

iAnywhere® Mobile Office

DATASHEET

FEATURES AT A GLANCE

- Extends Lotus Domino and Microsoft Exchange email & PIM data to wireless devices
- Supports iPhone, Nokia, Sony Ericsson and Windows Mobile operating systems
- Enables users to securely complete business workflow processes
- Enables device security with data encryption, lock-down and remote wipe
- Provides over-the-air provisioning and unattended client deployment

iAnywhere Mobile Office provides wireless email and the ability to complete business workflow securely on a variety of mobile devices.

WIRELESS EMAIL

Operating on the networks of all major carriers worldwide, iAnywhere Mobile Office extends email and PIM data to the latest Windows Mobile and Symbian powered devices, as well as iPhone.

- Usability – Integrated into the native applications available on supported devices, iAnywhere Mobile Office provides instant email delivery and rich PIM functionalities without requiring any special software knowledge. Highly optimized protocols ensure minimal impact to battery life.
- Administration – Over-the-air client provisioning and deployment, automatic unattended software upgrades and intuitive configuration tools make day-to-day operation easy. iAnywhere Mobile Office allows the use of standard service monitoring tools.
- Low cost of ownership – Optimized protocols minimize wireless air time requirements and data transfer costs. The use of standards for service monitoring and the automatic client upgrades reduce support costs. The iAnywhere Mobile Office architecture allows for extended scalability to reduce hardware requirements for globally distributed enterprise deployments.

SECURE ENTERPRISE APPROACH FOR IPHONE

The iPhone is penetrating the enterprise and causing IT administrators to rethink their mobile security policies. Many companies are treating the iPhone as “personal use” devices, likely being purchased by individual users especially in the current economic times. This creates the following challenges:

- How to “secure” the enterprise data without controlling the device
- In the event that a company needs to remove the “enterprise” data on a user’s iPhone, IT needs to be able to do so without affecting the user’s “personal” data and applications on that same iPhone

Sybase addresses these challenges by providing a unique enterprise sandbox approach to support the iPhone in the enterprise. The iAnywhere Mobile Office solution for iPhone ensures that the enterprise data on the device is protected while not affecting the user’s experience for non-enterprise usage of the device. It allows IT administrators to enforce security policies, including an application-specific password, on-device encryption of all the enterprise data at an operating system level and kill pill capabilities that only removes the enterprise data on the device.



In addition, iAnywhere Mobile Office integrates with Apple's push notification service to instantly notify users of new data, even when they are outside the application. Administrators can replicate the same security profiles for other devices, specifically for the iPhone, with the ability to control how many digits are required for the password.

BUSINESS WORKFLOW

iAnywhere Mobile Office provides extended functionalities to enable business and workflow processes on mobile devices. Users can take action from mobile devices to initiate or complete business processes, such as submission and approval of expense reports, human resources requisitions, travel requests and purchase orders. iAnywhere Mobile Office leverages existing enterprise services using Web Services and other technologies for seamless integration and speeds development with business process workflows – reducing the cost and effort necessary to mobilize business processes.

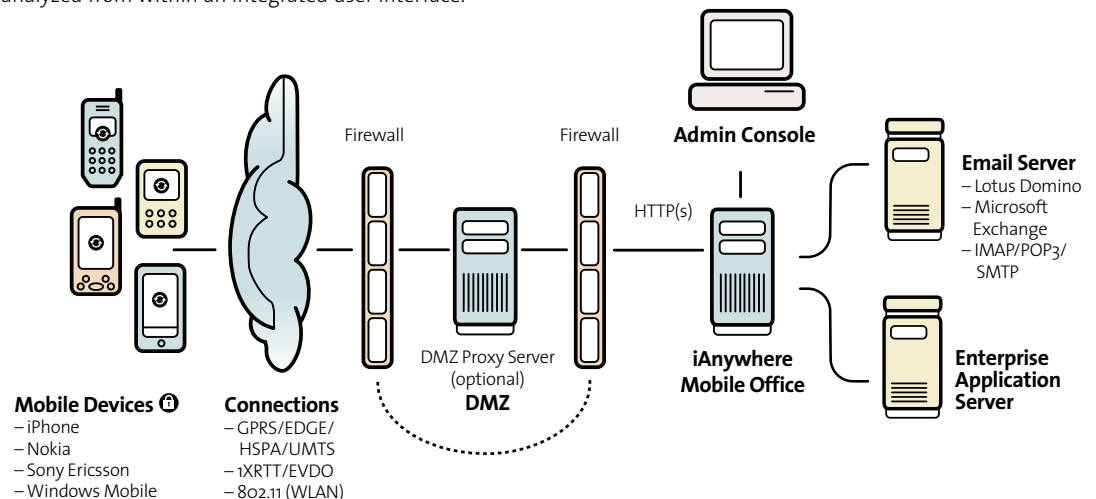
SECURITY

iAnywhere Mobile Office provides a DMZ component that enables iAnywhere's unique outbound connection model which adds an additional layer of security for connecting mobile devices. Enterprises do not need to open inbound communication ports to their messaging infrastructure — all mobile device connections end within the enterprise DMZ.

On the device, iAnywhere Mobile Office provides integrated client security, powered by Sybase's Afaria Security Manager technology. This includes on device password enforcement, data encryption, device lock-down and remote wipe capabilities to secure data if a device is lost or stolen.

ADMINISTRATION

iAnywhere Mobile Office provides an administration console that can be used from any workstation or laptop. The administration console utilizes the secure iAnywhere Mobile Office protocol and can be configured to connect to multiple servers to simplify the administration of multi-server deployments. In addition, all major administrative tasks can also be performed through a set of available Web Services; these can be used to allow the integration with existing enterprise management portals. The iAnywhere Mobile Office administration console also comes with an extensive set of diagnostic tools. Tracking of device and server events can be managed and captured data can be analyzed from within an integrated user interface.



ABOUT SYBASE

Sybase enables success at the front lines of business. Businesses around the world rely on Sybase's expertise as the largest independent mobile software provider.

For more information, please contact Sybase via email at: Contact_Us@ianywhere.com or via phone at 800-8SYBASE.

ENTERPRISE IT

Server Requirements

- Intel Pentium 4, 2 GHz or higher
- 2 GB RAM minimum – recommend 2 GB for up to 500 users, 4 GB for 500-1000 users
- 100 Mbit NIC minimum
- Microsoft Windows 2003 Server
- Lotus Domino: 7.x or greater
- Microsoft Exchange: MAPI/CDO 1.2.1

Communications Security

- Device ID-based white-listing
- 128-bit AES/1024-bit RSA algorithm for the best combination of security and performance
- RSA Security BSAFE Crypto-C Micro Edition – FIPS 140-2 Level 1 compliant

Administration

- Remote multi-server administration console
- Extensive set of administration Web Services
- Template-based individual user settings
- Roaming control for device connections

Groupware System

- IBM Lotus Domino R6.5/R7/R8/R8.5
- Microsoft Exchange 2003 Service Pack 2 and 2007
- IMAP/POP3/SMTP

Provisioning

- Allows SMS-based client provisioning and configuration seeding
- Provides over-the-air (OTA) client deployment capabilities

Device Security

- Provides password policies, on-device encryption, device lock-down and device wipe
- Allows users to receive emails on an encrypted and locked device

Business Workflow

- Provides business Workflow framework
- Provides SDK for enabling business processes
- Allows secure mobilizing of enterprise services using Web Services and other technologies

ENTERPRISE USER

Rich User Experience

- Delivers email and PIM data within seconds
- Minimal impact to device battery life

Email Support

- Write, send, receive and delete email
- Send, receive and view file attachments
- Subscribe to subfolders on your mobile device
- Directly dial a phone number from inside the text of an email

Calendar Support

- View calendar in day, week and month views
- Accept and decline meeting requests
- Support for repeating calendar entries and exceptions
- Schedule meetings, add, modify and delete calendar items

Address Book Support

- Add, modify and delete personal contacts

Task and Journal Support

- Add, modify and delete To Do Items
- Add, modify and delete Journal entries

Corporate Directory

- Search online for colleague's contact information within the corporate address book
- Provides seamless integration within the email and contact applications

Mobile Device Support

- iPhone
- Nokia Series 60 3rd and 5th Editions
- Sony Ericsson UIQ 3.0
- Windows Mobile 5 or greater (Professional and Standard)

Connectivity Options

- GPRS/EDGE/HSDPA/UMTS
- 1xRTT/EVDO
- 802.11 (WLAN)

Client Localization

- English
- Simplified Chinese
- Japanese
- French
- German