Good **for Government: iOS**

Protect and Manage U.S. Federal Government Data on the Most Popular Devices—iPhone, iPad, and iPod Touch

Good for Government helps IT administrators safely deploy and manage agency access on Apple's entire line of mobile devices.

The solution brings you and your IT department an efficient and cost-effective way to allow Federal government employees tremendous freedom of choice—as you also ensure secure access to the critical data they share with their constituents, vendors, and other agencies.

MILITARY-GRADE SECURITY

Designed specifically to meet the needs of the U.S. Department of Defense (DoD), Good for Government protects the confidentiality and integrity of sensitive information, including For Official Use Only (FOUO) and Sensitive But Unclassified (SBU) data. Our solution leverages FIPS-certified cryptographic libraries to encrypt government data over-the-air and at rest on the device.

All Good servers are deployed behind the firewall with a secure outbound connection using standard port 443. No inbound connections or firewall configuration changes are required.

To meet DoD Directive 8100.2 as well as Homeland Security Presidential Directive 12 (HSPD 12), Good for Government supports S/MIME and seamlessly integrates with National Security Agency (NSA)-approved Bluetooth Smartcard readers, providing the ability to sign, encrypt, and authenticate email messages while integrating with the DoD Global Directory Services (GDS) and Public Key Environment (PKE), as well as the ability to leverage DoD issued Common Access Cards[1] on an iOS device.

CONTAINING AGENCY DATA

Good for Government provides a secure, "contained" environment by encrypting data from the server and restricting its access within a hardened application on iOS devices.

All agency data, including FOUO/SBU data, is only stored within the Good application and is completely isolated from any personal data that may reside in other applications on the device. Good's container-based approach prevents any data from being leaked to other non-secure applications.

Inside the Good application, employees using iOS mobile devices can securely retrieve email; save, send, and manage files; and manage contacts and calender entries as if they were using Outlook on a desktop. They can also access critical agency resources behind the firewall, such as Intranets or other Web-enabled applications[2], with a secure browser.

ALWAYS AHEAD OF THE MARKET

To increase users' productivity on-the-go, Good provides a complete and secure email attachment and file handling solution. Good's File Repository functionality combines security with flexibility, allowing employees to save and send attachments using a secure partition and file system.

VISIBILITY AND CONTROL

Helpdesk personnel can quickly troubleshoot issues, with complete visibility into all iOS devices deployed within the agency. To protect agency data, you can enforce policies, such as requiring passwords and preventing cut/copy/paste from the Good app. You can also block unapproved applications such as YouTube, the Safari browser, camera, or the App Store. In the event the device is lost or stolen, you can remote-wipe agency data. Self-service capabilities allow you to empower employees with basic tasks, such as adding devices or remote wiping their own devices.

WEB-BASED MONITORING

To handle device management and security, you can access a universal dashboard through any Web browser. Provision new iOS devices, enforce passwords, establish role-based policies—from virtually anywhere, anytime. Spend less time managing software and more time protecting government data and improving employee productivity.

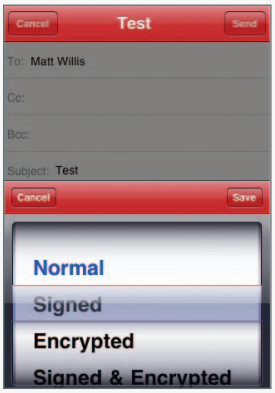
[1] Common Access Card (CAC) readers are supplied by 3rd parties. Good for Government is compatible with CAC readers from Biometric Associates Limited.

[2] CAC-based logon for Web-enabled applications is not supported.

Good™

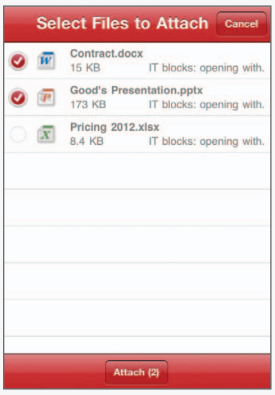
Good for Government: iOS

SECURE FEATURES THAT ARE EASY TO USE



Sign, encrypt or sign and encrypt email.

Protected messages require CAC PIN access.



Unique File Repository allows for secure document storage.

FEATURES	BENEFITS
Web-Based Management Console	Manage iOS (4.0+, 5.0+) devices as well as other platforms anywhere, anytime
Over-the-Air Management and Administration	Provide easy and scalable deployment to DoD and Federal government employees
Policy-Based Administration	Assign rights and permissions for different roles (help-desk, administrators, end users)
Policy-Based Management	Customize policies for different groups and assign to one or multiple users
End-to-End Encryption	Protect sensitive government data and meet regulatory requirements, with FIPS cryptographic libraries for on-device and over-the-air encryption
S/MIME Support and Integration with NSA-approved Bluetooth Smartcard readers	Enable employees to send and receive signed and encrypted emails from iOS devices; meet HSPD 12 and DoD Directive 8100.2 requirements
Jailbreak Detection	Protect agency networks and data by detecting and preventing jailbroken devices from connecting
Remote Wipe	Delete the Good application and encrypted data if device is lost or stolen—or wipe the entire device if necessary
Email, Calendar, Contacts and Secure Browser provided via a single, easy-to-use application	Speed adoption and maximize productivity
Secure Browser	Improve productivity with access to Intranets, command dashboards, IT monitoring portals, wikis, document repositories and more
File Repository	Unique secure partition and file system lets users store and manage e-mail attachments and other files

TECHNICAL SPECIFICATIONS	
Messaging servers	Microsoft Exchange 2003, 2007, and 2010
PKI Infrastructure	US Department of Defense PKI infrastructure
CAC cards	128K & 144K CAC cards issued by DMDC
Smartcard readers	Biometric Associates
Good software versions	Good Mobile Messaging server v6.3.1 and above

Good Technology
For more information visit www.good.com.

Global Headquarters
+1 408 212 7500 (main)
+1 866 7 BE GOOD (sales)

DS_GFG-iOS_Mar2012_US