MobileIron Connected Cloud from AT&T

MobileIron Connected Cloud from AT&T is a cloud-based Mobile Device Management that secures and manages mobile apps, docs and devices.

Highly Secure Multiplatform Control of Enterprise Smart Devices
MobileIron Connected Cloud from AT&T is the Software as a Service (SaaS) version of MobileIron VSP from AT&T on-premises solution. Offering a comprehensive mobile solution that also provides deep integration with enterprise IT infrastructure, MobileIron Connected Cloud from AT&T is a high availability service that can scale to thousands of users and devices and is highly certified for data and operations security.

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

- Full mobile device management (MDM), mobile app management (MAM), and mobile content management (MCM) capabilities.
- Comprehensive policy and compliance management and enforcement
- Layered security with posture detection, automated remediation and certificates
- Privacy controls, selective wipe, and separation of the enterprise workspace to secure data without compromising privacy in BYOD deployments
- Highly secure document access and data loss prevention (DLP) through Docs@Work
- Containerize apps to protect data-at-rest without touching personal data through AppConnect
- App Tunneling provides highly secure tunneling and access control to protect app data-in-motion

Tight Integration with Enterprise Resources
Mobile devices are now a critical computing platform requiring a connection to corporate resources and data. Therefore a successful mobile strategy must help connect mobile devices with these resources while enforcing security policies. MobileIron Connected Cloud from AT&T offers the ability to integrate with on-premises enterprise services, such as Microsoft Exchange, Active Directory and LDAP Directory. As a result of those integrations, MobileIron Connected Cloud from AT&T delivers a limited footprint cloud-based MDM solution.

iPhone and iPad Access to Essential Documents
Docs@Work gives the end user an intuitive way to access, store, and view documents from email and SharePoint and lets the administrator establish data loss prevention (DLP) controls to protect these documents from unauthorized distribution. Employees can now take full advantage of the iPhone and iPad for secure enterprise content and collaboration.

- Help keep corporate documents under enterprise control
- Assist in preventing unauthorized distribution of email attachments into consumer services like Dropbox
- High securely the native email experience on iOS and eliminate the need to use third-party email applications
- View and store SharePoint docs
- Help prevent data loss by controlling cut/copy/paste
- Lower administrative cost through tight integration with existing enterprise infrastructure

Potential Benefits
- Increased efficiency and flexibility through IT management of data on multiple OS and devices
- Provide mobile device management, mobile app management, and mobile content management capabilities
- Reduced costs by organizing device chaos and allowing employee-owned devices
- Integrate with on-premises enterprise services, such as AD/LDAP directory services and enterprise email
- Leverage the most trusted mobile IT cloud service, with SOC 2 Type 1 audit, TRUSTe Privacy Seal, EU Safe Harbor, and operational transparency
- Help secure the mobile app lifecycle while preserving user experience
- Keep corporate documents under enterprise control

Features
- Multi-OS Device Management
- Access Control (Sentry)
- Advanced Security
- Lost Phone Recovery
- Enterprise App Store
- Administration
- Enterprise Integration
- Exception and Abuse Control
(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 server. 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 VSP Software on one server and 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, policies 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 AT&T Application Service Desk is comprised of experienced, industry certified professionals who provide hands-on, comprehensive, proactive, managed services and technical support. This service is intended for customers who require the day-to-day administration of their managed services platform and leverage AT&T for triage, support, and how-to/FAQs.

The application support provided by AT&T includes the following:

• Standard application warranty – included with all application and solution deployments
• Three tiers of annual support package options
  – Silver
  – Gold
  – Platinum

Packages include varying levels of response times, support hours, and access to mobility solution SMEs to resolve technical issues.

(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:

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

MobileIron Connected Cloud provides the following features for iOS and Android platforms:

• Device management
• Over the Air (OTA) provisioning and application certificates thru Simple Certificate Enrollment Protocol (SCEP)
• Selective wipe (email)
• Enterprise app store
• Broadcast SMS. Email and Apple Push Notification Service (APNs)
• Event Center (triggers, actions)
• View documents
• Store documents securely on the device
• Protect data-at-rest with iOS data protection
• Selectively wipe documents

Enterprise Integration with:
• ActiveDirectory/LDAP integration (Connector)
• Exchange ActiveSync access control (Sentry)
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 MobileIron VSP. You will provision and set up and configure any load balancing equipment or software required to front end the MobileIron Sentry software.

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

Important Information:
Solution Components: A minimum initial purchase of 50 MobileIron Connected Cloud licenses is required. Hardware appliances (servers) are optional and, if purchased, an additional per appliance charge will apply. All fees paid for MobileIron Connected Cloud are non-refundable. Additional fees, charges, taxes and restrictions may apply.

Requirements; Technical Information: MobileIron Connected Cloud is available only to customers with a qualified AT&T Business Agreement. Customer’s end users must subscribe to a data plan on a compatible device with Short Messaging Service (SMS) capability. MobileIron Connected Cloud may not be accessible at all times.

Availability, security/privacy, delivery and timeliness of information are not guaranteed by AT&T MobileIron Connected Cloud is accessed via a Web portal and requires a PC with Internet connection. Improper or incomplete software configuration and/or downloads performed by you may result in service interruptions and/or device failures.

Software as a Service Agreement: MobileIron Connected Cloud from AT&T is subject to the software as a service agreement found at https://info.mobileiron.com/saasform.html. Failure to comply with the terms and conditions of the software as a service agreement may result in termination of the offer. The solution may require use of third-party products and/or services. All intellectual property rights used in providing or arising by virtue of (i) MobileIron Connected Cloud and (ii) any professional services and related materials provided hereunder are and will be sole and exclusive property of AT&T or MobileIron, as applicable. Neither ownership nor title of such intellectual property will pass to Customer. CUSTOMER’S SOLE AND EXCLUSIVE REMEDY FOR ANY DAMAGES, LOSSES, CLAIMS, COSTS AND EXPENSES ARISING OUT OF OR RELATING TO USE OF THE SERVICE WILL BE TERMINATION OF THE SERVICE.

Customer Personal Data: 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 Product Brief, 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 Sales Information that describes the availability of optional goods, content or services and AT&T’s Privacy Policy at http://www.att.com/gen/privacy-policy?pd=2506. Term and Termination: Minimum payment period is two years from date on which customer signs order acknowledgement. At expiration of the initial two year term, the parties’ agreement regarding MobileIron Connected Cloud will automatically renew for successive one month terms until terminated by either party by giving the other party 30 days’ prior written notice. If after service commencement AT&T terminates the MobileIron Connected Cloud or any component thereof for cause or if Customer terminates any component thereof other than for cause, in addition to amounts owed up to the effective date of termination, Customer will pay 50% of the charges for the terminated offer or offer component attributable to the unexpired term of the applicable minimum payment period. AT&T reserves the right to (i) modify or discontinue offering the MobileIron Connected Cloud in whole or in part and/or (ii) terminate at any time without cause.

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. Customer acknowledges that AT&T and Customer are independent contractors. 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 MobileIron Connected Cloud from AT&T. Customer must 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 and must be completed within 45 days of order placement. If Customer’s acts or omissions cause delay of installation and configuration beyond 45 days of order placement, AT&T will invoice Customer for the installation and configuration charges after the 45th day. If the professional services provided in connection with the MobileIron Connected Cloud are more complex than those described in this product brief, then a separate statement of work describes the activity and related terms and pricing will be executed. If impediments, complications or Customer-requested changes in scope arise (Changes), the schedule, MobileIron Connected Cloud and fees could be impacted. In the event any Change(s) affect the MobileIron Connected Cloud or fees, the parties will modify Customer’s order (or statement of work, if applicable) accordingly by executing a Change Order.