

Access apps and corporate data from virtually anywhere



We help customers unlock the benefits of mobile through cloud-based Unified Endpoint Management (UEM).

Organizations seeking the agility of the cloud to help them become mobile first turn to MobileIron Cloud from AT&T (the Solution). Through the Solution, enterprise IT can more easily establish security for mobile devices, apps, and content. And users can work faster, better, and smarter.

[MobileIron Cloud](#) delivers the layered security of the MobileIron platform via the cloud. It's scalable, so you can keep up with the rapid growth of devices, apps, and data. It helps you more seamlessly support up to millions of devices so that your global mobile enterprise can plan for today and adapt for the future.

Potential benefits

- Enhanced productivity with app management and content integration
- Provides data security and compliance that meets many federal guidelines and privacy certifications
- Integrates easily and cost-effectively
- Delivers a scalable, cloud-based Solution

Features

- MacOS, Windows 10, Android, and iOS management available
- TRUSTe Privacy Seal and FedRAMP Authority to Operate (ATO)
- Choices to maximize your budget; select from either per device or per user subscriptions
- Email+ provides an email/PIM
- Web@Work offers a highly secure native web browser
- Tunnel provides a highly secure tunnel-per-app VPN

Bundle	Silver	Gold	Platinum
24X7 customer support desk (CSD) – Help desk-to-help desk (tier 2) technical support.	•	•	•
Cloud admin console – A central administrative console.	•	•	•
Remote wipe options – Remove corporate apps and data from subscribed devices remotely.	•	•	•
AD/LDAP integration – Integration of customer’s Active Directory/Lightweight Directory Access Protocol with the Solution’s platform.	•	•	•
Sentry – An in-line intelligent gateway that manages, encrypts, and helps secure the traffic between mobile devices and back-end enterprise systems.	•	•	•
Kiosk Mode/Apple Business Manager – In the U.S., Apple allows accredited businesses with a DUNS number to automatically enroll new devices purchased directly from Apple onto the Solution’s platform.	•	•	•
Bridge and Derived Credentials Bridge – Bridge unifies mobile and desktop operations for Windows 10 using a single console. Derived Credentials is used by federal agencies so that mobile devices can access agency information without needing additional hardware.		•	•
Apps@Work – An enterprise app store that can be used to house public and in-house applications.		•	•
AppConnect – Containerizes apps to help protect corporate data-at-rest without touching users’ personal data.		•	•
Email+ – A highly secure email/personal information manager (PIM) app for iOS and Android.		•	•
Docs@Work – Enables users to annotate, share, and view business documentation from email, enterprise file repositories, and cloud file repositories.		•	•
Web@Work – A highly secure browser that lets users access web content within the enterprise’s intranet without requiring them to use a device-wide VPN.		•	•
Help@Work – A customizable tool for your IT help desk staff; it enables admins to remotely view and control end user devices to support resolving issues faster.			•
Tunnel – A per-app VPN for business apps and data that enables mobile apps to access corporate data and content that is behind a firewall.			•
ServiceConnect integrations* – Helps you integrate MobileIron Cloud with your ServiceNow Solutions or services to help streamline IT workflows.			•
MobileIron Access – A cloud security Solution that provides conditional access to cloud services from one or multiple mobile apps and browsers.	Add-on feature. Gold bundle recommended.		
MobileIron Threat Defense and MobileIron Threat Defense+ – Help guard against data loss from mobile threat events.	Add-on feature.		

* 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.

Bundle features

24X7 Customer Support Desk (CSD) support

Help desk-to-help desk (Tier 2) technical support.

Cloud Admin Console

Administrators have a central administrative console to simplify key tasks: enroll endpoints, manage and view endpoint profiles and user groups, and access customizable reports that provide current data and inventory status.

Remote wipe options

Allows you to remove corporate apps and data from subscribed devices. It's especially useful to protect data on lost or stolen devices.

AD/LDAP integration

Lets you integrate the Solution platform with your Active Directory/Lightweight Directory Access Protocol.

Sentry

This in-line, intelligent gateway manages, encrypts, and helps secure the traffic between mobile devices and back-end enterprise systems.

Kiosk Mode/Apple Business Manager

In the U.S., Apple allows accredited businesses with a DUNS number (Data Universal Numbering System – a unique ID number for a business) to automatically enroll new devices purchased directly from Apple onto the Solution's platform.

Bridge and Derived Credentials Bridge

Bridge unifies operations (mobile and desktop) for Windows 10 using a single console. It gives IT admins a more consistent platform to manage the broad variety of devices across the enterprise. Derived Credentials Bridge is used by federal agencies so that mobile devices can access agency information without needing additional hardware.

Apps@Work

Your organization's own app store. You can house all your public and in-house applications here for authorized users to access.

AppConnect

Manages the complete lifecycle of mobile apps and app data by enabling security and management features, distributing apps to authorized devices, delivering configurations and policies at runtime, and revoking privileges as necessary. It containerizes apps (apps reside and run in a passcode-protected, virtual container) to help protect corporate data-at-rest without touching users' personal data.

Email+

Manage your email and personal data (contacts, calendars, appointments, tasks, documents, and more) with this highly secure email and PIM. You can get the app for iOS and Android.

Docs@Work

Users can find and access—on the go—the documents, presentations, and files your company uses the most. Plus, they can annotate, share, and view business documents from email, SharePoint, network drives, and a variety of other content management systems.

Help@Work

A customizable tool for your IT help desk staff. It enables admins to remotely view and control end user devices to support resolving issues faster.

Tunnel

A highly secure per-app VPN for business apps and data. It enables mobile apps to access corporate data and content that is behind a firewall.

ServiceConnect integrations

Helps you integrate MobileIron Cloud with your ServiceNow Solutions or services to help streamline IT workflows.

Add-on features available

MobileIron Access

A cloud security Solution that provides conditional access to cloud services from one or multiple mobile apps and browsers. It helps you keep business data within IT bounds so it can't be stored on unsecured devices, connect to unmanaged apps, or share information with unsanctioned cloud services.

MobileIron Threat Defense and MobileIron Threat Defense+

Help guard and take defensive actions against mobile threats (such as device, network, app, and phishing attacks), even when the device is offline. Provides continuous protection against threats that exploit user behavior and security gaps. MobileIron Threat Defense+ includes additional reporting features.

Day-zero support

MobileIron Cloud quickly adapts new features with the release of devices, versions, and operating systems. It makes new features quickly available to organizations (such as support for Android for Work). Your IT team can help users stay productive on the latest iOS, Android, and Windows Phone devices.

Enterprise-grade security

MobileIron Cloud offers an intuitive experience to both IT administrators and device users—while remaining highly secure. IT administrators can readily create complex policies. They can also take instant action based on dynamic device states. Users can still search and interact with apps and content, just as they do with personal apps and files. The Solution integrates with everyday workflows and reduces the amount of training needed by IT or users.

Security and certifications

One of the most trusted mobile IT cloud services in the industry, the Solution’s operational and security processes have had a SOC 2 Type 2 assessment. This audits the operational and security processes of the service. The Solution’s operational and security processes have also earned the TRUSTe Privacy Seal, signifying that MobileIron’s privacy policy and practices have been reviewed for transparency, accountability, and choice for the protection of customer information. It also certifies compliance with EU privacy requirements.

In addition, MobileIron Cloud has received FedRAMPSM Authority to Operate (ATO). FedRAMP ATO recognizes that MobileIron Cloud meets federal risk management requirements for security for all cloud providers.

Certifications and compliance
FIPS (Federal Information Processing Standard) 140 Level 2
NIAP MDM PP (National Information Assurance Partnership mobile device management protection profile)
NSA (National Security Agency) approved
CJIS (Criminal Justice Information Services – a division of the FBI) compliant
Derived Credentials/PIV (personal identity verification) – a federally issued credential

MobileIron optional add-on features

Access

MobileIron Access is a cloud security solution. It provides conditional access to cloud services from mobile apps and browsers. Unlike traditional security, MobileIron Access correlates user identity with unique information feeds, such as device posture and app state. This helps keep business data within IT bounds so it can’t be stored on unsecured devices or

shared with unauthorized cloud services. The standards-based approach can help secure virtually any cloud service, including Office 365, without requiring proprietary integrations.

Supported browsers
Chrome – Windows and Mac
Safari – Mac, not Windows
Firefox – Windows and Mac

For the best performance, Gold bundles are advised.

MobileIron Access is only available in a per-user-subscription. It may be purchased for use with one or multiple cloud applications. Additional installation and configuration services may be required.

MobileIron Threat Defense

MobileIron Threat Defense protects and remediates against known and unknown threats on Android and iOS mobile devices, including zero-day attacks. Plus, it doesn’t disrupt users’ productivity. MobileIron Threat Defense+ includes additional reporting features. Installation has an additional cost of \$2,500 or \$5,000 depending on number of subscriptions.

Professional services

One of the following three configuration and training services is required for all installations of MobileIron Cloud from AT&T’s Customer Support Desk (CSD). On-boarding service is included in all configuration and training professional services.

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

Includes implementation services connected with subscriptions to the Silver bundle. Deployment is conducted remotely in a hosted environment, with the integration supported by an on-premises MobileIron Connector to an Active Directory in the customer’s data center.

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

Includes implementation services connected with subscriptions to the Silver bundle. Deployment is conducted remotely in a hosted environment, with the integration supported by an on-premises MobileIron Connector to an Active Directory in the customer’s data center and one Sentry.

3. Enterprise Support Configuration and Training – \$5,000 (Required with Gold and Platinum Bundles)

Includes implementation services connected with the purchase of the Gold or Platinum bundles. Deployment is conducted remotely in a hosted environment, with the integration supported by an on-premises MobileIron Connector to an Active Directory in the customer’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 Cloud 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.

Pricing options

Note: MRC = monthly recurring charge; ARC = annual recurring charge. User subscriptions may be downloaded on up to 3 devices.

Subscription and pricing options	Silver	Gold	Platinum
Annual subscription per device	\$48 ARC	\$72 ARC	\$90 ARC
Annual subscription per user	\$72 ARC	\$108 ARC	\$138 ARC
Monthly subscription per device	\$4 MRC	\$6 MRC	\$7.50 MRC
Monthly subscription per user	\$6 MRC	\$9 MRC	\$11.50 MRC

Feature add-on options		
Access User – annual subscription with a single enterprise cloud license	\$18 ARC	
Access User – annual subscription	\$48 ARC	
Access User – subscription	\$4 MRC	
MobileIron Threat Defense device – subscription	\$48 ARC	\$4 MRC
MobileIron Threat Defense user – subscription	\$72 ARC	\$6 MRC
MobileIron Threat Defense+ device – subscription	\$72 ARC	\$6 MRC
MobileIron Threat Defense+ user – subscription	\$108 ARC	\$9 MRC



For more information on AT&T Cybersecurity Mobile Endpoint Security Solutions, contact your sales representative or visit [our MobileIron webpage](#).

Important information

General: MobileIron Cloud 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 https://www.mobileiron.com/en/legal/customer_agreement; (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.

A minimum of 20 Solution subscriptions are 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.

Customer must accept the Additional Product Terms as the party liable for each CRU, and agrees in such case that the CRU will comply with the obligations under the Additional Product Terms, 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 U.S. Customer is responsible for providing each CRU of an enabled mobile device with a copy of the Additional Product Terms. The Customer and the CRU are individually and jointly liable under the Additional Product Terms. With regard to use of the Solution by residents of countries other than the U.S., 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 nonconforming 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. 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.

As between AT&T and the Customer, 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.



AT&T Cybersecurity helps to reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our SaaS-based solutions with advanced technologies including virtualization and actionable threat intelligence from AT&T Alien Labs and the Open Threat Exchange™, and our relationship with more than 40 best-of-breed vendors, accelerate your response to cybersecurity threats. Our experienced consultants and SOC analysts help manage your network transformation to reduce cybersecurity risk and overcome the skills gap. Our mission is to be your trusted advisor on your journey to cybersecurity resiliency, making it safer for your business to innovate.