MobileIron VSP from AT&T – Managed Hosted MDM Solution

MobileIron VSP from AT&T – Managed Hosted Mobile Device Management (MDM) (the “Solution”) is a cross carrier solution offering customers maximum flexibility in solving the challenges of the expanding mobile perimeter and enabling highly secure use of mobilized information. The Solution supports most popular smartphones and tablets and consists of the MobileIron Virtual Smartphone Platform (“VSP”) application, an optional Sentry email access control application, hosting infrastructure and lifecycle management.

This Solution combines MobileIron MDM software with AT&T-provided consultation, design, implementation, hosting and management, and is delivered as a turnkey solution. The Solution offers lower total cost of ownership and a compelling advantage over disparately assembled and self-managed on-premises mobile solutions.

Key Differentiators and Benefits

- AT&T’s experience in solution deployment, hosting, management and support reduces the risk in your investment
- Dedicated and highly customizable environments optimize lifecycle management and enable continual improvement of the Solution and your customer experience
- Highly secure and resilient options
- Uses an end to end AT&T MPLS network with no Internet vulnerabilities, making it ideal for industries where security is paramount
- Application Management Services provide flexible deployment options and low cost of ownership in an AT&T hosted environment
- Expertise that augments and complements your IT and security staff
- Robust integration with your IT organizations
- Highly secure document access and data loss prevention (DLP) through the optional Docs@Work feature
- Containerization of apps to protect data-at-rest without touching personal data through the optional AppConnect feature
- Highly secure tunneling and access control to protect app data-in motion through the optional AppTunneling feature
- Highly secure browser capability through the optional Web@Work feature
- Self-service device enrollment and management through the optional BYOD portal

Optional feature bundles are available – see your account representative for details.

Content and Mobile Web Apps

The Web@Work enterprise mobile browser enables near real time, highly secure access to internal websites and web applications, while helping to preserve a native web browsing experience.

- Provides IT visibility to corporate intranet
- Enables highly secure, containerized access to enterprise web resources from nearly any mobile device without the need for a VPN
- Provides support for HTML 5 web apps
- Helps retain the look-and-feel of industry standard mobile web browsers
- Enables passcode authentication

Potential Benefits

- Protect enterprise information on mobile devices
- Enforce end user compliance
- Reduce the total cost of ownership of mobile data solutions
- Enable more efficient end user engagement
- Increase productivity and effectiveness
- No need for capital expenditures

Features

- Over-the-air monitoring and enforcement of security policies
- Helps ensure that devices are performing properly
- Supports enterprise applications and processes
- Highly secure safeguards for enterprise information
- Real-time, over-the-air configuration and diagnostics
- Speeds up application and device deployment

Want to learn more?
Have us call you.

Share this with your peers

Access to Essential Documents

Docs@Work gives end users an intuitive way to access, store, and view documents from email and SharePoint and lets administrators establish data loss prevention (DLP) controls to protect these documents from unauthorized distribution. Users can now take full advantage of their devices for highly secure access to enterprise content and collaboration.

- Help keep control of enterprise documents
- Assist in preventing unauthorized distribution of email attachments into consumer email services
- Highly secure native email experience that eliminates the need to use third-party email applications
- View and store SharePoint documents
- Help prevent data loss by controlling use of cut/copy/paste
- Lower administrative cost through tight integration with existing enterprise infrastructure

World Class Highly Secure Hosting Infrastructure

- Tier 4 Internet Data Centers (highest available rating)
- Redundant Global Network Operation Centers
- Periodic Security audits standard
- Advanced Intrusion Detection & Firewall
- Remote Management (optional)
- Onsite/offsite backup and archiving (optional)

Solution Components

The Solution enables highly secure multiplatform control of enterprise smartphones via an AT&T managed service. This Solution is one of the first to combine data-driven smartphone management with real-time wireless cost control. It provides multiplatform visibility for industry-leading smartphones operating on all the most popular OSs. The VSP enables your IT team to know what's on a smartphone and how it's being used. It also gives them proactive visibility to both enterprise owned and employee-owned devices to better secure data and control costs without compromising privacy, even on employee-owned phones.

Advanced Management

The Solution helps your IT team quickly establish and maintain operational control of smartphones and manage all major smartphone operating systems from a single point. To help you proactively manage and cut wireless bills, the optional Mobile Activity Intelligence ("MAI") package is available for use on Windows Phone, BlackBerry and Symbian devices. MAI gives IT, finance and end users a detailed view of phone usage, so that bill shock can become a monthly ritual of the past.

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 MDM 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 hand off to ongoing support. The Project Manager will work with you to provide a smooth path to a successful implementation of the complete Solution – from hosting environment, to MDM configuration and installation, through on-boarding.

Operate, Manage and Optimize

AT&T provides a highly available and scalable environment for hosting and deploying the MDM application. Key elements include:

- Hosting – The MDM application is hosted in one of AT&T's world-class internet data centers
- Setup of MobileIron VSP – AT&T handles all aspects of the staging, configuration and testing of the MDM application
- Continuous Performance Monitoring – AT&T provides proactive monitoring and maintenance of systems, networks, application and interfaces on a 24x7x365 basis

Ongoing Support

The AT&T help desk provides lifecycle services for your Solution and helps ensure that it is available whenever you need to administer your mobile assets. AT&T's help desk includes:

- A single point of contact for your help desk to engage AT&T for triage, escalation and tracking/resolution of all service related events
- Change Management – We apply prompt, accurate and documented system changes to reduce disruption. We manage patches, fixes and updates to keep your applications stable and enable you to take advantage of new features as they become available
- High Availability – Our application management services are fully integrated into AT&T's robust, reliable and global infrastructure

(REQUIRED) MDM Software Installation and Configuration Services

(Required) Two Day Remote Engagement for Microsoft Exchange Installations

AT&T Mobility Solution Services ("MSS") will provide a pre-installation checklist to enable you to prepare your environment. AT&T will also provide a survey document to record your policy requirements by user group. AT&T will conduct a pre-installation call to review the data you provided, which AT&T will use during the software installation and configuration process. Then AT&T will:

- Remotely install the MobileIron Sentry software on one server
- Configure system parameters and set up administrator accounts and roles
- Configure and test integration with defined Customer servers and services including ActiveSync, Proxy, Exchange Server, BES Server, LDAP/AD, and SMTP
- Enroll and register up to 10 devices for a pilot group and test the registered devices for compliance

AT&T will also conduct a 2 hour administrator training via web-conference covering the administrator portal and the creation of user groups, polices and device registration.

Want to learn more?
Have us call you.

Share this with your peers

(REQUIRED) AT&T MSS Managed Services Application Service Desk (ASD)*

AT&T managed services support is provided by the AT&T MSS Managed Services Application Service Desk ("ASD") organization.
The ASD is comprised of experienced, industry certified professionals who provide hands-on, comprehensive, proactive, managed services and technical support. This service enables customers to rely upon AT&T for triage, support, and how-to/FAQs with additional options for customers who require day-to-day administration of their managed services platform. All such plans have a one-time setup fee.

ASD 9x5 Support is an option if you intend to provide the day-to-day administration of your MDM platform and prefer to utilize AT&T for triage, support, and How-To and FAQs during standard business hours. It includes:

- Help desk to help desk technical support from Monday to Friday, 8am-5pm local time, based on your support headquarters location provided from personnel in the US,, with the ability to report Severity 1 (outage) events 24x7x365
- Support from AT&T's carrier-class service desk to triage, escalate and attempt to resolve service issues and support requests
- Single point of contact for Tier 2+ support to address interoperability between multi-carrier mobile devices, network, MDM platform, mobile applications and hosted infrastructure
- Trained and experienced support staff with cross solution expertise with MDM, OEM, OS and application platforms (CCNA, CCNP, MCSA, CISSP)
- How-To and FAQ support for MDM platform use, configuration and best practices.

ASD 24x7 Support offers Customers all of the features of the 9x5 Plan plus:

- 24x7x365 Tier 2+ Technical Support
- Support after U.S. 9x5 hours may be provided by personnel outside the U.S.

Customer is solely responsible for its employees', agents' and subcontractors' use of the MDM Console, including, without limitation, the enrollment and retirement of MDM device users.

ASD Remote Administration Support Plan is a comprehensive program available in either Basic or Advanced format and designed for organizations that have limited internal support resources and mobile expertise. AT&T will hire, train and maintain the staff needed to administer the Customer's MDM platform, and provide a dedicated MDM consultant to assist the Customer.

In addition to the services included in the 24x7 Plan, the ASD Remote Administration Support Plan includes:

- A managed service solution for which AT&T provides comprehensive daily, ongoing configuration and lifecycle administration of the managed service that includes user management, policy management, device configuration management and app and content management. In addition, Customers have access to the Solution Console for the following: Dashboard View; Verify Device Enrollment or Registration; Passcode Reset/Unlock, Lock Device; Locate/Find; Send Messages; Run/Create Reports; Add/Delete Users; and Device Enrollment (Bulk or Individual) and Wipe
- An assigned MDM Consultant who will provide recommendations and ongoing consultation on the Customer's MDM design, implementation and administration
- Support that enables the Customer to update security policies and authorized device configurations quickly
- Annual Managed Service Health Checks for Customer installations with at least 500 devices

The Basic level of ASD Remote Administration Support includes:

- Multiple managed user groups
- Multiple device OS support
- Multiple device configuration profiles
- Application management
- No integration with email or other integration points

The Advanced level of ASD Remote Administration Support offers all the features of ASD Remote Administration Basic Support plus:

- Certificate management
- Complex network architecture support
- MDM special features support
- Support for MDM integration with email

AT&T will not provide technical support to end users and will not provide technical support for the applications and/or content that Customer chooses to distribute and which are not included in the Solution's feature list. Customer shall not instruct end users to call AT&T Customer Care at 611 or any other carrier's customer care center in connection with end users' use of AT&T.

Advanced Authentication Using Certificates and Kerberos Delegation

To use Certificate Authentication, your MDM server will need to be configured to issue certificates. Certificate authentication provides the ability to establish users' identity while eliminating the need for them to enter usernames and passwords on their mobile devices to access enterprise resources, such as Exchange ActiveSync, VPN and Enterprise Wi-Fi.

Service Scope

AT&T will implement and configure the integration settings to enable your VSP appliance to issue certificates to mobile devices from a supported interface to your Certificate Authority. AT&T will complete the Certificate Authority integration configuration and:

- Create one certificate template representing your 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
- Assist with the testing of each device profile on a single supported device**

Want to learn more?
Have us call you.

Share this with your peers

Important Information

A minimum of 500 Solution licenses is required for initial purchase.

The Solution's functionality is limited to certain mobile devices and operating systems. A list of compatible devices and operating systems is available by contacting an AT&T Account Executive. Not all features are available on all devices.

All fees paid for the Solution are non-refundable.

The Solution is available only to customers with a qualified AT&T business or government agreement ("Enterprise Agreement") and a Foundation Account Number ("FAN").

The Solution is available for use with multiple network service providers. Both Customer Responsibility Users ("CRUs") and Individual Responsibility Users ("IRUs") are eligible to participate in the Solution. For users subscribed to an AT&T wireless service, activation of an eligible AT&T data plan on a compatible device with short message service ("SMS") capabilities and software from MobileIron Inc. ("MobileIron") is required.

With respect to use of the Solution with devices subscribed to non-AT&T wireless providers, Customer is responsible for ensuring that Customer, its applicable end users and the Solution comply with all applicable terms of service of such other wireless carrier(s). All associated voice, messaging and data usage will be subject to the applicable rates and terms of such other wireless carrier(s). Refer to applicable wireless carrier(s) for such rates, terms and conditions. A compatible device with SMS capabilities and Solution software is required.

The Solution's administrative interface is accessed via a Web portal and requires a PC with Internet connection.

The Solution may be used as a tool to configure and customize certain settings and features and perform software updates only for compatible devices. Improper or incomplete configuration and/or downloads performed by Customer may result in service interruptions and/or device failures. AT&T does not guarantee compliance with such customized settings and/or updates.

AT&T reserves the right to (i) modify or discontinue the Solution in whole or in part and/or (ii) terminate the Solution at any time without cause.

Additional hardware, software, service and/or network connection may be required to access the Solution.

The Solution is subject to the terms and conditions of the applicable Enterprise Agreement between AT&T and Customer and a MobileIron User License Agreement ("EULA"), which is located at https://info.mobileiron.com/EULAClickTHrough_EULARegistrationPage.html

The EULA must be accepted at the time the client application is downloaded or before its first use. If Customer does not accept the terms of the n EULA, Customer must not use the Solution. Customer must accept the EULA as the party liable for each CRU and agrees in such case that each CRU will comply with the obligations under the EULA. Customer is responsible for providing each CRU of an enabled mobile device with a copy of the EULA. The Customer and the CRU are individually and jointly liable under the EULA. Customer shall not enroll IRUs or BYOD users in the Solution unless it has obtained and preserves proof that each IRU and BYOD user has reviewed and accepted the terms and conditions of the EULA, and Customer shall indemnify and hold harmless AT&T against all claims by any IRU relating to or arising from such IRU's or BYOD user's use of the Solution if the IRU or BYOD user has not accepted the terms and conditions of the EULA. In addition, if and to the extent that end users who are not residents of the United States, download and use the software outside of the United States, Customer agrees to be subject to the Country Specific Provisions in the Solution Service Guide located at http://serviceguidenew.att.com/sg_CustomPreviewer?attachmentId=00PC000000PL27iMAD

Data Privacy: Customer Personal Data may be transferred to or accessible by (i) AT&T personnel around the world (ii) third-parties who act on AT&T's or AT&T's supplier's behalf as subcontractors; and (iii) third-parties (such as courts, law enforcement or regulatory authorities) where required by law. Customer will only provide or make Customer Personal Data accessible when Customer has the legal authority to do so and for which it has obtained the necessary consents from its end users, and will camouflage or securely encrypt Customer Personal Data in a manner compatible with the VSP. As used in this Service Guide, the term Customer Personal Data includes, without limitation, name, phone number, email address, wireless location information or any other information that identifies or could reasonably be used to identify Customer or its end users. Customer is responsible for providing end users with clear notice of AT&T's and Customer's collection and use of Customer Personal Data obtained via the VSP and for obtaining end user consent to that collection and use. Customer may satisfy its notification requirements as to AT&T by advising end users in writing that AT&T and its suppliers may collect and use Customer Personal Data by providing for end user review the relevant links to the Product Brief or other sales information that describes the Solution and to AT&T's Privacy Policy at http://www.att.com/gen/privacy-policy?pid=2506.

Professional Services: Upon completion of Professional Services, Customer must either sign the acceptance document AT&T presents or provide within five business days of the service completion date written notice to AT&T identifying any non-conforming Professional Services. If Customer fails to provide such notice, Customer is deemed to have accepted the Professional Services. AT&T reserves the right to conduct work at a remote location or use, in AT&T's sole discretion, employees, contractors or suppliers located within or outside the United States to perform work in connection with the Solution. Customer will in a timely manner allow AT&T access as reasonably required for the Professional Services to property and equipment that Customer controls. Customer will ensure that the location(s) to which access is provided offer(s) a safe working environment, free of hazardous materials and reasonably suitable for the Professional Services. The Professional Services provided shall be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. The mandatory software installation and configuration is estimated to take two days. If the Professional Services provided in connection with the Solution are more complex than those described in this Product Brief, then a separate statement of work describing the activity and related terms and pricing will be executed. If impediments, complications or Customer-requested changes in scope arise (Changes), the schedule, Solution and fees could be impacted. In the event any Change(s) affect the Solution or fees, the parties will modify Customer's order (or statement of work, if applicable) accordingly by executing a Change Order.

AT&T reserves the right to perform work at a remote location or use, in AT&T's sole discretion, employees, contractors or suppliers located outside the United States to perform work in connection with or in support of the Solution.

Exclusive Remedy: Customer's sole and exclusive remedy for any damages, losses, claims, costs and expenses arising out of or relating to use of the Solution will be termination of service.

Share this with
your peers

For more information contact an AT&T Representative or visit att.com/mobilitysolutions.

*Customers that have previously subscribed to the now discontinued Silver, Gold or Platinum ASD plans should contact an Account Representative for details.

**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.