sendQuick® ConeXa

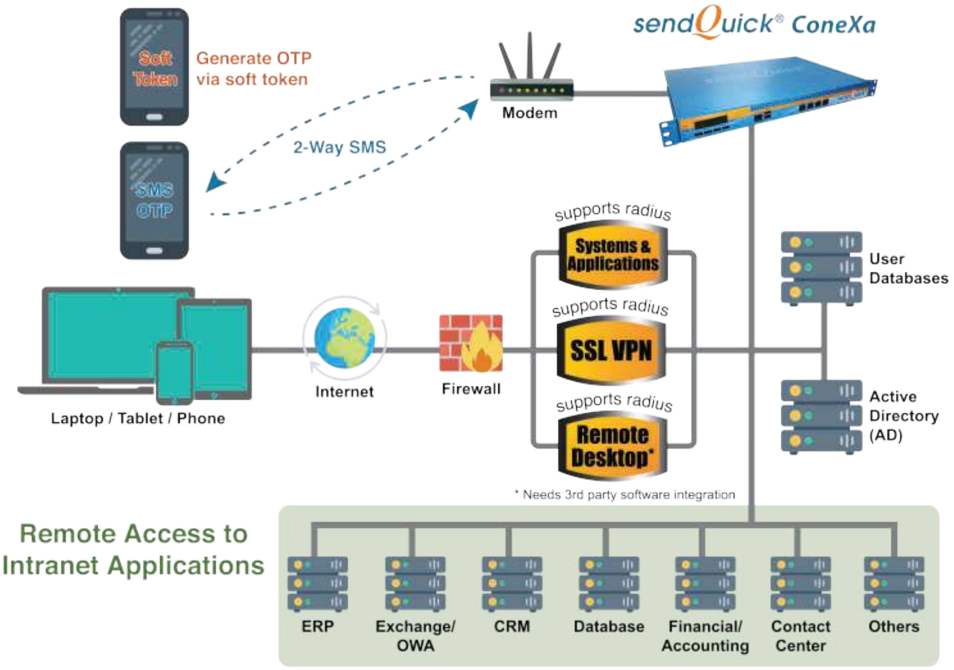
Secure Remote Access for Staff and Customers

- 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.



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 GSM 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 Messenger, Slack, WeChat, LINE, Viber, Telegram (Optional)

*server dependent
**network dependent