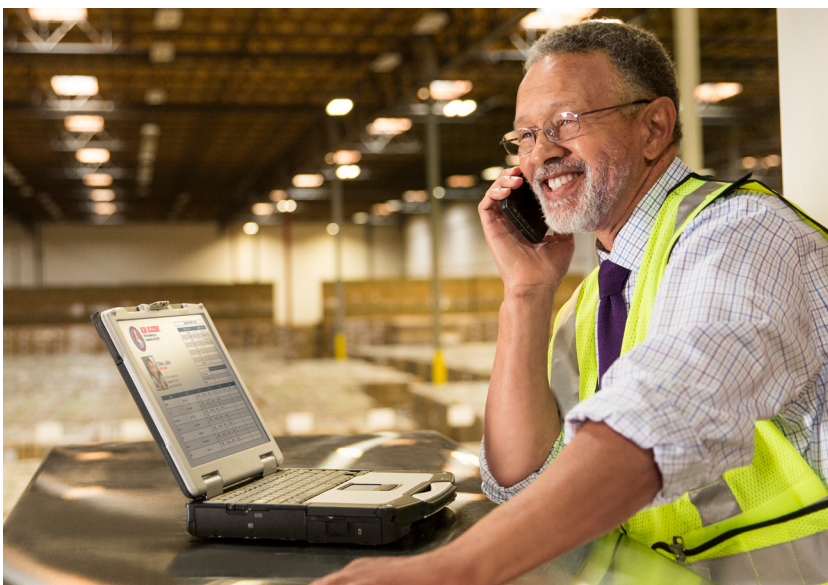


Unlock the benefits of mobility to work faster, better, and smarter



Organizations seeking the agility of the cloud to help them become mobile first turn to MobileIron from AT&T. Built to provide cloud-based Unified Endpoint Management (UEM), MobileIron from AT&T helps customers unlock the benefits of mobile.

Enterprise IT can more easily secure and manage mobile devices, applications, and content while end users can work faster, better, and smarter.

Cloud scale

[MobileIron Cloud](#) from AT&T helps organizations that want to harness the power of mobility and transform their business

dramatically with a cloud first approach. It delivers the layered security of the MobileIron platform via the cloud and is built on a scalable infrastructure to keep up with the proliferation of devices, apps, and data. More seamlessly support millions of devices so that your global mobile enterprise can plan for today and into the future.

Potential benefits

- Mac OS, Windows 10, Android management available
- Enhanced productivity with app management and content integration
- Effective data security and compliance
- Cost-effective and easy integration
- A scalable cloud-based solution

Features

- Licensing choices to maximize your budget; select from either per device or per user licenses
- Email+ provides an email/PIM
- Web@Work offers a secure native web browser
- Tunnel provides a highly secure tunnel per app VPN
- 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

Day-zero Support

MobileIron from AT&T quickly adapts new features with the release of devices, versions, and operating systems and makes them quickly available to

organizations (such as support for Android for Work). With MobileIron from AT&T always staying in step with the latest mobile developments, enterprise IT organizations can help users stay productive on the latest iOS, Android, and Windows Phone devices.

| Bundle features | Silver | Gold | Platinum |
|--|--------------------------------------|------|----------|
| 24X7 ASD Support | • | • | • |
| Cloud Admin Console | • | • | • |
| Remote Wipe Options | • | • | • |
| AD/LDAP Integration | • | • | • |
| Sentry | • | • | • |
| Kiosk Mode/ Apple Business Manager | • | • | • |
| Bridge and Derived Credentials | | • | • |
| Apps@Work | | • | • |
| AppConnect | | • | • |
| Email+ | | • | • |
| 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. | | |

*ServiceConnect 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.

Enterprise-grade security

MobileIron Cloud from AT&T has been designed to offer an intuitive experience to both IT administrators and end users without compromising on security. IT administrators can readily create complex policies and instantly take action based on dynamic device states, while users can search and interact with apps and content in the same way as they do with personal apps and files. Built to integrate with everyday workflows, MobileIron from AT&T delivers a virtually seamless experience and eliminates the excessive burden of training IT or end users.

Security and certifications

MobileIron Cloud from AT&T is one of the most trusted Mobile IT cloud services in the industry. We have completed a SOC 2 Type 2 assessment to audit the operational and security processes of the service. We have the TRUSTe Privacy Seal, signifying that the company's privacy policy and practices have been reviewed for transparency, accountability, and choice regarding the protection of customer information and certifying compliance with EU privacy requirements.

In addition, the MobileIron from AT&T platform has received FedRAMPSM Authority to Operate (ATO). FedRAMP ATO recognizes that MobileIron Cloud has passed the federal risk management process defining standard security requirements for all cloud providers.

| Certifications and compliances |
|--------------------------------|
| FISPI 140 Level 2 |
| NIAPP MDM PP |
| NSA Approved |
| CJIS |
| Derived Credentials/PIV |

MobileIron optional add-on features

Access + Authenticator

MobileIron Access + Authenticator is a cloud security solution that provides conditional access to cloud services from mobile apps and browsers. Unlike traditional security approaches, MobileIron Access + Authenticator 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.

| Supported browsers |
|------------------------------------|
| Chrome for Windows and Mac |
| Safari for Mac, No Windows support |
| Firefox for Windows and Mac |

For the best performance, Gold licenses are advised. MobileIron Access 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.

Professional services

One of the following four Configuration and Training Service options is required for all installations of MobileIron from AT&T. Application Service Desk (ASD) On Boarding service is included in all Configuration and Training Professional Service installations.

Basic Configuration and Training – \$500

AT&T will provide implementation services connected with the purchase of the Silver MobileIron Cloud Software Licenses. The deployment will be conducted remotely in a hosted environment.

Basic Plus Configuration and Training – \$1,000 (Required with Silver Bundle – Connector only)

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

Enterprise Support and Training – \$2,500 (Required with Silver Bundle – Connector and Sentry)

AT&T will provide implementation services connected with the purchase of the Silver MobileIron Cloud 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 - \$5,000 (Required with Gold and Platinum Bundles)

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.

Advanced Authentication using Certificates (Optional) – \$1,750

Certificate-based authentication provides enterprises with 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, or Corporate Wi-Fi. To use certificate-based authentication, your MobileIron from AT&T service will be configured to issue certificates from a built-in certificate authority. Additional professional service charges are required to configure this feature during installation.

| License and pricing options** | Silver | Gold | Platinum |
|-------------------------------|--------|-------|----------|
| 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 |

** "Subscription License" and "Monthly License" refer to annual and monthly payment terms, respectively.

| Feature add-on options*** | | | | | |
|---------------------------|------|---|------|--|-------|
| Access User Subscription | \$48 | MobileIron Threat Defense device subscription | \$60 | MobileIron Threat Defense+ device subscription | \$96 |
| Access User - MRC License | \$4 | MobileIron Threat Defense user subscription | \$90 | MobileIron Threat Defense+ Defense user subscription | \$144 |

***Features add-on options require Silver Bundle or higher licenses.

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



Important information

A minimum of 20 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 can be obtained by contacting an AT&T Account Executive. Not all features are available on all devices. All amounts paid for the Solution are non-refundable. Billing begins as of Effective Date of applicable order. Users may download licensed Software onto a maximum of 3 devices. If any user exceeds the 3 device limit per license, an additional monthly license fee will be charged.

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. Customer Responsibility Users ("CRUs"), Individual Responsibility Users ("IRUs") and Bring Your Own Device ("BYOD") users are eligible to participate in the Solution. With respect to 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 is required. 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 with SMS capabilities 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.

The Solution is subject to the terms and conditions of the applicable Enterprise Agreement between AT&T and Customer and the End User License Agreement (MobileIron Cloud EULA) located at www.mobileiron.com/en/legal/eula. Customer must agree to the terms of the MobileIron Cloud EULA before its first use of the Solution. If Customer does not accept the terms of the MobileIron Cloud EULA, Customer must not use the Solution. Customer must accept the MobileIron Cloud EULA as the party liable for each CRU, and agrees in such case that the CRU will comply with the obligations under the MobileIron Cloud EULA, including but not limited to the limitations of use in certain countries. See your account representative for additional information regarding use of the Solution outside the US. Customer is responsible for providing each CRU of an enabled mobile device with a copy of the MobileIron Cloud EULA. The Customer and the CRU are individually and jointly liable under the MobileIron Cloud EULA. Customer shall not permit any IRU or BYOD user to register as a user of the Solution unless it uses the procedures provided by AT&T to obtain and preserve proof that the IRU or BYOD user has accepted the MobileIron Cloud EULA. Upon reasonable request from AT&T, Customer shall permit AT&T to review Customer's records of users' acceptances. 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 MobileIron Cloud EULA. With regard to use of the Solution by residents of countries other than the US, Customer agrees to comply with the additional terms and conditions of use located in the Country Specific Provisions portion of the MobileIron Cloud Service Guide located at <http://serviceguidenew.att.com/>. Not all optional features are available in every country.

Data privacy: 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 behalf of AT&T or AT&T 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. 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 and Customer's collection and use of Customer Personal Data obtained via the Solution, including, without limitation, end user device location information, 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 Privacy Policy at <http://www.att.com/gen/privacy-policy?pid=2506>. Customer is responsible for notifying end users that the Solution provides mobile device management (MDM) capabilities and allows Customer to have full visibility and control of end users' devices, as well as any content on them. 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 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.

The Solution is provided "AS IS" with all faults and without warranty of any kind. AT&T HAS NO DEFENSE, SETTLEMENT, INDEMNIFICATION OR OTHER OBLIGATION OR LIABILITY ARISING FROM THE ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY BASED ON THE SOLUTION.

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 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.



To learn more about AT&T Mobile Security Solutions, visit www.att.com/emm or call us at 866.792.3278.

Share this with your peers 