MobileManager
The EnTelegent
Mobile Device Management
Solution

The Enterprise in Your Pocket

Users carry your enterprise in their pocket. They use their smartphones and tablets to access the corporate network, business applications, and your organization's crown jewels: **your enterprise data**.

The problem is these devices are all over the map. They go where your users go. Literally. **And that's risky**.

What if your users log into your network over an insecure network?

What if they lose their smartphone or tablet?

What if they download next year's strategic plan… and then leave the company?

Each of these can lead to data loss or breach, expose your network, and **threaten your compliance status**. What's required is best-in-class wireless device management and enterprise mobility.

Manage the Device Lifecycle

The influx of employee-owned (Individual Liable) devices in the enterprise places an extra burden on IT and the help desk. End users want freedom to use their device of choice, but enterprise security requires that you enforce consistent security policies across all devices.

MobileManager lets you manage the mobile device lifecycle like nobody else.

Do it **across every major platform** – iPhone, iPad, Android, BlackBerry, Symbian and Windows Mobile.

Secure End-to-End

Beyond wireless device management across the lifecycle, MobileManager **secures your mobile enterprise** end-to-end, across mobile devices, applications, the network, and data.

Choose Enterprise-Grade
Wireless Device Management

The most exacting Fortune 100 enterprises and government organizations use MobileManager for their wireless device management deployments because of its proven scalability, highly-available, secure architecture, and world-class service and support.

Deploy New Smartphones Efficiently

When VIP users acquire new mobile devices, more often than not they need quick activation and provisioning of devices with enterprise applications.

- MobileManger removes the complexity to streamline device activation from a convenient Web dashboard. A few clicks and your mobile users are off to a productive start with instant access to enterprise resources.

Track Expenses and Audit Security…
of All Mobile Devices

Monthly wireless telecom costs can quickly spiral out of control as a result of International and domestic employees, varying data and phone plans, and roaming users.

- Customers using MobileManager typically find they can reduce wireless spend by **up to 25%**.

- Smartphone security audits help avoid costly litigation or compliance lapses.

- MobileManager can track policies applied to the device, and even identify missing or removed policies.

Support Smartphone Users Effectively

Now you can **enhance the end user experience** by proactively finding and fixing mobile user and infrastructure issues.

- MobileManager is based on technology developed to help you eliminate those late night calls by solving problems before users are impacted.

Decommission Unused Devices

Use MobileManager to securely wipe enterprise data from employee- or corporate-owned devices before they leave the organization.

Track down lost or stolen devices using device locator capability and you're ready for safe decommissioning.

Get EnTelegent Mobile Device Management today!

MobileManager provides the following management and security capabilities:

Configure	• Differentiate between employee-owned versus company-issued devices (and establish appropriate configurations and policies for each) • Configure enterprise resources, including Wi-Fi, VPN, APN, AD or LDAP, PKI, and two-factor authentication • Configure security resources such as encryption of data-at-rest and Mobile Application Tunnels for dedicated app security and encryption of data-in-transit • Configure corporate email • Configure third-party email container • Make mobile applications available via an enterprise application store • Restrict mobile device resources and applications • Blacklist and whitelist applications, lock applications, push and remove applications • Set dynamic, context-aware policies
Provision	• Enable user self-service mobile device enrollment • Distribute packages of applications and policies by user, role, group and device type • Lock and enforce profile
Secure	• Set and enforce passcode policy (simple or complex); ascertain passcode history • Integrate with two-factor authentication for enhanced security and single sign-on • Auto-lock after inactivity period • Auto-wipe after certain number of failed login attempts • Block jailbroken or rooted devices • Enable Mobile App Tunnels for dedicated, encrypted connection, transaction performance and data compression • Use Secure Mobile Gateway to block unauthorized or non-compliant devices • Gain Mobile Security Intelligence and integrate with Security Information and Event Management (SIEM) solutions • Protect sensitive data with Mobile Data Leakage Prevention (DLP)
Support	• Provide remote user support; locate, lock, wipe and selectively wipe • Troubleshoot and remediate mobile device and service issues
Monitor	• Detect user, device, system, and service issues • Maintain application inventory • Maintain hardware inventory, including asset details; report on device statistics • Report on service details such as roaming, location, user inactivity and expenses
Decommission	• Identify inactive devices • Fully wipe devices, returning them to factory settings • Selectively wipe devices, removing business apps and data while leaving personal data intact