



Remo for Business

Security Overview

"Small-to-mid sized businesses increasingly have enterprise-grade needs, but typically fly well under the IT big guns' radar. Solutions like Remoba's Remo for Business allow operators to bring simple, secure and affordable wireless email/PIM solutions to this critically underserved segment."

Cliff Raskind,
Director of Wireless Enterprise Strategies
Strategy Analytics

Remo Security Overview

Remoba ensures that the services we provide meet the most stringent security requirements of enterprises so they can use the service effectively, routinely and without hesitation. Data security is the highest priority in the design, deployment and maintenance of our network, platform and services.

To ensure that critical information is protected from unauthorized users, Remo has been designed with a variety of security features. See Figure 1 for overall product architecture.

Remo takes advantage of the security provided by the device, corporate firewalls, Email and/or LDAP servers, and industry standard cryptographic protocols to provide a robust secure solution to a company's wireless data needs.

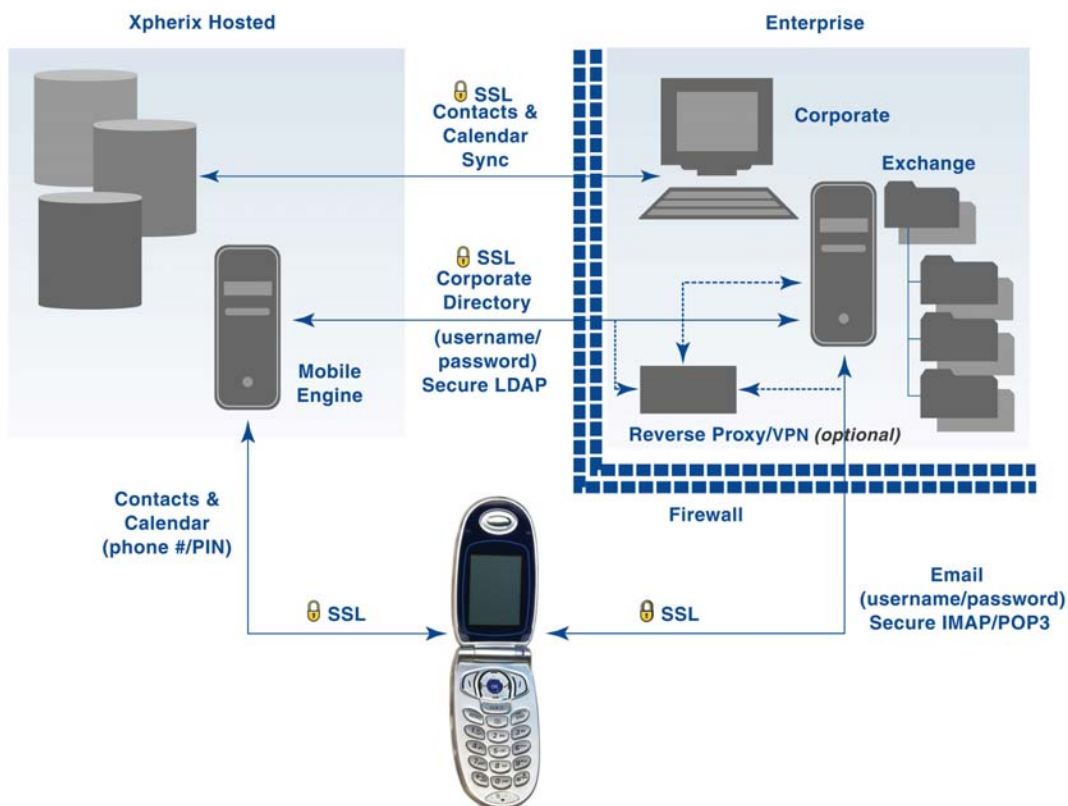


Figure 1. Overall product architecture.



Device Security

When a user exits Remo none of the Email is stored on the device, preventing a lost device from revealing important company secrets. The devices have a built-in security feature that allows users to password protect the device to prevent unauthorized use of any type.

SSL (Secure Socket Layer):

When Remo is configured to use security, no user data is transmitted until a secure connection has been established. Remo uses the SSL (Secure Sockets Layer) protocol to transmit data securely. SSL is the industry standard for transmitting sensitive information, like credit card numbers, over the Internet. SSL is a protocol that provides server authentication, data encryption and message integrity. With SSL security implemented, communications are transmitted in encrypted form between the BREW client and server. Only once the SSL connection has been established are the username and password transmitted to the server. Once the user has logged in, data can be securely transferred. Remo supports 128 bit SSL encryption.

IP Filtering:

The corporate network can be configured to reject requests to access Email or LDAP data based on the address of the device making the request. Remo receives its IP address from the wireless carrier out of a fixed pool of available IP addresses. By knowing the addresses that are available in this pool, a company can choose to allow access to addresses that were assigned by the carrier and reject other addresses from the Internet.

SSL VPN (Virtual Private Network):

Large corporate customers may choose to set up an SSL VPN (Virtual Private Network). SSL VPN devices are available from a variety of manufactures and move the burden of encryption from the Email/LDAP server to the VPN device. Any SSL VPN that allows SSL client access to IMAP, POP3, and SMTP services on their native ports should interoperate with Remo.

Additional Security Configuration Options:

Small companies may choose a configuration where Remo operates with a direct, user-defined IMAP/POP3 port connection through their firewall to Email. Similarly, corporate directory authentication and lookup is processed through a user-defined LDAP port. See Figure 2.

Medium to large companies may choose a configuration where Remo traffic and data requests redirect to a proxy server. Connection to the proxy server is through user-defined IMAP/POP3 and LDAP ports and the enterprise can choose which ports connect from the proxy server to the corporate servers. See Figure 2.

Large, national companies may choose a configuration where Remo traffic and data requests redirect to a proxy server that is connected to several, distributed servers. In this configuration, Remo connects to the proxy server via user-defined IMAP/POP3 ports and the enterprise chooses which ports connect from the proxy server to the Email servers. Additionally, corporate directory authentication and lookup can be handled from the proxy server directly to the correct Email server for global Address Book lookup. See Figure 2.



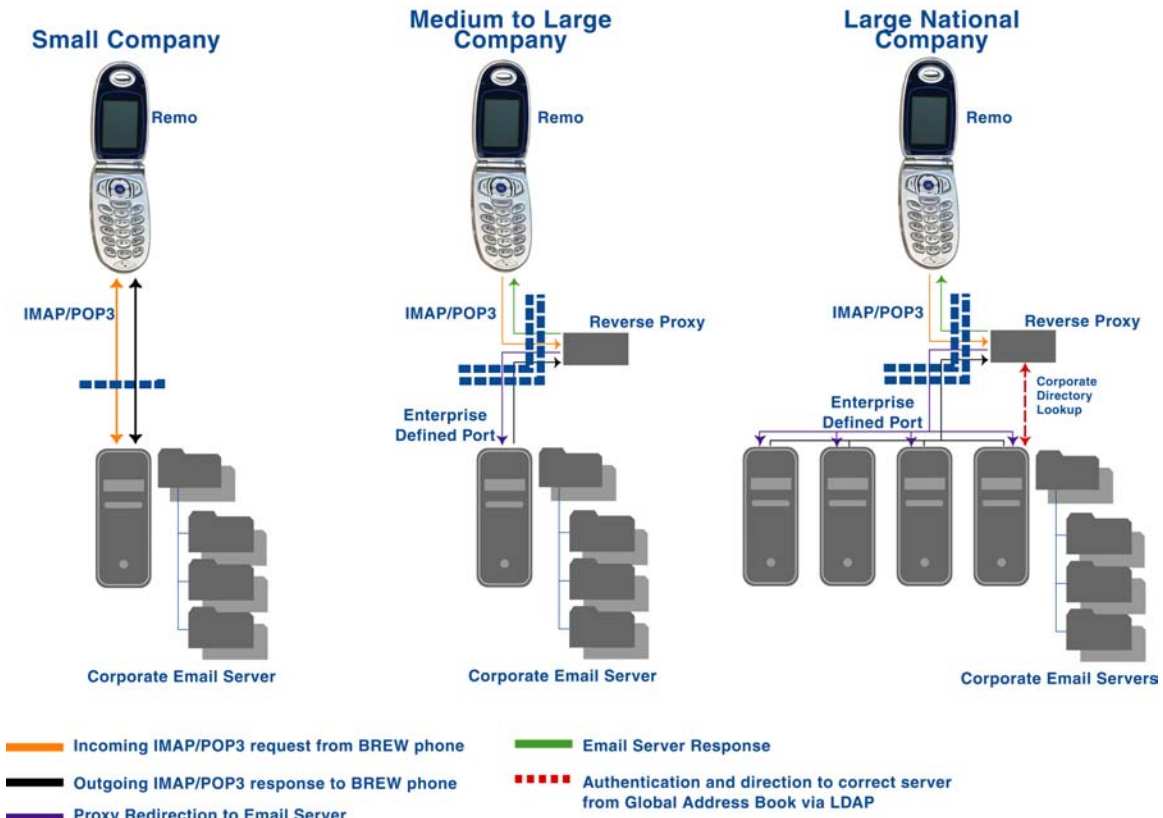


Figure 2. Additional security configuration options.

Remoba Data Center and Back Office Security

- ❑ Remoba servers and other equipment are housed in secure racks and cages at a leading co-location facility.
- ❑ Biometric scanners, electronic key readers, and security guards control access to this facility.
- ❑ Remoba employees must present valid identification before they are given access and are escorted to the Remoba co-location by facility personnel.
- ❑ As an added measure, closed-circuit surveillance cameras monitor the interior and exterior areas of the facility.
- ❑ All Remoba office facilities employ controlled access mechanisms and entry requires a valid key card.
- ❑ Remoba offices are also monitored by dedicated security services companies.

Firewalls

- ❑ Remoba utilizes firewalls to protect all of our networks. Our office firewalls are used to control and grant access to specific internal resources and to protect these resources from external threats.
- ❑ Two layers of firewalls are installed at our co-located facility to ensure the integrity of customer data.

End-User Access

- ❑ Secure access to personal data is a fundamental requirement for any company offering Web services.
- ❑ Remoba has taken specific measures to ensure secure access to customer data.
- ❑ Individual usernames and passwords are required to access the application.
- ❑ Administrative and call-center agent access, similarly, are password controlled.
- ❑ Additionally, the Remoba database is designed such that one enterprise or its administrator cannot access another enterprise's data.

Encryption

- ❑ Remoba utilizes 128 bit SSL encryption for all PC communication to our servers.

Administration

- ❑ The administration of Remoba services is performed by a limited number of employees.
- ❑ Pre-employment screening practices are well documented and followed for all personnel.
- ❑ System administration passwords are periodically changed.

Backup Measures

- ❑ Remoba follows industry best practices in backing up customer data to ensure that all data is quickly recoverable should a catastrophic event occur.
- ❑ Backup media is stored off-site in a secured location(s).
- ❑ Backup and disaster recovery procedures are available for review by prospective customers.

Security Audits

- ❑ Remoba contracts with an independent firm to periodically audit network and application security.
- ❑ We continue to tighten our security practices as recommended by the auditors.

www.remomobile.com