MasterTel USA
Technology Solutions for Business, Healthcare and Finance

MOBILE DEVICE MANAGEMENT

Your workforce carries your enterprise in their pocket. They use their smart phones and tablets to access the corporate network, business applications, and your corporate crown jewels; your enterprise data. The problem is that these devices are all over the map. They go wherever your users go…literally. And that's what'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. The solution is to install best in class wireless device management and enterprise mobility. If you have 100 mobile devices or greater accessing your network, you should consider MDM.

ZENPRISE · MobileIron · BoxTone Mobile Service Management · LANDesk · Sybase iAnywhere · Symantec · Trend Micro · MaaS360 by Fiberlink · Good · Afaria · SOTI.net We Manage Mobility · airwatch mobile device management · AMTEL MDM · OPENPEAK · MYMobileSecurity The N°1 in mobile security · M@D mobile active defense The Smartphone Security Company · Tangoe MDM

BENEFITS OF MDM:

1. **Complete Mobile Device Lifecycle Management**
2. **End to End Security**
3. **Efficiently Deploy New Devices via web interface**
4. **Proactive Mobile I.T. Management**
5. **Decommission Devices**
6. **Reduce Expenses when part of a total TEM package**

MasterTel USA
Technology Solutions for Business, Healthcare and Finance

The influx of employee owned (Individual Liable) devices that have entered the enterprise space, places an extra burden on I.T. 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. MDM enables you to manage the device lifecycle like no one else and do it **across every major platform…** iPhone, iPad, Android, Blackberry, Symbian and Windows Mobile.

MDM secures your enterprise end to end, across mobile devices, applications, the network, and data. MDM can track policies applied to each device and even identify missing or removed policies. Smart phone security audits help avoid costly litigation and compliance lapses.

When VIP users acquire new mobile devices, more often than not, they need quick activation and provisioning of devices with enterprise applications installed. MDM removes the complexity to streamline device activation from a web dashboard.

Enhance the end user experience by proactively finding and fixing mobile user and infrastructure issues. Our enterprise MDM platforms are based on technology developed to help you eliminate those late night calls by solving problems before users are impacted.

Speak to a Wireless Consultant

MDM can be used to securely wipe enterprise data from employee or corporate owned devices before the terminated employee leaves the organization. MDM also allows you to track down lost or stolen devices using a device locator capability so you can safely decommission.

OUR MDM SERVICES TYPICALLY PROVIDE THE FOLLOWING MANAGEMENT & SECURITY CAPABILITIES.

	• 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	• 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 jail-broken 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

The most exacting Fortune 100 Enterprises and Government Organizations use our "best of breed" MDM provider platforms for their wireless deployments because of its proven scalability, high availability, secure architecture, and world class service and support. Once size does not fit all. That is why MasterTel USA partners with the top 20 providers in the MDM space (Garner Magic Quadrant), including niche providers, in order to solve every business need.