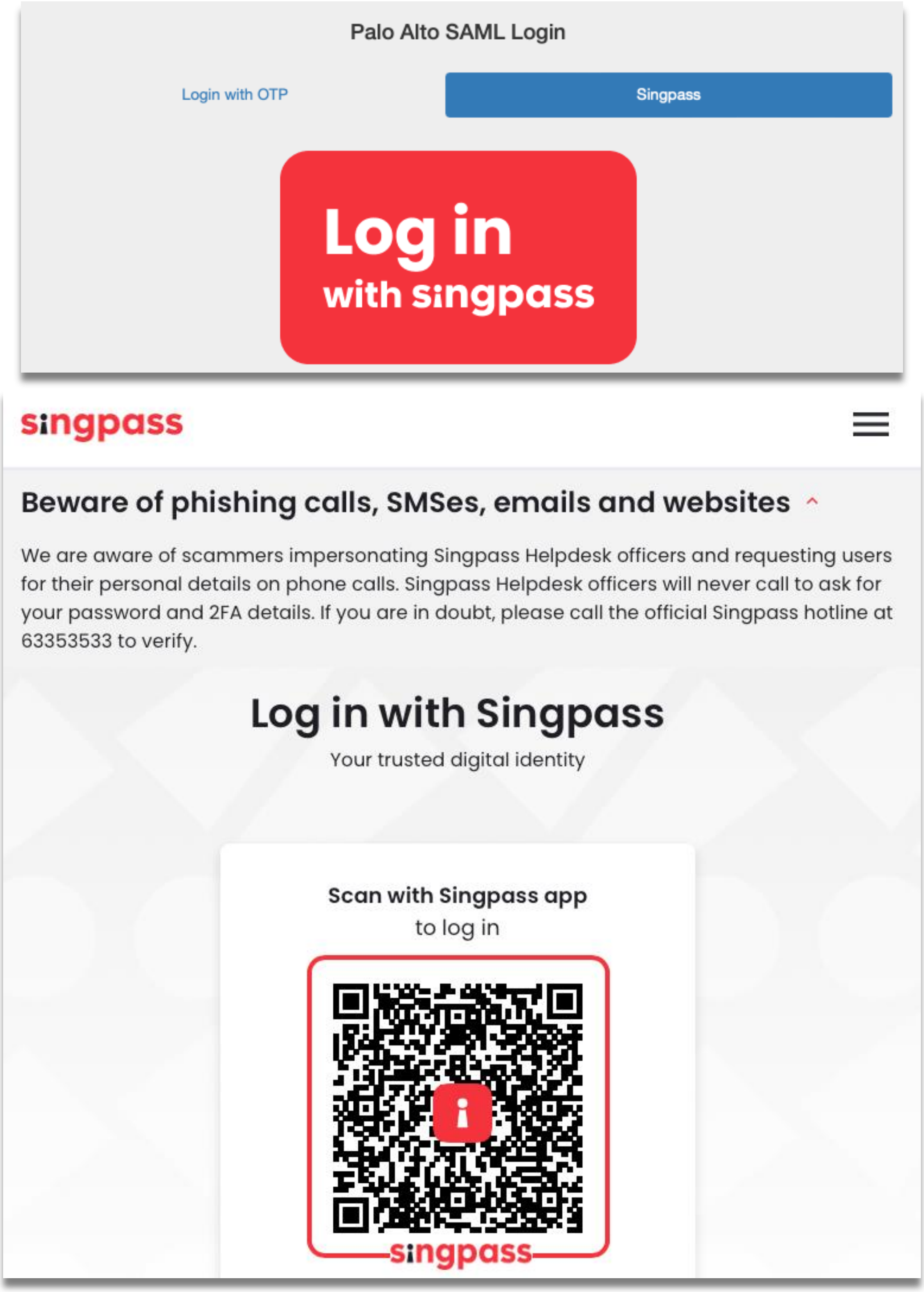


Figure 33 Enter OTP received on mobile device

Step 5: Alternatively, click “Singpass” tab and click on Log in with Singaoss button. You will be redirected to Singpass login page and scan Singpass QR to login.



Palo Alto SAML Login

Beware of phishing calls, SMSes, emails and websites

We are aware of scammers impersonating Singpass Helpdesk officers and requesting users for their personal details on phone calls. Singpass Helpdesk officers will never call to ask for your password and 2FA details. If you are in doubt, please call the official Singpass hotline at 63353533 to verify.

Log in with Singpass

Your trusted digital identity

Scan with Singpass app
to log in

Figure 34 Using Singpass for authentication

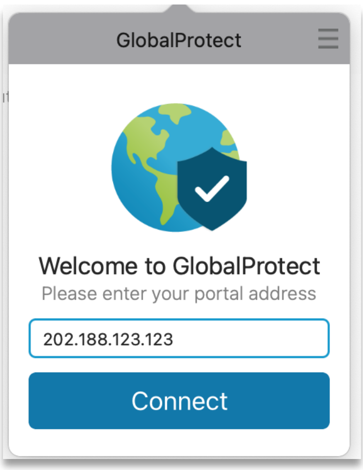
Step 6: Upon successful authentication of OTP or Singpass, login will be successful.

4.6 Access via GlobalProtect agent using SAML

You can also access the portal via GlobalProtect Agent.

Step 1: Download GlobalProtect agent from web portal.

Step 2: Enter your public portal address and click on Connect.



Welcome to GlobalProtect

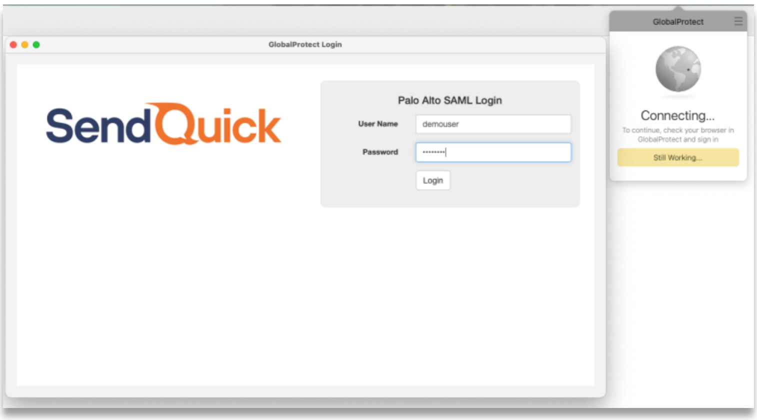
Please enter your portal address

202.188.123.123

Figure 35 Login via GlobalProtect Agent

Step 3: A new browser window "GlobalProtect Login" will pop up and prompt you to login.

Step 4: Enter your local user ID and password, click Sign In.



User Name: demouser

Password: ••••••••

Connecting...

To continue, check your browser in GlobalProtect and sign in

Figure 36 SAML Login page

Step 5: Receive the OTP via SMS, Email or Push message.

Step 6: Enter OTP received from SMS/Email or Soft Token app (if activated.)

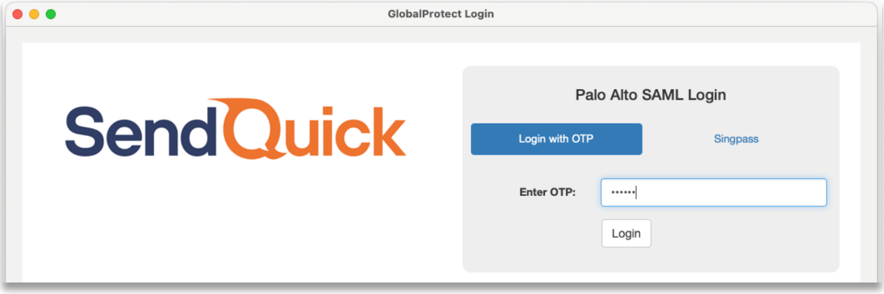


Figure 37 Option to use OTP or Singpass

Step 7: Alternatively, click “Singpass” tab and scan Singpass QR to login.

Step 8: Upon successful authentication, you will be connected to GlobalProtect.

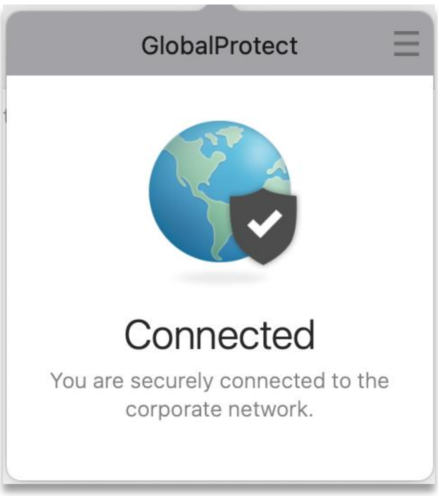


Figure 38 Connected to VPN