

Security OneBridge[®] Mobile Groupware

technical brief

In this growing mobile and wireless world, anytime, anywhere access to corporate data is becoming a necessity. Mobile workers are demanding access to mission-critical data in order to remain competitive in the market and efficient in their jobs. Now that corporate data can be accessed remotely and from a variety of devices, there are even more security challenges for the IT team. IT administrators must create and maintain corporate standards for secure mobile device access to corporate information.

OneBridge Mobile Groupware (formerly known as XTNDConnect Server) offers a variety of features to securely extend e-mail enterprise applications to mobile devices in both wireless and wired environments. OneBridge offers a comprehensive solution for IT administrators to securely manage a variety of mobile devices under a single server. With OneBridge mobile users can more securely connect their devices from inside the enterprise and outside the firewall. The OneBridge security features can be broadly classified into three categories:

- 1. infrastructure security.
- 2. data security.
- 3. device security.

infrastructure security

OneBridge is comprised of various components designed to provide a modular and distributed means for secure deployment.

- DMZ proxy—An application-specific HTTP proxy at the DMZ level
- OneBridge Sync Service—Synchronization and device management services along with authentication of mobile devices. This server is typically installed inside the firewall
- OneBridge desktop connector—Provides serial and USB connectivity to mobile devices

dmz proxy

The OneBridge DMZ proxy acts as an application-specific HTTP proxy. Through a userdefined HTTP or HTTPS port, this proxy perform the necessary security and packet validation checks on connections from mobile devices before letting the incoming packet data through to OneBridge. This allows administrators to set up various types of filters to secure traffic through the firewall. The DMZ proxy has its own public key and private key pair used to decrypt the message header (this header has the session ID information and packet key). Additionally, all data in the packet is encrypted with an AES

OneBridge Mobile Groupware formerly known as XTNDConnect Server



OneBridge

Mobile Groupware

offers a variety

of features to

securely extend

enterprise e-mail

applications

to mobile and

wireless devices.





- Acts as an application-specific HTTP proxy at DMZ
- Validates incoming packet before allowing traffic through the firewall
- Uses HTTP(S) to communicate with OneBridge
- Does not decrypt the data portion of the packet

authentication

With the DMZ proxy, OneBridge can be securely deployed inside the firewall. OneBridge also uses HTTP(S) to act as its transport protocol to communicate with rest of the OneBridge components. OneBridge has a two-tier authentication mechanism. The first tier is with the Windows NT/Active



Extended

directory, Notes, Database, RADIUS and SecureID. This tier is used to authenticate the user credentials and obtain the necessary group information to determine the actions that a user is authorized to run on OneBridge. The second tier provides authentication against groupware and database servers for synchronization. This two-tier authentication enables secure deployment of OneBridge and adapters at different locations.

- Uses HTTP(S) to communicate between DMZ proxy and adapters
- Deployed securely inside the firewall
- · Provides two-tier authentication to validate user credentials
- First tier: Windows NT, Notes, Database, RADIUS and SecureID

Live Connect

even with an always-on and automatic delivery of information through Live Connect technology, security is never compromised with OneBridge Mobile Groupware. IT can utilize the existing security policies in place to provide wireless"push" as the product supports most corporate authentication schemes like Windows ADS, RADIUS, RSA SECURE ID, etc. IT can also configure how long an authenticated session can last before users have to re-enter their credentials.

- Does not require saving password
- Support RSA secure ID (HW/SW tokens)
- · Administration configurable persisted sessions
- User authentication required for automatic delivery

OneBridge desktop connector

The OneBridge desktop connector serves as a desktop proxy and provides an easy way for users to connect their devices to OneBridge from their Windows desktops and laptop machines without the need for third-party software. This significantly reduces any security breaches because the access and management of information is controlled by the IT Administrator rather than the mobile user. While device users can use any desktop connector to connect back to OneBridge, they are still required to input their credentials on the device to connect to OneBridge.

- Serves as a desktop proxy for mobile devices
- Eliminates the need for varying third-party desktop sync software
- User credentials are still required for connecting with OneBridge





Extended Systems®

data security

OneBridge provides end-to-end data security by encrypting the data between the server and the device. In addition, it does not stage or store data anywhere within OneBridge other than in the original data source. For encryption, OneBridge uses a combination of RSA for key exchange, and AES for encrypting the data. This combination of asymmetric and symmetric algorithms provides the best security and performance. Because public-key cryptography is more computationally expensive than symmetric cryptography, public-key cryptography will be used to encode a secret key for symmetric cryptography; then the system falls back on a faster symmetric cryptography system. With 128-bit encryption AES key, a widely embraced stream cipher, performs extremely well on mobile devices with limited processing power.

- End-to-end data security with 1024-bit RSA-OAEP key exchange and 128-bit AES-CFB symmetrical encryption
- Does not store or stage data outside of the data sources
- · Sync engine uses a change-log-based algorithm, which does not store any data

device security

Device security essentially refers to securing the data within the device in the event the device is lost or stolen. OneBridge uses a variety of methods enabling IT administrators to protect data on devices. The administrator has the capability to force the device user to enter his credentials each time he/she connects to the server. Even in cases where the user is allowed to store credentials on the device, these credentials are encrypted with the server's public key thereby making it virtually impossible for unauthorized access. The IT administrator also can force the power-on password to be enabled. This requires users to key in their password to access their device.

- OneBridge administrators can force users to enter credentials each time the user connects
- All credential information (if allowed to be stored on the device) is encrypted with the server's public key
- OneBridge administrators can enforce power-on passwords on all devices (Palm, CE, Symbian, RIM)

conclusion

With the emerging "always-on" wireless devices and networks, it will be increasingly challenging to control devices and their access to enterprise applications. OneBridge provides IT an excellent opportunity to proactively control these devices by putting the right infrastructure in place to effectively monitor mobile usage without any user initiation. OneBridge research and development teams continue to actively work with these new technologies to ensure secure mobile device data access and synchronization

Extended Systems provides the expertise, strategy and solutions to help enterprise organizations realize their business goals through mobile technology. The company's software and services portfolio includes mobile data management solutions; mobile applications for sales, service and pharmaceutical professionals; mobile application development tools and services; client/server database management system; and Bluetooth and IrDA wireless connectivity software.

All trademarks and registered trademarks are the properties of their respective companies. Information subject to change without notice.

OneBridge Mobile Groupware formerly known as XTNDConnect Server

United States Boise Headquarters

5777 North Meeker Avenue Boise, Idaho 83713 Tel: (800) 235-7576 Tel: (208) 322-7800 info@extendedsystems.com

Benelux

IJsselsingel 42 5215 CM 's-Hertogenbosch Tel: +31 (0)73 - 623 5359 info@extendedsystems.nl

Canada

175 Bloor Street East North Tower, Suite 1200 Toronto, Ontario M4W 3R8 Tel: (416) 214-9711 info@extendedsystems.com

France

Parc des Erables, Bâtement 4 66 route de Sartrouville 78230 LE PECQ cedex Tel: +33 01 30 09 23 23 info@extendedsystems.fr

Germany

Schwarzwaldstr. 99 71083 Herrenberg Tel: +49 (0) 7032 / 798 - 0 info@extendedsystems.de

United Kingdom

7-8 Portland Square Bristol BS2 8SN United Kingdom Tel: +44 (0)117 901 5000 info@extendedsystems.co.uk

For information and a list of distributors visit our web site: **www.extendedsystems.com**

