sendQuick® ConeXa

Secure Remote Access for Staff and Customers

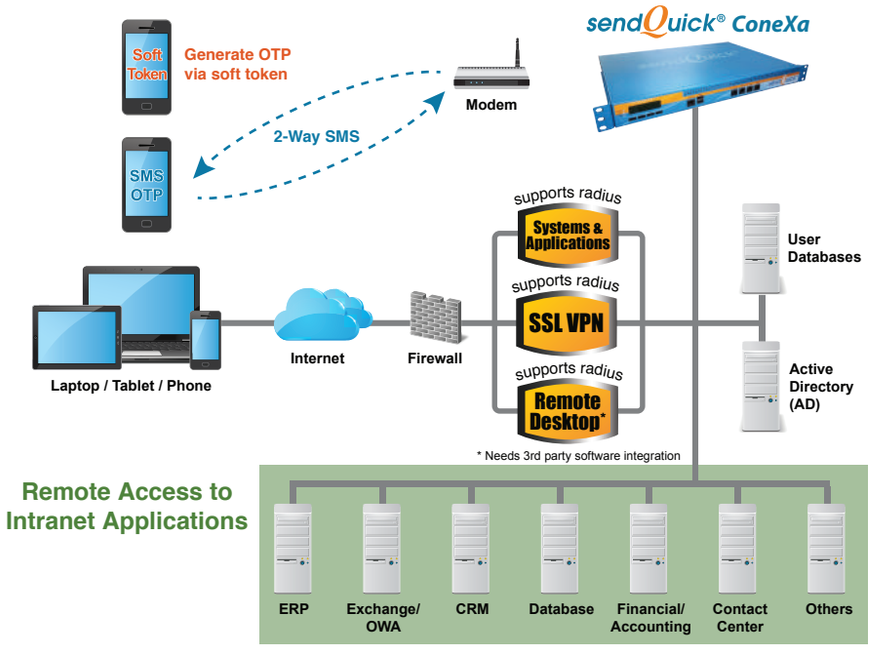
- Easy deployment with SMS OTP, Mobile Soft Token, and Email OTP
- Flexible 2-factor authentication for all usage scenarios
- Integrates to local/external databases or Microsoft Active Directory
- Supports all RADIUS based SSL VPN

With the advent of mobile technology and greater connectivity, it is very commonplace to see a large percentage of the workforce in any industry to be mobile. This mobility enables employees to work remotely away from the physical office for greater efficiency.

However, with greater mobility, comes an even bigger issue – security. The increase in cyberattacks on the organisation's IT network has highlighted the need for companies to secure the remote access for their staff and customers. Today, most companies use either SSL VPN or IPSec to secure the remote access. However, this does not address the authenticity of the remote users. 2-factor authentication (2FA) is an industry accepted solution for remote user authentication.

There are various types of 2FA solutions in the marketplace. Today, mobile phones are ubiquitous and provide an easy and low-cost method to implement 2FA. The widely popular SMS OTP, as well as, OTP generated through soft token (smartphones) can be easily delivered on all mobile phones, making 2FA implementation effortless for companies. sendQuick Conexa is the ideal solution for all companies seeking low cost and seamless way to implement 2FA. It has a built-in SMS OTP, Soft Token and Email OTP with Authentication and Authorisation (AA) capability, Radius server and an SMS transmission engine, all in a single appliance. sendQuick Conexa fulfills all the 2FA requirements of organisations and easily integrates with the existing enterprise network management system.

With the growing popularity of instant messengers for business communication, sendQuick now provides the option to integrate with social messengers including Facebook, Slack, WeChat, LINE, Viber and Telegram. Companies can send messages to end users using SMS, Email and Instant Messengers improving internal workflow and boosting productivity.



KEY FEATURES

- All-in-one appliance for 2-factor authentication using SMS OTP, Email OTP & Soft Token
- Supports multiple SSL VPN's for multiple remote access authentication
- Supports multiple authentication types (Challenge/Response, Single Sign-On, Single Page Token)
- Able to work with most* SSL VPN solutions
- OTP Characteristics:
  - 4-10 characters
  - Customizable User Message
  - Configurable OTP expiry time (minutes)
- Supports SMS OTP & Soft Token
- Scalable to support up to 32 modems
- Secure and does not depend on external or 3rd party networks
- Able to work with most** mobile networks (GSM, CDMA, 3G, 4G)
- Easy to implement system (plug & play)
- Low maintenance server
- Option for RAID and High Availability (HA) for zero down-time implementation
- Integration with instant messaging applications - Facebook, Slack, WeChat, LINE, Viber, Telegram (Optional)

*server dependent
**network dependent

sendQuick ConeXa 100

Unlimited SMS OTP, up to 100 Soft Token users
(supports single AD for authentication)

sendQuick ConeXa 300

Unlimited Soft Token & SMS OTP
(supports multiple AD for authentication)

BENEFITS OF SMS OTP & SOFT TOKEN

- No hard token required when using SMS OTP & Soft Token
- Easy deployment as everyone owns a mobile phone
- Low maintenance and support cost for companies
- Soft Token is immune to latency, network coverage, and delivery issues
- Convenient, easy to use and affordable
- Industry accepted solution for secure remote access

REMOTE ACCESS APPLICATIONS SUPPORTED

- RADIUS-based applications
- Checkpoint SSL VPN
- Cisco SSL VPN
- Juniper SSL VPN
- F5 SSL VPN
- SonicWall VPN / Avantail SSL VPN
- Citrix Netscaler
- VMWare View
- Windows Login
- Palo Alto SSL VPN

DATABASE SUPPORTED

- MySQL
- SQL Server
- PostGreSQL
- Oracle
- RADIUS
- Microsoft Active Directory (AD)
- LDAP

SOFT TOKEN SUPPORTED

- iOS - Google Authenticator
  - Free OTP
- Android - Free OTP

Authorised Distributor/Reseller

2-Factor Authentication Using SMS One Time Password & Soft Token

HARDWARE SPECIFICATIONS

sendQuick ConeXa 100

- Intel® CPU
- Hardened Linux OS
- 4GB RAM
- 500GB HDD
- 1U rack mountable [432(W) x 275(D) x 43(H) mm]
- 4 x 10/100/1000BT NIC card
- 2G/3G modem with WCDMA 850/1900/2100 Mhz
- Estimated weight: 4.3kg
- 4 x USB, 1 x RS232, 1 x VGA
- Certification: CE, FCC, UL RoHS

sendQuick ConeXa 300

- Intel® CPU
- 4GB RAM
- 500GB HDD
- 1U rack mountable [432(W) x 305(D) x 43(H) mm]
- 4 x 10/100/1000BT NIC card
- 2G/3G modem with WCDMA 850/1900/2100 Mhz
- Estimated weight: 5.5kg
- 6 x USB, 1 x RS232, 1 x VGA
- Certification: CE, FCC, UL RoHS

SOFTWARE SPECIFICATIONS

- All software (Linux, PostgreSQL, Web server, Email, FreeRADIUS) pre-installed

VM

- 2 Core CPU
- 4GB RAM
- 250GB HDD

TALARIAX
simplify mobility

+65 6280 2881
info@talariax.com
www.talariax.com
www.facebook.com/sendQuick
www.linkedin.com/talariax-pte-ltd
76 Playfair Road #08-01 Singapore 367996

Copyright © 2002-2017 TalariaX Pte Ltd. All Rights Reserved. sendQuick product name is a registered trademark of TalariaX Pte Ltd, a company incorporated in the Republic of Singapore. Pentium and Celeron are service names, trademarks or registered trademarks owned by their respective owners. Microsoft, Microsoft Exchange Microsoft Outlook, Outlook, Outlook 2007 are registered tradenames and trademarks of Microsoft Corporation. IBM, Lotus, Lotus Notes, Domino are registered tradenames and trademarks of IBM Corporation. All other trademarks mentioned in this document are the property of their respective owners.