GO! Enterprise™ Office

Achieve Greater Employee Productivity & Collaboration ...while **Protecting** Critical Business Data

YOUR Enterprise GO!es MOBILE

The Challenge

Today's employees demand mobile access to office information in order to maximize their productivity and they expect that enterprise collaboration and communication tools should be simple and mobile-enabled just like their favorite social network. Despite "consumerization" of IT which is actually driving these requests, enterprises cannot rely on consumer-based mobility solutions because they often lack elementary enterprise features like encryption, policy-based access control, user provisioning and central management. Moreover, traditional IT systems are usually inadequate for enterprise mobility solutions because they do not cope with the proliferation of mobile device platforms and the respective security and management challenges.

The Solution

GO!Enterprise Office is a mobile office productivity solution which enables secure and controlled access to enterprise information like email, files, contacts, calendar, tasks and notes from any mobile device. Employees can securely access the corporate intranet and any other internal web application through the secure mobile browser of **GO!Enterprise Office**. Additionally, they can collaborate while on the go, using the embedded enterprise instant messaging functionality for one-to-one chatting and group discussions. **GO!Enterprise Office** is ideally suited for the implementation of Bring Your Own Device (BYOD) mobility strategies.

GLOBO™

Push Email & PIM

GO!Enterprise Office provides secure access to enterprise email accounts from any mobile device. Mobile employees can view, create, forward, delete, search or reply to emails as if they were in the office and they can also view attachments or add attachments to outgoing emails. Additionally, **GO!Enterprise Office** provides secure mobile access to personal information management (PIM) data like contacts, calendar, tasks and notes. All email and PIM updates are synchronized using bi-directional push technology and the user is alerted via push notifications and badges on the icons of the respective GO!Apps. **GO!Enterprise Office** incorporates a number of technologies like data compression and on-demand downloading that help minimize over-the-air bandwidth usage and hence the related costs. It can seamlessly synchronize with Microsoft Exchange, Lotus Domino or Office 365 and can be easily extended to support other on-site or cloud-based email & PIM solutions.

File Access & Sharing

GO!Enterprise Office provides easy and secure access to enterprise file servers from any mobile device. Mobile employees can copy, rename or delete files and folders according to the policies defined in the enterprise's active directory. Searching for specific files or folders is a snap and attaching selected files to emails is one tap away. Furthermore, it is possible to preview typical office files like Excel, Word and PowerPoint from any mobile device without the need for additional software and with minimum over-the-air bandwidth consumption. The GO!Files app also enables downloading and storing of corporate files within the secure mobile client of **GO!Enterprise Office**. Effectively, it eliminates the need for local or cloud-based file syncing which can pose serious threats to information security.

Secure Document Editing

GO!Enterprise Office features an add-on for secure document editing, based on Picsel's Smart Office technology. Users can view, edit, annotate and print documents on their smartphones or tablets from within the secure mobile client of GO!Enterprise Office. Supported document types include Word, Excel, PowerPoint, PDF and many others. **Smart Office** is a unique mobile document editing solution which maintains the security of corporate documents throughout the viewing and editing lifecycle:

- Files are loaded and saved between Smart Office and the secure mobile client of **GO!Enterprise Office** through an in-memory API. Confidential content is never written to persistent storage outside of the secure mobile client.
- **Smart Office** runs as a component within the secure mobile client, and does not require launching external apps.

These measures ensure that even malware running on a compromised device cannot access private data.

KEY BENEFITS

- **Comprehensive set of mobile office productivity apps for all mobile platforms**
- **Secure container separates personal and enterprise data on mobile devices**
- **Ideally suited for BYOD initiatives**
- **Secure mobile access to files on company servers and workstations**
- **End-to-end encryption**
- **Centralized management of users, apps and mobile clients**
- **Easily extensible with custom add-on apps built with GO!Development Studio**

Supported platforms:

android | iOS | BlackBerry | Windows Phone | Windows 8

Enterprise Instant Messaging

GO!Enterprise Office includes a flexible instant messaging infrastructure which can be leveraged to enhance enterprise collaboration and speed up information sharing. Using **GO!Enterprise Office**, mobile employees can securely exchange one-to-one instant messages and set-up their own public or private groups per department or project team where they can post status updates, news or other useful information. Identifying which users are "online" is very easy, as well as finding older messages and continuing discussions.

Secure Browser

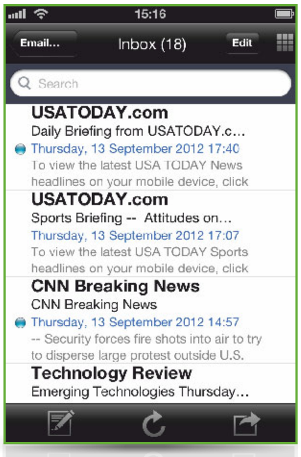
GO!Enterprise Office enables safe remote access to the corporate intranet or any other internal web-based application through a secure mobile browser. The browser leverages a proprietary secure browsing gateway which resides behind the corporate firewall and is only accessible by authenticated employees using the secure **GO!Enterprise Office** client. Enterprises can rely on the secure browsing infrastructure of **GO!Enterprise Office** to rapidly mobilize corporate web-based applications and eliminate the need for costly mobile VPNs and virtualization platforms.

MANAGEMENT PLATFORM INCLUDED

- **Web-based management console**
- **User and device provisioning is centralized and fully automated**
- **Access is provided only to authenticated users with authorized devices**
- **Custom add-on apps can be centrally distributed and updated**
- **Security policies can be enforced per user, app, device, network or connection type**
- **Remote lock & wipe can be applied on enterprise apps and data only**
- **All mobile apps and their data reside in a secure managed container.**
- **Logging and geo-tracking of user activity**

Secure Camera

GO!Enterprise Office leverages the embedded camera of the mobile device, to enhance overall user experience. Using the GO!Camera app, mobile employees can shoot photos or videos which are automatically stored in the secure mobile client of **GO!Enterprise Office** and can be then attached to emails or securely uploaded to corporate file servers.



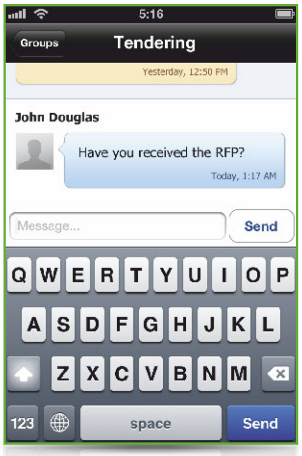
USATODAY.com
Daily Briefing from USATODAY.c...
Thursday, 13 September 2012 17:40
To view the latest USA TODAY News headlines on your mobile device, click

USATODAY.com
Sports Briefing -- Attitudes on...
Thursday, 13 September 2012 17:07
To view the latest USA TODAY Sports headlines on your mobile device, click

CNN Breaking News
CNN Breaking News
Thursday, 13 September 2012 14:57
-- Security forces fire shots into air to try to disperse large protest outside U.S.

Technology Review
Emerging Technologies Thursday...

Securely
check your **email**
on the go

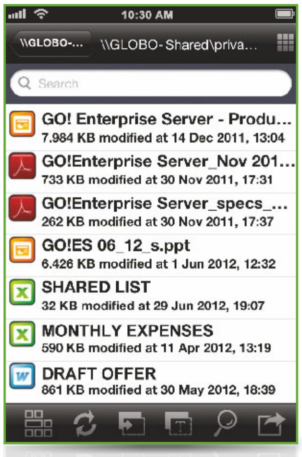


Yesterday, 12:50 PM

John Douglas
Have you received the RFP?
Today, 1:17 AM

Message...
Send

Send
instant messages
to your colleagues



GO! Enterprise Server - Produ...
7.984 KB modified at 14 Dec 2011, 13:04

GO!Enterprise Server_Nov 201...
733 KB modified at 30 Nov 2011, 17:31

GO!Enterprise Server_specs_...
262 KB modified at 30 Nov 2011, 17:37

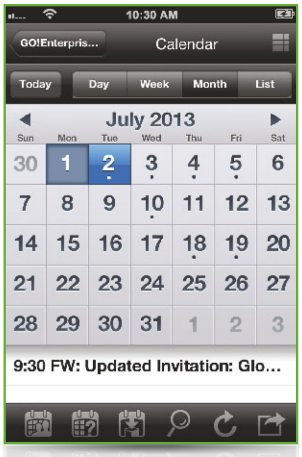
GO!ES 06_12_s.ppt
6.426 KB modified at 1 Jun 2012, 12:32

SHARED LIST
32 KB modified at 29 Jun 2012, 19:07

MONTHLY EXPENSES
590 KB modified at 11 Apr 2012, 13:19

DRAFT OFFER
861 KB modified at 30 May 2012, 18:39

Preview **documents**
on the company's
file server



July 2013

Sun	Mon	Tue	Wed	Thu	Fri	Sat
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3

9:30 FW: Updated Invitation: Glo...

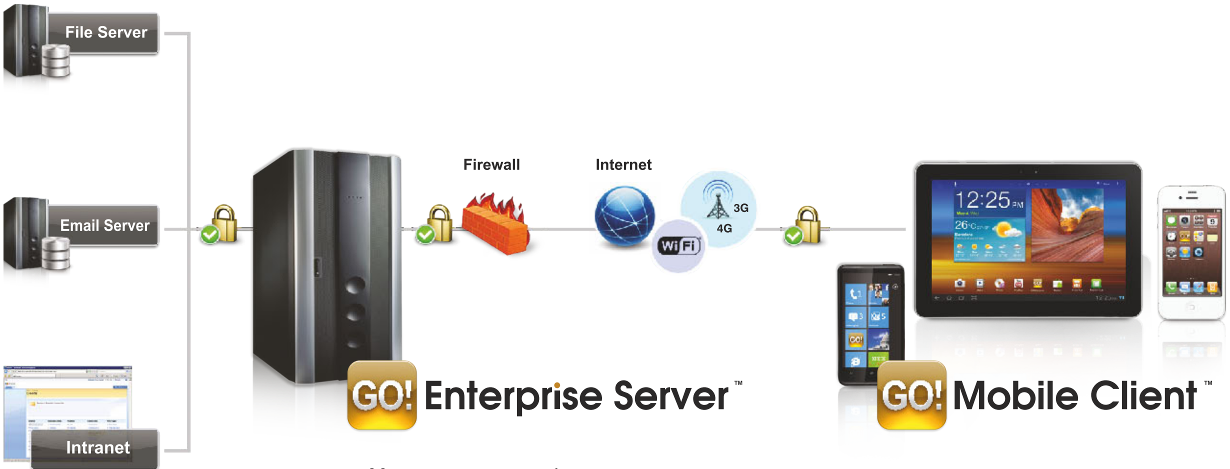
Check appointments
on your corporate
calendar

Bring Your Own Device

GO!Enterprise Office is ideal for the implementation of Bring Your Own Device (BYOD) strategies, since it allows employee-owned devices to access corporate office data in a secure and centrally controlled manner, without imposing limitations on personal applications and device configurations or on the use of personal data. This is made possible because **GO!Enterprise Office** is deployed to mobile devices via **GO!Mobile Client**, a secure native container which provides controlled access to GO!Apps and separates enterprise and personal data.

For the user, **GO!Mobile Client** is a mobile app with encrypted data, whereas for system administrators, it is a fully controlled environment with enterprise management features like logging, secure authentication and user management.

Typical GO!Enterprise Office Architecture



- Management console
- Data synchronization
- Access control & security
- GO! Enterprise™ Office back-end platform

Extend with GO!Enterprise Mobilizer

The functionality of **GO!Enterprise Office** is further extended with custom or 3rd-party packaged GO!Apps powered by **GO!Enterprise Mobilizer.** GO!Apps can provide secure and centrally controlled mobile access to any enterprise system such as ERP, CRM, ordering, billing, ticketing, etc. They are built with **GO!Development Studio**, a rapid cross-platform development environment. **GO!Enterprise Mobilizer** enables centralized distribution and enterprise-grade management of custom and 3rd-party packaged GO!Apps.

End-to-end Security

GO!Enterprise Office is part of the **GO!Enterprise** unified mobility platform which was designed from the ground up with security in mind. Thus, GO!Enterprise Office inherits a wealth of security features that minimize the risk of unauthorized access, data leakage and other security breaches.

Security Feature	Description
Gateway-based communication	**GO!Enterprise Office** mobile apps do not communicate directly with backend systems. Instead, all communication goes through **GO!Enterprise Server** which usually resides in the corporate DMZ and acts as a proxy for all communications requiring access to corporate email, collaboration and file servers. This architecture eliminates the need for costly mobile VPN solutions.
Encryption	**GO!Enterprise Server** provides end-to-end FIPS compliant encryption for corporate data. Data on the server component of the platform is protected using 3DES 192-bit encryption. Data sent over the air or at rest on the device is protected using AES 256-bit encryption. Data transmission can be further secured with the use of SSL encryption.
Authentication	Each user has to provide a username and a password in order to log in to **GO!Enterprise Office**. Authentication can be performed against LDAP, Active Directory or **GO!Enterprise Server**'s internal directory. **GO!Enterprise** can be extended to support third-party authentication services.
Client Certificates	**GO!Enterprise** provides built-in support for the creation, safe distribution and use of client certificates on mobile devices. Deployment of client certificates offers significant security advantages: ▪ Advanced two-factor authentication which requires a password and a certificate that is specific to the device used. ▪ Fully secure enrollment of mobile devices which includes the use of a one-time registration code before the secure transmission and installation of a client certificate. ▪ Extra security layer for access to **GO!Enterprise Server** which will additionally require a valid client certificate before accepting a properly formatted and encrypted request from an authenticated user.
Access Control Management	Access can be controlled from the **GO!Enterprise Administration** web console on the basis of user roles, connection types, IP addresses and devices: ▪ System administrators can assign access rights and permissions to user groups (managers, staff, etc.) and apply custom permissions to specific users. ▪ Access to specific applications can be granted according to the type of connection (Wi-Fi or cellular) or the network used. ▪ Access to specific applications can be granted to approved devices only or to specific device types. ▪ Access to the administration and GO!App deployment functionality of **GO!Enterprise Server** can be restricted to specific IP addresses.
Containerization	All GO!Apps, including those of **GO!Enterprise Office** are accessible via **GO!Mobile Client**, the secure native container which ensures separation of enterprise and personal data.
Mobile Data Leakage Prevention	**GO!Mobile Client** provides advanced protection against data leakage threats: ▪ Remote lock of the mobile client. ▪ Remote wipe of data and apps in the mobile client. ▪ Control of copy-paste from GO!Enterprise Office apps to third-party apps outside the secure container. ▪ Centrally-enforced client passcode. ▪ Automatic wipe after a period of inactivity or a number of false passcode entries.
Geo-tracking	**GO!Enterprise** supports automated location tracking of **GO!Mobile Clients**. Geo-tracking can be enforced as a security policy to specific users or groups and provide: ▪ The current location of lost or stolen devices. ▪ Geo-tagging information within user activity logs. ▪ Visual trail of the locations where a GO!Mobile Client was used for a specific number of days in the past. **GO!Enterprise** will also provide geo-fencing functionality which will allow an administrator to limit the availability or the functionality of mobile clients and apps within specific geographical areas.
Mobile Client Management	System administrators have full control over every **GO!Mobile Client** in order to: ▪ Wipe data remotely for lost devices ▪ Lock-down access from specific devices ▪ Update security policies and user access rights ▪ Enforce new application settings
Logging	**GO!Enterprise Server** provides extensive logs and log management functionality for tracking and monitoring unauthorized access in a secure and tamperproof environment.

GO! Enterprise™ Office

Achieve Greater Employee Productivity & Collaboration ...while **Protecting** Critical Business Data

System Requirements

Platform Component	Requirements
Server	▪ Intel® Pentium® IV, at least 2 GHz ▪ At least 4GB RAM ▪ MS Windows Server 2003, 2008 or 2012 ▪ Microsoft .NET framework 3.5 ▪ IIS 6.0 or later
Repository	MS SQL Server 2005, 2008 or 2012 (Standard, Enterprise or Express editions)
Mobile Client	Android, BlackBerry, iOS, Windows Phone, Windows 8/RT

Visit our site **globoplc.com** to learn more about **GO!Enterprise** and **GLOBO**'s mobility solutions.

New York
247 West 35th Street
NY 10001
Tel: +1 (646) 307 1614

San Jose
1054 South De Anza Blvd.
Suite 105, CA 95129
Tel: +1 (408) 777 7930

London
41 Lothbury
EC2R 7HG U.K.
Tel: +44 (0) 207 378 8828

Athens
67 E. Antistaseos Street
152 31 Halandri, Greece
Tel: +30 21 21 21 7000

GLOBO™

New York | San Jose | Ohio | London | Athens | Dubai | Limassol | Singapore
globoplc.com, **info@globoplc.com**