

**> ENTERPRISE MOBILITY
MANAGEMENT**

While business users may be thrilled by the capabilities of iPhone and other smartphones – and are quickly adopting them as their handheld computers – it is unlikely their IT counterparts share in this excitement because their IT vendors have not provided the tools to effectively secure and manage them. That is until now.

Trust Digital's EMM for smartphones provides a Web Services platform to manage and secure smartphones and ruggedized devices regardless of device manufacturer. This robust management platform addresses the nuances of smartphone technology while also providing tools similar to those used by IT to manage and secure laptops and desktops. The Trust Digital platform includes:

- **Heterogeneous Device Support**
Policy-based security and control for iPhone and other non-Blackberry devices that includes: device loss protection, endpoint security, data leakage protection, network access control (NAC) and identity management
- **Centralized Management**
Enterprise-grade device management, providing centralized provisioning, compliance enforcement, asset reporting, help desk diagnostics and a self-service user portal via a secure over-the-air SSL connection
- **User Compliance Facilities**
Reporting and enforcement facilities to ensure user compliance with IT mobility policies

Furthermore, a comprehensive enterprise mobility strategy must satisfy stakeholder requirements throughout an IT organization including Information Assurance, Administration & Operations and the user-facing Help Desk team – what Trust Digital likes to call the 360° of Enterprise Mobility Management.

Information Assurance

The Trust Digital EMM platform provides an organization's security administrator with a policy editor accessible from the EMM console which allows policies to be created for each user based on the type of smartphone used and the security posture associated with the user's job. Policy assignments can also be made based on the user's membership within group associations stored within the enterprise's directory service.

Two best-practices security policies are provided to illustrate how IT can implement incremental degrees of security to protect corporate data and access to corporate services, for example a corporate executive may require a more liberal security policy while a field sales representative might need a higher security policy because there is greater opportunity for device loss. In this example both policies describe what IT administrative capabilities are supported by the EMM platform to effectively secure smartphones and other handheld devices. In addition, both policies specify encryption and password data protection for user email, contacts, calendars, and documents.



| | | Data Protection Security Policy (Example: Corporate Executive) | High Security Policy (Example: Field Sales Representative) |
|---|---------------------|---|---|
| Administrative Support Functionality | General | •Admin PW Access & Reporting | •Admin PW Access & Reporting |
| | Help Desk | •Wipe, Remote Unlock, Uninstall | •Wipe, Remote Unlock, Uninstall |
| Data Protection | Encryption Method | •AES 256 | •AES 256 |
| | Protect Files | •PIM & "Office" Docs and IE | •PIM & "Office" Docs and IE |
| User Authentication | Password | •6 Character PIN, 10 Attempts, Wipe After Failure, Idle Timer 5 mins | •6 Character PIN, 10 Attempts, Wipe After Failure, Idle Timer 5 mins |
| Peripheral & Resource Control | Infrared "Beaming" | •On | •Blocked |
| | WiFi | •On | •Blocked |
| | Bluetooth | •On | •Blocked |
| | Camera | •On | •Blocked |
| | SD Card | •Allowed / Encrypted – All Files | •Allowed / Encrypted – All Files |
| Application Management | Image Lock | •Off | •On |
| | SMS/MMS Supervision | •Off | •On |
| | IP Supervision | •Off | •On |
| | Web Browser | •Allowed | •Blocked |
| Administrative Controls | Login Monitor | •On –After 15 days, device will automatically Wipe | •On –After 15 days, device will automatically Wipe |

All policies are delivered over-the-air to the smartphone agent that enforces the policy. Console reporting tools can be used to track the security posture of each user device for compliance reporting. NAC capabilities are also an essential part of the Trust Digital platform and gives the IA team a way to ensure user compliance.

Administration & Operations

The Trust Digital EMM Audit & Compliance Service provides IT administrators with a way to discover, and catalog all deployed handheld mobile devices. This capability gathers extensive details about device hardware, software, and status. Information about the population of mobile enterprise devices—such as numbers of devices, serial numbers, model numbers—are provided by reporting tools found within the EMM Console and can be used to help plan and maintain an enterprise-wide deployment.

While helping to maintain and track each device, Trust Digital EMM also provides policy controlled and automated deployment of applications, simplifying the deployment of a trusted application environment for mobile users. Furthermore, Trust Digital supports the installation and upgrading of applications by group policy.

Help Desk

An enterprise cannot effectively deploy or maintain a diverse community of devices without the proper help desk tools. The Trust Digital EMM platform provides the appropriate tools for image management, deployment, and reporting while also providing remote interactive diagnostics that help resolve issues without requiring users to surrender their devices. In addition, Trust Digital offers an EMM Self-Service Portal that helps offload the help desk of routine issues such as forgotten password and unlocking their device. This resource is accessible to users from a web browser on their mobile device or laptop. The portal offers

capabilities that when combined form a highly effective way to offload rudimentary tasks from help desk staff while ensuring user satisfaction.

Summary

The Trust Digital EMM is key to the implementation of your mobility management strategy, providing you with a mobility management platform that:

1. Eliminates operational expense by simplifying how IT administrators and help desk specialists implement policies, assist users and enforce compliance for mobile applications across the enterprise
2. Gives IT the ability to secure and manage a truly heterogeneous smartphone environment while having the ability to assist in addressing the needs of a mobile workforce
3. Helps the CIO control smartphone costs while also protecting corporate information

These capabilities enable the CIO to provide choices of smartphones and applications to best meet the mobility needs of their workers.

Today, Trust Digital is the leading provider of enterprise mobility management software for government organizations and Global 2000 companies. IT organizations rely on Trust Digital's solution to cost-effectively secure, rapidly deploy and centrally manage their smartphones. Trust Digital's unique software-overlay methodology simplifies how IT administrators and help desk specialists implement policies, assist users and enforce compliance for mobile applications. Trust Digital is the trusted mobility company.

For more information about the 360° of Enterprise Mobility Management, please visit our website, www.trustedigital.com.