AT&T Unified Endpoint Management
MobileIron Core from AT&T

AT&T Business

Unlock the benefits of mobility to work faster, better, and smarter

The MobileIron Core from AT&T solution provides organizations with the platform required to more effectively secure mobile apps, content, and devices.

Users benefit from near seamless access to the business processes and content on mobile devices of their choice, while providing IT the ability to more effectively secure corporate data on both corporate and personally owned mobile devices. By providing a modern Unified Endpoint Management (UEM) solution that supports both business productivity and IT security requirements, MobileIron Core enables today's enterprises to become mobile first.

The MobileIron Core from AT&T bundles are specifically designed to support the 3 main phases of the mobile first journey: 1) Device and Email Security, 2) Mobile App and Content Enablement,

Potential benefits

- Mac OS, Windows 10, iOS, and Android management available
- Multi-OS Security
- Effective data security and compliance
- Secure the mobile app lifecycle while preserving user experience
- Help Desk and IT reporting and efficiency

Features

- Secure enterprise gateway
- Secure applications and app specific VPNs
- Single sign on
- Enterprise app store
- Workflow integration
- Visibility and reporting
- End-user and self-service via BYOD portal
- Access provides conditional access to services from mobile apps and browsers
- MobileIron Threat Defense provides a view into malicious threats using one app on iOS and Android devices

and 3) Business and IT Transformation. Each bundle provides essential capabilities required to successfully deploy each phase of the mobile first journey. With the MobileIron Core from AT&T platform, organizations have the foundation they need to build a mobile security program that enables choice while addressing specific mobile security requirements.

Core Silver bundle

The Silver bundle provides all the essential capabilities required to build the foundation of a mobile first enterprise. The UEM Silver bundle includes capabilities that allow for near seamless device onboarding, configuration of security settings, app distribution, policy enforcement, and remediation.

Core Gold bundle

The Gold bundle is designed for customers ready to take the next step of the mobile-first Journey by providing highly secure apps and content on any mobile device.

Core Platinum bundle

The Platinum bundle is designed for organizations that have a solid mobile foundation and are ready to enter the advanced stages of the mobile-first Journey. The Platinum bundle provides additional capabilities including highly secure per-app VPN, Help Desk tools for remote viewing and control over end-user devices, and integrations with specific third-party products and services.

MobileIron optional add-on features

Access

MobileIron Access is a cloud security solution that provides conditional access to cloud services from mobile apps and browsers. Unlike traditional security approaches, MobileIron Access correlates user identity with unique information feeds such as device posture and app state. MobileIron helps ensure that business data stays within IT bounds so it can't be stored on unsecured devices or shared with unauthorized cloud services. With MobileIron Access Authenticator, organizations benefit from a standards-based approach that can more effectively secure any cloud service, including Office 365, without requiring proprietary integrations.

For the best performance, Gold licenses are advised for the best performance, Gold licenses are advised. MobileIron Access Authenticator is only available in a per User – Subscription License. Additional installation and configuration services may be required.

MobileIron Threat Defense

MobileIron Threat Defense guards your company from data loss from mobile threat events. With one app, detect and remediate known and zero-day attacks on the mobile device without disruption to user productivity.

AT&T Business

	Silver	Gold	Platinum
Core Portal	•	•	•
Sentry	•	•	•
Apps@Work	•	•	•
AppConnect	•	•	•
Email+	•	•	•
Kiosk Mode/ Apple Business Manager	•	•	•
Bridge and Derived Credentials		•	•
Docs@Work		•	•
Web@Work		•	•
Help@Work			•
Tunnel			•
ServiceConnect integrations*			•
MobileIron Access + Authenticator	Add on SKU. Gold bundle recommended.		
MobileIron Threat and MobileIron Threat Defense+	Add on SKU.		
License and pricing options			
Device perpetual license	$75	$110	$140
User perpetual license	$110	$165	$210
Device maintenance - AT&T support	$15	$22	$28
Device maintenance - MobileIron support	$17.30	$25.30	$32.20
User maintenance - AT&T support	$22	$33	$42
User maintenance - MobileIron support	$25.30	$37.95	$48.30
Device subscription license	$48	$72	$90
User subscription license	$72	$108	$138
Device MRC license	$4	$6	$7.50
User MRC license	$6	$9	$11.50

*SerivceConnect integrations available with the Platinum bundle includes MobileIron developed software to integrate with specific thrid-party products and services. API-based integrations do not require the purchase of the Platinum bundle.

Derived credentials with Entrust

MobileIron has worked with Entrust to create a derived credential solution that will enable enterprise and government agencies to extend their existing security investments, such as common access cards (CAC), and personal identity verification (PIV), to give mobile devices highly secure access to agency resources without requiring employees to use additional hardware like sleds or smart card readers. The solution is compliant with government regulations and security standards such as Homeland Security Presidential Directive-12 (HSPD-12), Federal ICAM initiatives, FIPS 201 and NIST SP:800-157.

Additional installation and configuration services may be required.

AT&T Business

Enterprise Support configuration and training – $3,500 (required with Silver licenses)

AT&T will provide implementation services connected with the purchase of the Silver MobileIron Software Licenses. The deployment will be conducted remotely in a hosted environment with the integration supported by on-premises MobileIron Connector to Active Directory in the client's data center and one Sentry.

Enterprise Support configuration and training – $7,500 (required with Gold & Platinum licenses)

AT&T will provide implementation services connected with the purchase of the Gold or Platinum MobileIron Software Licenses. The deployment will be conducted remotely in a hosted environment with the integration supported by on-premises MobileIron Connector to Active Directory in the client's data center and two Sentries.

Installation of one additional MobileIron Sentry – $995 (optional)

If you require the installation of an additional MobileIron Sentry, AT&T will install it on a server that you provide and integrate it with MobileIron Core. Customer will provision, set up, and configure any load-balancing equipment or software required to front-end the MobileIron Sentry software.

Topics include:

- Overview of Core architecture and features
- User management
- Device registration and retirement
- Policy management and security
- Device configuration management
- Application management
- Device troubleshooting
- Reports and logs

Feature add-on options	
Access user subscription	$48
Access user - MRC license	$4
MobileIron Threat Defense device subscription	$60
MobileIRon Threat Defense user subscription	$90
MobileIron Threat Defense+ device subscription	$96
MobileIron Threat Defense+	$144

*SerivceConnect integrations available with the Platinum bundle include MobileIron developed software to integrate with specific third-party products and services. API-based integrations do not require the purchase of the Platinum bundle.

AT&T Business

MobileIron administrator training – $1,500 (optional)

For additional training for system administrators, AT&T will coordinate a web conference for up to 10 people. This half-day training will be a mixture of slide presentation, lecture, and demonstration regarding the MobileIron virtual smartphone platform.

High Availability – $6,000 (optional)

Customers who wish to create a redundant MobileIron Core from AT&T, can utilize the High Availability professional service:

- Review of the customer's existing traffic management and monitoring system required to redirect network traffic to the redundant Core
- Installation of a redundant VSP on the customer-provided platform and one optional sentry (an existing in-service Core is required)
- Installation and testing of the synchronization script between Core. Note: Customer is responsible for providing a server/VM/appliance for the installation of the second Core and to provide a traffic management and monitoring system to redirect network traffic to the redundant Core

Advanced Authentication using Certificates and Kerberos Delegation – $1,750 (optional)

To use Certificate Authentication, the customer's EMM 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 Core 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 settings:

- 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 EMM-issued identity certificate
- Define one-device policy profile for VPN client auto-configuration using anidentity certificate
- Define one-device policy profile for preferred WiFi network auto-configuration using an identity certificate
- Configure the service accounts in ActiveDirectory (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.*

AT&T Unified Endpoint Management
MobileIron Core from AT&T

AT&T Business

Important Information:

General: MobileIron Core as described in this product brief (the "Solution") is available only to eligible customers with a qualified AT&T agreement ("Qualified Agreement"). The Solution is subject to (a) the terms and conditions found at https://info.mobileiron.com/EULAClickTHrough_EULARegistrationPage.html ("Additional Product Terms"); (b) the Qualified Agreement; and (c) applicable Sales Information. For government customers, any Additional Product Terms not allowable under applicable law will not apply, and the Qualified Agreement will control in the event of any material conflict between the Qualified Agreement and the Additional Product Terms. Any service discounts, equipment discounts, and/or other discounts set forth in the Qualified Agreement do not apply to the Solution. The Solution may not be available for purchase in all sales channels or in all areas. Additional hardware, software, service and/or network connection may be required to access the Solution. Availability, security, speed, timeliness, accuracy and reliability of service are not guaranteed by AT&T. Additional fees, charges, taxes and restrictions may apply.

Requirements: The Solution is available for use with multiple network service providers. Both Corporate Responsibility Users ("CRUs") and Individual Responsibility Users ("IRUs") are eligible to participate in the Solution. Activation on an eligible AT&T data plan on a compatible device is required for end users subscribed to an AT&T wireless service. With respect to use of the Solution with devices subscribed to non-AT&T wireless providers, Customer is responsible for ensuring that its 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 is required.

The Solution software requires a MobileIron operating environment server or, where available, the purchase of a MobileIron appliance from AT&T. Customer is responsible for the configuration of the appropriate Domain Name System (DNS) prior to AT&T installation activities. Core integration with enterprise public key infrastructure is not included. The Core is accessed via a Web portal and requires a PC with Internet connection. Improper or incomplete software configuration and/or downloads performed by Customer may result in service interruptions and/or device failures. Optional hardware appliances (servers) are available only to US customers at an additional charge of $7,000 or $20,000 each.

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 Core. As used herein, 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.

Use of the solution outside the U.S.: Customer agrees to comply with the additional terms, conditions and restrictions located at MobileIron Core Service Guide that apply to downloading and use of the Solution outside the United States. AT&T reserves the right to make changes to these terms and conditions and restrictions from time to time.

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. 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 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 Core 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, Core and fees could be impacted. In the event any Change(s) affect the Core 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 (i) modify or discontinue the Solution in whole or in part and/or (ii) terminate the Solution at any time without cause. 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.

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.

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

Share this with your peers