



**sendQuick® ConeXa**

---

**SendQuick ConeXa  
Licensing Agreement and  
User Manual  
Version 2.0**

---

*Prepared by*

**TalariaX Pte Ltd**

76 Playfair Road  
#08-01 LHK2  
Singapore 367996

Tel: +65 62802881  
Fax: +65 62806882

E-mail: [info@talariax.com](mailto:info@talariax.com)  
Web: [www.talariax.com](http://www.talariax.com)

# SendQuick Conexa Software License Agreement

For SOFTWARE PRODUCT, content and software information marked with © TalariaX or © TalariaX Pte Ltd the following license agreement applies to you:

This is a legal agreement between you, the end user or User Corporation, and TalariaX Pte Ltd, Singapore. By purchasing and starting (power-up) the Server with the sendQuick software (SOFTWARE PRODUCT) installed in the Server, you agreed to be bound by the terms of this agreement. If you do not agree to the terms of this agreement, promptly stop the start-up process by shutting down the system and return the product package to the place you obtained it for a full refund (subject to relevant terms and conditions for refund) provided the product package is in its original condition.

## 1. Grant of license

TalariaX Pte Ltd grants you the right to use one copy of the enclosed SOFTWARE PRODUCT - the SOFTWARE - on a single Server that it is being installed in by TalariaX. The SOFTWARE is in use on a computer when it is loaded into memory or installed into permanent memory of that computer. This license is attached with the hardware (Server) that was originally installed by TalariaX.

This license does not permit or allow or warrant any rights to redistribute, duplicate, compile, reverse compile or any acts that will remove or seek to remove the SOFTWARE from the original server that it was installed in. The effort for the above stated actions include both software or hardware related including but not exclusive to hard disk duplication, network transfer, network duplicate or any acts that may cause the removal of the SOFTWARE from the original storage position. Any of such acts stated herein shall amount to a breach of the copyright and this licensing agreement and is punishable by the Court of Law in Singapore and your respective countries. Duplication, copying or whatsoever acts or intent pertaining to remove the SOFTWARE from this server is strictly prohibited.

## 2. Additional grant of license

In addition to the rights granted in Section 1, TalariaX Pte Ltd grants you a nonexclusive right to use the SOFTWARE in the Server by an unlimited number of users or application servers to send messages to an unlimited number of recipients.

## 3. Copyright

This software is owned by TalariaX Pte Ltd or its suppliers and is protected by Singapore and international copyright laws and treaties. Therefore you must treat the SOFTWARE like any other copyrighted material. Except that if the SOFTWARE is not copy protected you may either make one copy of the SOFTWARE solely for backup purpose or transfer the SOFTWARE to a single hard disk provided that you keep the original for backup or archive purposes. You may not copy the product manuals or any written material accompanying the SOFTWARE.

Some of the components that support the SOFTWARE are owned by independent owners and developers. The copyrights of these components are owned by their respective owners and developers and TalariaX does not claim to own or develop these components.

Some of the components distributed with this SOFTWARE are owned by independent owners and developers, and the respective licenses contained in the package which distributes this SOFTWARE (e.g. GNU General Public Licenses, Apache Licenses) apply to such components. TalariaX Pte Ltd does not claim to own or develop any of the copyright or any other rights in the components distributed with the SOFTWARE which have copyright notices other than “© TalariaX” or “© TalariaX Pte Ltd”.

- For programs under the GNU General Public License: The programs are free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version. The programs are distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with the programs. If not, see <http://www.gnu.org/licenses/>.
- For programs under the Apache License, Version 2.0: you may not use those files except in compliance with the Apache License, Version 2.0. You may obtain a copy of the License at <http://www.apache.org/licenses/LICENSE-2.0>. Unless required by applicable law or agreed to in writing, software distributed under the Apache License, Version 2.0 is distributed on an “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the Apache License, Version 2.0 for the specific language governing permissions and limitations under the license.

The receiver of this SOFTWARE is expected to abide by the terms and conditions of all of the licenses contained in this package.

TalariaX Pte Ltd disclaims all liability for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, infringement of local regulation, or other pecuniary loss) arising out of the use of or inability to use this SOFTWARE product and/or the components distributed with this SOFTWARE product, even if TalariaX Pte Ltd has been advised of the possibility of such damages, to the maximum extent permitted by law.

#### **4. Other restrictions**

You may not rent or lease the SOFTWARE, but you may transfer your rights under this license agreement on a permanent basis if you transfer all copies of the SOFTWARE with the server hardware and all written material, and if the recipient agrees to the terms of this agreement.

You may not reverse engineer, de-compile or disassemble the SOFTWARE and any such acts and intent is considered a violation of copyright law in Singapore and your respective countries.

#### **Limited warranty**

TalariaX Pte Ltd warrants that the SOFTWARE will perform substantially in accordance with the accompanying product manual(s) or the online manual for a period of 365 days from the purchase date. This limited warranty period also applies to the hardware and the GSM modem. TalariaX reserves the right to amend the limited warranty period without prior notice.

#### **Customer remedies**

TalariaX Pte Ltd entire liability and your exclusive remedy shall be, at TalariaX Pte Ltd's option, either

- a return of the price paid or
- repair or replacement of the SOFTWARE that does not meet the limited warranty and which is returned with a copy of your receipt

The limited warranty is void if failure of the SOFTWARE has resulted from accident, abuse or misapplication by the user/licensee. Any replacement SOFTWARE will be warranted for the remainder of the original warranty period but at least for 30 days.

#### **No other warranties**

To the maximum extent permitted by applicable law, TalariaX Pte Ltd disclaims all other warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to the SOFTWARE, hardware, the accompanying product manual(s) and written materials. The limited warranty contained herein gives you specific legal rights.

#### **No liability for consequential damage**

To the maximum extent permitted by applicable law, TalariaX Pte Ltd and its suppliers shall not be liable for any other damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, infringement of local regulation, or other pecuniary loss) arising out of the use of or inability to use this SOFTWARE PRODUCT, even if TalariaX Pte Ltd has been advised of the possibility of such damages. In any case, TalariaX Pte Ltd's entire liability under any provisions of this agreement shall be limited to the amount actually paid by you for this SOFTWARE.

TalariaX cannot guarantee that messages sent by using TalariaX's SOFTWARE PRODUCTS for wireless (SMS) messaging reach their addressees. Neither can TalariaX guarantee that the SOFTWARE PRODUCT receives all messages through the used mobile equipment they have been sent to.

TalariaX is not liable for any consequential damages arising from the fact that messages tried to send by sendQuick Server products do not reach their target addressees (mobile phones, pagers) or that messages sent to the mobile equipment used with the SOFTWARE PRODUCT will be recognized and read by the SOFTWARE PRODUCT.

#### **For any clarifications, please contact:**

##### **TalariaX Pte Ltd**

76 Playfair Road

#08-01 LHK2

Singapore 367996

Tel: 65 – 62802881

Fax: 65 – 62806882

E-mail: [info@talariax.com](mailto:info@talariax.com)

Web: [www.talariax.com](http://www.talariax.com)

# sendQuick Conexa

## User Manual 2.0

### Table of Contents

1.0 INTRODUCTION.....	5
2.0 SET-UP AND CONFIGURATION.....	5
2.1 Set-up steps.....	5
2.2 Login Procedures.....	6
2.1.1 Login Types.....	6
2.2 Dashboard.....	7
2.3 Logs.....	8
2.3.1 Server Log.....	8
2.3.2 Authentication Log.....	8
2.4 Authentication Configuration.....	9
2.4.1 Radius Client Configuration.....	9
2.4.2 VPN Configuration.....	10
2.4.3 Remote DB Configuration.....	13
2.5.4 LDAP Configuration.....	14
2.5.5 System Configuration.....	17
2.6 User Management.....	17
2.6.1 All Users.....	17
2.6.2 Upload User.....	18
2.7 Soft Token Management.....	19
2.7.1 Soft Token User Management Work flow:.....	19
2.7.2 Soft Token Users Overview.....	19
2.7.3 Add Soft Token Users - Manually.....	20
2.7.4 Add Soft Token Users - By CSV file.....	21
2.7.5 Add Soft Token Users - By LDAP/Active Directory.....	22
2.7.6 Delete Soft Token Users.....	23
2.7.7 Update Soft Token Users.....	24
2.7.8 Activate Soft Token Users.....	24
2.7.9 Deactivate Soft Token Users.....	25
2.7.10 Reset Soft Token User's Secret Key.....	25
2.7.11 Resynchronize Soft Token User's Time.....	26
2.7.12 Edit Soft Token Account Activation Templates.....	27
2.8 Soft Token User Login.....	28
3.0 REFERENCES.....	30
3.1 Authentication Types.....	30
3.1.1 One Factor.....	30
3.1.2 Two Factor Static (Password + OTP).....	30
3.1.3 Two Factor Static (OTP).....	30
3.1.4 Two Factor Static (SMS Reply).....	31
3.1.5 Two Factor Access Challenge.....	31
3.1.6 Two Factor Access Challenge (Username Only).....	31
3.2 OTP On Demand SMS template.....	32
3.3 Recommended OATH-compliant Soft Token Mobile Application.....	32

# SENDQUICK CONEXA USER MANUAL 2.0

## 1.0 INTRODUCTION

This documentation is prepared for administrator to configure users' VPN access using various authentication methods (OTP or SOFT TOKEN). Administrator also configure which authentication server (LDAP/Active Directory, local users, remote database, remote RADIUS server) to authenticate users. If companies opt to enable SOFT TOKEN feature, administrator needs to manage and import soft token users from external source like LDAP/Active Directory or batch upload with CSV file.

## 2.0 SET-UP AND CONFIGURATION

### 2.1 Set-up steps

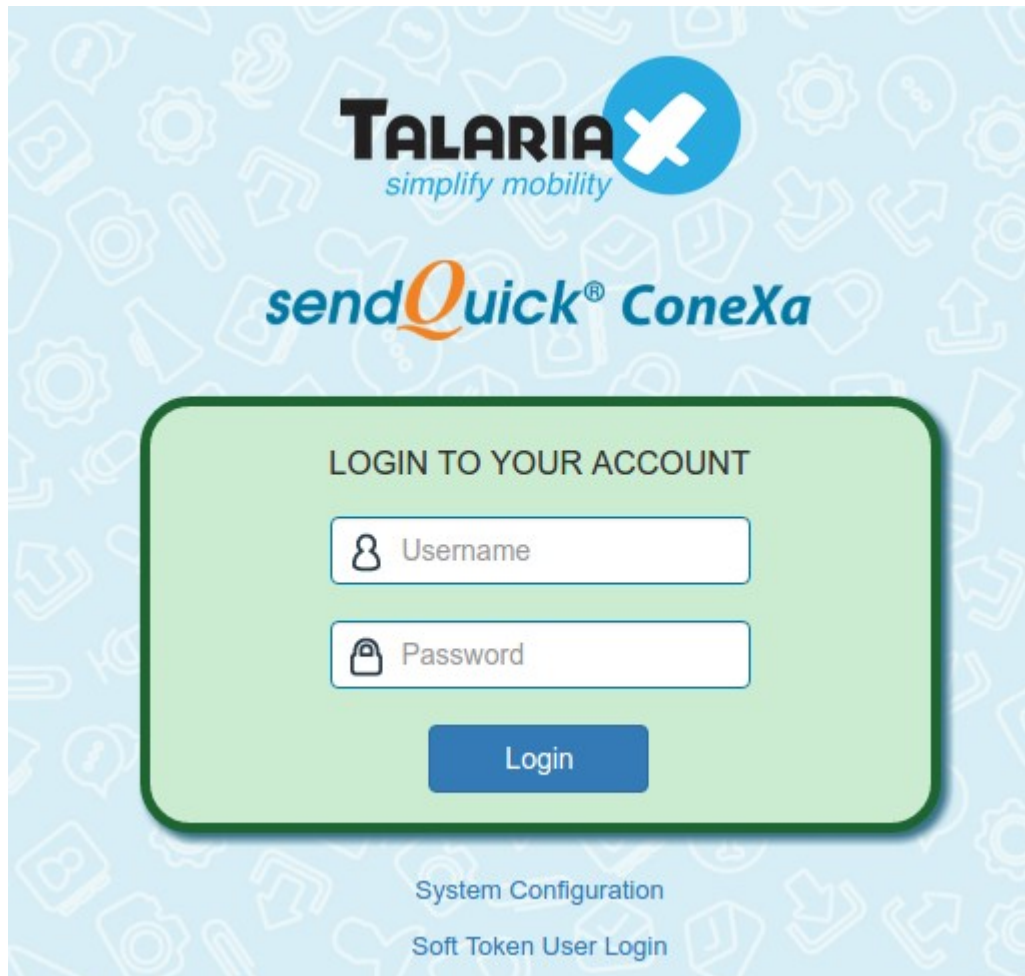
Typical set-up steps as follow:

1. Add RADIUS client, configure shared secret.
2. Add VPN configuration
3. Add authentication server (local users, LDAP/Active Directory, remote database or remote Radius)
4. Additional configurations:
  - a. Add LDAP/Active Directory configuration (If LDAP/Active Directory is chosen as authentication server)
  - b. Add Remote Database configuration (If Remote Database is chosen as authentication server)
  - c. Add Local Users profile (if Local Users is chosen as authentication server)

## 2.2 Login Procedures

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

**URL: [https://\[Conexa's server IP\]/otp](https://[Conexa's server IP]/otp)**



Enter the default Administrator's Log-in Name and Password to access the system. The default Username and Password is as below:

**Username:** otpadmin **Password:** admin123

You can change the password after logging-in.

### 2.1.1 Login Types

There are three(3) types of user accounts:

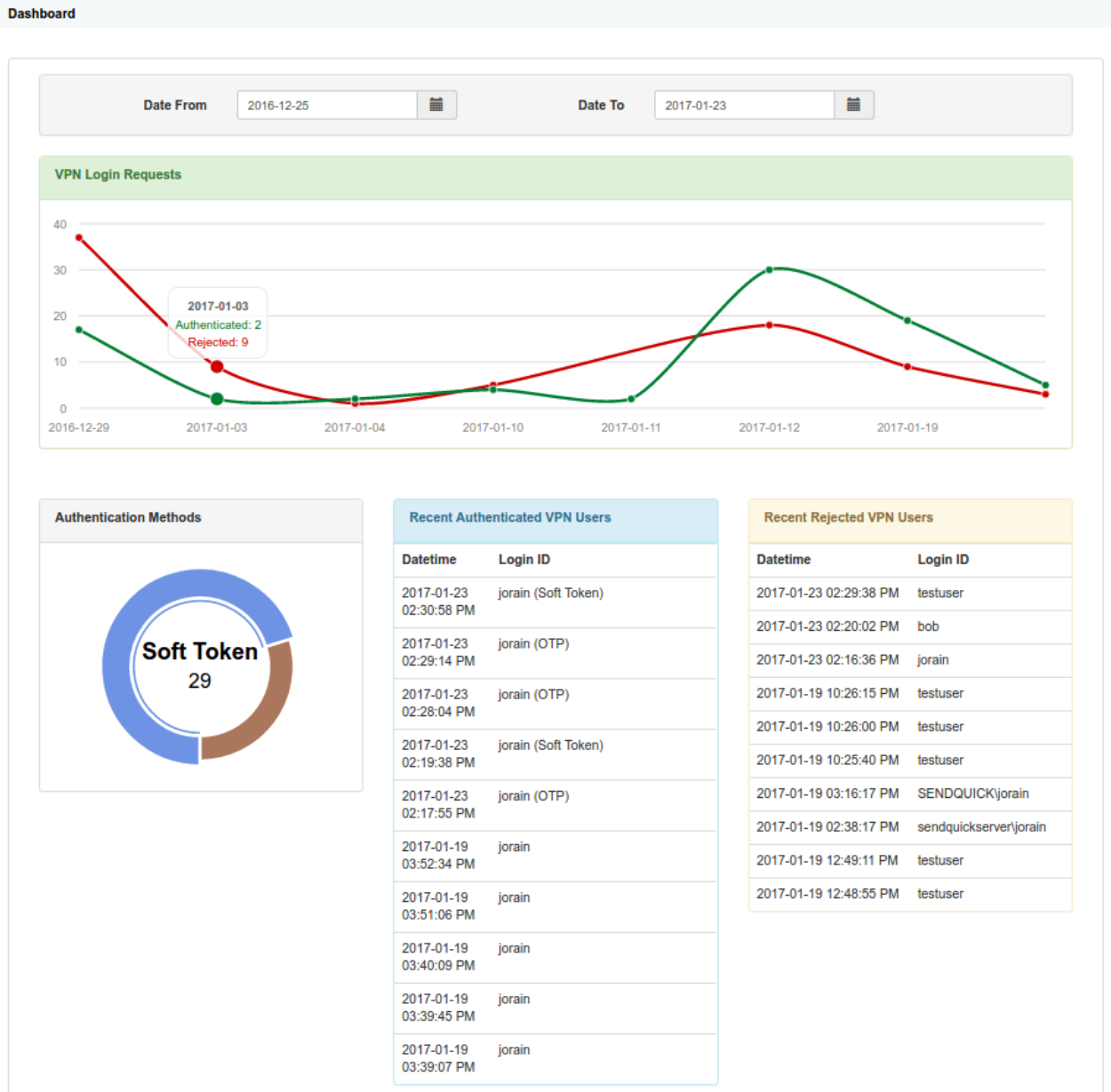
1. Super Admin
2. Admin
3. User

Super Admin and Admin have full access rights to every features. The only different is Super Admin 'useradmin' account is the default admin account and cannot be deleted.

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

## 2.2 Dashboard

This page will display summary for all login requests, authentication methods, recent authenticated and rejected VPN users. Admin can select date range to generate summary report. Default reporting period is 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 TalariaX support for quick troubleshooting.

Logs > **Server Log**

**Server Log**

```

2017-01-23 14:29:14 Radius[5568] (OTPapi) Request from jorain (192.168.1.4). 2FC ACCEPT
2017-01-23 14:29:38 Radius[5568] (OTPapi) *****Request from NAS-IP-Address:192.168.1.4 NAS-Identifier:conexapublicdemovpn- (testuser)****
2017-01-23 14:29:38 Radius[5568] (OTPapi) Using LDAP (AD213) Server 1 (192.168.1.213:389)
2017-01-23 14:29:38 Radius[5568] (OTPapi) CheckValidLdapUser (AD213) 49 & User: CN=testuser,CN=Users,DC=testserver,DC=com message=Cannot Authenticate to AD:
LDAP_INVALID_CREDENTIALS
2017-01-23 14:29:38 Radius[5568] (OTPapi) CheckValidLdapUser (AD213) for testuser, Mode:loginid, Server(192.168.1.213:389) failed
2017-01-23 14:29:38 Radius[5568] (OTPapi) Authentication failed. Invalid Password (testuser)
2017-01-23 14:29:38 Radius[5568] (OTPapi) Request from testuser (192.168.1.4). 2FC REJECT
2017-01-23 14:30:06 Radius[5568] (OTPapi) *****Request from NAS-IP-Address:192.168.1.4 NAS-Identifier:conexapublicdemovpn- (jorain)****
2017-01-23 14:30:06 Radius[5568] (OTPapi) Using LDAP (AD213) Server 1 (192.168.1.213:389)
2017-01-23 14:30:06 Radius[5568] (OTPapi) CheckValidLdapUser (AD213) for jorain, Mode:loginid, Server(192.168.1.213:389) success
2017-01-23 14:30:06 Radius[5568] (OTPapi) 2-FA AC 1st authentication (2FC) success (jorain)
2017-01-23 14:30:06 Radius[5568] (OTPapi) GenerateUserOTP | OTP=2354 |digest:Digest::SHA256 otlength:4 timestep:30 counter: 49505100
2017-01-23 14:30:06 Radius[5568] (OTPapi) Using LDAP (AD213) Server 1 (192.168.1.213:389)
2017-01-23 14:30:06 Radius[5568] (OTPapi) GetLdapUserInfo (AD213) for jorain, Mode:loginid, Server(192.168.1.213:389) : (mobile:83604556 , email:jorain@talariax.com)
2017-01-23 14:30:06 Radius[5568] (OTPapi) SendSMS ASCII | tar_num:83604556 ; tar_msg:sendQuick Conexa One Time password: 2354 Expire in: 3 mins ; label=
2017-01-23 14:30:07 Radius[5568] (OTPapi) Sending email to: jorain@talariax.com (From: otp@talariax.com)
2017-01-23 14:30:07 Radius[5568] (OTPapi) Send SMS & Email (otp:2354) to jorain (83604556,jorain@talariax.com)
2017-01-23 14:30:07 Radius[5568] (OTPapi) Request from jorain (192.168.1.4). 2FC CHALLENGE
2017-01-23 14:30:07 Radius[5568] (OTPapi) *****Request from NAS-IP-Address:192.168.1.4 NAS-Identifier:conexapublicdemovpn- (jorain)****
2017-01-23 14:30:58 Radius[5568] (OTPapi) Request from jorain (192.168.1.4) Return Class=IT,testgrp,Remote Desktop Users,Administrators
2017-01-23 14:30:58 Radius[5568] (OTPapi) Request from jorain (192.168.1.4) Return Filter-Id=IT,testgrp,Remote Desktop Users,Administrators
2017-01-23 14:30:58 Radius[5568] (OTPapi) 2-Factor AC authentication (2FC) success (jorain SOFT TOKEN:248494)
2017-01-23 14:30:58 Radius[5568] (OTPapi) Request from jorain (192.168.1.4). 2FC ACCEPT
                
```

[Refresh](#)

Download Log: [Current](#) | [log 1](#) | [log 2](#) | [log 3](#) | [log 4](#) | [log 5](#) | [log 6](#)

### 2.3.2 Authentication Log

This page displays complete authentication requests log. Admin can check every incoming login authentication request from all VPN.

Logs > **Authentication Log**

Date From :  Date To :  Login ID :  VPN Name :  Status :

Show  records Search:

No.	Datetime	Login ID	VPN Name	Status	Auth Method	Reject Reason
1	2017-01-23 14:16:36	jorain	joraintest	Reject		Invalid Password/OTP
2	2017-01-23 14:17:21	jorain	joraintest	Challenge		
3	2017-01-23 14:17:55	jorain	joraintest	Success	OTP	
4	2017-01-23 14:19:27	jorain	joraintest	Challenge		
5	2017-01-23 14:19:38	jorain	joraintest	Success	SOFT TOKEN	
6	2017-01-23 14:20:01	bob	joraintest	Reject		Invalid Password/OTP
7	2017-01-23 14:20:24	jorain	joraintest	Challenge		
8	2017-01-23 14:27:52	jorain	joraintest	Challenge		
9	2017-01-23 14:28:04	jorain	joraintest	Success	OTP	
10	2017-01-23 14:29:06	jorain	JUNIPER DEMO	Challenge		

Showing 1 to 10 of total 14 records [Previous](#) [1](#) [2](#) [Next](#)



## 2.4 Authentication Configuration

Administrator will configure VPN, RADIUS client, LDAP/Active Directory, Remote Database and System configuration in this section.

### 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 Conexa server.

Authentication Configuration > RADIUS Client Configuration

Show 10 records Search:

No.	Name	RADIUS Client IP	Update	
1	Test	192.168.1.216		<input type="checkbox"/>
2	jr	192.168.1.151		<input type="checkbox"/>
3	juniper	192.168.1.4		<input type="checkbox"/>

Showing 1 to 3 of total 3 records Previous 1 Next

#### Create/Edit Radius Client Configuration

### Radius Client ✕

**RADIUS Client IP**

**Name**

**Shared Secret**

RADIUS Client IP	VPN's gateway IP address. This is the IP address captured in 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 (Conexa).

## 2.4.2 VPN Configuration

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

Authentication Configuration > VPN Configuration

Show  records Search:

No.	Name	NAS IP / NAS ID	Description	Authentication Type	Authentication Server	Update	
1	TestVPN	192.168.1.216		Two Factor Access Challenge	LDAP		<input type="checkbox"/>
2	jrtest	192.168.1.151		Two Factor Access Challenge	LDAP		<input type="checkbox"/>
3	junipervpn	192.168.1.4	demo	One Factor	Local Users		<input type="checkbox"/>

Showing 1 to 3 of total 3 records Previous **1** Next

### Create/Edit VPN Configuration

#### VPN Configuration ✕

**NAS-IP / NAS-ID**

NAS-IP-Address
  NAS-Identifier
  None

**Name**

**Description**

**Authentication Type**

**Authentication Server**

Use either NAS-IP-Address or NAS-Identifier to communicate with Conexa. Select None if NAS-IP-Address and NAS-Identifier are empty.

Unique name of this VPN

Fields	Description
NAS-IP / NAS-ID	VPN IP address or identifier
Name	Unique name to identify VPN
Description	Short description for VPN. For reference only.
Authentication Type	<ul style="list-style-type: none"> <li>One Factor</li> <li>Two Factor Static (Password + OTP)</li> <li>Two Factor Static (OTP)</li> <li>Two Factor Static (SMS Reply)</li> <li>Two Factor Access Challenge</li> <li>Tow Factor Access Challenge (Username Only)</li> </ul> Refer to 3.1 Authentication Types for more details.
Authentication Server	<ul style="list-style-type: none"> <li><b>Local Users</b> <ul style="list-style-type: none"> <li>Username/Password in User Management</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• <b>RADIUS</b> <ul style="list-style-type: none"> <li>◦ Authenticate through remote radius server. Remote radius server IP, port and secret are required.</li> </ul> </li> <li>• <b>LDAP</b> <ul style="list-style-type: none"> <li>◦ Authenticate through LDAP server such as Active Directory or OpenLDAP. Select LDAP server from list which are predefined in LDAP Configuration section.</li> </ul> </li> <li>• <b>Multiple LDAP (Only available for Conexa300)</b> <ul style="list-style-type: none"> <li>◦ Authenticate through LDAP servers (max 10 servers)</li> </ul> <p><b>Search Options -&gt; [Recursive   Predefined]</b>  <b>Recursive:</b> Search through all LDAP servers in sequence.  <b>Predefined:</b> 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</p> </li> <li>• <b>Remote DB</b> <ul style="list-style-type: none"> <li>◦ Authenticate through external DB server [SQL Server, MySQL, PostgresSQL or Oracle DB]. Select Remote DB from list which are predefined in Remote DB Configuration section. Table name and column name of userid and password are required.</li> </ul> </li> </ul>
LDAP Return Option	For LDAP or Multiple LDAP, 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 one time password generated by OATH compliant Soft Token mobile application.
Enable OTP	Allow user to authentication through one time password generated by built-in sendQuick ConeXa algorithm.
OTP On Demand Keyword	Unique keyword to request OTP. For Two Factor Static (Password + OTP) or (OTP) mode, users can send SMS to Conexa to request OTP before they logging-in VPN.
SMS Reply Template	For Two Factor Static (SMS Reply) mode, 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.
Access Challenge Validity	For 2FA Access Challenge mode. Valid period before challenge request timeout. Enter 0 to disable.

OTP Prompt Message	Prompt message on access challenge page. ^M = User's mobile number ^E = User's email
OTP Type	[ <b>One Time Pin (OTP)</b>   <b>Short Term Pin (STP)</b> ] OTP: One time usage only. STP: Limited times of usage over validity period.
OTP Delivery Method	[ <b>SMS</b>   <b>EMAIL</b>   <b>BOTH</b> ]
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	[ <b>Normal Text</b>   <b>Message Overwrite</b>   <b>Flashtext</b> ]  <ul style="list-style-type: none"> <li>• <b>Normal Text:</b> Send as normal SMS text message.</li> <li>• <b>Message Overwrite:</b> Replace previously received SMS with the new SMS.</li> <li>• <b>Flashtext:</b> Flash SMS appears directly on phone's screen, instead of Inbox.</li> </ul>
SMS Priority	1 to 9 (Highest = 1 , Lowest = 9)
Modem Label	Send SMS via specific modem label
User Contact List	<ul style="list-style-type: none"> <li>• Check on 'Same as authentication server' to use the same user list in authentication server.</li> <li>• <b>Local Users</b> <ul style="list-style-type: none"> <li>◦ Mobile and Email in User Management.</li> </ul> </li> <li>• <b>LDAP</b> <ul style="list-style-type: none"> <li>◦ Select from a list of predefined LDAP servers. Mobile and email attributes are required.</li> </ul> </li> <li>• <b>Remote DB</b> <ul style="list-style-type: none"> <li>◦ Select from a list of predefined Remote DB. Required table name and column name for user id, mobile and email.</li> </ul> </li> </ul>

## 2.4.3 Remote DB Configuration

Administrator to add remote database configuration to populate option in

- Authentication Configuration->VPN Configuration->Add/Edit VPN->Authentication Server
- Authentication Configuration->VPN Configuration->Add/Edit VPN->User Contact List

Authentication Configuration > Remote DB Configuration

Show  records Search:

No. ▲	Name ⇅	Type ⇅	Host ⇅	Port ⇅	Database ⇅	Update	<input type="checkbox"/>
1	postgres	psql	192.168.1.243	5432	mctestdb		<input type="checkbox"/>
2	mssql	mssql	192.168.1.213	1433	testappdb		<input type="checkbox"/>

Showing 1 to 2 of total 2 records

### Create/Edit DB Configuration

Unique name for DB

Description

Database Type

Database Host  Port

Login Name

Login Password

Database Name

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

## 2.5.4 LDAP Configuration

Administrator to add remote database configuration to populate option in:

- Authentication Configuration->VPN Configuration->Add/Edit VPN->Authentication Server
- Authentication Configuration->VPN Configuration->Add/Edit VPN->User Contact List
- Soft Token Management->Soft Token Users->Upload User->by LDAP/Active Directory

Authentication Configuration > LDAP Configuration

Show 10 records Search:

No.	Name	Description	Server 1	Server 2	Login Mode	Base DN	Scope	Test Query	Update	
1	AD1	company AD	10.10.2.34	10.10.2.35	loginid	dc=company, dc=com	sub	<input type="button" value="Test Query"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	AD213		192.168.1.213		loginid	dc=testserver,dc=com	sub	<input type="button" value="Test Query"/>	<input type="checkbox"/>	<input type="checkbox"/>

Showing 1 to 2 of total 2 records Previous **1** Next

### Create/Edit LDAP Configuration

#### LDAP Configuration

<b>Name</b>	<input type="text" value="AD213"/>	Unique name for LDAP server
<b>Description</b>	<input type="text"/>	
<b>Server 1</b>	<input type="text" value="192.168.1.213"/> Port <input type="text" value="389"/>	Primary LDAP Server IP and port number. LDAP default port : 389.
<b>Server 2</b>	<input type="text"/> Port <input type="text"/>	Secondary LDAP Server IP and port number. LDAP default port : 389.
<b>Type</b>	<input type="text" value="Active Directory"/>	
<b>Service Account Bind DN</b>	<input type="text" value="conexaadmin"/> <input type="text" value="Test"/>	Valid login DN & password, which will be used for binding and searching.
<b>Service Account Password</b>	<input type="password" value="....."/>	
<b>Login Mode</b>	<input type="text" value="Login ID"/>	
<b>Base DN</b>	<input type="text" value="dc=testserver,dc=com"/>	Base DN of the location of user list
<b>Search Scope</b>	<input type="text" value="Sub"/>	
<b>Additional LDAP Filter String</b>	<input type="text"/>	Enter additional LDAP search filter string.

Field	Description
Name	Unique name to identify LDAP
Description	Short description

Server 1 & port	First LDAP server IP and port. Default LDAP port: 389												
Server 2 & port	Second LDAP server IP and port number. Default LDAP port: 389												
Type	[ <i>Active Directory</i>   <i>LDAP</i> ]												
Service Account Bind DN	Valid LDAP username which will be used to bind and search												
Service Account Password	Valid LDAP password which will be used to bind and search												
Login Mode	Type of Login ID, check against the following attributes in LDAP server. <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 25%;">Login Mode</th> <th style="width: 35%;">Active Directory Attributes</th> <th style="width: 40%;">LDAP Attributes</th> </tr> </thead> <tbody> <tr> <td>Display Name</td> <td>displayName</td> <td>displayName</td> </tr> <tr> <td>Login ID</td> <td>sAMAccountName</td> <td>uid</td> </tr> <tr> <td>Email</td> <td>mail</td> <td>mail</td> </tr> </tbody> </table>	Login Mode	Active Directory Attributes	LDAP Attributes	Display Name	displayName	displayName	Login ID	sAMAccountName	uid	Email	mail	mail
Login Mode	Active Directory Attributes	LDAP Attributes											
Display Name	displayName	displayName											
Login ID	sAMAccountName	uid											
Email	mail	mail											
Base DN	Base DN of the location of user list												
Search Scope	<ul style="list-style-type: none"> <li><b>Sub</b> : Search the whole tree below and including the base object.</li> <li><b>Base</b> : Search only the base object.</li> <li><b>One</b> : Search the entries immediately below the base object.</li> </ul>												
Additional LDAP Filter String	Default is empty. For example, to allow all users in VPNUsers group, (memberOf=CN=VPNUsers,CN=Users,DC=testserver,DC=com)												

### Test LDAP Query

Authentication Configuration > LDAP Configuration

Show  records Search:

No.	Name	Description	Server 1	Server 2	Login Mode	Base DN	Scope	Test Query	Update
1	AD1	company AD	10.10.2.34	10.10.2.35	loginid	dc=company, dc=com	sub	<input type="button" value="Test Query"/>	<input type="checkbox"/>
2	AD213		192.168.1.213		loginid	dc=testserver,dc=com	sub	<input type="button" value="Test Query"/>	<input type="checkbox"/>

Showing 1 to 2 of total 2 records Previous **1** Next

Enter LDAP user ID and click on “Query Attributes”

Authentication Configuration > LDAP Configuration

LDAP Server

AD213

User ID

mc2

Query Attributes

Reset

RESULT

Using 192.168.1.213:389

Base DN: dc=testserver,dc=com

Search String: sAMAccountName=mc2

objectClass => top

objectClass => person

objectClass => organizationalPerson

objectClass => user

cn => Man Choy Kau

telephoneNumber => 0166338486

givenName => mc1

distinguishedName => CN=Man Choy Kau,CN=Users,DC=testserver,DC=com

instanceType => 4

whenCreated => 20161108021905.0Z

whenChanged => 20170110040759.0Z

displayName => mc

uSNCreated => 300406

uSNChanged => 303965

name => Man Chov Kau



## 2.5.5 System Configuration

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

### System Configuration

<b>Debug Mode</b>	Enable
<b>Syslog Server IP</b>	192.168.1.123
<b>Syslog Server Port</b>	514
	<input type="button" value="Test"/>

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 Server IP & port	sendQuick ConeXa will send VPN authentication logs to this Syslog server.

## 2.6 User Management

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

### 2.6.1 All Users

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

#### User Management > All Users

Show  records Search:

No. ^	Login ID ⇅	Username ⇅	Role ⇅	Mobile Number ⇅	Email ⇅	Update	
1	otpadmin	admin	Admin				<input type="checkbox"/>
2	testaccount	testaccount	Admin	01299889988	testaccount@gmail.com		<input type="checkbox"/>

Showing 1 to 6 of total 6 records Previous **1** Next

## 2.6.2 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.*

<b>Login ID</b>	Max 50 characters. Contain alphabets, digits and - _ . only.
<b>Username</b>	Max 100 characters. Contain alphabets, digits, space and - _ only.
<b>Password</b>	Max 50 characters. Optional
<b>Mobile Number</b>	A valid mobile number, Eg. +6591234567 / 81234567
<b>Email</b>	A valid email address
<b>Role</b>	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::

No file chosen

- 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:

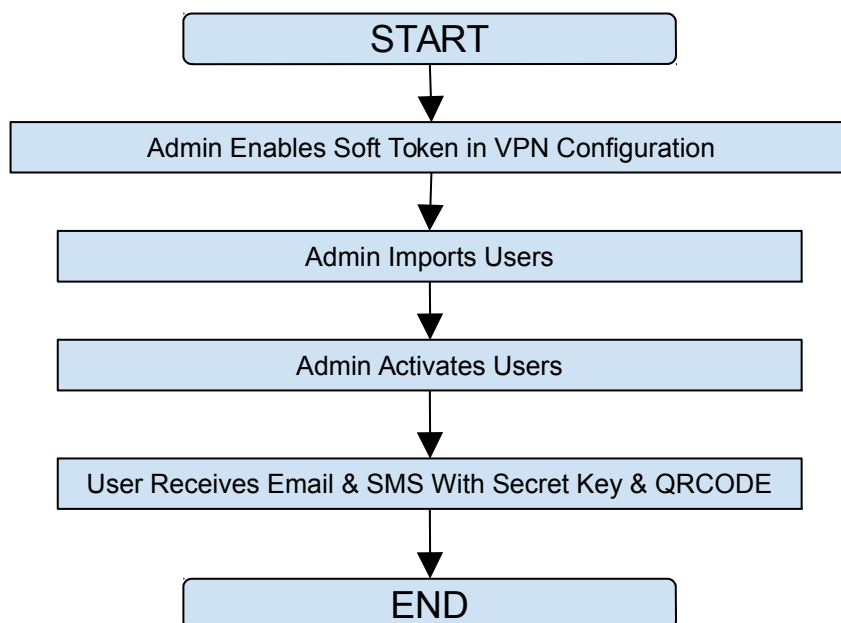
```
user1,username1,password,91234567,user1@company.com,U
user2,username2,password,81234567,,U
user3,username3,,user3@company.com,U
admin1,adminname1,1234,+6598888888,admin1@company.com,A
admin2,adminname2,,admin2@company.com,A
```

## 2.7 Soft Token Management

Administrator to manage soft token users by:

- Add soft token user
- Delete soft token user
- Update soft token user
- Activate user’s soft token account
- Deactivate user’s soft token account
- Regenerate user’s secret key
- Resynchronize user’s time
- Edit account activation SMS & EMAIL templates

### 2.7.1 Soft Token User Management Work flow:



### 2.7.2 Soft Token Users Overview

Account:  
otpadmin

English ▼ [Logout](#)

Soft Token Management > **Soft Token Users**

VPN: All ▼ Activated: All ▼ Search

Show 10 ▼ records Search:

No.	Login ID	VPN	Mobile Number	Email	Activated	Resync Time	Update	
1	csv-user3	MC VPN (192.168.1.175)		manchoyy@gmail.com	Yes	<span style="color: blue;">○</span>	<a href="#">🔗</a>	<input type="checkbox"/>
2	csv-user2	MC VPN (192.168.1.175)	01912345678	manchoyy@gmail.com	Yes	<span style="color: blue;">○</span>	<a href="#">🔗</a>	<input type="checkbox"/>
3	csv-user1	MC VPN (192.168.1.175)	0126338487	manchoyy@gmail.com	Yes	<span style="color: blue;">○</span>	<a href="#">🔗</a>	<input type="checkbox"/>
4	haiza	MC VPN (192.168.1.175)		haiza@talariax.com	No	<span style="color: blue;">○</span>	<a href="#">🔗</a>	<input type="checkbox"/>
5	sou1_u3	MC VPN (192.168.1.175)		sou1_u3@test.com	No	<span style="color: blue;">○</span>	<a href="#">🔗</a>	<input type="checkbox"/>
6	sou2_u2	MC VPN (192.168.1.175)		sou2_u2@test.com	No	<span style="color: blue;">○</span>	<a href="#">🔗</a>	<input type="checkbox"/>
7	sou3_u1	MC VPN (192.168.1.175)		sou3_u1@test.com	No	<span style="color: blue;">○</span>	<a href="#">🔗</a>	<input type="checkbox"/>
8	sou2_u1	MC VPN (192.168.1.175)		sou2_u1@test.com	No	<span style="color: blue;">○</span>	<a href="#">🔗</a>	<input type="checkbox"/>
9	sou1_u1	MC VPN (192.168.1.175)		sou1_u1@test.com	No	<span style="color: blue;">○</span>	<a href="#">🔗</a>	<input type="checkbox"/>
10	mou_u2	MC VPN (192.168.1.175)		mou_u2@test.com	No	<span style="color: blue;">○</span>	<a href="#">🔗</a>	<input type="checkbox"/>

[New User](#)
[Upload User](#)
[Actions](#)

### 2.7.3 Add Soft Token Users - Manually

Click on “New User” button to start.

7	sou3_u1	MC VPN (192.168.1.175)
8	sou2_u1	MC VPN (192.168.1.175)
9	sou1_u1	MC VPN (192.168.1.175)
10	mou_u2	MC VPN (192.168.1.175)

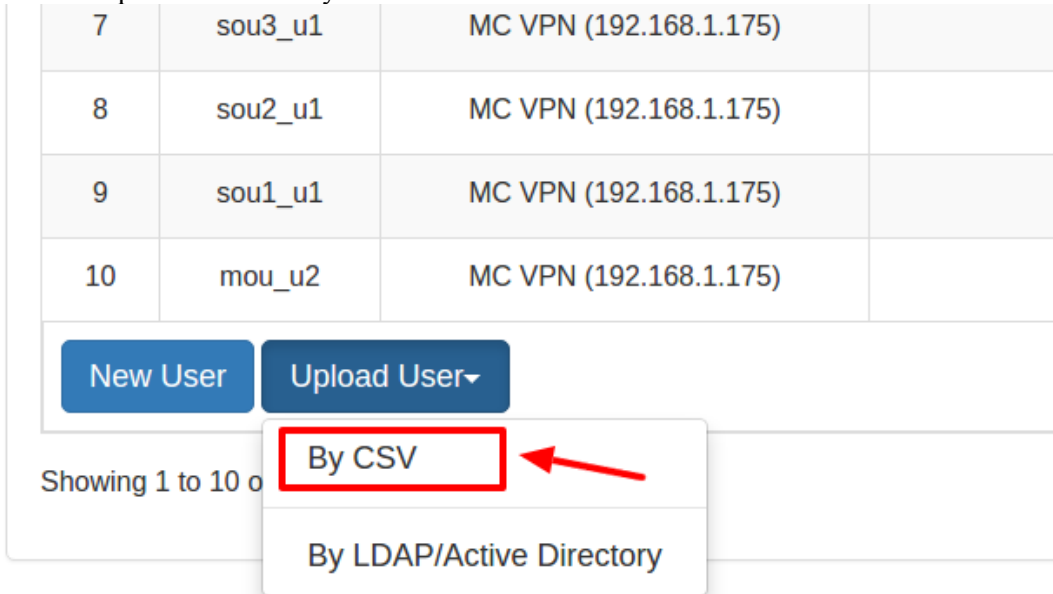
Showing 1 to 10 of total 21 records

Fill up all fields and press “Save” button to create new soft token user.

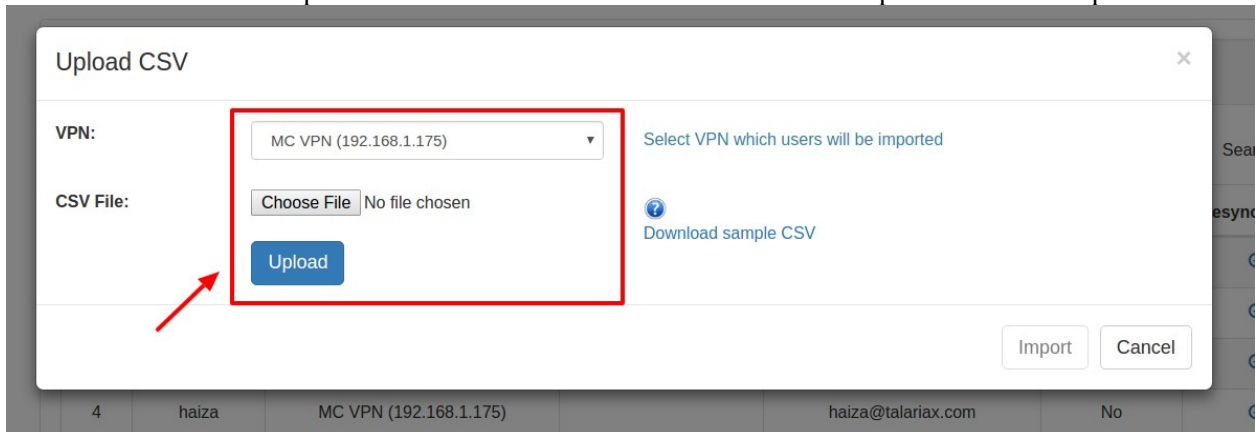
Field	Description
Login ID	VPN login id
VPN	Choose VPN to access from dropdown list.
Email	sendQuick ConeXa will send Soft Token activation email to this email.
Mobile Number	sendQuick ConeXa will send Soft Token activation SMS reminder to this mobile number.

## 2.7.4 Add Soft Token Users - By CSV file

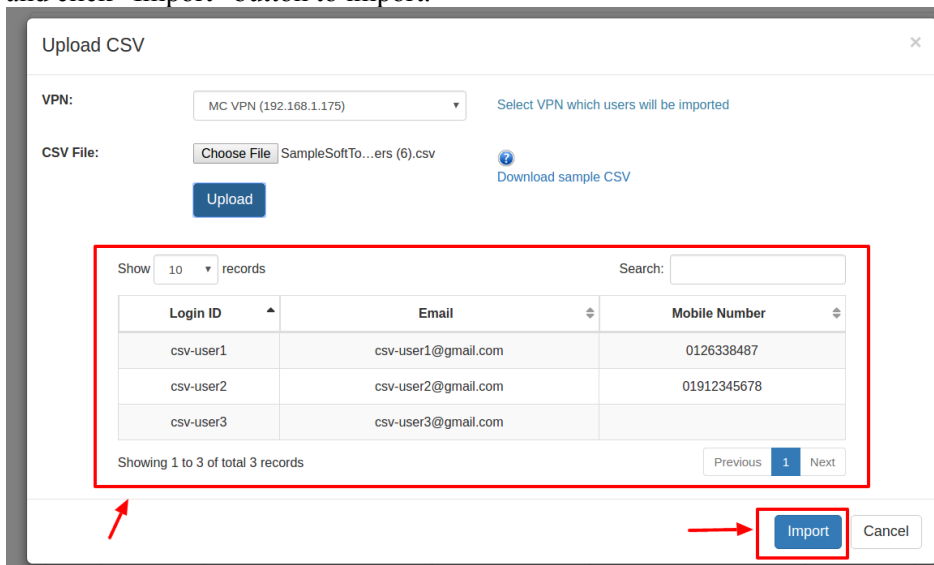
Click on “Upload User” > “By CSV” button to start.



Select VPN 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.

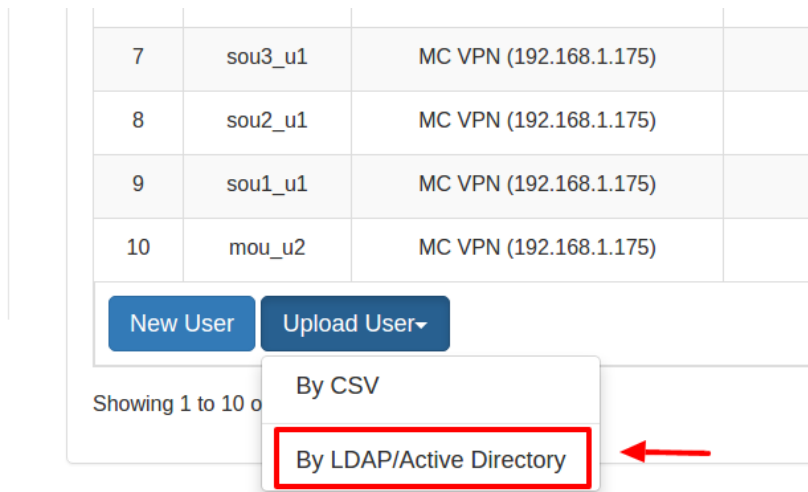


Once upload is done, system will display a list of users ready to be imported. Confirm accuracy of data and click “Import” button to import.

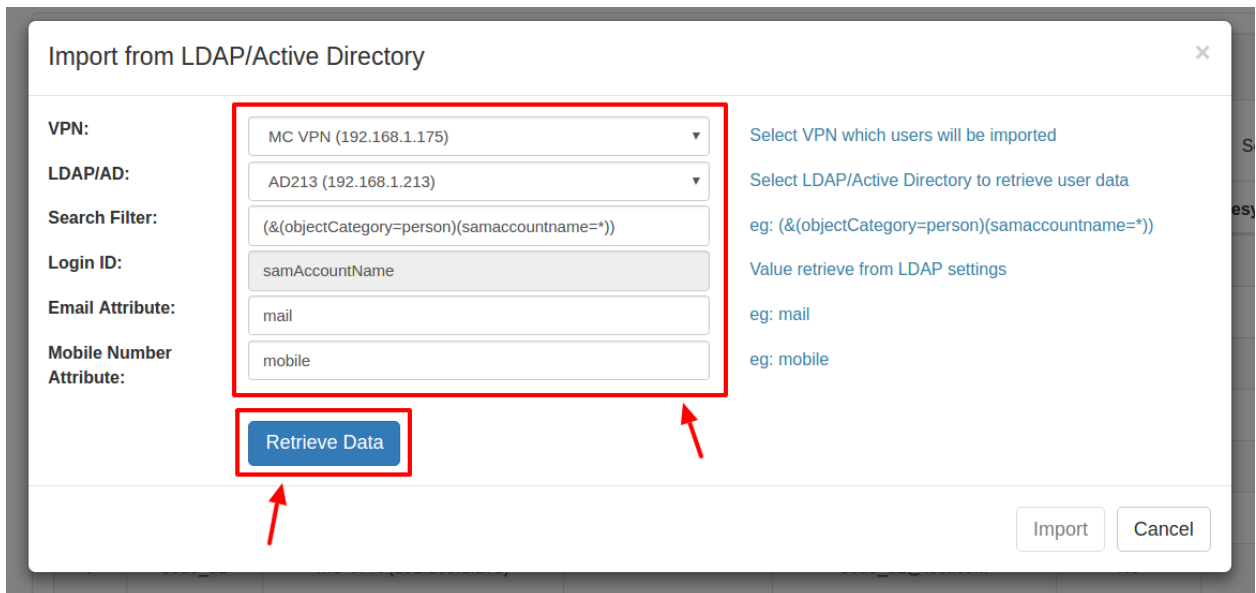


## 2.7.5 Add Soft Token Users - By LDAP/Active Directory

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



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



Field	Description
VPN	Choose which VPN to import users
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
Mobile Attribute	Mobile number field in LDAP

If the LDAP/Active Directory data retrieval is succeed, 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.

Email Attribute:  eg: mail

Mobile Number Attribute:  eg: mobile

Login ID	Email	Mobile Number
aye	thet@talariax.com	
haiza	haiza@talariax.com	
jorain	jorain@talariax.com	83604556
jorain5	jorain@talariax.com	84263040
mc	manchoy@talariax.com	
mou_u1	mou_u1@test.com	11111111
mou_u2	mou_u2@test.com	
ou_user1	ou_user1@gmail.com	91111111
ou_user2	ou_user2@gmail.com	92222222
sou1_u1	sou1_u1@test.com	

Showing 1 to 10 of total 15 records

Previous **1** 2 Next

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

### 2.7.6 Delete Soft Token Users

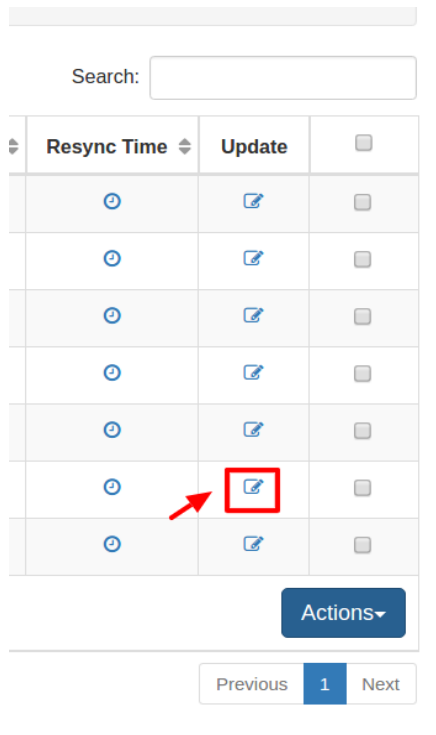
Select user to remove by ticking the checkbox and press “Actions” > “Delete” button to remove user permanently.

Search:

Activated	Resync Time	Update	
Yes			<input type="checkbox"/>
Yes			<input type="checkbox"/>
Yes			<input checked="" type="checkbox"/>
No			<input type="checkbox"/>
No			<input type="checkbox"/>
No			<input type="checkbox"/>
No			<input type="checkbox"/>
No			<input type="checkbox"/>
No			<input type="checkbox"/>

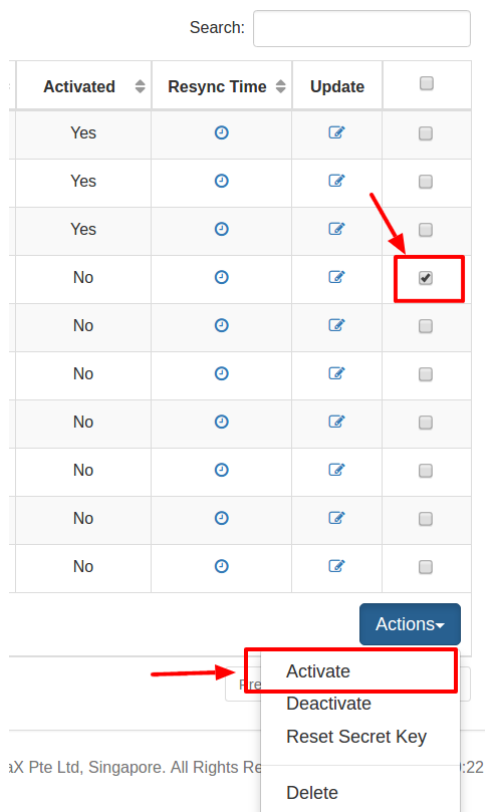
## 2.7.7 Update Soft Token Users

Select user to update by clicking the pencil icon and an update popup window will display.



## 2.7.8 Activate Soft Token Users

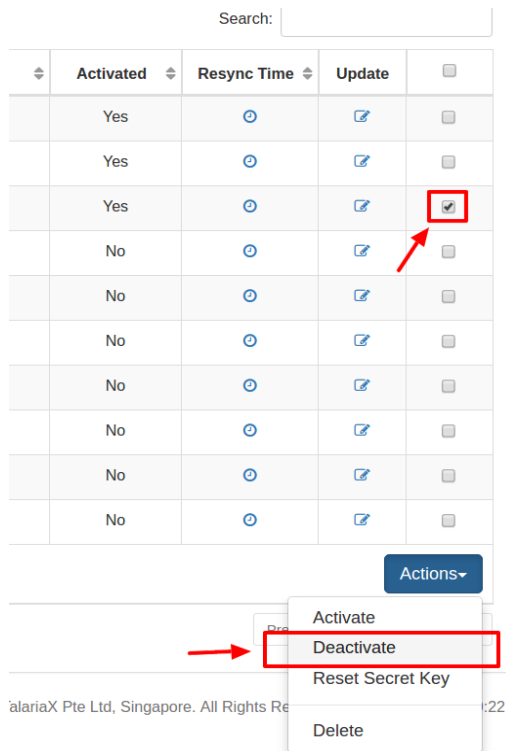
Select user to activate by ticking checkbox and click on “Actions” > “Activate” button. A **NEW** secret key and QR code will be generated and delivered to user’s email address. User has to follow instruction in the email to activate and use soft token.





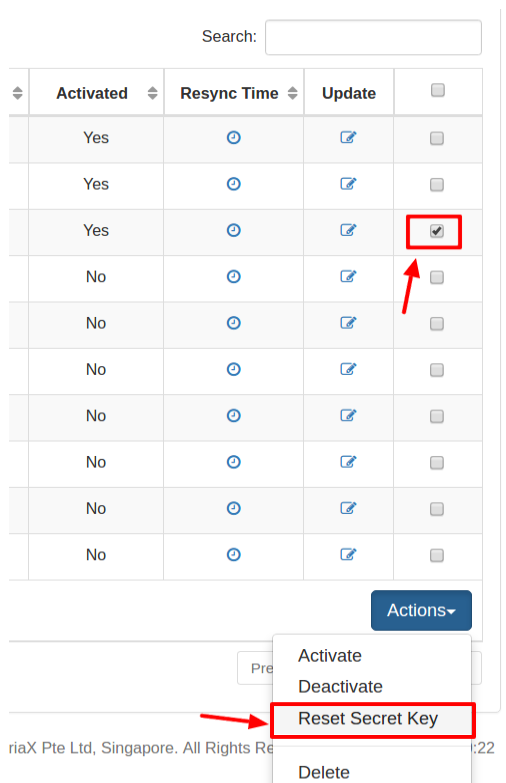
## 2.7.9 Deactivate Soft Token Users

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.



## 2.7.10 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.







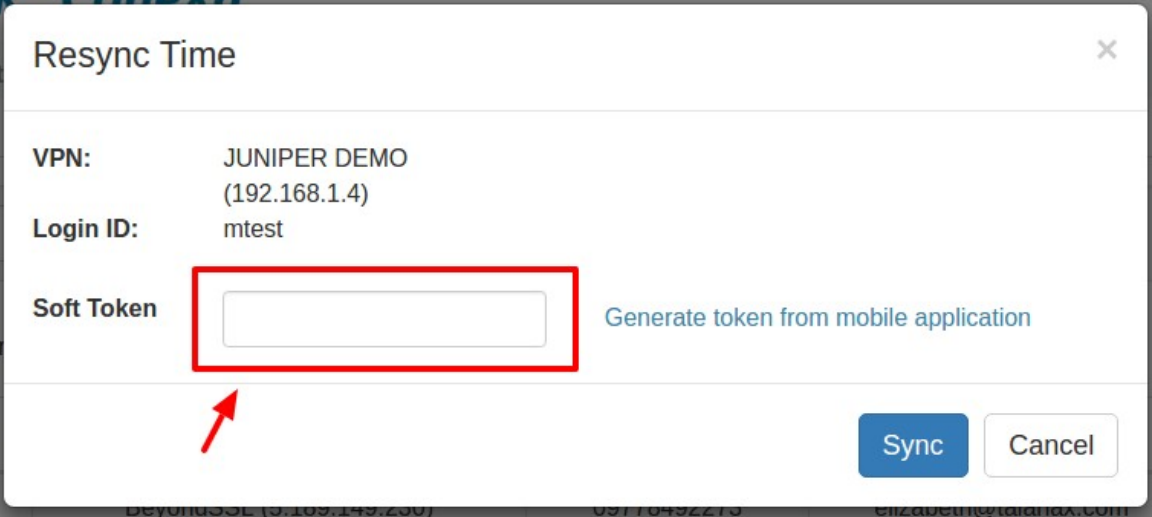
## 2.7.11 Resynchronize Soft Token User's Time

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.

Search:

Email	Activated	Resync Time	Update	
manchoyy@gmail.com	Yes			<input type="checkbox"/>
manchoyy@gmail.com	Yes			<input type="checkbox"/>



**Resync Time** [Close]

VPN: JUNIPER DEMO  
(192.168.1.4)

Login ID: mtest

Soft Token  [Generate token from mobile application](#)

## 2.7.12 Edit Soft Token Account Activation Templates

Click on “Soft Token Management” > “Soft Token Activation Templates” to edit SMS and EMAIL templates.



Available keywords in Email template:

-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

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

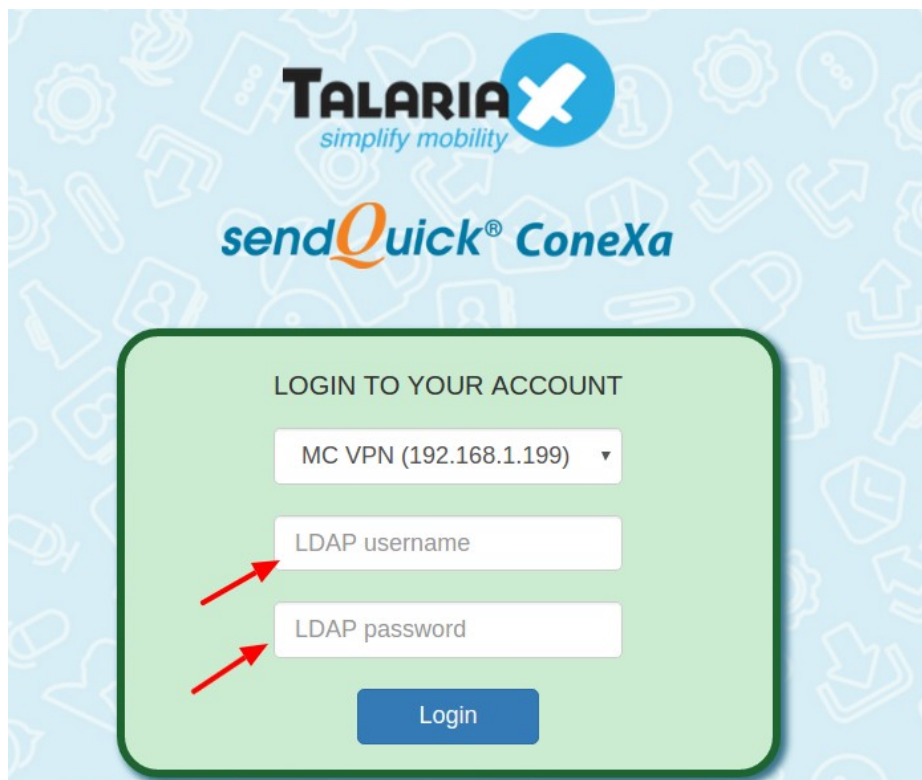
## 2.8 Soft Token User Login

Soft token users login to sendQuick Conexa after received activation email to synchronize mobile clock. Soft token users have to perform this step at least once to record offset time between mobile phone and sendQuick ConeXa server.

1. Visit [http\[s\]://\[ConeXa IP\]/otp/](http[s]://[ConeXa IP]/otp/) and click on “Soft Token User Login”:



2. Login with pre-configured authentication type in VPN configuration (LDAP or local user account)



\* System will inform user to enter appropriate credentials.

3. Enter secret key attached in user's soft token activation email and soft token generated from mobile application.



Soft Token Management > Resync Time

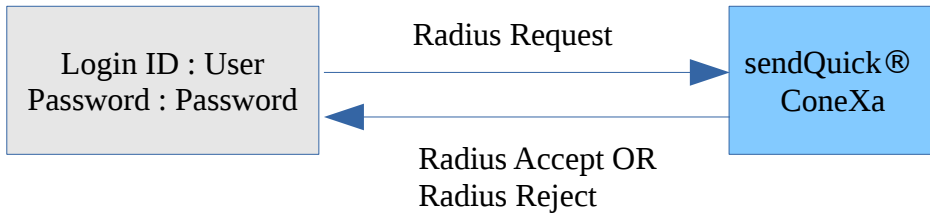
VPN Name	JUNIPER DEMO (192.168.1.4)	
Last Resync	2017-01-04 03:12:08 PM	
Secret Key	<input type="text"/>	Attached in your soft token activation email
Soft Token	<input type="text"/>	Generate token from mobile application
	<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

### 3.0 REFERENCES

#### 3.1 Authentication Types

Authentication can be one factor or two factor. OTP may refer to SMS OTP, Email OTP or Soft Token.

##### 3.1.1 One Factor

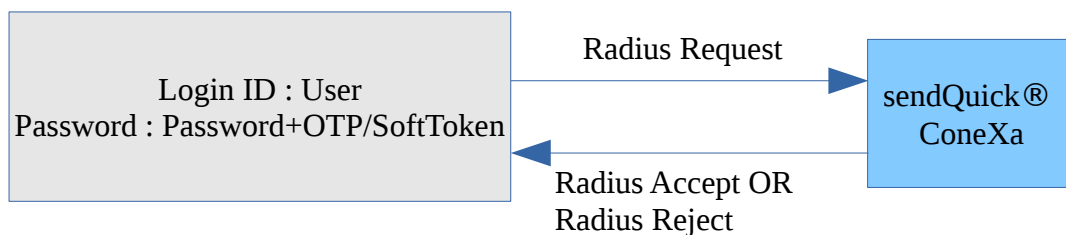


##### 3.1.2 Two Factor Static (Password + OTP)

User requests OTP via SMS and receives OTP

OR

User triggers Soft Token from mobile application

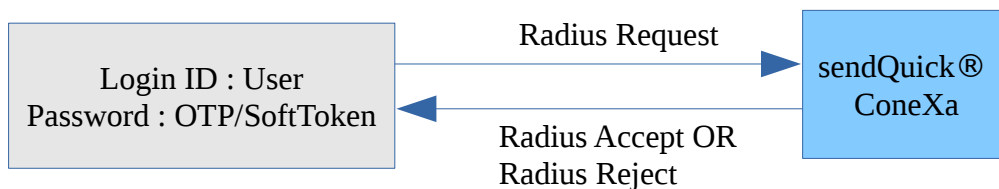


##### 3.1.3 Two Factor Static (OTP)

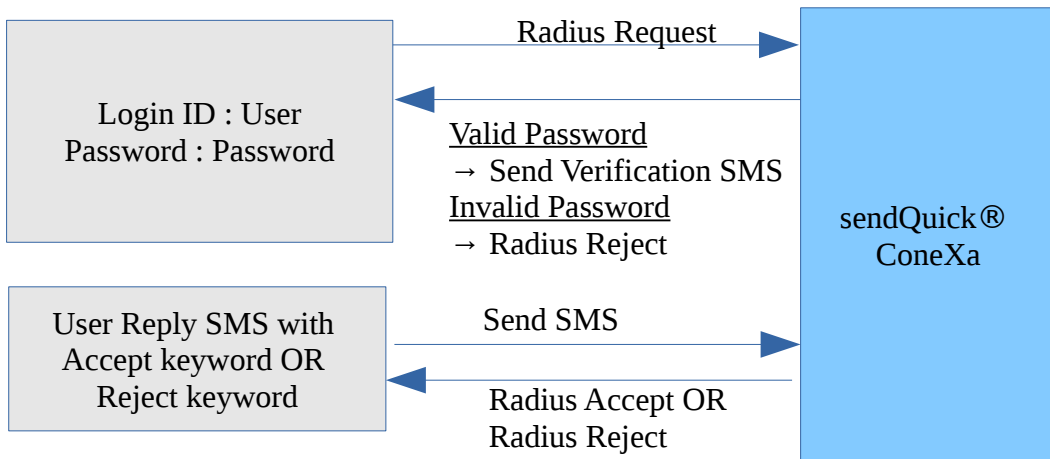
User requests OTP via SMS and receives OTP

OR

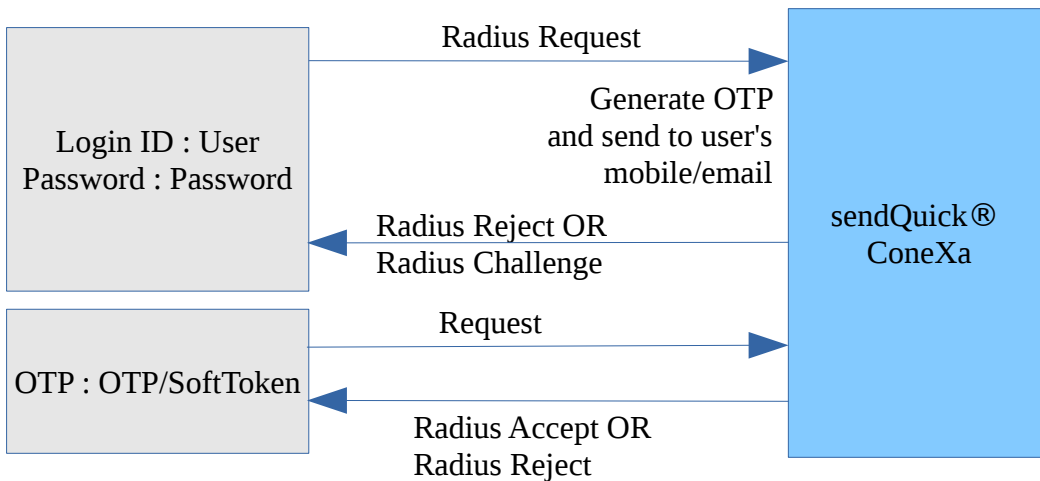
User triggers Soft Token from mobile application



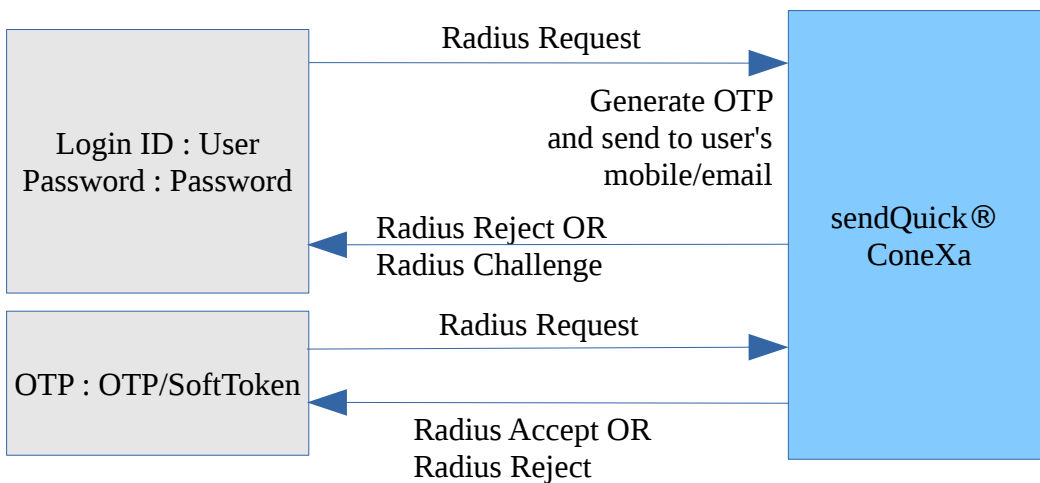
### 3.1.4 Two Factor Static (SMS Reply)



### 3.1.5 Two Factor Access Challenge



### 3.1.6 Two Factor Access Challenge (Username Only)



### 3.2 OTP On Demand SMS template

For 2FA Static (Password + OTP) and 2FA Static (OTP) authentication type, user can send SMS to 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

### 3.3 Recommended OATH-compliant Soft Token Mobile Application

Mobile applications listed below are tested against Soft Token feature in sendQuick ConeXa.

Mobile App Name	Android version	iOS version
 <p><b>ForgeRock Authenticator</b> By: <i>ForgeRock</i></p>	<p><a href="https://play.google.com/store/apps/details?id=com.forgerock.authenticator&amp;hl=en_GB">https://play.google.com/store/apps/details?id=com.forgerock.authenticator&amp;hl=en_GB</a></p>	<p><a href="https://itunes.apple.com/us/app/forgerock-authenticator/id1038442926?mt=8">https://itunes.apple.com/us/app/forgerock-authenticator/id1038442926?mt=8</a></p>
 <p><b>Salesforce Authenticator</b> By: <i>Salesforce</i></p>	<p><a href="https://play.google.com/store/apps/details?id=com.salesforce.authenticator&amp;hl=en">https://play.google.com/store/apps/details?id=com.salesforce.authenticator&amp;hl=en</a></p>	<p><a href="https://itunes.apple.com/us/app/salesforce-authenticator/id782057975?mt=8">https://itunes.apple.com/us/app/salesforce-authenticator/id782057975?mt=8</a></p>
 <p><b>SAASPASS Authenticator</b> By: <i>SAASPASS</i></p>	<p><a href="https://play.google.com/store/apps/details?id=com.solidpass.saaspass&amp;hl=en">https://play.google.com/store/apps/details?id=com.solidpass.saaspass&amp;hl=en</a></p>	<p><a href="https://itunes.apple.com/us/app/saaspass-authenticator-multi/id849132027?mt=8">https://itunes.apple.com/us/app/saaspass-authenticator-multi/id849132027?mt=8</a></p>
 <p><b>FreeOTP</b> By: <i>Red Hat</i></p>	<p><a href="https://play.google.com/store/apps/details?id=org.fedorahosted.freeotp&amp;hl=en">https://play.google.com/store/apps/details?id=org.fedorahosted.freeotp&amp;hl=en</a></p>	<p><a href="https://itunes.apple.com/us/app/freeotp-authenticator/id872559395?mt=8">https://itunes.apple.com/us/app/freeotp-authenticator/id872559395?mt=8</a></p>

If user prefers to use other Soft Token mobile applications, administrator to ensure settings below are configured and found in mobile application:

Algorithm	<b>SHA256</b>
Length	<b>6</b>
Interval	<b>30 seconds</b>

\* New 6 digits Soft Token will be generated every 30 seconds by mobile application, use generated soft token to test VPN access.