MobileIron Hosted from AT&T is a cross carrier solution designed to offer customers the maximum flexibility in solving the challenges of the expanding mobile perimeter and secure use of mobilized information. The solution consists of MobileIron Virtual Smartphone Platform (VSP) application and the optional Sentry email access control application, hosting infrastructure and lifecycle management, supporting multiple smartphone models and tablets. This solution combines MobileIron’s MDM software, offering the ability to manage mobile applications, documents and devices, with AT&T provided consultation, design, implementation, hosting and management. Delivered as a turnkey solution, MobileIron Hosted from AT&T delivers a compelling advantage over disparately assembled and self-managed on-premise mobile device management solutions.

Key Differentiators and Benefits
- The experience and power of AT&T to deploy, host, manage and support your application reduces risk in your investment
- Dedicated, scalable environment to support customer needs
- SLA of 99.9%
- Highly secure and resilient options
- Complete application management services that provide flexible deployment options and low cost of ownership in a hosted environment across the app lifecycle
- Expertise to augment and complement customer IT and security staff
- Robust integration with customer IT organizations and the highly secure AT&T hosting infrastructure
- Tier 4 Internet Data Centers (IDC)

Robust Security
MobileIron Hosted from AT&T provides highly secure data access across the lifecycle while preserving privacy:
- Data loss prevention for email through Sentry
- Two-phase authentication and access control for email through Sentry
- Selective wipe for business data with privacy protection for personal data
- SSL certificate management from enrollment through renewal
- Protected sign-in and personalized configuration for multi-user shared devices

Potential Benefits
- Protect corporate information on mobile devices
- Help secure the mobile app lifecycle while preserving user experience
- Ensure end-user compliance
- Reduce the total cost of ownership of mobile data enterprise solutions
- Enable more efficient end-user engagement
- Increase productivity and effectiveness
- Improve revenue flow

Features
- Over-the-air monitoring and enforcement of security policies
- Ensure that devices are performing properly
- Helps support enterprise applications and processes
- Provide reliable security safeguards
- Real-time, over-the-air configuration and diagnostics
- Help speed up application and device deployment
Full Integration
MobileIron Hosted from AT&T provides deep integration with existing IT infrastructure:

• Central console for leading mobile OS platforms
• Tight integration with AD/LDAP groups and attributes
• Monitoring of international roaming for telecom expense management
• Workflow integration through rich web services API and Assemble toolkit
• Highly scalable self-service enrollment

Consulting, Design and Integration
AT&T Mobility Solutions Services (MSS) has deep mobility application, network and device experience based on years of working with customers, network suppliers and application providers. AT&T mobility professionals are trained directly by the mobile device management platform suppliers. In addition, AT&T mobility professionals hold a wide range of certifications from Microsoft, Cisco and other industry recognized organizations, including (ISC)²’s CISSP certification.

Project Management
AT&T will provide an experienced Project Manager to act as the key point of contact for all activities from kickoff call through service hand off to support. The Project Manager will work with you to ensure a smooth path to a successful implementation of the complete solution – from hosting environment, to configuration and installation of MDM, through on-boarding.

Operate, Manage and Optimize
AT&T provides a highly available and scalable environment for hosting and deploying a customer’s MDM application. Key elements include:

• Hosting – MDM application is hosted in an AT&T world-class internet data center
• Setup of MobileIron Hosted from AT&T – AT&T handles all aspects of the MobileIron VSP application and Sentry (if applicable): staging, configuration and testing
• Continuous Performance
  • Monitoring – Proactive monitoring and maintenance of systems, networks, application and interfaces on a 24x7x365 basis. The AT&T help desk provides lifecycle services for your MobileIron Hosted from AT&T solution and helps ensure that your application is available whenever you need to administer your mobile assets. AT&T help desk includes:
    – Single point of contact for customer’s help desk to engage AT&T Triage, escalation and tracking/resolution of all service related events
    – Change Management – AT&T applies prompt, accurate and documented system changes to reduce disruption. We manage patches, fixes and updates to keep your applications stable and allow you to take advantage of new features as they become available

Advanced Authentication Using Certificates and Kerberos Delegation
To use Certificate Authentication, the customer’s MDM server will need to be configured to issue certificates. Certificate authentication provides enterprises the ability to establish identity while eliminating the need for end users to enter usernames and passwords on their mobile devices to access corporate resources, such as Exchange ActiveSync, VPN and Corporate Wi-Fi.

Service Scope
AT&T will implement and configure the integration settings to enable the MobileIron Virtual Smartphone Platform (VSP) appliance to issue certificates to mobile devices from a supported interface to the customer’s Certificate Authority. AT&T will complete the Certificate Authority integration configuration and:

• Create one certificate template representing the customer’s desired type of identity certificate
• Define one device policy profile for Exchange ActiveSync auto-configuration using an MDM-issued identity certificate
• Define one device policy profile for VPN client auto-configuration using an identity certificate
• Define one device policy profile for preferred WiFi network auto-configuration using an identity certificate
• Configure the service accounts in Active Directory (User or Computer object) for Kerberos authentication delegation and create service principal names (SPNs) if necessary
• Configure the email proxy service to request Kerberos delegated credentials on behalf of device users for mailbox access

AT&T will assist with the testing of each device profile on a single supported device.*

For more information contact an AT&T Representative or visit www.att.com/mdmservices and www.att.com/mobileiron.

* Diagnosis and remediation of failed test cases to verify that a certificate of the correct type is issued by the Certificate Authority and installed within the device certificate store. The customer is responsible for any diagnosis or remediation of authentication or authorization failures within the authentication, authorization and accounting (AAA) infrastructure.

06/03/13 AB-2652
© 2013 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.