SendQuick®

SendQuick® Conexa
User Manual
Version 3.0 (14 July 2023)

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

Table of Contents

1.0 Introduction 4
1.1 About SendQuick 4
1.2 About SendQuick Conexa 4
1.3 Purpose of Document 4
1.4 Prerequisite 5
2.0 Setup and Configuration 6
2.1 Login Procedures 7
2.1.1 Login Types 7
2.2 Dashboard 8
2.3 Logs 8
2.3.1 Server Log 8
2.3.2 Authentication Log 9
2.4 Radius OTP Configuration 9
2.4.1 Radius Client Configuration 9
2.4.2 VPN Configuration 10
2.5 SAML SP Configuration 15
2.5.1 SP Configuration 15
2.6 Auth API Configuration 19
2.6.1 Auth API Client 19
2.6.2 Web OTP Client 21
2.7 Portal Configuration 24
2.7.1 Controller Configuration 24
2.7.2 Blacklisted Mobile 26
2.8 User Management 26
2.8.1 All Users 26
2.8.2 Upload User 26
2.8.3 Remote DB Configuration 28
2.8.4 LDAP Configuration 28
2.9 Soft Token Management 30
2.9.1 Soft Token Users 30
2.9.2 Soft Token User Synchronization 34
2.9.3 Soft Token Activation Templates 35
2.9.4 Soft Token Configuration 36

2.10 System Configuration 37
2.11 VPN User Login 38
3.0 REFERENCES 39
3.1 RADIUS Authentication Types 39
3.2 SAML Authentication Types 42
3.3 OTP On Demand SMS template 43
3.4 Soft Token Mobile Application 44

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 Multi-Factor Authentication (MFA) implementation.

It has a built-in SMS OTP, Soft Token, Push Auth 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 for administrator to configure users' access using various authentication methods (OTP, SOFT TOKEN, PUSH, Digital ID). Administrator also configure which authentication server (LDAP/Active Directory, local users, remote database, remote RADIUS server) to authenticate users.

1.4 Prerequisite

Function	Requirement
IP setup	IP, Netmask and GW for SendQuick Conexa
Send SMS	SIM card, if using Modem Cloud SMS account, if using Cloud SMS
Send Email	Email Gateway IP User credential if required authentication
Radius Authentication	Radius Client (VPN/Firewall) IP address Shared Secret
AD Integration	AD Server IP, Base DN Service Account ID and Password (Domain User) AD Attribute name to retrieve user's mobile and email. User's mobile and email need to be configured in AD user properties.
Remote DB Integration	Server Type : Oracle, PostgreSQL, MSSQL or MYSQL Database Server IP and port number Database Name Database User Name and Password Table name and column name for user ID, password, mobile and email
Secure QR code	Public DNS with valid SSL cert
Push OTP / Push Auth to SendQuick app	Public DNS with valid SSL cert
Digital ID (Singpass)	Public DNS with valid SSL cert

2.0 Setup and Configuration

Typical set-up steps as follow:

1. Configure User from
    a. Local User (Create or Upload user to SendQuick Conexa)
    b. Connect to Active Directory / LDAP
    c. Connect to Remote Database (MSSQL, MySQL, PostgreSQL, Oracle)

2. If using RADIUS method
    a. Add RADIUS client and configure shared secret
    b. Add VPN Configuration

3. If using SAML method
    a. Create a new SAML SP Configuration with the details provided by service provider.
    b. Provide service provider with SAML IdP metadata from SendQuick Conexa.

4. If using HTTP API method
    a. Create Auth API or Web OTP client.
    b. Provide third party application with the client credential and API specs.

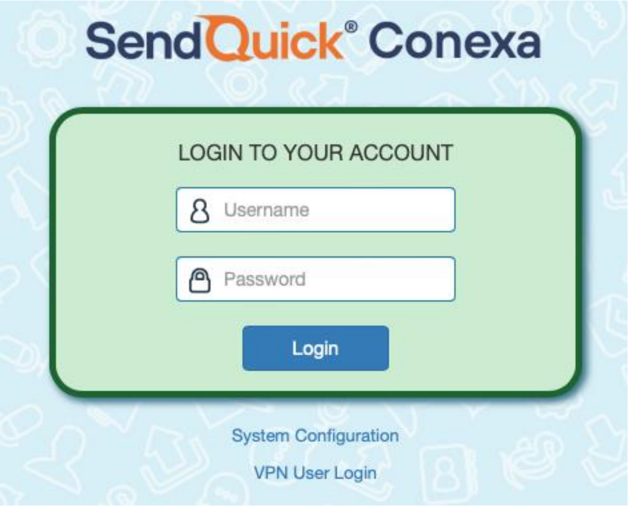
5. If integrating with Captive Portal
    a. Create a new controller configuration
    b. Provide third party WIFI controller with captive portal URL

6. If using Soft Token
    a. Create soft token user
    b. Activate soft token user

2.1 Login Procedures

Use a web browser to access SendQuick Conexa's server IP, you will be redirected to the login page.

URL: http[s]://[Conexa's server IP]/otp/



Enter the default Administrator’s Log-in Name and Password to access the system. The default Username is **otpadmin** and the password should have been provided to you during installation. If you do not have the password, please contact our technical support for assistance.

You can change the password after logging-in.

2.1.1 Login Types

There are three (3) types of user accounts:

- Super Admin (otpadmin)
- Admin
- User

Super Admin and Admin have full access rights to every feature. The only difference is Super Admin 'otpadmin' account is the default admin account and cannot be deleted.

User level login is for the local users in SendQuick Conexa to update their personal details such as login password, mobile and email to receive OTP.

2.2 Dashboard

These dashboard pages will display summary of all login requests for different request types.

Radius OTP
Radius requests usually come from VPN / Firewall. SendQuick Conexa acts as a Radius Server. This page shows summary of Radius login requests, authentication methods, recent authenticated and rejected VPN users. Admin can select date range to generate summary report. The default reporting period is the last 30 days.

Web OTP
Application can integrate with Web OTP to provide two-factor authentication. This page shows a summary of Web OTP requests of the day. Admin can select different date ranges to generate reports.

Portal
Captive portal is usually used to provide login page for public Wi-Fi and it integrates with Wi-Fi controller. This page will display a summary of Captive Portal login request of the day.

Auth API
Application can integrate with Auth API to provide two-factor authentication. This page shows a summary of Auth API requests, authentication methods, recent authenticated and rejected users. Admin can select date range to generate report. Default is the last 30 days.

SAML OTP
SAML requests can be sent from Firewall, VPN or any application that supports SAML authentication. SendQuick Conexa acts as an Identity Provider (IdP). This page will display summaries for all SAML login requests. Admin can select date range to generate summary report. The default reporting period is the last 30 days.

2.3 Logs

SendQuick Conexa allows administrator to access Server and Authentication logs to backtrack and examine recorded activities performed by SendQuick or users.

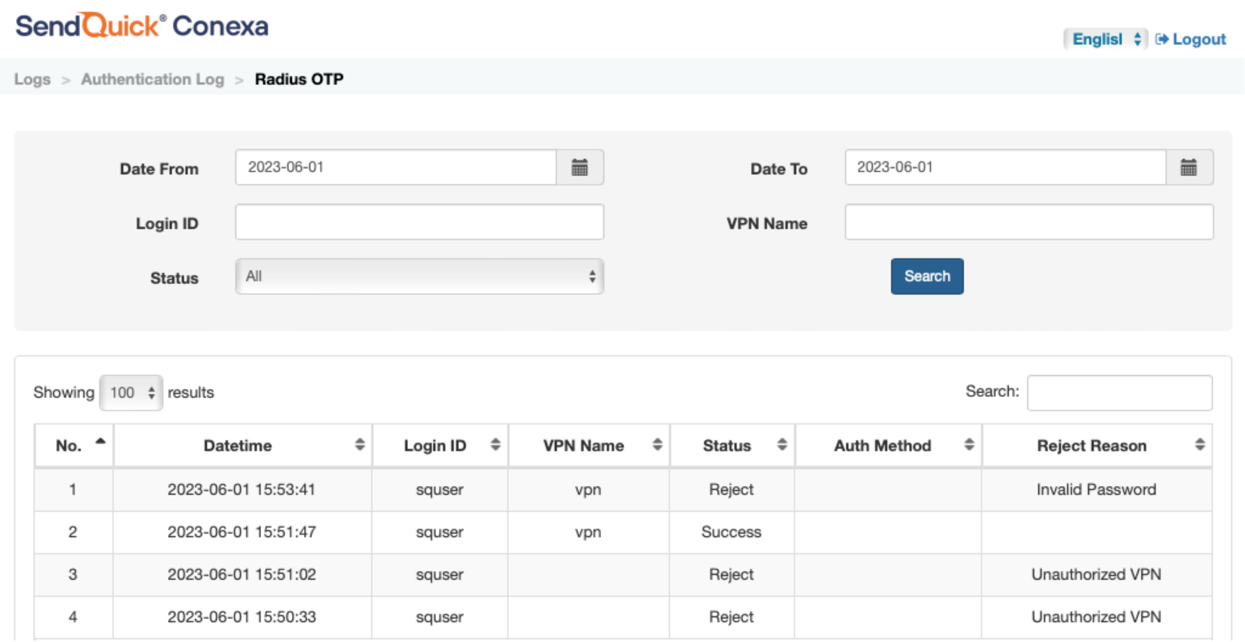
2.3.1 Server Log

Other than viewing current server log, administrator also can download server logs for the past 7 days and send to SendQuick support for quick troubleshooting.

Server Log is useful to check the authentication process once receive a new request. Admin can view server log for Radius, Web OTP or SAML and Auth API request.

2.3.2 Authentication Log

This page displays the complete authentication requests log. Admin can check every incoming login authentication request from Radius, Web OTP, SAML, Auth API and Portal.



Logs > Authentication Log > Radius OTP

Date From: 2023-06-01
Date To: 2023-06-01
Login ID:
VPN Name:
Status: All

Showing 100 results
Search:

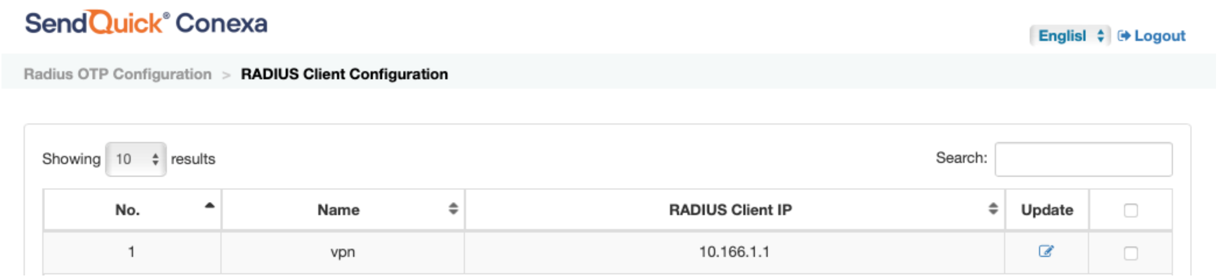
No.	Datetime	Login ID	VPN Name	Status	Auth Method	Reject Reason
1	2023-06-01 15:53:41	squser	vpn	Reject		Invalid Password
2	2023-06-01 15:51:47	squser	vpn	Success		
3	2023-06-01 15:51:02	squser		Reject		Unauthorized VPN
4	2023-06-01 15:50:33	squser		Reject		Unauthorized VPN

2.4 Radius OTP Configuration

The administrator will configure RADIUS client and VPN in this section. SendQuick Conexa acts as a RADIUS server and process RADIUS auth requests from RADIUS client such as VPN , Firewall or other application.

2.4.1 Radius Client Configuration

Administrator needs to create RADIUS client configuration for each VPN before it can send authentication request to SendQuick Conexa. RADIUS shared secret must be configured on both VPN and SendQuick Conexa server.

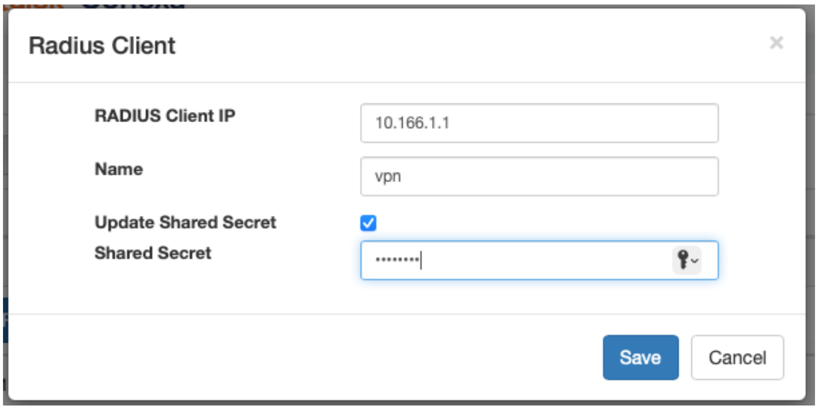


Radius OTP Configuration > RADIUS Client Configuration

Showing 10 results
Search:

No.	Name	RADIUS Client IP	Update	□
1	vpn	10.166.1.1	✎	□

Create/Edit Radius Client Configuration



Radius Client

RADIUS Client IP: 10.166.1.1

Name: vpn

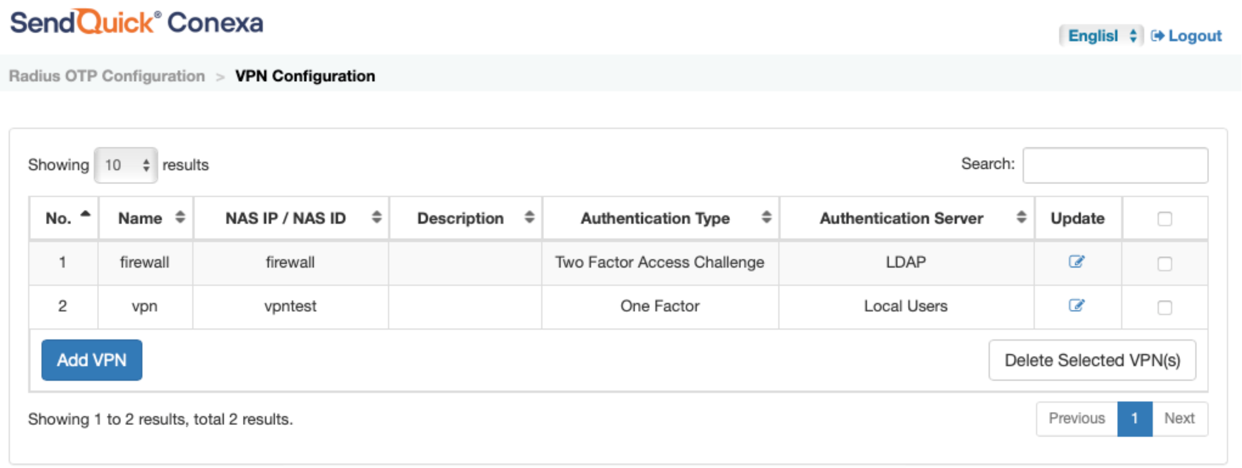
Update Shared Secret: ☑

Shared Secret: ••••••••

Fields	Description
RADIUS Client IP	VPN's gateway IP address. This is the IP address captured in SendQuick Conexa when receiving Radius request.
Name	Unique name to identify radius client
Shared Secret	Radius server shared secret. Shared secret must be configured on both Radius client (VPN) and Radius server (SendQuick Conexa).

2.4.2 VPN Configuration

The Administrator can set different configuration for each VPN to meet requirement for different login requests, such as authentication server, OTP delivery mode, Soft Token and OTP message template etc.



No.	Name	NAS IP / NAS ID	Description	Authentication Type	Authentication Server	Update	□
1	firewall	firewall		Two Factor Access Challenge	LDAP	✎	□
2	vpn	vpntest		One Factor	Local Users	✎	□

Showing 1 to 2 results, total 2 results.

Create/Edit VPN Configuration

Fields	Description
Captive Portal Controller Name	Select Controller Name if this configuration is used for captive portal. Default : None
NAS-IP / NAS-ID	VPN IP address or identifier Use either NAS-IP-Address or NAS-Identifier to communicate with SendQuick Conexa. Select None if both NAS-IP-Address and NAS-Identifier are empty.
Name	Unique name to identify VPN
Description	Short description for VPN. For reference only.
Authentication Type	• One Factor • Two Factor Static (Password + OTP) • Two Factor Static (OTP) • Two Factor Static (SMS Reply) • Two Factor Access Challenge • Tow Factor Access Challenge (Username Only) Refer to "References: RADIUS Authentication Types" for more details.
Access Challenge Validity	Valid period in minutes before challenge request timeout. Default is 0, which is disabled.
Authentication Server	• Local Users • RADIUS o Authenticate through remote radius server. Remote radius server IP, port and secret are required. • LDAP o Authenticate through LDAP server such as Active Directory or OpenLDAP. Select LDAP server from list which are predefined in LDAP Configuration section. • Multiple LDAP (Only available for Conexa300) o Authenticate through LDAP servers (max 10 servers) Search Options -> [Recursive | Predefined] Recursive: Search through all LDAP servers in sequence. Predefined: Required ldapname\userid in login name. For example, if LDAP server name is ldap1, user needs

	to enter ldap1\userid in the login ID field - Remote DB Authenticate through external DB server [SQL Server, MySQL, PostgreSQL or Oracle DB]. Select Remote DB from list which is predefined in Remote DB Configuration section. Table name and column name of userid and password are required.
LDAP Return Option	For LDAP or Multiple LDAP, SendQuick Conexa can return LDAP group as Radius Attribute 11 (Filter ID) and/or Radius Attribute 25 (Class)
Enable Soft Token	Allow user to authenticate through 6-digit token generated by SendQuick app or other authenticator like Google or Microsoft Authenticator
Push OTP	Enable Push OTP to be sent to soft token user's SendQuick app
Push Auth	Enable Push Auth to be sent to soft token user's SendQuick app. Push Auth Expiry default to 1 minute.
Enable OTP	Allow user to authenticate through one time password generated by SendQuick Conexa and send to user via SMS, Email, MIM or other delivery channels.
Skip OTP	Do not send OTP SMS/Email if Soft Token has been activated for login user.
OTP On Demand Keyword	Unique keyword to request OTP. For Two Factor Static (Password + OTP) or (OTP) mode, users can send SMS to SendQuick Conexa to request OTP before they logging-in VPN.
SMS Reply Template	For Two Factor Static (SMS Reply) mode, SendQuick Conexa will send this message to user's mobile for second level authentication. User needs to reply SMS with keyword to accept or reject the login access. Available variables: ^V = VPN Name ^Y = Keyword to accept ^N = Keyword to reject ^M = Validity period (in minutes) ^D = Date (YYYY-MM-DD) ^T = Time (HH:MM:SS)
SMS Reply Keyword (Accept)	Users need to reply SMS with this keyword to confirm access through their user accounts.

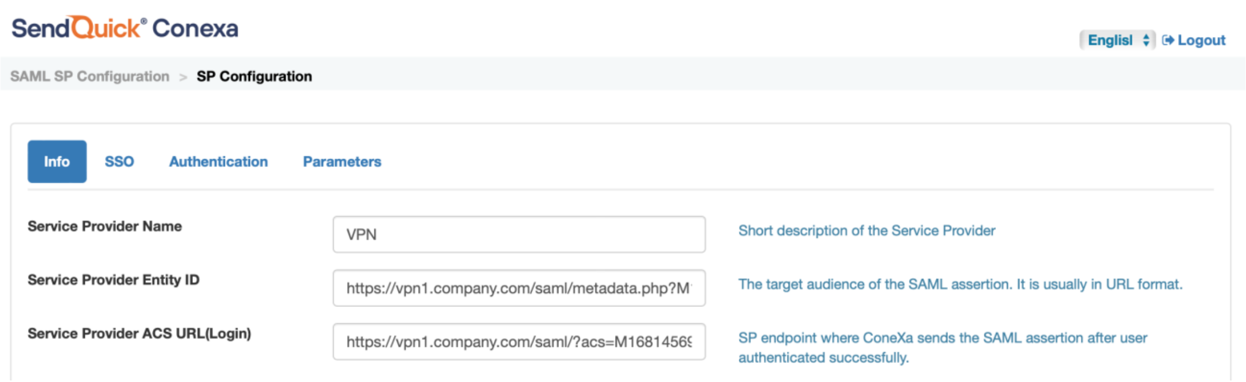
SMS Reply Keyword (Reject)	Users need to reply SMS with this keyword to reject access through their user accounts.
SMS Reply Validity(minute)	Users need to reply within this validity period, otherwise the request will be rejected.
OTP Prompt Message	Prompt message on access challenge page. ^M = User's mobile number ^E = User's email Default : Enter OTP:
OTP Type	[One Time Pin (OTP) | Short Term Pin (STP)] OTP: One time usage only. STP: Limited times of usage over validity period.
OTP Delivery Method	[SMS | EMAIL | SMS & Email]
OTP Length	4 to 10 characters in numeric or alphanumeric format.
OTP Email Subject	Subject of OTP delivery email
OTP Email From	Sender of OTP delivery email
OTP Validity Period (minute)	Validity period before OTP expires
OTP Message Template	SMS template message received by user. ^P = OTP Token ^E = OTP Validity Period(minute) ^D = Date (YYYY-MM-DD) ^T = Time (HH:MM:SS)
Short-term PIN Validity Period	Validity period before STP expires
Short-term PIN Maximum Usage Count	Maximum number of STP reuse count.
OTP Message Mode	[Normal Text | Message Overwrite | Flashtext] • Normal Text: Send as normal SMS text message. • Message Overwrite: Replace previously received SMS with the new SMS. • Flashtext: Flash SMS appears directly on phone's screen, instead of Inbox.

SMS Priority	1 to 9 (Highest = 1 , Lowest = 9)
Modem Label	Send SMS via specific message label
Allow Update Contact	Allow VPN user login to update contact manually. Enter T&C or End User Agreement. This message will be shown, and user need to agree with it before updating their contact details
User Contact List	• Check on 'Same as authentication server' to use the same user list in authentication server. • Local Users ○ Mobile and Email in User Management. • LDAP ○ Select from a list of predefined LDAP servers. Mobile and email attributes are required. • Remote DB ○ Select from a list of predefined Remote DB. Required table name and column name for user id, mobile and email.

2.5 SAML SP Configuration

SendQuick Conexa is a SAML Identity Provider (IdP) and processes SAML requests from SAML Service Provider (SP).

2.5.1 SP Configuration



Service Provider Name	VPN	Short description of the Service Provider
Service Provider Entity ID	https://vpn1.company.com/saml/metadata.php?M	The target audience of the SAML assertion. It is usually in URL format.
Service Provider ACS URL(Login)	https://vpn1.company.com/saml/?acs=M1681456	SP endpoint where ConeXa sends the SAML assertion after user authenticated successfully.

<u>Create/Edit SAML SP Configuration</u>

Fields	Description
Info	
Service Provider Name	Short description of the Service Provider
Service Provider Entity ID	Entity ID or Issuer of the SAML Service Provider.
Service Provider ACS URL (Login)	Service Provider endpoint where SendQuick Conexa sends the SAML assertion after user authenticated successfully.
ACS Binding	HTTP Binding Method when sending SAML assertion to SP. Default is HTTP-POST
Service Provider SLS URL (Logout)	Service Provider endpoint where SendQuick Conexa should redirect to after performing single logout.
SLS Binding	HTTP Binding Method when sending sign out response to SP. Default is HTTP-POST
Sign Assertion	Default is disabled
Sign Response	Default is enabled
Encrypt Assertion	Default is disabled
Service Provider X.509 Certificate	SP's public key certificate in X.509 format.
Template	Choose from predefined template or upload own template.

SSO	
IDP Issuer	Entity ID of SendQuick Conexa SAML IdP
IDP SSL URL	Single sign-on URL to receive SAML authentication request from service provider
IDP SLO URL	Single logout URL to receive SAML logout request from service provider.
X.509 Certificate	SAML signing certificate.
Download metadata from SendQuick Conexa	
Authentication	
SAML Authentication Type	• One Factor • Two Factor Access Challenge • Two Factor with Singpass only Refer to "References: SAML Authentication Types" for more details.
Authentication Server	• Local Users • RADIUS ○ Authenticate through remote radius server. Remote radius server IP, port and secret are required. • LDAP ○ Authenticate through LDAP server such as Active Directory or OpenLDAP. Select LDAP server from list which are predefined in LDAP Configuration section. • Multiple LDAP (Only available for Conexa300) ○ Authenticate through LDAP servers (max 10 servers) Search Options -> [Recursive | Predefined] Recursive: Search through all LDAP servers in sequence. Predefined: Required ldapname\userid in login name. For example, if LDAP server name is ldap1, user needs to enter ldap1\userid in the login ID field • Remote DB ○ Authenticate through external DB server [SQL Server, MySQL, PostgreSQL or Oracle DB]. Select Remote DB from list which is predefined in Remote DB Configuration section. Table name and column name of userid and password are required.

Enable Soft Token	Allow user to authenticate through 6-digit token generated by SendQuick app or another authenticator like Google Authenticator or Microsoft Authenticator
Push OTP	Enable Push OTP to be sent to soft token user's SendQuick app
Push Auth	Enable Push Auth to be sent to soft token user's SendQuick app. Push Auth Expiry default to 1 minute.
Enable Singpass	Allow user to sign in with Digital ID (Singpass)
Enable OTP	Allow user to authenticate through one time password generated by SendQuick Conexa and send to user via SMS, Email, MIM or other delivery channels.
Skip OTP	Do not send OTP SMS/Email if Soft Token has been activated for login user.
OTP Prompt Message (Access Challenge)	Prompt message on access challenge page. ^M = User's mobile number ^E = User's email Default: Enter OTP
OTP Length	4 to 10 characters in numeric or alphanumeric format.
OTP Validity Period (minute)	Validity period in minutes before OTP expires
OTP Message Template	SMS template message received by user. ^P = OTP Token ^E = OTP Validity Period(minute) ^D = Date (YYYY-MM-DD) ^T = Time (HH:MM:SS)
SMS OTP	Enable SMS OTP
SMS Priority	1 to 9 (Highest = 1 , Lowest = 9)
Modem Label	Send SMS via specific message label
Email OTP	Enable Email OTP
OTP Email Subject	Subject of OTP delivery email
OTP Email From	Sender of OTP delivery email
User Contact List	• Check on 'Same as authentication server' to use the same user list in authentication server. • Local Users

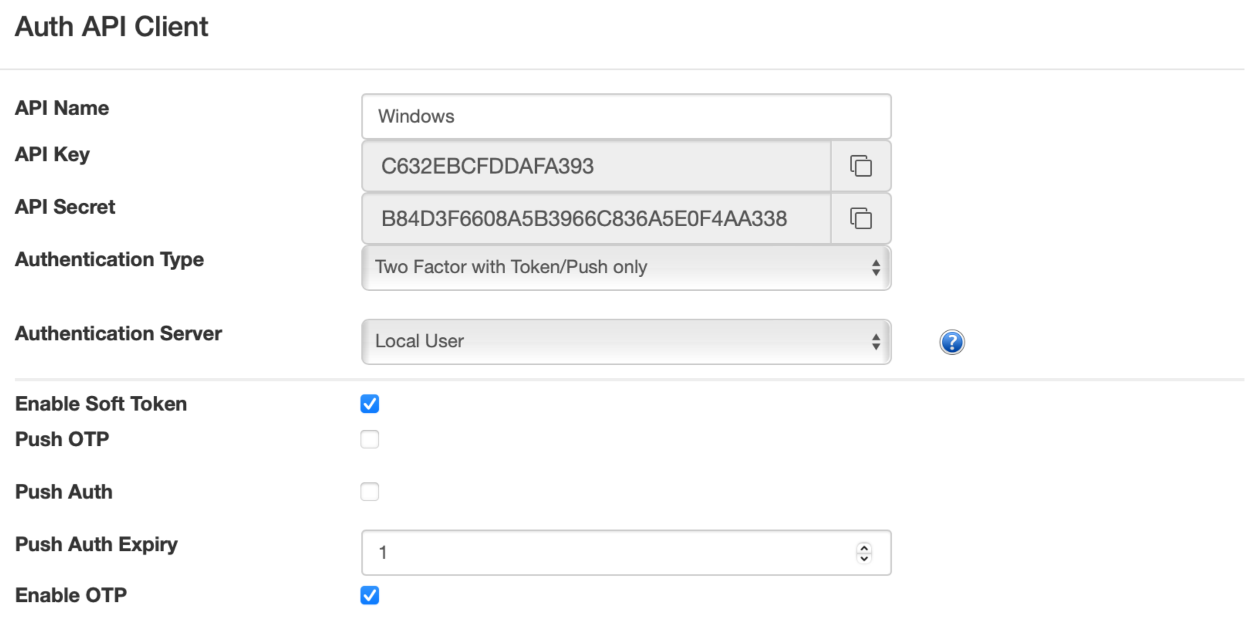
	○ Mobile and Email in User Management. • LDAP ○ Select from a list of predefined LDAP servers. Mobile and email attributes are required. • Remote DB ○ Select from a list of predefined Remote DB. Required table name and column name for user id, mobile and email.
Parameters	
NameID	Mandatory field. Set the value of SAML name identifier to be returned to service provider.
Add other parameters name and set the values from different server and attributes. - Local User: Login ID, Username, Mobile, Email - LDAP: Select LDAP server and attribute name - Remote DB: Select Remote DB server and configure table name and column name. - Fixed Value	

2.6 Auth API Configuration

There are two types of API. Auth API which is able to process full cycle of user authentication whereas Web OTP API is used to trigger and validate OTP.

2.6.1 Auth API Client

User can utilise Auth API to process multifactor authentication request from application or windows login.



Auth API Client

API Name	Windows
API Key	C632EBCFDDAFA393
API Secret	B84D3F6608A5B3966C836A5E0F4AA338
Authentication Type	Two Factor with Token/Push only
Authentication Server	Local User
Enable Soft Token	☑
Push OTP	□
Push Auth	□
Push Auth Expiry	1
Enable OTP	☑

Create/Edit Auth API Client

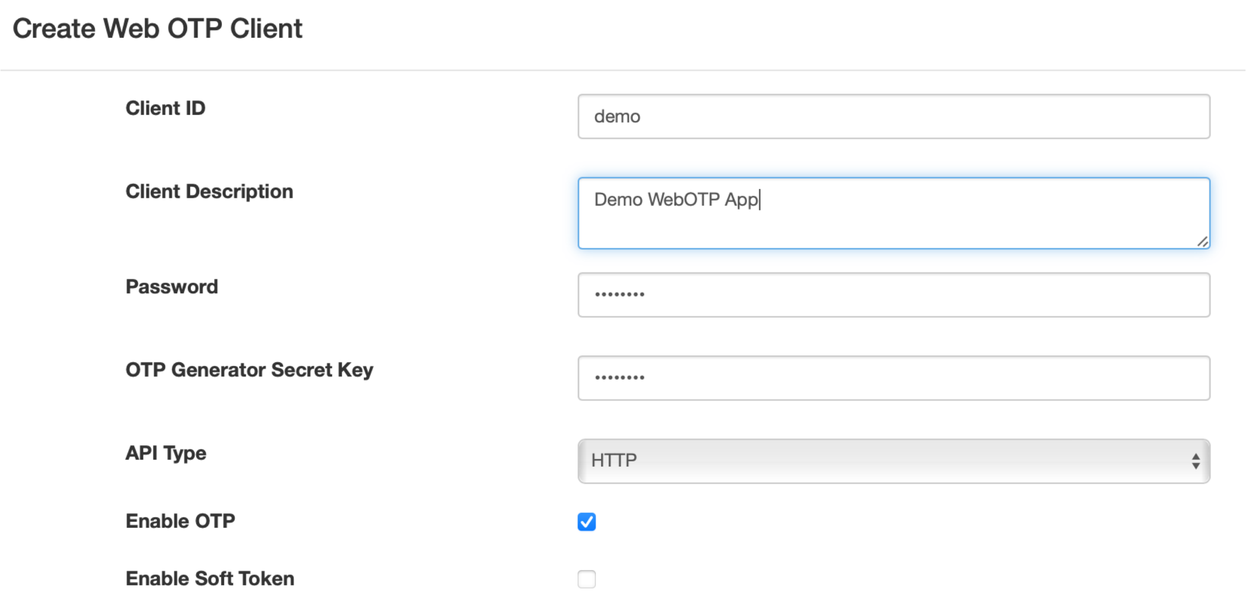
Fields	Description
API Name	Short description of the application
API Key & Secret	API key and secret to authenticate application
Authentication Type	• One Factor • Two Factor Access Challenge • Two Factor with Token/Push only Refer to "References: Auth API Authentication Types" for more details.
Authentication Server	• Local Users • LDAP ○ Authenticate through LDAP server such as Active Directory or OpenLDAP. Select LDAP server from list which are predefined in LDAP Configuration section. • Multiple LDAP (Only available for Conexa300)

	○ Authenticate through LDAP servers (max 10 servers) Search Options -> [Recursive | Predefined] Recursive: Search through all LDAP servers in sequence. Predefined: Required ldapname\userid in login name. For example, if LDAP server name is ldap1, user needs to enter ldap1\userid in the login ID field • Remote DB ○ Authenticate through external DB server [SQL Server, MySQL, PostgreSQL or Oracle DB]. Select Remote DB from list which is predefined in Remote DB Configuration section. Table name and column name of userid and password are required.
Enable Soft Token	Allow user to authenticate through 6-digit token generated by SendQuick app or another authenticator like Google Authenticator or Microsoft Authenticator
Push OTP	Enable Push OTP to be sent to soft token user's SendQuick app
Push Auth	Enable Push Auth to be sent to soft token user's SendQuick app. Push Auth Expiry default to 1 minute.
Enable Singpass	Allow user to sign in with Digital ID (Singpass)
Enable OTP	Allow user to authenticate through one time password generated by SendQuick Conexa and send to user via SMS, Email, MIM or other delivery channels.
Skip OTP	Do not send OTP SMS/Email if Soft Token has been activated for login user.
OTP Prompt Message (Access Challenge)	Prompt message on access challenge page. ^M = User's mobile number ^E = User's email Default: Enter OTP
OTP Length	4 to 10 characters in numeric or alphanumeric format. Default: 6
OTP Validity Period (minute)	Validity period in minutes before OTP expires. Default: 3 minutes
OTP Message Template	SMS template message received by user. ^P = OTP Token

	^E = OTP Validity Period(minute) ^D = Date (YYYY-MM-DD) ^T = Time (HH:MM:SS)
SMS OTP	Enable SMS OTP
SMS Priority	1 to 9 (Highest = 1, Lowest = 9)
Modem Label	Send SMS via specific message label
Email OTP	Enable Email OTP
OTP Email Subject	Subject of OTP delivery email
OTP Email From	Sender of OTP delivery email
User Contact List	Check on 'Same as authentication server' to use the same user list in authentication server. • Local Users ○ Mobile and Email in User Management. • LDAP ○ Select from a list of predefined LDAP servers. Mobile and email attributes are required. • Remote DB Select from a list of predefined Remote DB. Required table name and column name for user id, mobile and email.

2.6.2 Web OTP Client

Web OTP API handles OTP request and OTP validation. It is useful for those application that can process user authentication before sending to WebOTP API to request OTP.



Create Web OTP Client

Client ID	demo
Client Description	Demo WebOTP App
Password	········
OTP Generator Secret Key	········
API Type	HTTP
Enable OTP	☑
Enable Soft Token	☐

Fields	Description
Client ID	Unique identifier of the application. This will be used in API client authentication.
Client Description	Short description of the application
Password	Password for this client.
OTP Generator Secret Key	Optional. Random String value for OTP generator. Increase OTP randomness and uniqueness for each application.
API Type	• HTTP • XML • SOAP Web OTP request method. Refer to Web OTP API
Enable OTP	Enable OTP
Enable Soft Token	Enable Soft Token
Skip OTP	Do not send OTP SMS/Email if Soft Token has been activated for login user.
Push OTP	Enable Push OTP to be sent to soft token user’s SendQuick app
Push Auth	Enable Push Auth to be sent to soft token user’s SendQuick app. Push Auth Expiry default to 1 minute.
OTP Delivery Mode	• SMS • Email • SMS and Email Web OTP delivery mode.
SMS Priority	1 to 9 (Highest = 1, Lowest = 9)

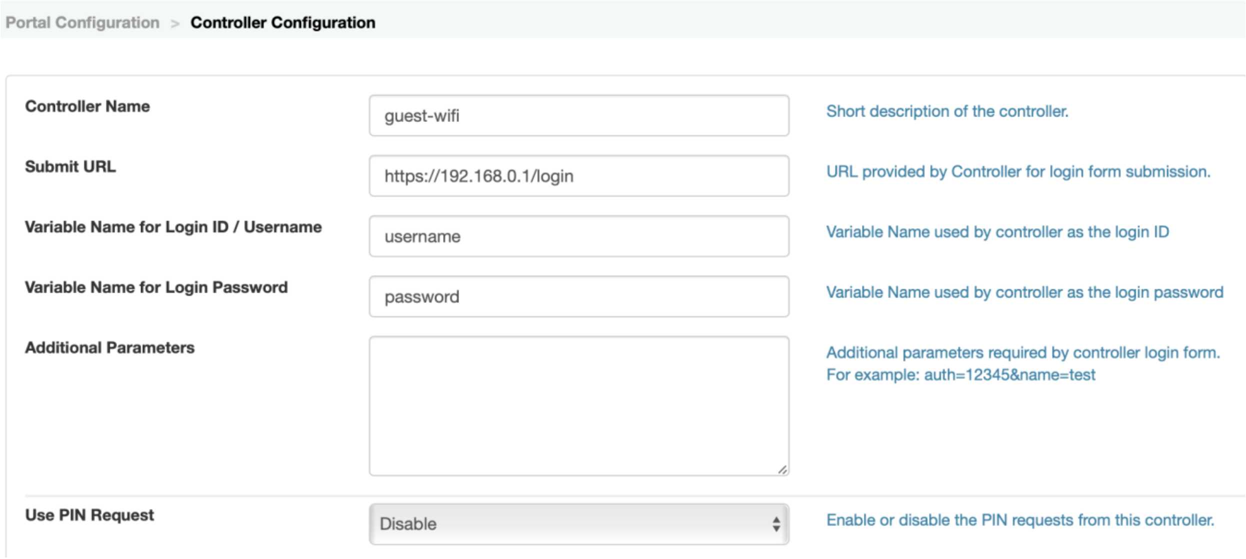
SMS Label	Send SMS via specific message label
SMS Mode	• Normal SMS • Message Overwrite • Flash SMS Default: Normal SMS. Message Overwrite and Flash SMS mode are depending on mobile phones.
Email OTP From	Valid email address for sending Email OTP
Email OTP Subject	Email Subject for Email OTP
OTP Type	• OTP (One Time PIN) ○ Use for one time only within minutes. • STP (Short Term PIN) ○ Can be used for multiple times within hours.
OTP Validity	
OTP Format	• Numeric • Alpha Numeric • Alpha Numeric – Case Sensitive OTP characters format. Default: Numeric.
OTP length	Length of the OTP. Default: 6
Session ID Format	• Alphabets • Alpha Numeric Session ID paired with OTP. Format: [Session ID]-[OTP]. Default: Alphabets
Session ID Length	Length of session ID. Default: 4
OTP Message	OTP message template. Available variables: • * use xPINx to replace PIN. • * use xEXPIRYx to replace expiry time. • * use xSESSIONIDx to replace session id. • * use xMONTHx to replace current Month. • * use xDAYx to replace current Day. • * use xHHx to replace current Hour. • * use xMMx to replace current Minute. • * use xSSx to replace current Second. Variables are case-sensitive.

	Default Message: Your PIN is xSESSIONIDx-xPINx and expired in xEXPIRYx minutes. Send DTM: xHHx:xMMx
Maximum OTP Resend	Maximum Resend times for OTP.

2.7 Portal Configuration

SendQuick can integrate with WIFI Controller to provide captive portal for user to login and connect to the network.

2.7.1 Controller Configuration



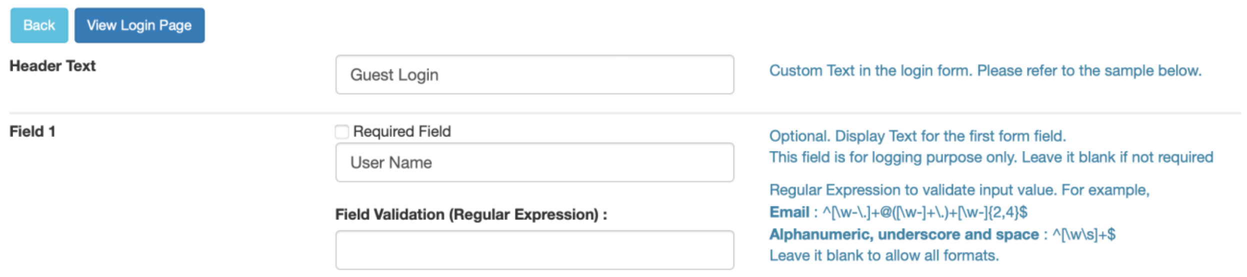
Portal Configuration > Controller Configuration

Controller Name	guest-wifi	Short description of the controller.
Submit URL	https://192.168.0.1/login	URL provided by Controller for login form submission.
Variable Name for Login ID / Username	username	Variable Name used by controller as the login ID
Variable Name for Login Password	password	Variable Name used by controller as the login password
Additional Parameters		Additional parameters required by controller login form. For example: auth=12345&name=test
Use PIN Request	Disable	Enable or disable the PIN requests from this controller.

Fields	Description
Controller Name	Short description of the controller
Submit URL	URL provided by Controller for login form submission
Variable Name for Login ID / Username	Variable Name used by controller as the login ID
Variable Name for Login Password	Variable Name used by controller as the login password
Additional Parameters	Additional parameters required by controller login form. For example: auth=12345&name=test
Use PIN Request	Enable or disable the PIN requests from this controller.
PIN Request Timeout	Set timeout(in seconds) for PIN request upon clicked. Default is 30 seconds.
Use Captcha	Force user to enter captcha text before requesting PIN
Show Terms &	Force user to agree to the terms & conditions before they are

Conditions	allowed to submit login
Show before PIN request	Show Terms & Conditions before PIN request.
Terms & Conditions Text	This text will appear in the popup window when user view Terms & Conditions
Default Country	Select default country for requesting mobile number
PIN Template Message	SMS Message Template for Guest Login PIN. • use xPINx to replace PIN. • use xEXPIRYx to replace expiry time. • use xMONTHx to replace current Month. • use xDAYx to replace current Day. • use xHHx to replace current Hour. • use xMMx to replace current Minute. • use xSSx to replace current Second. Variables are case-sensitive. Default: Your PIN is xPINx. Expired in xEXPIRYx minutes. xHHx:xMMx:xSSx.
PIN Validity	PIN Validity in minutes. Default is 5 minutes.
Maximum PIN Request (Day)	Maximum PIN Request from the same mobile number for each day. Default is Unlimited. Mobile number will be blocked temporarily if the number of requests exceeded.
Maximum PIN Request (Week)	Maximum PIN Request from the same mobile number for each week. Default is Unlimited. Mobile number will be blocked temporarily if the number of requests exceeded.
Blacklist Message Template	Error message that will be prompted on login page when user requests PIN from the blacklisted mobile number.

Customize Portal login page



Header Text Guest Login

Custom Text in the login form. Please refer to the sample below.

Field 1

□ Required Field

User Name

Optional. Display Text for the first form field.
This field is for logging purpose only. Leave it blank if not required

Field Validation (Regular Expression) :

Regular Expression to validate input value. For example,
Email : ^[\w-\.]+@([\w-]+\.)+[\w-]{2,4}$
Alphanumeric, underscore and space : ^[\w\s]+$
Leave it blank to allow all formats.

Change the login form header text and upload images. Enable more fields if more user information is required for logging purpose.

2.7.2 Blacklisted Mobile

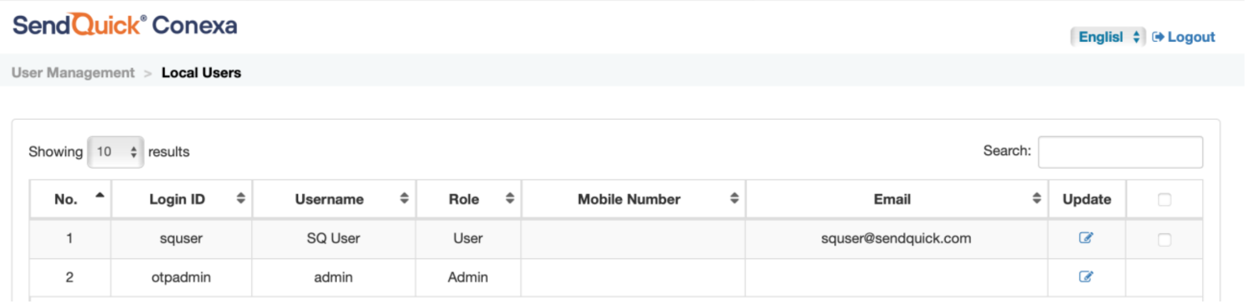
Admin can add mobile number into blacklist manually or from the logs. Blacklisted mobile numbers are not allowed to request OTP. Admin can delete the blacklist record to release the user from blacklist.

2.8 User Management

Local user list in SendQuick Conexa can be used as Authentication Server or Contact List in VPN, SAML SP or Auth API configuration, which can be configured to check user credential in local users and/or to send OTP to mobile or email in local user list.

2.8.1 All Users

Administrator to add/update/delete local users in SendQuick Conexa local database. Local users can be imported by CSV file.

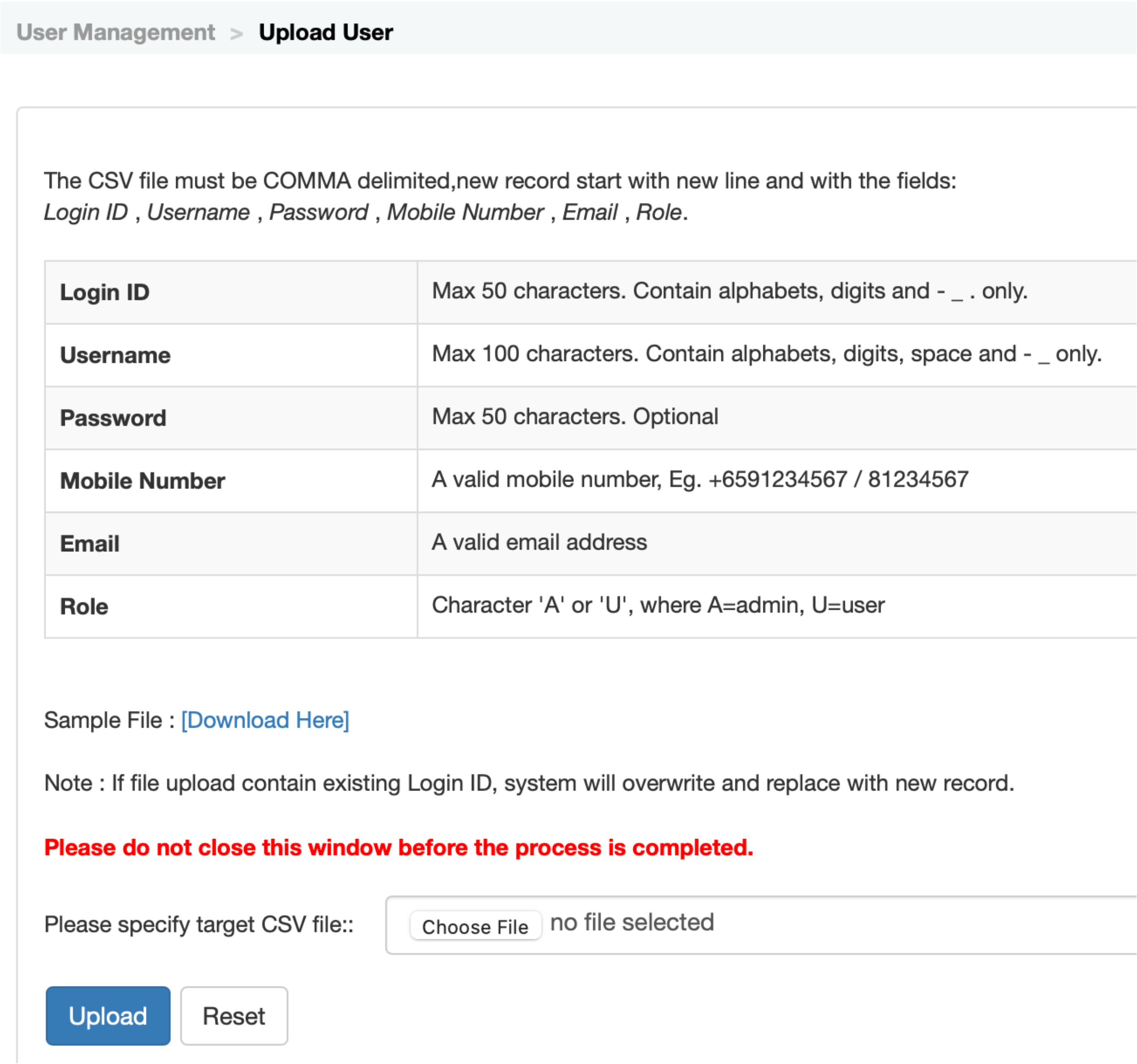


No.	Login ID	Username	Role	Mobile Number	Email	Update	□
1	squser	SQ User	User		squser@sendquick.com	✎	□
2	otpadmin	admin	Admin			✎	

Fields	Description
Login ID	Unique identifier of user. User’s login ID
Username	User’s name.
Password	User’s login password.
Mobile Number	User’s mobile number to receive SMS OTP
Email	User’s email address to receive Email OTP
Role	• User • Admin Default: User

2.8.2 Upload User

Administrator to upload local users in SendQuick Conexa local database.



User Management > **Upload User**

The CSV file must be COMMA delimited,new record start with new line and with the fields:
Login ID , Username , Password , Mobile Number , Email , Role.

Login ID	Max 50 characters. Contain alphabets, digits and - _ . only.
Username	Max 100 characters. Contain alphabets, digits, space and - _ only.
Password	Max 50 characters. Optional
Mobile Number	A valid mobile number, Eg. +6591234567 / 81234567
Email	A valid email address
Role	Character 'A' or 'U', where A=admin, U=user

Sample File : [Download Here]

Note : If file upload contain existing Login ID, system will overwrite and replace with new record.

Please do not close this window before the process is completed.

Please specify target CSV file::

1) Select CSV file by pressing “Choose File” button.

2) Press on “Upload” button to start import.

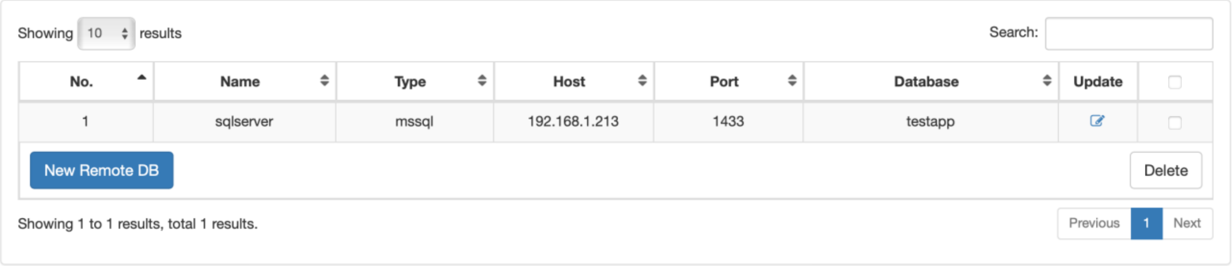
Note : If file upload contain existing Login ID, system will overwrite and replace with new record.

Sample CSV content:

```
user1,username1,password,91234567,user1@company.com,U

user2,username2,password,81234567,,U

admin1,adminname1,1234,+6598888888,admin1@company.com,A
```

2.8.3 Remote DB Configuration

Administrator to add remote database profile. These profiles can be selected from VPN, SAML SP and Auth API Configuration as an Authentication server or User Contact List.



No.	Name	Type	Host	Port	Database	Update	☐
1	sqlserver	mssql	192.168.1.213	1433	testapp	✎	☐

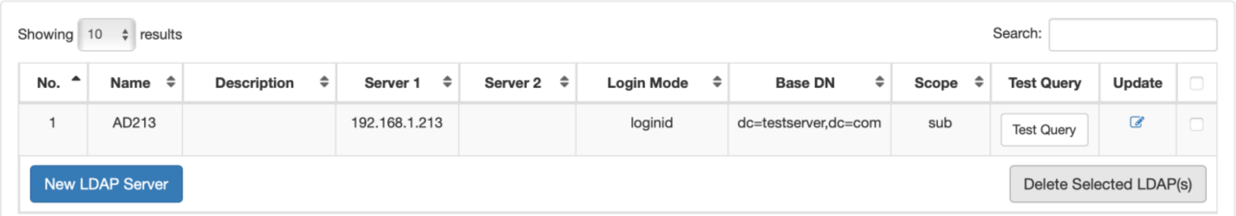
Showing 1 to 1 results, total 1 results.

<u>Create/Edit DB Configuration</u>

Fields	Description
Unique name for DB	Unique name to identify remote database
Description	Short description for this database
Database Type	• ORACLE • Postgres SQL • MSSQL • MYSQL
Database Host	Valid IP address / Host of remote database server
Port	Database port number. Default port number for each database: • Oracle: 1521 • Postgres SQL: 5432 • MSSQL: 1433 • MYSQL: 3306
Login name	Username to access database
Login password	Password to access database
Database Name	Remote database name

2.8.4 LDAP Configuration

Administrator to add LDAP server profile. These profiles can be selected from VPN, SAML SP and Auth API Configuration as an Authentication server or User Contact List. Admin can also download soft token users from LDAP server profile.



Showing 10 results Search:

No.	Name	Description	Server 1	Server 2	Login Mode	Base DN	Scope	Test Query	Update	□
1	AD213		192.168.1.213		loginid	dc=testserver,dc=com	sub	Test Query	✎	□

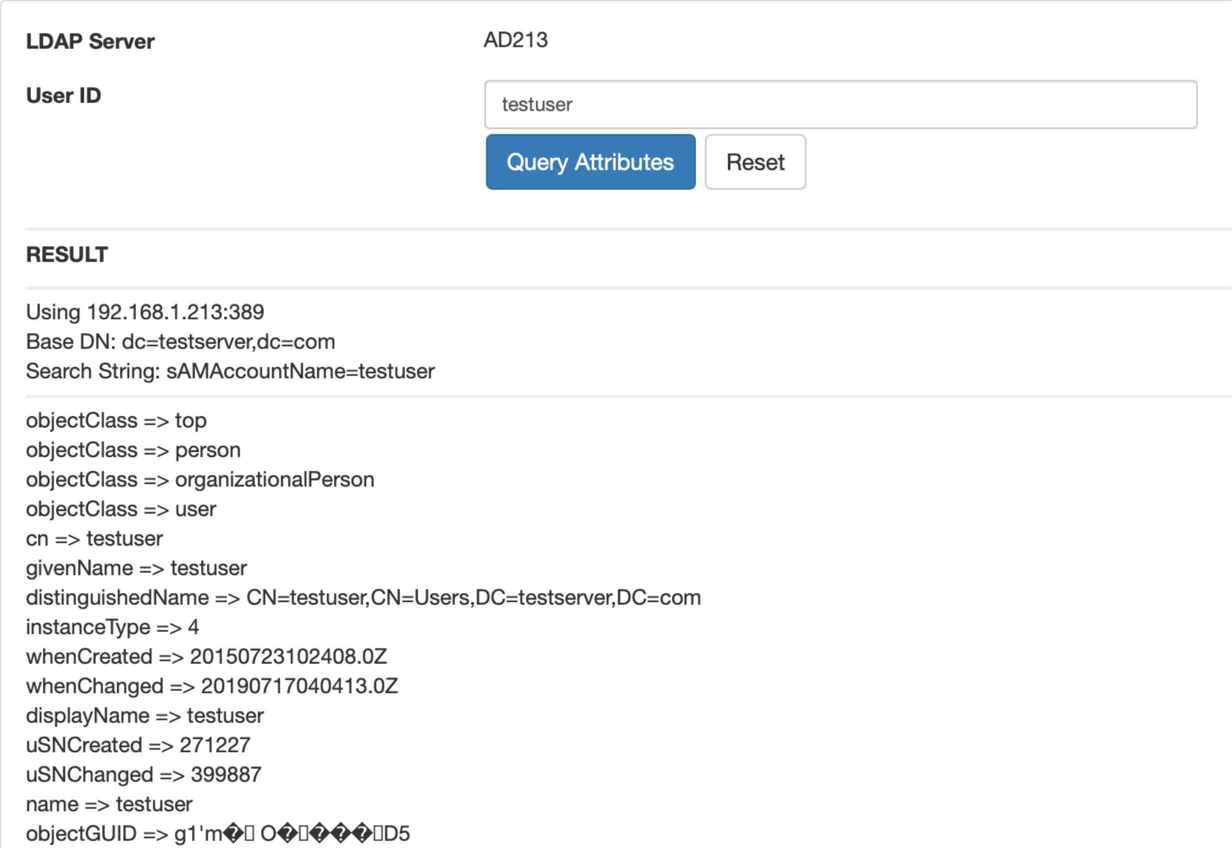
New LDAP Server Delete Selected LDAP(s)

Create/Edit LDAP Configuration

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Name</td><td>Unique name to identify LDAP</td></tr>
<tr><td>Description</td><td>Short description</td></tr>
<tr><td>Server 1 , Port and Timeout</td><td>First LDAP server IP, port and timeout(s). Default LDAP port: 389. Use ldaps://IP if using secure LDAP</td></tr>
<tr><td>Server 2 , Port and Timeout</td><td>Second LDAP server IP, port number and timeout(s) Default LDAP port: 389. Use ldaps://IP if using secure LDAP</td></tr>
<tr><td>Type</td><td><ul><li>Active Directory</li><li>LDAP</li></ul></td></tr>
<tr><td>Service Account Bind DN</td><td>Valid LDAP username which will be used to bind and search</td></tr>
<tr><td>Service Account Password</td><td>Valid LDAP password which will be used to bind and search</td></tr>
<tr><td>Login Mode</td><td>Type of Login ID, check against the following attributes in LDAP server.
<table>
<tr><th>Login Mode</th><th>Active Directory Attributes</th><th>LDAP Attributes</th></tr>
<tr><td><b>Display Name</b></td><td>displayName</td><td>displayName</td></tr>
<tr><td><b>Login ID</b></td><td>sAMAccountName</td><td>uid</td></tr>
<tr><td><b>Email</b></td><td>mail</td><td>mail</td></tr>
</table></td></tr>
<tr><td>Base DN</td><td>Base DN of the location of user list</td></tr>
<tr><td>Search Scope</td><td><ul><li>Sub : Search the whole tree below and including the base object.</li><li>Base : Search only the base object.</li><li>One : Search the entries immediately below the base object.</li></ul></td></tr>
<tr><td>Additional LDAP Filter String</td><td>Default is empty. For example, to allow all users in VPNusers group, (memberOf=CN=VPNusers,CN=Users,DC=testserver,DC=com)</td></tr>
</table>

Test LDAP Query

From the LDAP server profile list, click on “Test Query” button. Enter User ID and click “Query Attributes”. All user attributes will be shown if the user is found in LDAP server. If there is no result, make sure your LDAP server configuration is correct and the User ID is valid.



LDAP Server AD213

User ID testuser

RESULT

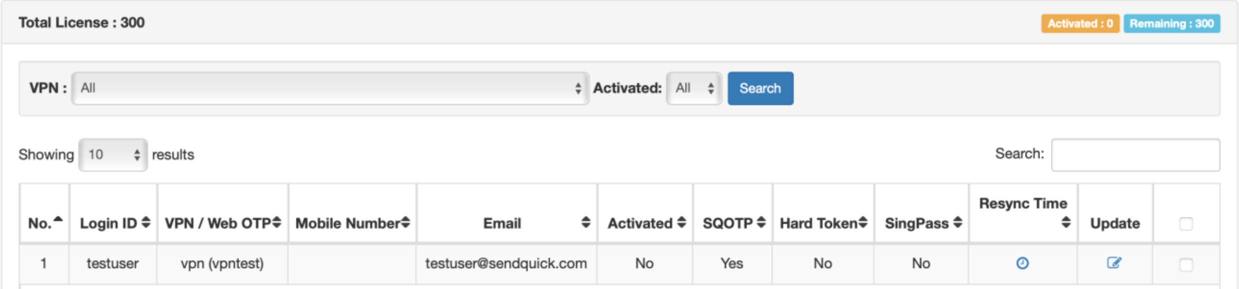
```
Using 192.168.1.213:389
Base DN: dc=testserver,dc=com
Search String: sAMAccountName=testuser

objectClass => top
objectClass => person
objectClass => organizationalPerson
objectClass => user
cn => testuser
givenName => testuser
distinguishedName => CN=testuser,CN=Users,DC=testserver,DC=com
instanceType => 4
whenCreated => 20150723102408.0Z
whenChanged => 20190717040413.0Z
displayName => testuser
uSNCreated => 271227
uSNChanged => 399887
name => testuser
objectGUID => g1'm�▯ O�▯���▯D5
```

2.9 Soft Token Management

Each SendQuick Conexa has a default number of soft token user license. Activated soft token user profile will utilise one license. The license is required for using soft token, push OTP, push Auth, hard token and digital ID like Singpass.

2.9.1 Soft Token Users

Admin can create soft token user manually, by file upload or download or synchronized from LDAP or active directory server.



Total License : 300

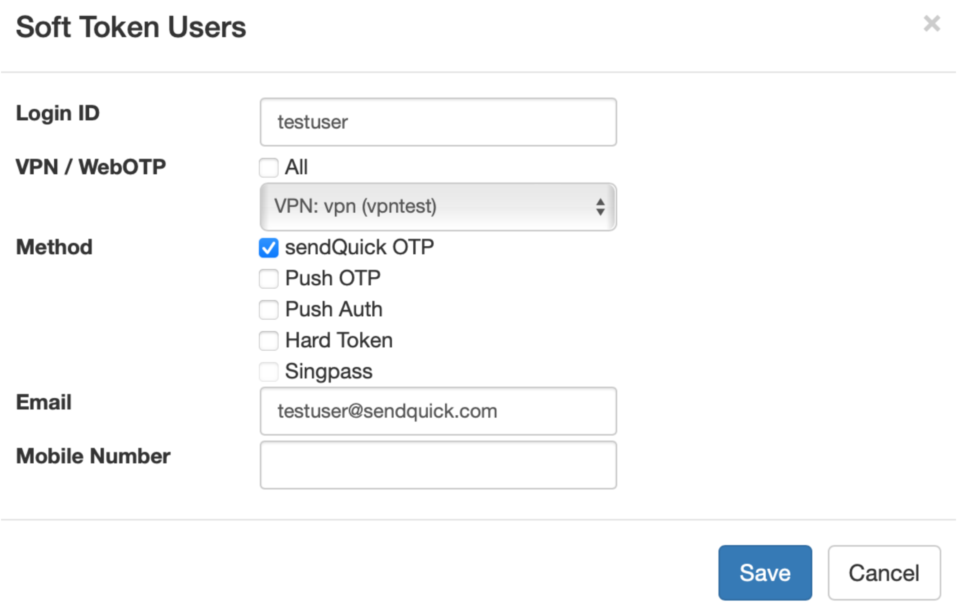
VPN : All Activated: All

Showing 10 results

Search:

No.	Login ID	VPN / Web OTP	Mobile Number	Email	Activated	SQOTP	Hard Token	SingPass	Resync Time	Update	□
1	testuser	vpn (vpntest)		testuser@sendquick.com	No	Yes	No	No	⊙	✎	□

Add Soft Token Users - Manually



Soft Token Users

Login ID: testuser

VPN / WebOTP: □ All

VPN: vpn (vpntest)

Method:
- ☑ sendQuick OTP
- □ Push OTP
- □ Push Auth
- □ Hard Token
- □ Singpass

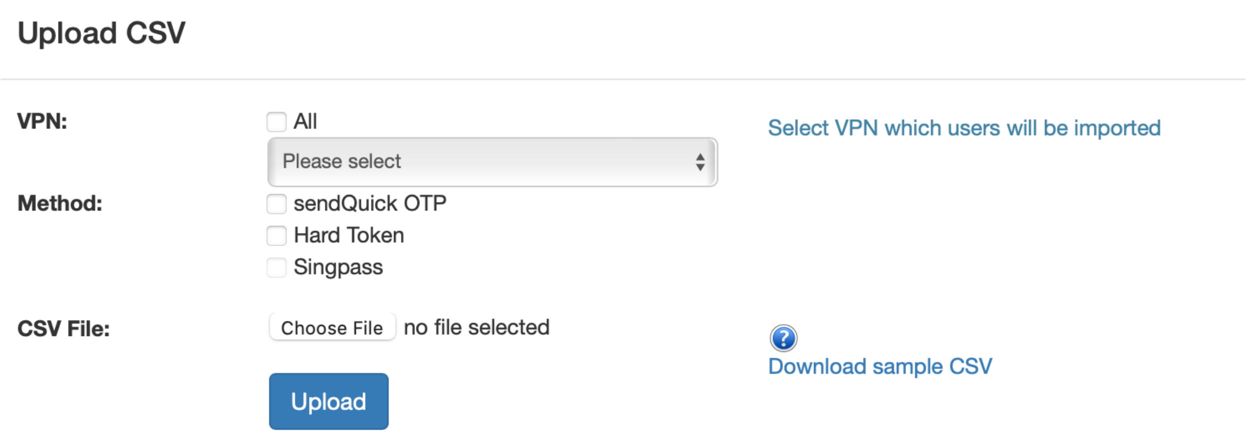
Email: testuser@sendquick.com

Mobile Number:

Field	Description
Login ID	VPN login id
VPN / WebOTP	Choose single profile to access from dropdown list. Check on “All” checkbox to allow this soft token to be used for all VPN, WebOTP, SAML OTP and Auth API profiles.
Method	• SendQuick OTP (Soft Token) • Push OTP • Push Auth • Hard Token • Singpass
Email	SendQuick Conexa will send Soft Token activation email to this email.
Mobile Number	SendQuick Conexa will send Soft Token activation SMS reminder to this mobile number.

Upload Users by CSV

Click on “Upload User” > “By CSV” button to start.



Upload CSV

VPN: □ All
Please select

Method: □ sendQuick OTP
□ Hard Token
□ Singpass

CSV File: Choose File no file selected

Select VPN which users will be imported

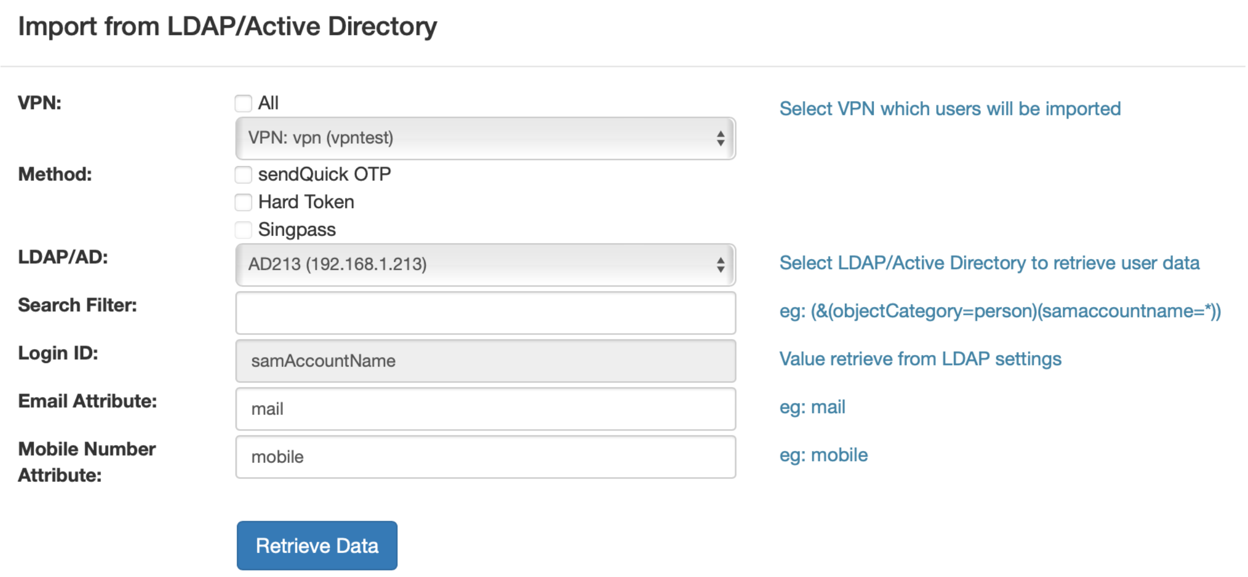
Download sample CSV

Select All or single VPN/WebOTP/SAML/Auth API profile which users will be imported and choose CSV file to upload by clicking on “Choose File”. Click on “Download sample CSV” link to view CSV file format. Click “Upload” button to upload.

Once upload is done, system will display a list of users ready to be imported. Confirm accuracy of data and click “Import” button to import.

Upload Users by LDAP/Active Directory

Click on “Upload User” > “By LDAP/Active Directory” button to start.



Import from LDAP/Active Directory

VPN: □ All
VPN: vpn (vpntest)

Method: □ sendQuick OTP
□ Hard Token
□ Singpass

LDAP/AD: AD213 (192.168.1.213)

Search Filter:

Login ID: samAccountName

Email Attribute: mail

Mobile Number Attribute: mobile

Select VPN which users will be imported

Select LDAP/Active Directory to retrieve user data

eg: (&(objectCategory=person)(samaccountname=*))

Value retrieve from LDAP settings

eg: mail

eg: mobile

Fill up all fields and click on “Retrieve Data” to pull users data from selected LDAP or Active Directory profile.

Field	Description
VPN	Choose single profile to access from dropdown list. Check on "All" checkbox to allow this soft token to be used for all VPN, WebOTP, SAML OTP and Auth API profiles.
Method	• SendQuick OTP (Soft Token) • Hard Token • Singpass
LDAP/AD	Choose which LDAP/AD server to retrieve users data
Search Filter	LDAP filter string
LoginID	Login ID will be populated automatically based on selected LDAP settings.
Email Attribute	Email field in in LDAP. Soft Token activation email will be sent to this email.
Mobile Attribute	Mobile number field in LDAP. SendQuick Conexa will send Soft Token activation SMS reminder to this mobile number.

If the LDAP/Active Directory data retrieval is succeeded, a preview of users that ready to import will be displayed. Verify accuracy of users' data and click on "Import" button to import all users.

If existing user found during the import process, new user data will overwrite existing data.

Activate Soft Token Users

Select user to activate by ticking checkbox and click on "Actions" > "Activate" button. A NEW secret key and QR code will be generated and delivered to user's email address. User has to follow instruction in the email to activate and use soft token.

Deactivate Soft Token Users

Select user to deactivate by ticking checkbox and click on "Actions" > "Deactivate" button. A disabled soft token user account will be denied from VPN access.

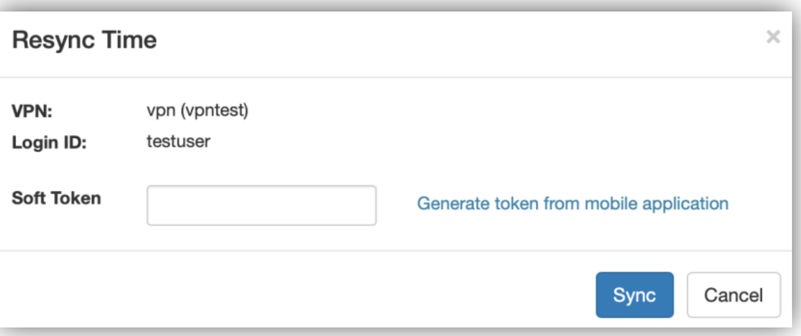
Reset Soft Token User's Secret Key

Select user to reset secret key by ticking checkbox and click on "Actions" > "Reset Secret Key" button. NEW secret key and QR code will be delivered to user's email. User has to rescan new QR Code to gain access to VPN.

Resynchronize Soft Token User’s Time

If user’s mobile phone clock is different from SendQuick Conexa server, user may not be able to login with soft token. Soft token is time sensitive. To mitigate such problem, user’s time offset must be recorded by performing this step.

Select user to synchronize by clicking on clock icon. System will display a popup window, enter soft token generated from mobile application and click on “Sync” button to synchronize.

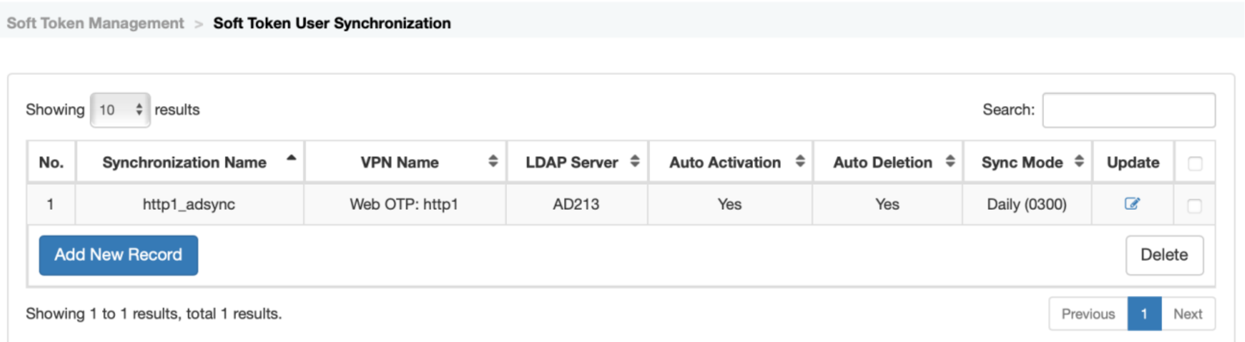


Resync Time

VPN: vpn (vpntest)
Login ID: testuser
Soft Token

2.9.2 Soft Token User Synchronization

Admin can create rules to synchronize soft token users with LDAP/AD server.



Soft Token Management > Soft Token User Synchronization

Showing 10 results Search:

No.	Synchronization Name	VPN Name	LDAP Server	Auto Activation	Auto Deletion	Sync Mode	Update	□
1	http1_adsync	Web OTP: http1	AD213	Yes	Yes	Daily (0300)	✎	□

Showing 1 to 1 results, total 1 results.

Field	Description
Synchronization Name	Short name for this synchronization profile.
VPN	Choose All or single VPN/WebOTP/SAML/Auth API profile to be synchronized.
Method	• SendQuick OTP (Soft Token) • Push OTP • Push Auth • Hard Token • Singpass
LDAP/AD	Choose which LDAP/AD server to retrieve user data

Search Filter	LDAP filter string
Email Attribute	Email field in in LDAP
Mobile Number Attribute	Mobile number field in LDAP
Auto Activation	If checked, all new users in LDAP/AD will be added and auto activated if not exceeding Soft Token license limit..
Auto Deletion	If checked, all deleted users in AD will be deleted from Soft Token user list. If not checked, all deleted users will be deactivated in Soft Token user list.
Sync Mode	Disable or perform daily synchronization.
Time (HHMM)	Daily synchronization time.

2.9.3 Soft Token Activation Templates

There are two types of activation templates, Soft Token and Singapss. If both methods are activated for a soft token user, user will receive two emails. Soft token email will contain a QR code, which should be scanned by user's mobile app. Singpass activation email will contain a SendQuick Conexa VPN User portal link. User needs to login with a valid account credential before they can register their Singpass account with SendQuick Conexa.

SMS Template is optional. Leave it empty if you do not want to send SMS notification after soft token activated.

Available Keywords to be used in Email Template:

Field	Description
-QRCODE-	Display QR Code to allow users scan and generate soft token.
-SECRETKEY-	Users will use this secret key to resync time offset between server and mobile phone.
-LOGINID-	User's VPN Login ID
-VPNNAME-	VPN Name
-SPLINK-	VPN User login link

* Keywords will be replaced by actual user data during email delivery.

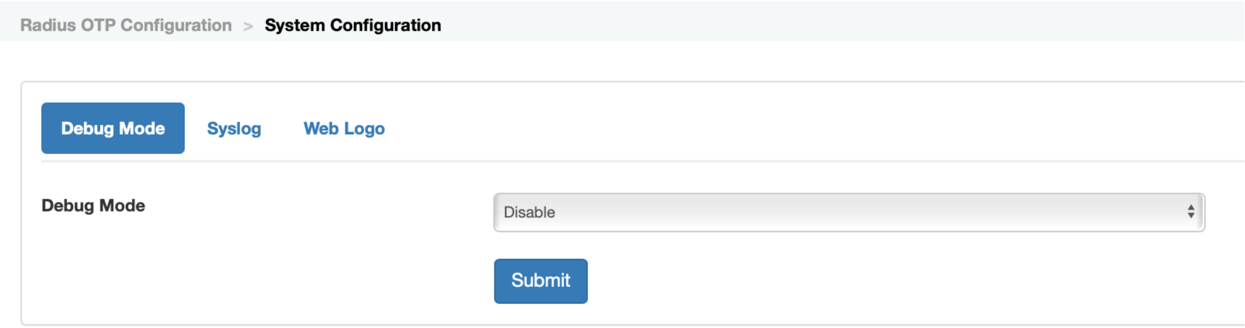
2.9.4 Soft Token Configuration

Field	Description
Soft Token Name	Soft Token profile name to be displayed on Soft Token mobile application after user scan QR code from activation email. Default: xSERVERNAMEx is the VPN/WebOTP/SAML/Auth API profile name.
Soft Token Description	Profile description in Soft Token mobile application. Default: xLOGINIDx-xSERVERNAMEx-xCDATExxCTIMEx Variables: • xLOGINIDx : User's login ID • xSERVERNAMEx : VPN or WebOTP client name • xCDATEx : Created Date (YYYYMMDD) • xCTIMEx : Created Time (HHMMSS)
Valid Soft Token Window	Default is 2 minutes. Set this to higher value will allow more valid soft token.
Require Secret Key	Require user to enter secret key when doing self-synchronizing soft token time via VPN User login portal.
Secure QR Code	Default : Disable Secure QR code is to enhance security of the QR code sent to user's email. This feature only compatible with SendQuick mobile application and public domain/IP is required. Once user scanned the secure QR code, SendQuick app will access to public URL hosted in SendQuick Conexa to verify and retrieve user details, so the SendQuick app can create new soft token profile for that user. Enable this option if need to use Push Auth or Push OTP to SendQuick app.
Push Server URL	SendQuick Push Server URL.
Push ID & Key	ID and Key used to push notification to SendQuick Push Server
Allow Multiple Scan	For Secure QR Code and SendQuick app only. If not allowed, the QR code can be scanned once only and subsequent scan will fail. Default is Yes.
Singpass URL	Singpass URL for production or staging.
Singpass Client ID	The default Singpass Client ID. This will be used for Singpass registration and login for soft token users with the All VPN

	profile or any profile that doesn’t have the client ID configured.
Singpass Redirect URI	Singpass will redirect user to these URIs upon successful authorization for user registration and user login. These URIs need to be submitted to Singpass when onboarding.
JWKS Endpoint URL	JWKS URL for Singpass to acquire SendQuick Conexa's public keys during authentication process and need to be submitted to Singpass when onboarding.
Singpass Login Error Message	Error message when non-registered user login with Singpass.

2.10 System Configuration

Administrator to enable/disable debug mode in this section. A detailed diagnostic file will be created for troubleshooting purposes once debug mode is enabled.



Debug Mode: Disable

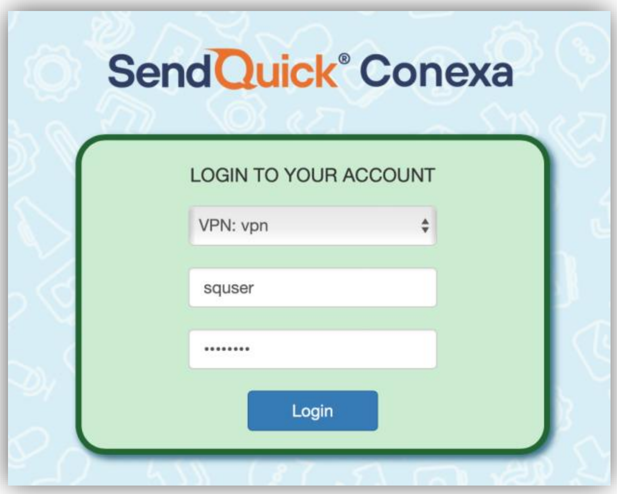
Field	Description
Debug Mode	For troubleshooting purpose, enable debug mode and make some VPN authentication. After that, create diagnostic file at system admin page (System Configuration) and send to sendQuick for troubleshooting. Only enable this when required as this will create logs. Disable debug mode will clear all debug logs.
Syslog	SendQuick Conexa will send authentication logs to this Syslog server.
Web Logo	Upload logo to be shown on SendQuick Conexa portal.

2.11 VPN User Login

VPN users can login to SendQuick Conexa after receiving activation email to synchronize mobile clock. Soft token users only have to perform this step if their mobile phone time and SendQuick Conexa server time are different by 1 minute or more. Time synchronization can be

1. Visit http[s]://[Conexa IP]/otp/ and click on “VPN User Login”:

2. Login with pre-configured authentication type in VPN configuration (Local user, LDAP or Remote DB)



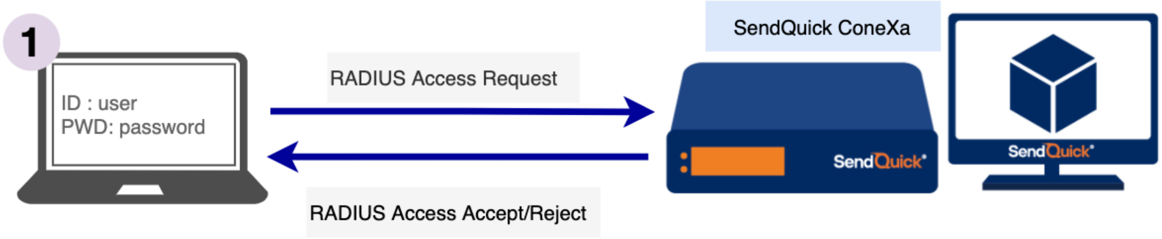
3. After login, user will see one or more of the following menu:

- Resync Time
  - Enter secret key from soft token activation email if prompted
  - Enter Soft Token from your mobile app
  - Submit and resync time
- Update Contact
  - If this is allowed in VPN configuration, user may update their mobile number and email to User contact list server, which could be Local User, LDAP/AD or Remote DB
- Singpass
  - For SAML profile, user can sign in with Singpass and authorize login to SendQuick Conexa. Once completed, users may use Singpass to login to SAML SP.

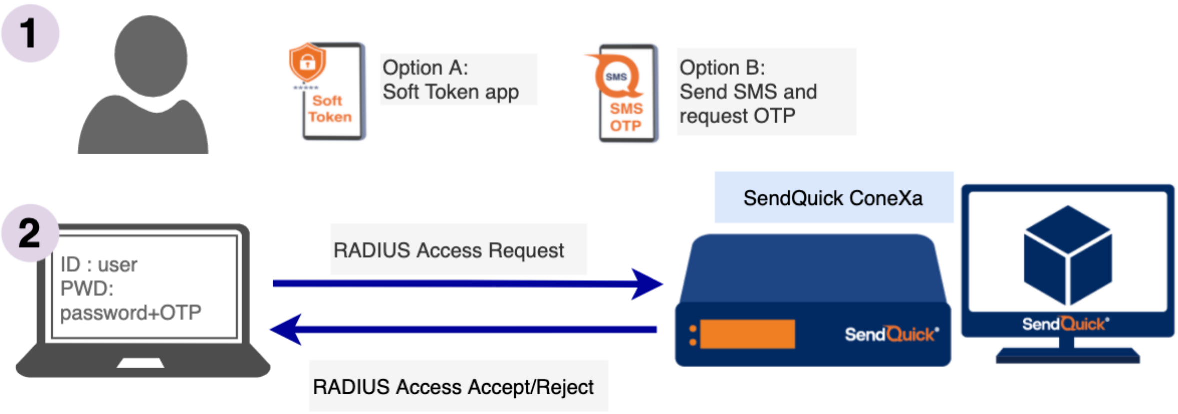
3.0 REFERENCES

3.1 RADIUS Authentication Types

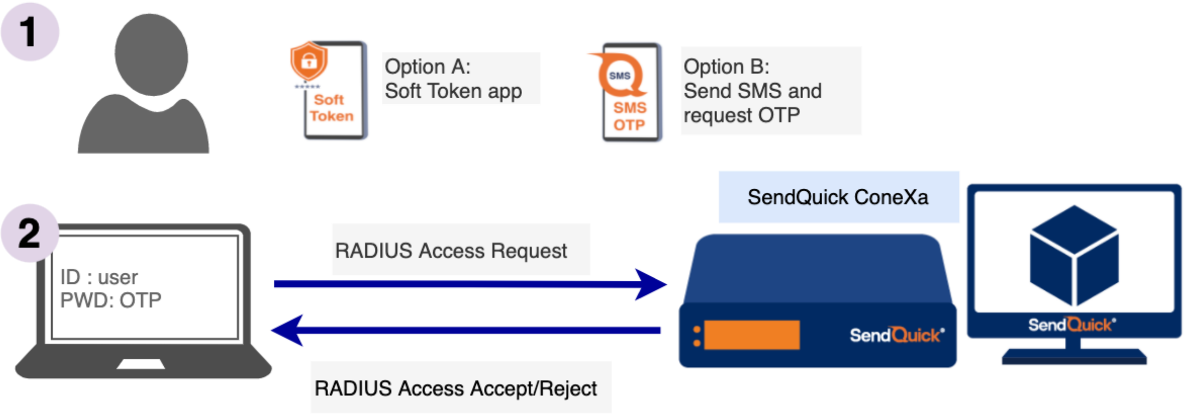
Radius Authentication - One Factor



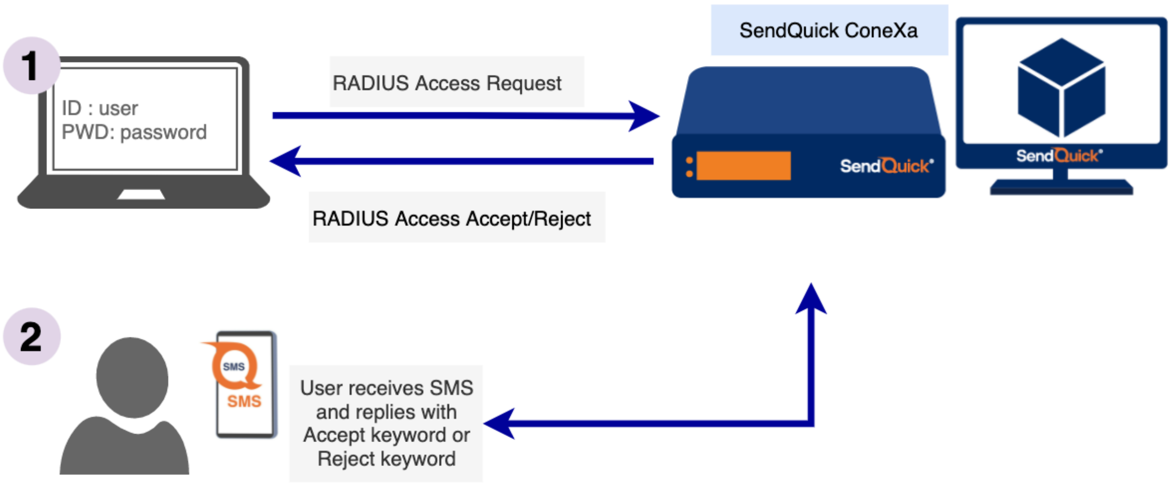
Radius Authentication - Two Factor Static (Password + OTP)



Radius Authentication - Two Factor Static (OTP)

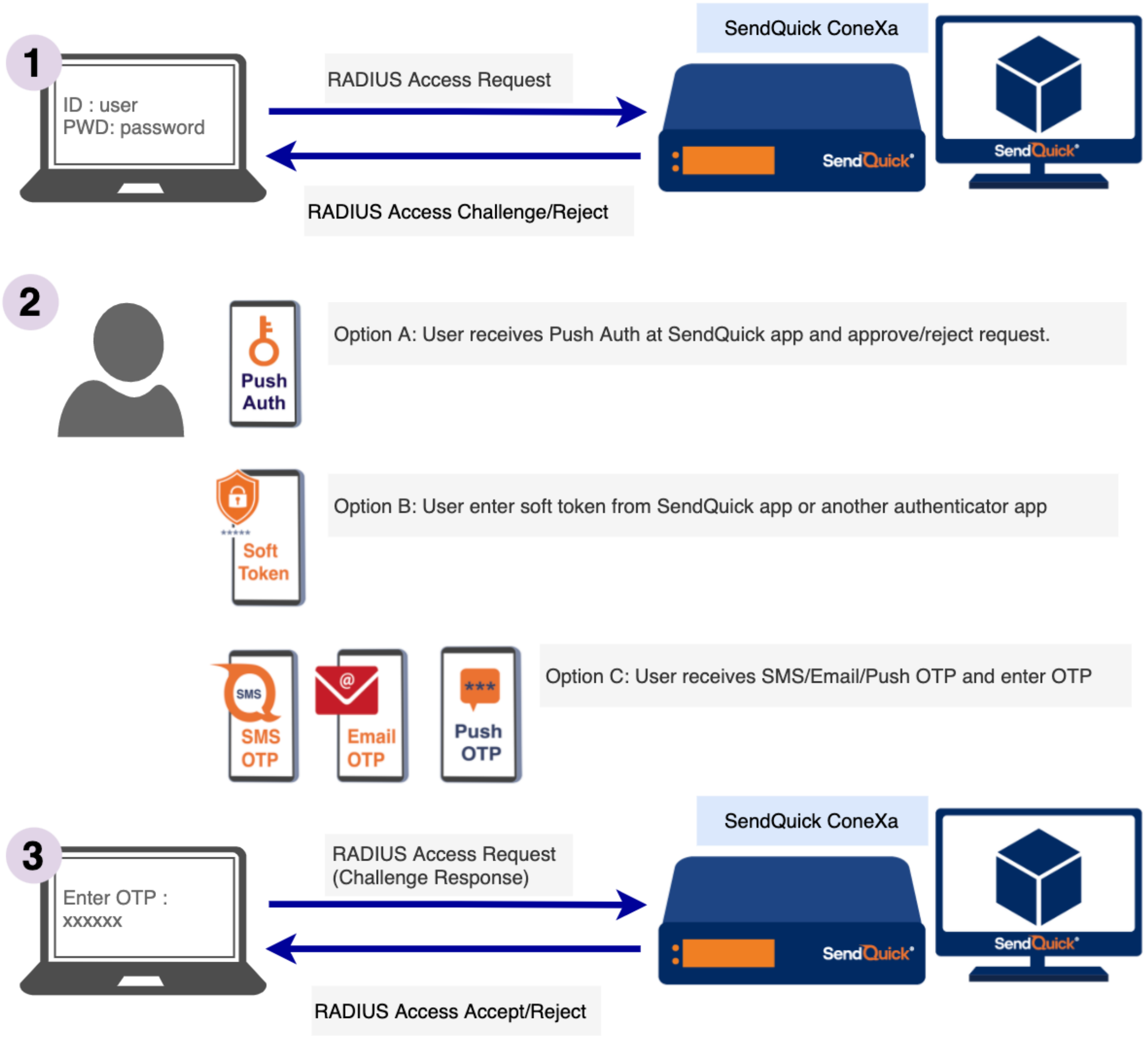


Radius Authentication - Two Factor Static (SMS Reply)



User receives SMS and replies with Accept keyword or Reject keyword

Radius Authentication - Two Factor Access Challenge

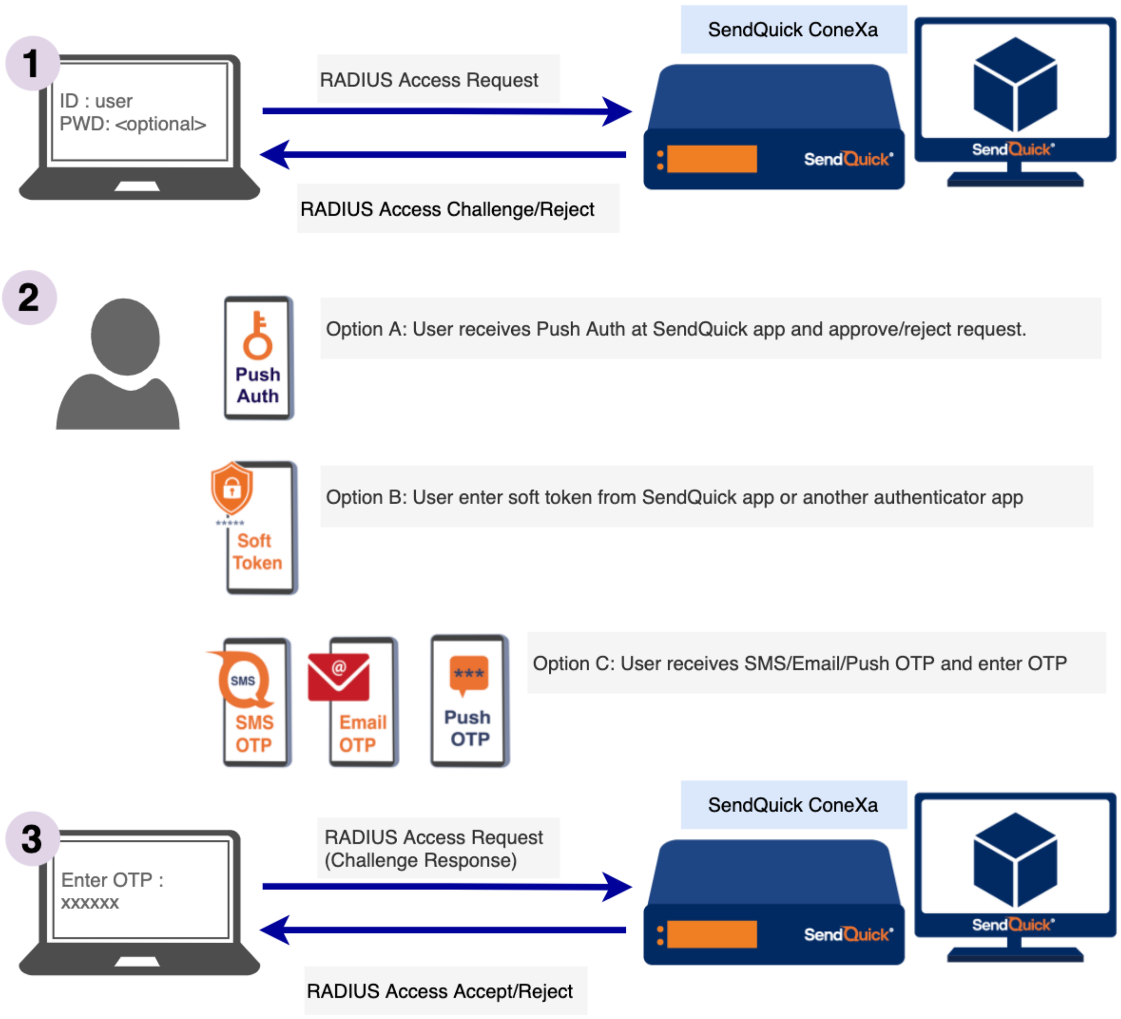


Option A: User receives Push Auth at SendQuick app and approve/reject request.

Option B: User enter soft token from SendQuick app or another authenticator app

Option C: User receives SMS/Email/Push OTP and enter OTP

Radius Authentication - Two Factor Access Challenge (Username Only)



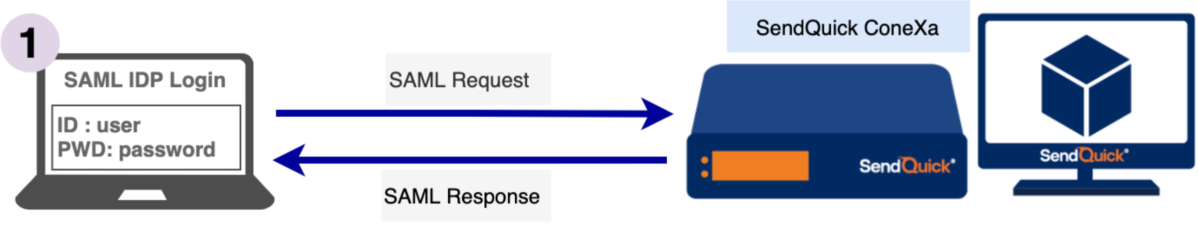
Option A: User receives Push Auth at SendQuick app and approve/reject request.

Option B: User enter soft token from SendQuick app or another authenticator app

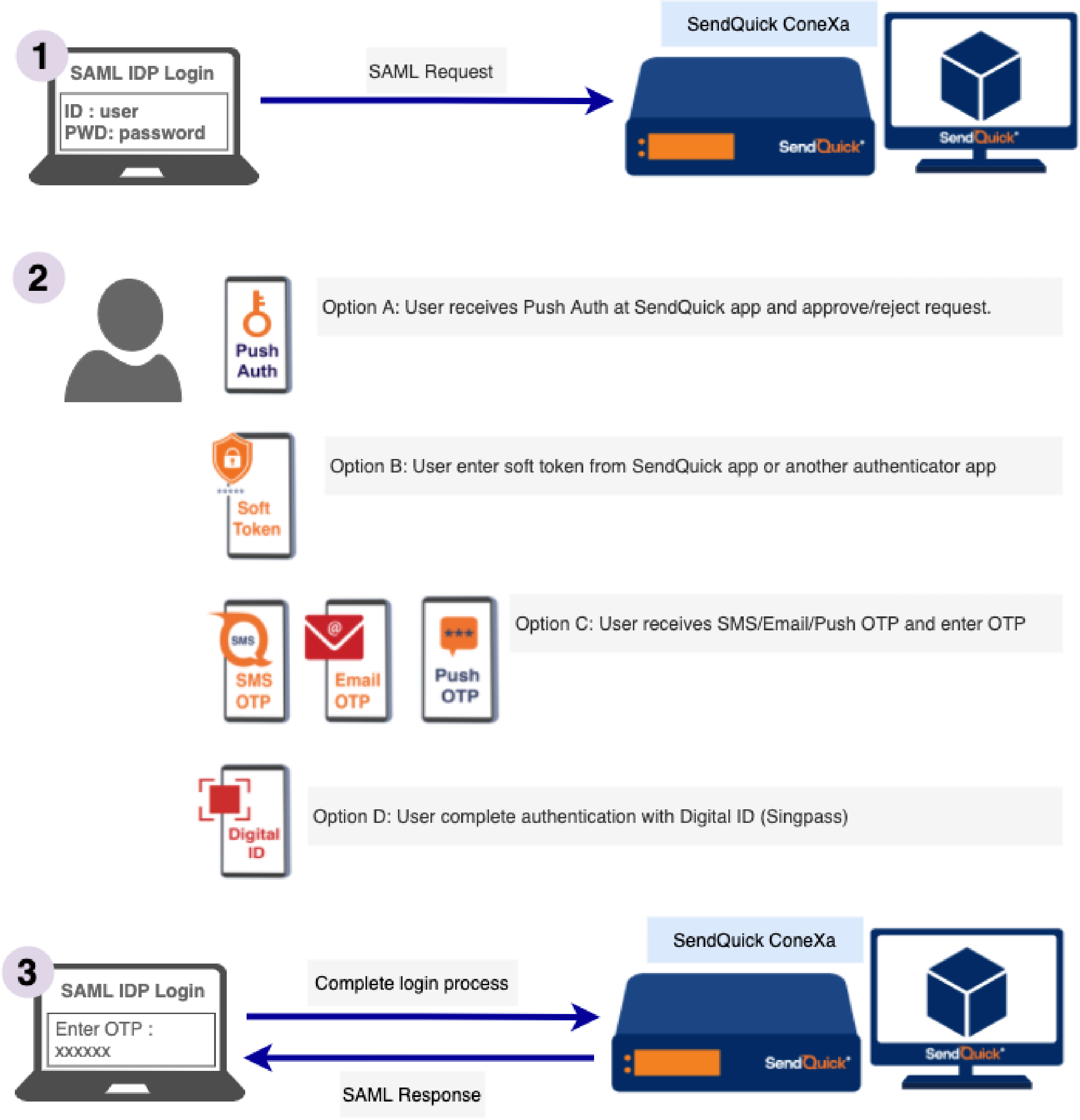
Option C: User receives SMS/Email/Push OTP and enter OTP

3.2 SAML Authentication Types

SAML Authentication - One Factor



SAML Authentication - Two Factor Access Challenge

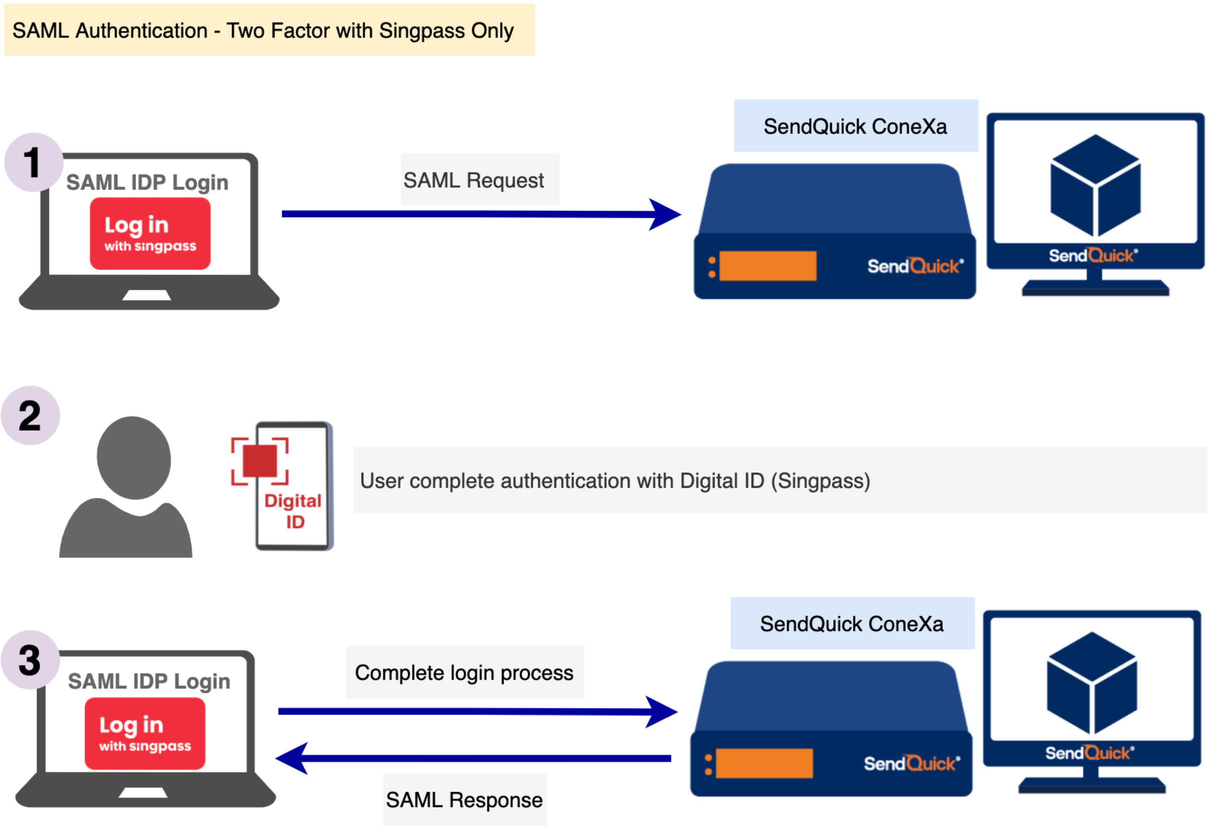


Option A: User receives Push Auth at SendQuick app and approve/reject request.

Option B: User enter soft token from SendQuick app or another authenticator app

Option C: User receives SMS/Email/Push OTP and enter OTP

Option D: User complete authentication with Digital ID (Singpass)



3.3 OTP On Demand SMS template

For 2FA Static (Password + OTP) and 2FA Static (OTP) authentication type, user can send SMS to SendQuick Conexa to trigger OTP before user can use that OTP to login. OTP keyword can be configured under VPN Configuration.

For contact list : Local user, LDAP, Remote DB

<otp_on_demand_keyword>

E.g. SMS Message : otp

For contact list : Multiple LDAP

<otp_on_demand_keyword> <ldap_server_name>

E.g. SMS Message: otp ad1

3.4 Soft Token Mobile Application

We recommend users to download SendQuick app from App Store or Play Store.

SendQuick
SendQuick

iOS version:

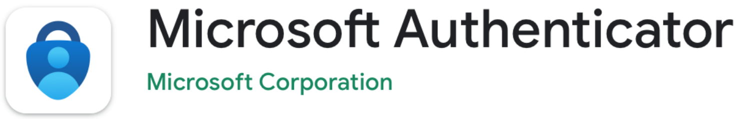
https://apps.apple.com/us/app/sendquick/id1645225958

Android version:

https://play.google.com/store/apps/details?id=com.talariax.sendquickapp

Other mobile applications compatible with SendQuick Conexa soft token:

Google Authenticator
Google LLC



Microsoft Authenticator
Microsoft Corporation