MobileIron Connected Cloud from AT&T (the Solution) is a cloud-based mobile device management (MDM) solution that manages mobile applications, documents and devices in a highly secure manner.

**Highly Secure Multiplatform Control of Smart Devices**

MobileIron Connected Cloud from AT&T is the Software as a Service (SaaS) version of the MobileIron VSP from AT&T on-premises solution. Offering a comprehensive mobile solution that also provides deep integration with enterprise IT infrastructure, the Solution is a high availability service that can scale to thousands of users and devices and helps keep data and operations highly secure.

Currently available for iOS and Android devices, MobileIron Connected Cloud from AT&T provides:

- Robust mobile device management (MDM), mobile app management (MAM), and mobile content management (MCM) capabilities
- Comprehensive policy and compliance management and enforcement
- 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
- Help@Work provides a help desk tool for remote view of end-user devices
- 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 HTML5 web apps
- Enables passcode authentication
- Simplify authentication using Kerberos Proxy

**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
- Highly secure native email experience that eliminates the need to use third-party email applications

**Potential Benefits**

- Increased efficiency and flexibility through IT management of data on multiple OSs and devices
- Provide mobile device management, mobile app management, and mobile content management capabilities
- Integrate with on-premises enterprise services, such as AD/LDAP directory services and enterprise email
- Manage the mobile app lifecycle while preserving user experience
- Help keep enterprise documents under control

**Features**

- Multi-OS Device Management
- Access Control Advanced Security
- Lost Phone Recovery/Wipe
- Accessible from Enterprise App Store
- Integration with enterprise directories
• View and store SharePoint documents
• Help prevent data loss by controlling use of cut/copy/paste

Our new Platinum bundle includes all these optional features for $7 per month per device, or $10 per month per user. See your account representative for details.

(REQUIRED) MDM Software Installation and Configuration Services

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 if necessary
• 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.

(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 ASD plans have a one-time setup fee.

MobileIron Connected Cloud from AT&T provides the following capabilities for iOS and Android platforms:

• Device management
• Over the Air (OTA) provisioning
• Send alerts of policy violations
• Accessible from enterprise app store
• Broadcast SMS, Email and Apple Push Notification Service (APNs)
• Help protect data at rest

Optional integration with enterprise systems:

• ActiveDirectory/LDAP
• Exchange ActiveSync

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 U.S., 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 your MDM platform, and provide a dedicated MDM consultant to assist you.

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 you to update security policies and authorized device configurations quickly
• Annual Managed Service Health Checks for 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

(OPTIONAL) MDM Readiness Workshop
If you do not know how to get started in developing your mobility governance and do not have any policies defined, the MDM Readiness Workshop may be a good starting point. During this four hour interactive workshop, the following activities will be facilitated:

Data Classification
Starting with a generic data taxonomy, a facilitated discussion will produce an enhanced data classification schedule for the mobility initiative.

User Classification
Starting with a generic user constituency taxonomy, a facilitated discussion will produce a list of defined user groups and qualification criteria.

Application Inventory
Starting with a generic list of common horizontal applications built into mobile devices, an expanded list of applications required by the mobility initiative will be identified.

Interface Model
Using the application inventory, a finite number of interface models will be derived for application access to enterprise data.

User/Application Data
Sensitivity Matrix - A matrix showing the sensitivity of data accessed by each user group for each application will be developed. The highest sensitivity level for data accessed by each user group will be identified.

Device Inventory
A list of mobile device operating systems to be supported will be developed. At the conclusion of this session you will have a set of workbooks to continue to define your classifications which you can use as the foundation for mobility policy development.

(OPTIONAL) MobileIron Health Check
AT&T recommends an annual review of your existing MobileIron system. The Health Check service is a review of:

• Up to two Sentrys
• VM inspection
• Software configurations state and error logs
• Policy definitions (for errors)
• Mobile device status

Following the review, AT&T will provide you a summary report of the findings and recommendations, including a list of registered mobile devices that are no longer under management. This service is performed remotely.

(OPTIONAL) Installation of One Additional MobileIron Sentry
If you require the installation of one additional MobileIron Sentry, AT&T will install it on a server that you provide and integrate it with the Solution. You will provision and set up and configure any load balancing equipment or software required to front end the MobileIron Sentry software.

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 you the ability to establish identity while eliminating the need for end users to enter usernames and passwords on their mobile devices to access enterprise resources, such as Exchange ActiveSync, VPN and Corporate Wi-Fi.

Service Scope
AT&T will implement and configure the integration settings to enable you 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 the 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.

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.
Important Information and Additional Terms

A minimum of 50 Solution licenses is required for initial purchase.

The Solution's functionality is limited to certain mobile devices and operating systems. A list of supported operating systems is available at AT&T.com http://www.att.com/#bid=11uq, JBa28n or 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 whose devices are 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's applicable end users and the Solution complies 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.

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 Solution. 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 Solution 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.

The Solution is subject to the terms and conditions of the applicable Enterprise Agreement between AT&T and Customer and a separate MobileIron Connected Cloud Software as a Service ("SaaS Agreement") with MobileIron in order to access and use the Solution MobileIron is solely responsible for all items provided pursuant to the SaaS Agreement. The SaaS Agreement must be accepted before Customer's first use of MobileIron Connected Cloud. If Customer does not accept the terms of the MobileIron SaaS Agreement, Customer must not use the Solution. Customer must accept the SaaS Agreement as the party liable for each CRU, and agrees in such case that the CRU will comply with the obligations under the SaaS Agreement. Customer is responsible for providing each CRU of an enabled mobile device with a copy of the SaaS Agreement. The Customer and the CRU are individually and jointly liable under the SaaS Agreement. A copy of the SaaS Agreement is found at https://info.mobileiron.com/saasform.html. 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 SaaS Agreement, and Customer shall indemnify and hold harmless AT&T against all claims by any IRU or BYOD user 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 SaaS Agreement. In addition, if and to the extent that end users who are not residents of the United States download and use the Solution software on devices 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=00PC0000000000PMjvcMAX.

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 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.

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

**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.

***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.