



Open Your Possibilities™

Good for Government





Good for Government White Paper
2009

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com/gov

CONTENTS

- 1** Introduction
- 4** Good System Overview
- 10** Good Security Architecture
- 17** Good Over-the-Air (OTA) Management Architecture
- 20** Conclusion



INTRODUCTION

THE REALITY OF THE WIRELESS GOVERNMENT

Government executives and professionals are spending more time on the road doing business. These mobile employees must be readily accessible to constituents, partners and colleagues. In order to deliver the highest levels of service, they also need mobile access to email, personal information like contacts and calendars and access to critical behind-the-firewall applications, information and resources.

Once a luxury for top-ranking government officials, mobile technology is fast becoming a necessity for field-based government employees to stay ahead of the game. There is mounting proof that confirms mobile access to government information systems drives productivity and efficiency. Handheld mobile applications are changing the way that Department of Defense employees and contractors conduct business. These technologies can improve government processes in multiple areas such as defense and intelligence operations and military strategic plans, yielding better performance and efficiency.

THE SECURITY CHALLENGE

For all the promise of these new technologies, security is the Achilles' heel of the mobile revolution and must be addressed before the benefits can be fully realized. CIOs consistently rank security as one of their top IT priorities and the unique nature of mobility outside the four walls of government agencies adds heightened awareness of the threat.

Security breaches put organizations' most valuable information at risk. Military intelligence, strategic plans and personnel files can not be compromised in order to mobilize. As a result, CIOs demand stringent security standards to ensure that mobile users are allowed access to key organization data only as authorized, that such data are safeguarded both during transmission and while resident on handhelds, and that the core IT infrastructure is not jeopardized.

THE ESSENTIAL ELEMENTS OF WIRELESS SECURITY

Maintaining security is complex when providing mobile workers with anytime, anywhere access to the information they need. The move toward wireless data access extends the government agency network beyond the physical boundaries of the organization and utilizes public networks, raising a multitude of security issues. In such an environment, protecting government IT infrastructure requires a thorough understanding of the risks associated with mobilizing applications onto handheld devices over wireless networks.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov



The mobilized workforce is fundamentally different from those employees working within the four walls of the government. Integrating them into the overall IT infrastructure creates incremental security risks. To ensure security across the entire system, enterprises must recognize and address risks across four components of the mobility system: secure messaging, the primary firewall, over-the-air (OTA) data transmission, and device security.

Secure Messaging

When e-mail is sent over the internet, there is a potential risk that it may be intercepted by an intruder. Therefore, highly security-conscious organizations, like the Department of Defense (DoD), have implemented the security standards of S/MIME which protects against these threats. For these organizations, wireless messaging solutions must support the ability to extend the S/MIME security standards to wireless handhelds.

Primary Firewall Security

For government agencies to provide mobile workers access to mission-critical systems like email, enterprise instant messaging, trouble ticket systems or the agency Intranet they must maintain the security of the internal network through strict firewall protection policies. In order to maintain firewall integrity, programs running inside the firewall must not open avenues of potential attack from external programs. In order to adhere to stringent policies IT needs to address perimeter security considerations:

- **Authentication** — Each component of a wireless system must be able to prove that it is authorized to communicate on the network. It must not be possible for any software or device to impersonate a handheld or server, thereby misleading authentication services and allowing unauthorized communication or access.
- **Administrative security** — Government agencies need to ensure that different administrative tasks are accessible only to the appropriate administrator. For example, modifying system-wide security policies could be performed only by the most senior system administrators while lower level administrators may provision new users.

Transmission/Over-the-Air (OTA) security

When internal information is transmitted over the public Internet and/or a wireless network, the data must be protected against interception or “man-in-the-middle” attacks. Data packets can be intercepted and read if unencrypted or a weak encryption is employed. With the right information garnered over the air, intruders can use it to gain unauthorized access to a user’s device or even the backend systems.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov



Handheld security

Once government information is received and on a handheld, that information must be protected against unauthorized access by people or programs who may act maliciously. Handheld security must also address government requirements for control of various functions on the device (like use of Wi-Fi, Bluetooth,[®] cameras, speakers, etc.) as well as provide IT managers with a mechanism to control which applications are allowed or restricted.

Good for Government provides robust end-to-end security across these four critical links without adversely affecting the user experience. Security is viewed as strictly IT's domain and belongs in the in the hands of IT managers, with no requirement for users to set security parameters or make any security decisions. This white paper outlines, in detail, the security features of the Good for Government solution.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov





GOOD SYSTEM OVERVIEW

Good for Government is a comprehensive platform providing end-to-end, wireless, real-time messaging and enterprise application access supported by comprehensive device management and security. The Good system provides mobile professionals with up-to-date information when and where they need it and gives IT the means to secure and manage a diverse fleet of smartphones and mobile devices. The data path through the Good system is encrypted end-to-end; from the behind-the-firewall enterprise servers all the way to wireless handhelds (see Figure 1).

Good for Government is a complete enterprise mobility solution. Users easily access, in real-time, their e-mail, contacts, calendar, tasks, notes, as well as information from line of business systems like Microsoft Office SharePoint server, Office Communication server, and Remedy. Users can view and send rich attachments, including graphics, Word and Excel® files and stay abreast of headlines with real-time RSS news feeds. Good Mobile Access provides secure, wireless access to behind-the-firewall applications, data, and resources. The Good platform is built on industry standards in order to provide government agencies with maximum flexibility when mobilizing their organization and selecting handhelds. Organizations can avoid getting locked into a proprietary wireless system. Good Mobile Messaging S/MIME is available on a range of smartphones powered by Windows Mobile® 6 and 6.1 operating systems. Good Mobile Messaging S/MIME is available for Microsoft Exchange 2003 and Microsoft Exchange 2007.

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com/gov

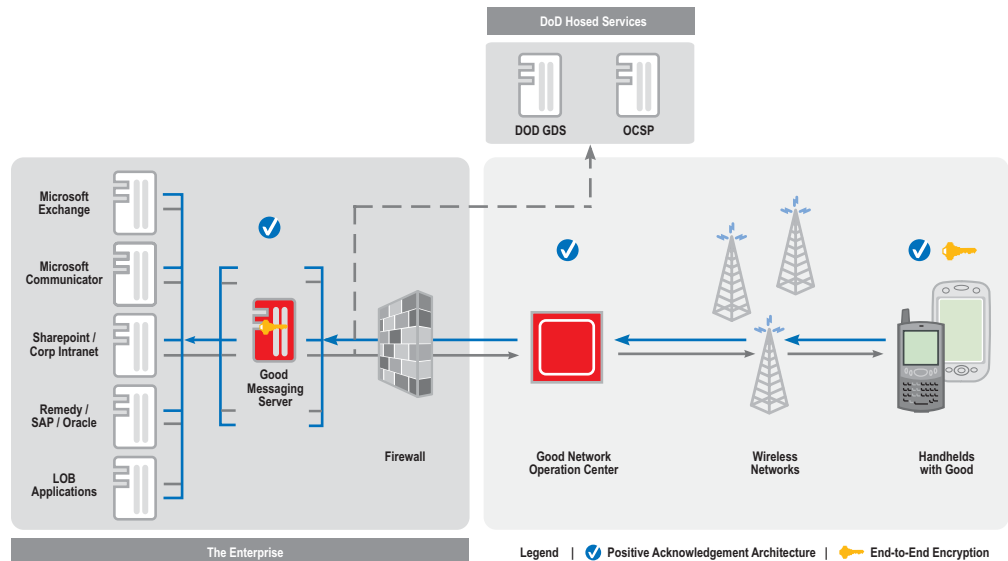


Figure 1: The Good System

The integrated product suite includes all the necessary components to support a government agency's mobility initiative.

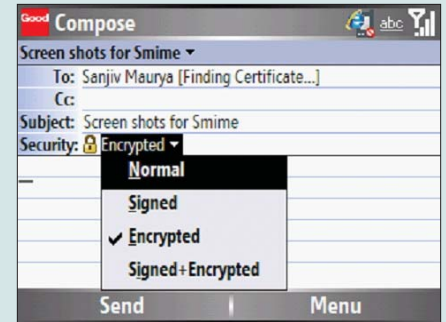


Good Mobile Messaging S/MIME

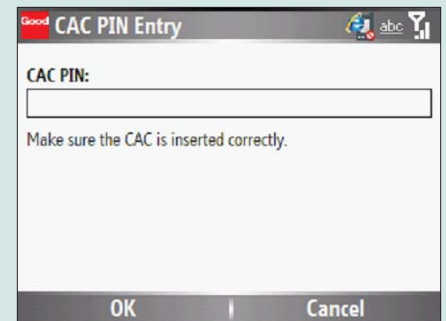
Good Mobile Messaging S/MIME offers up-to-date wireless access to signed and encrypted e-mail and personal information management (PIM) functions of Microsoft® Outlook® including e-mail, contacts, calendar, notes and tasks. Good Mobile Messaging S/MIME integrates seamlessly with the industry approved Bluetooth Smart Card readers (CAC readers) and with the Department of Defense CAC and PKI infrastructure to ensure that sensitive emails are encrypted for confidentiality, authenticated for privacy and validated for integrity. The cradle-free system continuously synchronizes data between the wireless handheld and the Good Messaging server behind the firewall.

- **Composing Secure E-mails from the Handheld:** Users compose e-mails the same way they compose normal emails. A drop down pick list allows the user to Sign, Encrypt or Sign+Encrypt e-mails. Depending on the CAC PIN cache intervals, the user may be prompted for a CAC PIN.
- **Reading Secure E-mails from the Handheld:** The inbox displays normal e-mails using a sealed envelope for unread messages and an opened envelope for read messages. Signed e-mails show an additional certificate seal icon. Signed+Encrypted E-mails or Encrypted E-mails are indicated with an additional lock icon.
- **Verifying Signatures:** The Good Mobile Messaging server will verify most messages from the server, which reduces the process load on the device and the amount of bandwidth consumed. The handheld user has the additional option to verify signatures from the handheld.

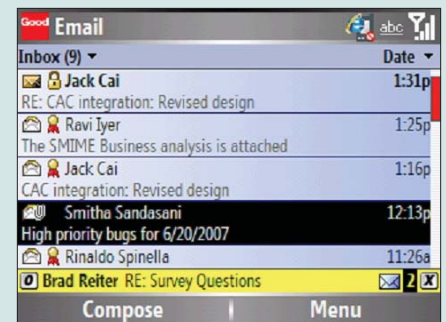
Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com/gov



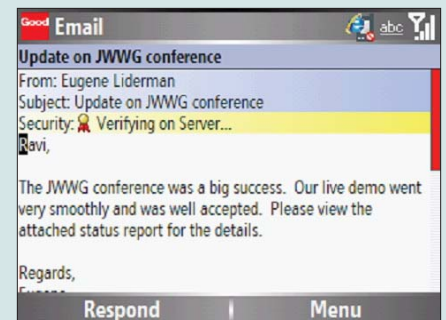
Send signed and encrypted messages.



Support for secure Bluetooth and USB CAC reader communication.



Easily identify signed and encrypted e-mails.



Automatically verify certificates from the server.



Good Mobile Messaging Server

Specifically designed to meet the needs of IT managers, the Good Messaging server reduces costs of deployment and support via its zero-desktop software architecture. Good Messaging server software monitors the user's Exchange mailbox and synchronizes any mailbox activity with the Good Network Operations Center (NOC), which then passes the e-mail and data through the wireless network to the user's handheld. Changes made on the handheld are sent to the Good NOC via the handheld's radio transmitter and the wireless network, and they return from the Good NOC via the Good Messaging server to the organization's messaging server. As a result, e-mail and data are available on both the user's desktop and handheld, ready to be read and filed from either location. Messages sent over the Good System are encrypted end-to-end using Advanced Encryption Standard (AES) security technology.

The Good Mobile Messaging server is extremely flexible and capable of serving Good Mobile Messaging S/MIME and Good Mobile Messaging clients simultaneously. This provides Department of Defense organizations the opportunity to reduce the cost of ownership enabling a mixed-mode environment (Good Mobile Messaging S/MIME for certain users and standard Good Mobile Messaging for others) from a single server.

Good Mobile Access

Good Mobile Access is a platform for mobile workers to securely access enterprise applications anytime, anywhere. Good Mobile Access connects mobile workers with behind-the-firewall applications utilizing Good's proven secure transport with FIPS certified, 192 bit AES encryption. The Good Access client server architecture enables standard TCP based applications to be deployed without requiring a proprietary SDK or customizing back end systems. In addition to enabling standard application access the Good Access server, in conjunction with Good Mobile Control, can control access to Department of Defense systems based on IP address or subnet, protocol, or service. Good Mobile Access enables mobilizing applications:

- Enable Intranet access; portals like SharePoint can be accessed enabling mobile users to view or download documents.
- Rich Client Applications written in .Net CF, J2ME, C++, or other standard programming language have the necessary access to intranet resources.
- 3rd party applications like Instant Messaging, CRM tools, Field Service, even remote IT management can all be mobilized
- File sharing of field data; pictures, videos, text based reports can immediately be reported to back-end systems.

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com/gov





Good Mobile Control

Good Mobile Control supports the entire operation with comprehensive over-the-air (OTA) management capabilities, granular security enforcement, and end-to-end visibility for troubleshooting and support. Good Mobile Control's enterprise-class device management and security is accessed through a single, web-based console, providing IT access to system functionality from virtually anywhere.

Good Mobile Control provides an easy to use, intuitive dash board with customizable views and role based management that simplifies handheld fleet management and carrier relations. The web interface provides easy access to the Good Mobile Control capabilities without requiring desktop software. The web API also allows for automating some of the administrative tasks streamlining processes such as new employee on-boarding.

- **User and server management** — IT managers can add, delete and monitor users and servers. In addition, they can also access detailed information about the handheld and servers, and assess performance such as coverage history.
- **Secure OTA management** — IT managers can enable Good users without ever touching the individual handhelds. Secure OTA also allows IT managers to push out third-party applications, and enforce password and other handheld policies. In addition to being able to upgrade an entire company with one command, IT managers can also schedule regular OTA upgrades of Good products or third-party applications as needed.
- **Role-based administration** — IT managers can distribute management tasks across a hierarchy of administrators by using role-based administration that offers a set of roles, with varying permissions, for administering the Good server and users.

By assigning appropriate roles to administrators, IT can better manage assets and increase security. Routine tasks, such as loading software, can be delegated to a wider group of administrators across multiple locations. More sensitive tasks, such as setting global policies or remotely erasing a handheld when lost or stolen, can be restricted to a smaller group.

- **User-group management** — Administrators can create groups to organize and manage Good users. All policies and software distribution can be managed at the global, group or individual user level. This provides IT with more granular control and reduces the time it takes to manage users, especially in larger deployments.
- **System License Management** — IT administrators can efficiently track and allocate grants for Good for Enterprise. The Good License Portal accessed through Good Mobile Control's interface supports tracking and managing Good Data Plans and Good Secure Transport Service (STS) grants. (The Good STS is for users who are not on a Good Data Plan from a Good-reseller carrier. Either a Good Data Plan with a reseller carrier or a Good STS plan is required for each Good user.)

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov



Good for Government White Paper 2009

- **Enhanced Logon Security** — IT administrators have the option of enabling Smartcard (CAC) Logon to the Good Mobile Control Web Console.

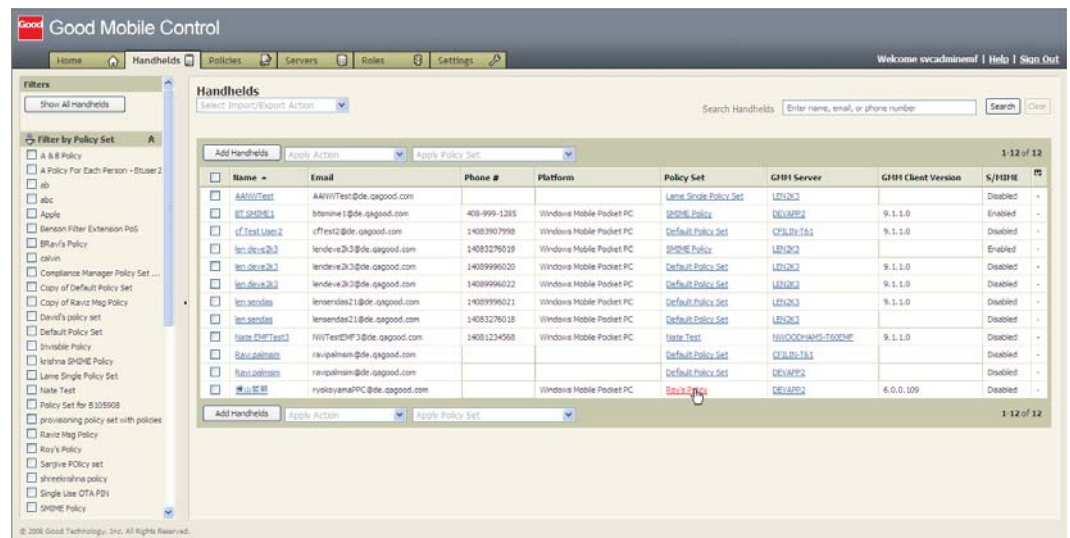


Figure 2: Filtering allows administrators the ability to view select groups of users based on one or more user or device attributes.

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com/gov





Good Network Operations Center (NOC)

The Good NOC provides the necessary capabilities to ensure fast, reliable synchronization between the Good for Government servers and the handheld. The Good NOC provides a number of benefits.

- **Push-based e-mail** — With the Good NOC, customers get more timely delivery of messages and more efficient battery use on the handheld. Even when users have been out of coverage, they have e-mail delivered to them in the correct order as soon as they come back into coverage.
- **Session / Connection Persistence** — Good's NOC maintains connections that are resilient to changes in device IP addresses due to network address translation (NAT) when roaming. The NOC also maintains sessions that may be affected by sketchy coverage or intermittent connectivity loss.
- **Positive Acknowledgement Architecture** — With the Good NOC, IT managers have data-path visibility with a built-in receipt of delivery so that they can ensure that messages were delivered to the right recipients.
- **Multiple networks** — The Good NOC makes it possible to manage connections to multiple carriers and networks, including Code Division Multiple Access (CDMA) 1XRTT, General Packet Radio Service (GPRS) and 3G networks. The Good servers can support handhelds on all of these networks and will be able to support new networks in the future.
- **Standard firewall settings** — The Good NOC is key to allowing Good for Government to be installed without requiring any changes to the external firewall. The server makes a secure outbound connection using the standard port 443. No inbound connections are required.
- **Optimized battery life** — The Good NOC communication logic provides efficient data delivery decreasing handheld retries and data compression algorithms support faster attachment downloads both contributing to improved battery life.
- **Fleet monitoring** — Through Good Mobile Control's web API the NOC provides valuable information regarding the enterprise's handheld fleet. This means that IT not only has visibility to the server status but also into individual handhelds, including handheld type and ROM, radio status and more.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov



GOOD SECURITY ARCHITECTURE

The Good System has been specifically designed to meet the security needs of even the largest, most security-sensitive organizations, such as the Department of Defense. It provides an end-to-end system designed to protect government information at all times—in transit over the network and in residence on the handheld. The Good System combines industry security standards, such as Advanced Encryption Standard (AES) and Federal Information Processing Standards (FIPS) 140-2, with Good's own security technologies. Installation of the Good for Government does not require any modifications to the firewall and leverages the existing network security infrastructure.

NETWORK PERIMETER AND TRANSMISSION SECURITY

Connections from the Good servers to the Good NOC utilize Hypertext Transport Protocol (HTTP) and are protected by the Secure Sockets Layer (SSL). Since the connection is established in the outbound direction, there is no need to create an inbound opening in the corporate firewall. Most corporate security policies allow this type of traffic through port 443 without reconfiguring the firewall. However, IT managers may use port 3101 or port 4662 instead. Connections to the Good NOC are used only for sending data to and receiving data from the NOC. Since all handheld traffic is managed through the NOC, this feature adds another layer of security.

End-to-End Encryption

When the IT administrators set up handheld devices for users, Good Mobile Control generates a unique AES encryption key for each user and places the keys on the handheld device and in the user's messaging server account. Once these keys are established, Good Mobile Messaging and Good Mobile Access use end-to-end encryption to protect every data packet from the server to the handheld device and vice versa. Since the client and server share encryption keys, any attempt to use a different encryption key would cause decryption to fail and the packet to be discarded. The Good NOC does not have access to the keys and cannot decrypt messages flowing through it. The Good Mobile Messaging server is configured to rotate the encryption key for handhelds every 30 days, preventing the unauthorized use of a compromised key and raising security by changing the encryption on a regular basis. The default value of 30 days can be modified by changing the value in the windows registry of the Good Mobile Messaging server.

Advanced Encryption Standard (AES)

When a Good server is communicating with a Good Mobile client, all packets are encrypted using AES. AES is a standard selected by the US National Institute of Standards and Technology (NIST) for its combination of resistance to attack, ease of implementation, efficiency and scalable design. Good's implementation of AES uses key lengths of 192 bits. Good uses 256 bit AES encryption for data stored on the device.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov



FIPS 140-2 Validation

FIPS certification is a critical security standard for many government organizations. The Good platform has been successfully tested by the NIST and certified FIPS 140-2 compliant. FIPS 140-2 certification covers the operation of Good's cryptographic module, which implements AES encryption. FIPS 140-2 also ensures the integrity of the cryptographic module in the field.

Reliable Data Packet Delivery

The Good System uses a unique Positive Acknowledgement Architecture to confirm delivery of all data packets, in the correct order with no duplicates, from the server to the handheld and vice versa.

HANDHELD DEVICE SECURITY

Locking the Handheld with a Password

The handheld may be configured with a password. When the handheld is locked, Good applications will not display any of the user's data and the handheld operating system turns off access to the USB port, which could otherwise be used to download data from the handheld to a PC. Access can be restored only by entering the correct password. IT policy controls the actions taken by a device if an unauthorized user tries to guess the password too many times. Based on policy the Good client software can:

- Do nothing and allow continuous retries
- Lock the device thus requiring the user to contact IT to have a new temporary password established or
- Wipe the device of data and applications.

Enterprise Resource Password Protection

For users with Good Mobile Access enabled, additional password security can be employed. The NT LAN Manager (NTLM) password is used to authorize the Good Mobile Access client with the Good Mobile Access server. This is an optional parameter set by policy. Having the NTLM password requirement in place provides another layer of security for users seeking access to behind-the-firewall applications and resources. Once access is granted at the Good Mobile Access server level the corporate resources may also require a password as well, like logging into the enterprise ERP system. These additional layers of security ensure only those with proper authority have access to sensitive corporate data in systems behind the firewall.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov



Device Locking with Common Access Cards (CAC)

IT Administrators can set different policies for locking the device and CAC usage depending on their security requirements. The following options are available for locking the device:

- 1. Password Optional:** Option to lock device is at the user's discretion. IT administrators do not enforce users to lock the device. The presence of a CAC inside a CAC Reader is not required to unlock the device. The user is prompted for a CAC PIN when signing and encrypting e-mails. This option provides the lowest level of device security.
- 2. Password Required:** In this option the device is locked with a password. IT has the option to set the password and other granular password characteristics. Users need only the password to unlock the device and to send a signed message. The presence of a CAC inside a CAC Reader is not required to unlock the device.
- 3. Password Required:** Rather than require the user to remember a password separate from the CAC PIN (as in option 2), the IT administrator can set the device password to be the same as the CAC PIN. The presence of a CAC inside a CAC Reader is not required to unlock the device. User is prompted for a CAC PIN when signing and encrypting e-mails.
- 4. Password Required, Password as CAC PIN, and CAC Required:** This is the strongest mechanism available to the IT administrator to protect the device. To unlock the device, the user will have to enter the CAC PIN. At this time, the CAC must be inserted in the CAC Reader to communicate with the device. This provides 2-factor authentication to the handheld device. To sign a message, the user must provide his CAC PIN.

Remote Erase of Lost or Stolen Devices

If a user's handheld is lost or stolen, the IT administrator can use Good Mobile Control to remotely disable the handheld and remove all Good application data. If a handheld device is recovered, Good Client applications can be restored OTA. Additionally, IT managers can set policies for "bit-wiping" data stores on the handheld according to various parameters like number of failed password attempts. IT managers can also manually bit-wipe a handheld if it is lost or stolen. The bit-wipe policy can be enforced on the device and the SD card or just the device. The actual bit-wipe function is analogous to a hard reset of the handheld unit.

Device Usage Control

Good allows IT to remotely set and enforce policies for controlling data transfer ports (e.g., HotSync,[®] Wi-Fi, Bluetooth, infrared) as well as locking down handheld features such as cameras, microphones, speakers, etc.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov

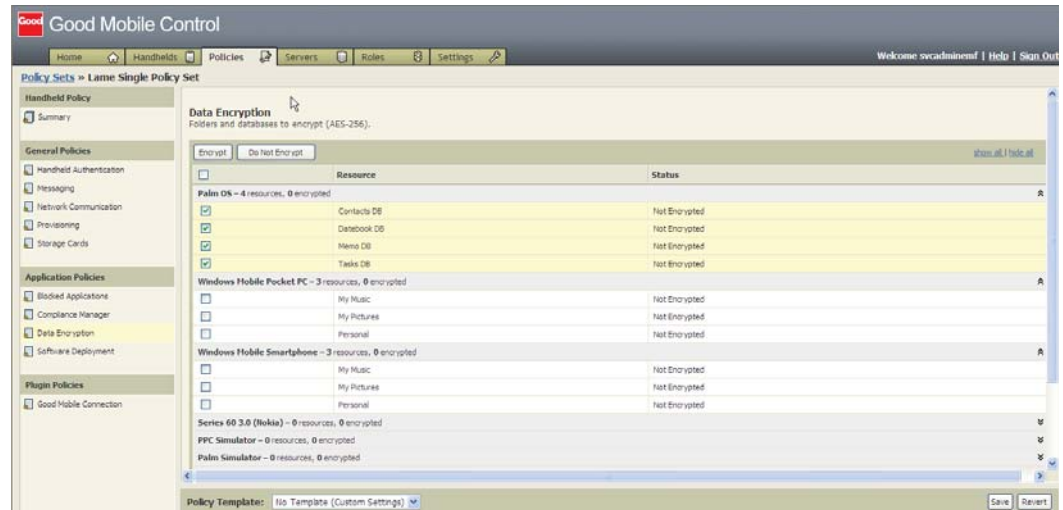


Figure 3: Robust policy implementation is made simple with the use of policy templates within policy sets.

Encryption on the Handheld

The Good client encrypts the local databases, which store the user's e-mail, calendar, contacts, notes and tasks. Sensitive corporate data is protected using strong 256 bit AES encryption. Additionally, IT managers can remotely set policies for encrypting selected device databases and the external Secure Digital (SD) card. If a user is using desktop synchronization software (e.g., HotSync or ActiveSync®) to synchronize other handheld applications, Good client databases will not be copied onto the PC. Furthermore if the device is currently in password protect mode any attempt to connect to it with a synchronization product will be denied. If the device is connected and then becomes password protected because of a time-out the connection is immediately dropped.

Restricting Handhelds by Operating System

The Good platform allows administrators to control the types of devices, based on operating system, that are allowed to install and run Good Mobile clients. For example, for management simplicity, IT managers may want to standardize on handhelds running a certain operating system (like Windows Mobile Pocket PC) and prohibit all other handhelds. For various reasons, some customers consider certain mobile operating systems to have more security vulnerabilities than others. When this is the case, IT managers can prohibit use of Good on all devices with that particular operating system.

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com/gov



Security Considerations for Handhelds with SD Cards

On handhelds that support external SD cards, Good applications can be backed up, allowing the Good client to later reconnect to the enterprise. This backup can be useful in the event that the battery drains completely, which causes memory on some handhelds to be lost. Without the SD backup, the user would need to return the handheld to the IT department for re-provisioning or go through re-provisioning via the OTA setup process. Information on the SD card is strongly encrypted with a pass code and is matched to the serial number of the handheld, thus providing two-factor authentication for the SD backup.

Mandatory Application Checking

The Good Compliance Manager can check for mandatory applications, like virus protection, that must be installed and/or running on the handheld before the Good client can be started. If a handheld fails a periodic check, for what ever reason, then the user is automatically taken to an application download screen on his or her device where they must download required applications before they can launch the Good client. All of this is done without requiring IT intervention.

AUTHENTICATION

The Good platform provides a number of safeguards against unauthorized access. The Good servers reside behind the corporate firewall and any handheld attempting to contact them is required to complete a three-step authentication process between:

- The Good NOC and the Good Control server.
- The handheld and the Good NOC.
- The handheld and the Good server.

Authenticating the Server

Before the Good NOC can communicate with a Good server, the server must authenticate itself to the Good NOC. This authentication is handled using SSL server authentication through an outbound port. Once this secure connection with the Good NOC is established, the server authenticates itself to the Good NOC using the server name, serial number, and license key which uniquely identify that enterprise server to the NOC.

Authenticating the Handheld

The handheld connects with the Good NOC and two checks are performed to ensure that the device is authorized to access Good Mobile Messaging. First, the Good NOC ensures that the handheld has a valid data plan, either provided directly from Good or through a Good carrier reseller. Second, the handheld provides the unique serial number burned into its ROM or SIM card and requests permission to communicate with a specific Good server. The Good NOC checks its database of handheld serial numbers and Good servers with which each handheld is authorized to communicate. If the handheld passes both of these tests, it is authenticated to the NOC. This, however, is not the final step. Passing this authentication does not yet permit access to enterprise data managed by the enterprise's Good server.



Connecting Server and Client

To complete the process for access to enterprise data beyond the Good server the handheld must be explicitly authorized to talk to that server. This authorization is handled by the Good NOC. Once the handheld is authorized to communicate with an enterprise's Good server, the user can access enterprise data via that server, sending and receiving information.

ADMINISTRATIVE SECURITY

The Good platform offers Role-Based Administration (RBA) that allow system administration privileges to be assigned according to the needs and qualifications of each IT administrator (see Figure 4). By controlling IT administrator's access according to their roles and the associated permissions, RBA provides a tool for managing IT assets and layering security. Routine tasks—such as adding a new user or loading software—can be delegated to a wider group of IT managers across multiple locations. More sensitive permissions, such as those required for setting global policy, can be restricted to a smaller group, increasing the overall security of the system. RBA also encourages the most efficient use of IT resources, since permissions can be based on skill and job function.

Among the permissions that can be granted to administrators:

- Create new user
- Delete user
- Manage Good servers
- Change user policy
- View only administration
- Load handheld software
- Erase handheld data
- Manage handheld policy and software
- Manage roles



Figure 4: Role based administration provides levels of security for command and control of the Good system

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov



USER-GROUP MANAGEMENT

Good provides user-group management so that administrators can create groups to organize and manage Good users. All policies and software distribution can be managed at the global, group or individual user level. This allows IT managers to more efficiently deploy different security policies to different user groups. Additionally, the IT administrator can import user groups via .csv files.

E-MAIL SECURITY

Virus Protection

Preventing the spread of viruses is an ever-present concern for IT departments and end users. Viruses commonly infect a user's system by delivering executable code or scripts via an e-mail or an e-mail attachment then getting the user to run the code inadvertently. The Good client application will not run executable code within an e-mail or attachment and thus is less vulnerable to viruses from e-mail. Good users can use their devices to read e-mails or attachments without concern about viruses. If the user suspects an e-mail to be malicious, he or she can safely delete that e-mail from the handheld rather than risk opening it from the laptop or desktop. Additionally, using Good's ability to distribute handheld software OTA, enterprises can enhance corporate compliance by ensuring that employees are running the latest mobile security applications such as Symantec® AntiVirus for Handhelds.

APPLICATION AND SITE ACCESS SECURITY

Walled Garden/Browser Lockdown

Utilizing features in the Good Mobile Access server, IT managers can enable a "walled garden" feature, which limits users' ability to access sites, servers, and applications. IT can allow or restrict access of Good Mobile Access users to behind the firewall applications, data, and resources by several means. Users can be restricted by individual IP or subnet address, by protocol type (i.e. TCP or UDP), or by service such as HTTP or FTP. Additionally, IT managers can specify substitute URLs that users are directed to when they request certain URLs. These functions allow IT departments to reduce bandwidth consumption associated with users accessing applications and sites that are not relevant to their job function.

Smartcard (CAC) Logon/Two-Factor Authentication to Web Sites

By leveraging Windows Mobile and the Bluetooth Smartcard Reader over the secure Good Mobile Connection VPN tunnel, users can now authenticate to and browse secure Government websites that require Smartcard (CAC) Logon as a form of two-factor authentication.

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com/gov



GOOD OVER-THE-AIR (OTA) MANAGEMENT ARCHITECTURE

OTA DEPLOYMENT SECURITY CONSIDERATIONS

Good provides Secure OTA setup of Good Mobile Messaging and Good Mobile Access without IT personnel needing to physically handle a user's device. The Good Secure OTA capability encompasses several features, including deploying and upgrading the Good client software, installation of any additional handheld software and delivery of handheld policies and updates.

Good Secure OTA Process Flow

In order to explain the security model, the high-level process flow for Good Secure OTA setup of handhelds is as follows:

1. Using Good Mobile Control, an IT administrator sets the version of Good client software to be deployed when users perform Good Secure OTA setup. The version can be set on a global or per-user basis. Global setup is a one-time operation.
2. Using Good Mobile Control, the IT administrator gives permission for a user to wirelessly provision OTA, without needing prior knowledge about the user's device.
3. Good Mobile Control generates a random 15-character personal identification number (PIN) and e-mails the PIN to the user, along with instructions for OTA setup.
4. The Good NOC stores the user's e-mail address, Good server name and a hash of the PIN.
5. The end user downloads the Good OTA Setup application from <https://get.good.com> via the Web browser on the device.
6. When Good OTA Setup runs, it asks the user to enter his or her e-mail address and PIN.
7. Good OTA Setup initiates the authentication sequence.
8. After the authentication sequence succeeds, Good OTA Setup downloads a package of provisioning information from the Good server.
9. Once Good OTA Setup receives the provisioning info, it downloads the Good client software version set by the IT administrator and runs it.
10. When the client runs, it performs the normal provisioning process, connecting each of the client applications with its server behind the firewall.
11. This process may be repeated if for some reason the client application is deleted from the handheld. Note that the PIN is not stored by Good Messaging client software—it must be provided again by the end user. Once a handheld is provisioned using a PIN, the PIN cannot be used with any other handheld.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov



Access Control

IT administrators must explicitly give permission for users to provision OTA. Permission may be granted to a group of users added to the Good Messaging server from the Exchange server Global Access Lookup (GAL) or the Domino Directory. If the IT administrator has not given permission for a user to provision OTA, the Good NOC will prevent Good OTA Setup from communicating with the Good Messaging server behind the firewall.

Network Perimeter

The Good platform does not require any inbound connections through the enterprise firewall. This advantage is applicable to Good OTA Setup as well. All communications between Good OTA Setup and the Good servers run through the same outbound connection that Good servers are operationally configured to use. Good OTA Setup initiates a connection to the Good NOC and once the authentication sequence has succeeded, Good OTA Setup is permitted to use the network channel between the Good NOC and a Good Messaging server.

Authentication

When Good OTA Setup runs, it first authenticates to the Good NOC. The Good NOC does not store the user's PIN; rather, it stores a one-way hash of the PIN and uses that hash to provide authenticated access to the OTA provisioning system, based on the user's e-mail address. Once the user is authenticated to the Good NOC, the NOC permits Good OTA Setup to negotiate an authentication protocol with the user's Good Messaging server. An authentication protocol is used where the client and server each encrypt data with the user's PIN. The PIN itself is not transmitted. If the authentication sequence fails more than 10 times, the Good System assumes that an unauthorized user is attempting to gain access and that user is prevented from making further attempts. The IT administrator will have to delete and re-enable the user for OTA Setup for the user to retry. The Good Control server contains a new right for which IT administrators can enable users for OTA Setup. When an authorized administrator uses Good Mobile Control to generate a PIN, it is sent to the end user via e-mail. Since the PIN is confidential, it is not shown to IT personnel by default. The Good service administrator may choose to make the PIN accessible to some IT administrators using a feature in Good Mobile Control. This action may be necessary to provision a user who does not have access to his or her corporate email. If desired, Good OTA Setup can use a PIN longer than 15 characters. The length of the PIN is provided in a Windows® registry key on the Good Messaging server machine.

Traffic Encryption

In order to protect all traffic between Good OTA Setup and the Good Messaging server, all communication during the provisioning process runs over HTTP/SSL. The package of provisioning information is further encrypted using an AES key derived from the user's OTA PIN. After the client receives the package of provisioning information, it begins to use the normal end-to-end encryption capabilities that Good uses in its standard operating environment.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov



OTA SOFTWARE INSTALLATION SECURITY CONSIDERATIONS

The Good OTA software distribution system supports distribution of three classes of software: Good applications, Good partner applications and custom applications provided by the enterprise's internal IT department.

Digital Signatures

Good software and partner software are digitally signed using X.509v3 certificates. When Good OTA Setup downloads the Good client software it checks the signature value and the validity of the Good certificate. If signature verification fails, the installation is interrupted with a message warning the user that the software is from an unknown source and waits for the user to select continue or quit. Good recommends that users not install the software unless they are absolutely sure of the source. In addition, the certificate used to sign the software package is checked against the Certificate Revocation List (CRL) published by VeriSign, Inc.

Encryption for Application Delivery

When the IT department wants to provide an application to its users, it is possible that the application contains confidential information, e.g., a trading application for a financial services company. Therefore, before the custom software package is uploaded, it is encrypted using a key generated by Good Mobile Control using Microsoft CryptoAPI. The key is then communicated to the client via Good's AES-encrypted communications channel.

Software Versions

Good Mobile Control provides a policy for IT managers to specify the version of client software that will be installed. Good OTA Setup receives this policy along with other provisioning information and downloads the correct version. In this way, IT managers can ensure that users receive only the client software that has been tested and approved.

Mandatory Installation

IT managers may mark software packages as mandatory or optional. If a software package is optional, users may decline to download and install it. If a software package is mandatory, the Good client will automatically download and run the installer for that application. In either case, users may defer the installation for a short time if they are using the handheld and do not wish to be interrupted.

Off-Peak Downloads

When the IT department initiates an upgrade or distribution of other handheld software on a global basis, the Good Mobile Messaging client will begin the download at a random time overnight. This is designed to prevent overloading wireless infrastructure by having a large population of users all downloading a large program at the same time. Individual users may override this setting and begin the download immediately.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov



CONCLUSION

No longer an exclusive luxury for top-ranking government or military officials, mobile technology has become a necessity for government field forces. Mobile access to enterprise information systems drives productivity and efficiency. However, for mobile deployments to succeed, they must be planned and executed with security in mind. Protecting the corporate IT infrastructure requires a deep understanding of the risks associated with mobile applications, handhelds and wireless networks. In any client/server wireless mobility system, a number of security challenges must be addressed.

Good has that deep understanding of those risks gained over years of experience and thousands of deployments. The Good platform provides the most comprehensive security for mobile messaging and data access deployments. Good's security includes: network, transmission, handheld, authentication, administrative and e-mail functions. When deployed securely, handheld and mobile application technologies can improve business processes and yield substantial ROI all with lower total cost of ownership (TCO). Individual users may override this setting and begin the download immediately.

Good Technology

Phone: 866-7-BE-GOOD

Online: www.good.com/gov

©2009 VISTO Corporation and Good Technology, Inc. All rights reserved. Good, Good Technology, the Good logo, Good for Enterprise, Good for Government, Good for You, Good Mobile Messaging, Good Mobile Intranet, and Powered by Good are trademarks of Good Technology, Inc. ConstantSync, Constant Synchronization, Good Mobile Client, Good Mobile Portal, Good Mobile Exchange Access, Good Mobile Platform, Good Easy Setup, Good Social Networking and Good SmartIcon are either trademarks or registered trademarks of VISTO Corporation. All third-party trademarks, trade names, or service marks are the property of their respective owners and are used only to refer to the goods or services identified by those third-party marks. Good and VISTO technology is protected by U.S. Patents 6,085,192; 5,968,131; 6,023,708; 5,961,590; 6,131,116; 6,151,606; 6,233,341; 6,131,096; 6,708,221 and 6,766,454 and the following NTP U.S. Patents: 5,436,960, 5,438,611, 5,479,472, 5,625,670, 5,631,946, 5,819,172, 6,067,451, 6,317,592 and various other foreign patents. Other patents pending.

