



Product Brief

AirWatch On-Premises Solutions from AT&T

Virtually Anytime and Anywhere

AirWatch On-Premises Solutions from AT&T is a Customer premises deployed enterprise mobility management software application for compatible smartphones, tablets, laptops, and rugged devices. The solution can help you control your mobile inventories and help safeguard your organization while extending the parameters of your workforce. The Solution is offered via four generally available management suites (Green, Orange, Blue and Yellow), as well as two suites for primary and secondary educational institutions. The suites are offered in progressive layers to deliver a Customer's specific needs for features and functionality. All suites include AirWatch On-Premises MDM, AirWatch MAM, AirWatch Container and AirWatch App Catalog.

AirWatch On-Premises Mobile Device Management ("MDM")

The Solution's core is AirWatch On-Premises MDM, which enables broad scale deployment of mobile devices with quick enrollment and easy configuration. Updates are provided over-the-air, and IT administrators can enforce policies, set restrictions, and help to secure devices while in use and if lost or stolen. This Solution supports Android, iOS, BlackBerry, Apple Mac OS, and Windows operating systems



from a single console. Customers can manage many functions of MDM and other supported solutions from a single administrative portal (the "AirWatch Admin Console") using the same user name and password.

Mobile Application Management ("MAM")

AirWatch Mobile Application Management simplifies mobile application management by offering a comprehensive set of services and tools that can be used to provide highly secure delivery, management, and tracking of mobile applications deployed on end users' devices. MAM supports the management of internal, public, and purchased applications from the AirWatch Admin Console.

AirWatch Container

AirWatch Container separates corporate and personal data on iOS or Android smartphone devices, helping to ensure that Customer resources are highly secure and employee privacy is maintained. AirWatch Container creates a virtual container on devices where both AirWatch and Customer developed applications, may be viewed inside and outside the AirWatch Container view but are secured through use of a shared container passcode. Access to the Customer's applications is granted to end users as apps in the container and can be managed by an administrator at the application level rather than the device level.

AirWatch App Catalog

AirWatch App Catalog enables Customers to manage and distribute enterprise applications via the AirWatch Admin Console. Customers' end users can locate and access applications

Features

- Fast user configuration from a single console
- Policy customization and administration
- Lock/Wipe lost or stolen devices
- Enterprise integration
- Multi-tenant architecture

To learn more about AirWatch On-Premises Solutions from AT&T, visit www.att.com/emm or [have us contact you.](#)

Share this with your peers



within the App Catalog based on policy settings established within the console, which can distribute, update, track and recommend applications in the AirWatch App Catalog to end users.

The Solution is offered in four suites: Green, Orange, Blue and Yellow, as well as two suites for educational institutions. All suites include AirWatch On-Premises MDM, AirWatch MAM, AirWatch Container and AirWatch App Catalog. The features available with each suite are described in the Optional Software Features section below.

Optional Features

The following optional features are available individually or as components of the suites described in the table below:

AirWatch Mobile Content Management – View

AirWatch Mobile Content Management – View provides highly secure document distribution and mobile access to Customer documents using mobile applications on users’ devices. AirWatch Mobile Content Management – View helps protect sensitive content in the highly secure container and provides users a central application they

can use to access Customer documents from their mobile devices. Access to mobile applications is available for use on iOS, Android and Windows devices.

AirWatch Mobile Content Management – Collaborate

AirWatch Mobile Content Management – Collaborate offers the features and functionality of AirWatch Mobile Content Management – View plus the ability to manage personal files and folders. Collaboration features such as editing, annotation and commenting capabilities on shared files are also included. The AirWatch Secure Content Locker Sync™ desktop functionality provides users with two-way synchronization of content between desktops and devices. AirWatch Secure Content Locker for PCs provides PC users with highly secure access to corporate content on their personal computers. The web-based self-service portal allows PC users to add, manage and share individually created content. Additional Professional Services are required.

AirWatch Application Wrapping

AirWatch Application Wrapping (“App Wrapping”) is an optional feature that

allows a Customer to incorporate additional functionality into its developed applications that may reduce or eliminate the need for development or code changes. The process of wrapping an application is initiated directly from the AirWatch Admin Console. Once an application is wrapped, the Customer can perform a number of administrative actions on the application, including actions to increase security.

AirWatch App Wrapping functionalities include the ability to:

- Detect and prevent access to compromised devices
- Prevent data-loss by disabling the copy and paste, Bluetooth and camera functions (on Android and iOS devices)
- Control devices’ ability to access networks based on network type or by service set identifiers (“SSID”s)
- Control offline access to applications
- Redirect traffic using App Tunneling with the AirWatch Mobile Access Gateway (“MAG”). (Requires purchase of MAG Installation Professional Service)

Solution Bundles	Green Management Suite	Orange Management Suite	Blue Management Suite	Yellow Management Suite	K12 EDU Management Suite†	K12 EDU with Teacher Tools Management Suite†
AirWatch MDM	•	•	•	•	•	•
AirWatch Mobile Application Management	•	•	•	•	•	•
AirWatch Container	•	•	•	•	•	•
AirWatch App Catalog	•	•	•	•	•	•
AirWatch Inbox		•	•	•	•	•
Application Wrapping			•	•	•	•
AirWatch Browser			•	•	•	•
Mobile Content Management View			•	•	•	•
Mobile Content Management Collaborate				•		
AirWatch Advanced Telecom				•		
AirWatch Teacher Tools						•

† This suite is only available to primary and secondary educational institutions.

AirWatch Software Developer Toolkit

AirWatch Software Developer Toolkit (“SDK”) is included as part of the App Wrapping option and allows SDK functionality to be applied to Customer developed iOS and Android applications, as well as other AirWatch applications. Customers can choose to apply SDK profile settings and policies at an Organization Group (“OG”) level. These options are shared across applications located in the OG. Customers can also customize SDK profiles for SDK, App Wrapping, and other AirWatch applications. Options are mirrored in each area.

Note: SDK technical support is available directly from AirWatch and requires Customer to purchase 8 hours of AirWatch Professional Services Support. Customers must also agree to the terms and conditions of a separate AirWatch Software Development Kit License Agreement. A copy of the AirWatch Software Development Kit License Agreement is found at: <http://www.air-watch.com/downloads/legal/201411-SDK-License-Agreement.pdf>

AirWatch Inbox

AirWatch Inbox is a fully containerized email management solution for iOS, Windows , and Android devices. AirWatch Inbox enables administrators to remotely configure and manage enterprise email accounts while keeping end users’ personal and enterprise data separated. It supports Exchange ActiveSync and uses AES 256-bit encryption to keep email messages and attachments highly secure.

AirWatch Inbox functionalities include the ability to:

- Set a passcode required to access applications
- Configure usage restrictions such as disabling copy/paste
- Remove email messages and attachments

AirWatch Browser

AirWatch Browser is a highly secure Internet browsing alternative to native Internet browsers and provides customers the ability to configure and enforce browsing policies for Internet and Intranet sites without requiring a device-level VPN. Browsing is enabled by utilizing one of these modes:

Restricted Mode: This mode applies controls to the browser’s functionality and its ability

to access specified web content. For example, administrators can restrict web access from certain websites or provide an Internet portal for devices used as a mobile point of sale.

Kiosk Mode: This mode restricts the AirWatch Browser to a specific home page. It also disables the navigation bar, which limits navigation to links that appear on the home page.

AirWatch Video

AirWatch Video provides a highly secure way to distribute videos to end users, manage access for sensitive video content, and deliver updates in real-time to any size audience. Customers can:

- Manage videos, devices, apps and content from a single console
- Define video channels, metadata and effective/expiration dates
- Delegate management with role-based access and multi-tenant architecture
- Define granular user access through dynamic smart groups
- Enforce Wi-Fi only downloads to control data costs
- Encrypt downloaded data stored on devices (Android only)
- Restrict application access if a device is noncompliant
- Custom brand the app to meet company standards
- Purchase this feature a la carte with any Management Suite
- Additional Professional Services are required

AirWatch Advanced Telecom

AirWatch Advanced Telecom includes the capabilities available with AirWatch Mobile Device Management plus advanced capabilities to define users’ usage plans, set usage thresholds and enforce compliance policies. AirWatch Advanced Telecom can create telecom usage plans, either per device or by group, and define usage thresholds for voice, SMS and data usage based on plan limits. Compliance policies can be configured around usage thresholds to help prevent end users from going over plan limits for voice, SMS and data usage by automatically

triggering alerts or removing profiles at specified thresholds. Additional Professional Services are required.

Teacher Tools

AirWatch Teach for teachers and AirWatch Learn for students gives teachers real-time management capabilities to organize classes and supervise students. AirWatch Teach allows teachers to associate each student with an assigned device in the class, helping them to manage all devices in a classroom.

The AirWatch Teacher Tools include the following features:

- App Lock/Content Lock: Provides teachers the ability to lock individual students or a whole class into an approved application, website, or selected content, either at will or for a defined period
- All Eyes Up Front: Lets teachers temporarily disable students’ devices during class instruction to minimize distraction
- Clear Passcode: Allows teachers to help manage student devices if a student forgets his or her passcode

Supported Devices

The AirWatch Teach and AirWatch Learn apps are supported for first and second generation iPad minis. Second generation iPads are supported, but 3rd and 4th generation iPads are recommended. iPads and iPad minis must run iOS 7 or higher and have Bluetooth and Wi-Fi capabilities.

Requirements

- AirWatch Teacher Tools require use of the AirWatch Admin Console version 7.2 and higher
- All devices must have Bluetooth and Wi-Fi turned on
- All teachers and students must be enrolled in the same organization group

Teacher Devices Must

- Have an administrator account in the AirWatch Admin Console
- Have the AirWatch Teach app installed on their device

Student Devices Must

- Be supervised devices

- Be enrolled with the AirWatch Agent
- Have the AirWatch Learn app installed as a managed app pushed from the Console to Smart Groups. All other compatible apps must also be pushed from the Console.

(REQUIRED) EMM Software Installation and Configuration Services

One of the four immediately following Installation and Configuration Services options is required.

Basic Installation and Training (Required for AirWatch Core MDM Server)

AT&T will provide implementation services in an AirWatch environment, an optional AirWatch Connector ("ACC") in the Customer's data centers and deployment of an initial pilot set of devices. This service consists of two meetings.

Basic Plus Configuration and Training for On-Premises Installation (Required for AirWatch Core MDM Server when supporting multiple devices with multiple users)

The Basic Plus On-Premises Service includes all the features of the Basic Installation and Training Service plus the configuration of the AirWatch Secure Launcher feature for the setup of shared Android devices.

Premium Installation and Training Services for EMM Software (Required for designs that contain a Secure Email Gateway ("SEG") and an AirWatch Connector)

AT&T will install components located on the Customer's premises, including the AirWatch Console, an optional AirWatch Connector ("ACC"), and either a Secure Email Gateway ("SEG") or a PowerShell Integration for email management and an initial pilot set of devices. These services include four meetings.

Premium Plus Installation and Training for use of EMM Software (Required for the installation of AirWatch Enterprise Mobility Software and a Secure Email Gateway and a Mobile Access Gateway)

Premium Plus Installation and Training Services include all the features of Premium Installation and Training as well as installation of a Mobile Access Gateway for content management or highly secure browsing.

Mobile Content Management Collaborate Add-On Installation and Training (Add-On Service to Premium Plus)

AT&T will provide implementation services connected with the purchase of the associated AirWatch software licenses. The deployment includes two meetings that will be conducted in Customer's on-premises environment, with integration provided by an existing Mobile Access Gateway.

Advanced Telecom Configuration and Training

AT&T will provide implementation services associated with the purchase of AirWatch Advanced Telecom. The deployment includes one meeting that will be conducted in an existing AirWatch on-premises environment.

AirWatch Video Configuration and Training

AT&T will provide implementation services associated with the purchase of AirWatch Video. The deployment includes one meeting and will be conducted in an existing AirWatch on-premises environment.

AirWatch Secure Email Gateway ("SEG") Implementation and Configuration (Required for Customers using AirWatch SEG)

AT&T will remotely configure and integrate one SEG into an existing AirWatch environment. Setup will include basic SEG configuration and integration with Customer's existing (Exchange or Lotus Notes) email environment. For high-availability environments, configuration of the network load balancer cluster and monitoring for cluster member management is the sole responsibility of Customer.

AirWatch Mobile Access Gateway ("MAG") Implementation and Configuration (Required for Customers using AirWatch MAG)

AT&T will remotely configure and integrate one Mobile Access Gateway ("MAG") into an AirWatch environment (on-premises). Setup will include integration to one or all of the following:

- Internal document repositories and content using the AirWatch Secure Content Locker ("SCL")

- Internal websites using the AirWatch Secure Brower
- Internal web applications with access to internal resources

AirWatch Connector (ACC) Implementation and Configuration

AT&T will remotely configure and integrate one AirWatch Connector. Setup will include integration to one Active Directory server. Customer is responsible for provisioning a server in accordance with the configuration checklist provided.

EMM Operations Training (Optional)

AT&T will conduct knowledge share and training for Customer's technical staff on the Solution. The engagement is up to five hours in duration. The training is delivered remotely via web conference and includes Customer hands on configuration of AirWatch Inbox container setup, Application Wrapping of one Customer developed application, Secure Browsing and Bookmarks, Mobile Content Management files on the AirWatch On-Premises Platform, Mobile Content Management - Collaborate with files on the AirWatch On-Premises platform.

Presentation Topics that can be selected by the Customer include the following:

- User management
- Device registration and retirement
- Policy management and security
- Device configuration management
- Reports and logs

AT&T will coordinate the web conference and a pre-call will be set-up with the Customer by AT&T to review the session agenda and logistics.



Managed Service Health Check (Optional)

AT&T will remotely inspect and review the current state of the Customer's MDM platform and validate that the server, software implementation and configuration are consistent with the managed solution platform vendor's and AT&T's best practices and recommendations. This health check is typically delivered remotely over two days by an AT&T Professional Services Consultant.

AirWatch Public Key Infrastructure ("PKI") Integration and Identity Certificate Device Configuration (Optional)

AT&T will implement and configure the integration settings to enable AirWatch to issue certificates to mobile devices from the Customer's Certificate authority using the Customer's AirWatch-supported PKI integration interface. AT&T will also assist with the testing of each device profile on a single supported device.

All meetings described above are conducted remotely unless otherwise agreed. All are subject to a cancellation fee of up to \$500 if Customer cancels less than 24 hours before the scheduled meeting.

Customer shall not instruct end users to call AT&T Customer Care at 611 or any other wireless carrier's customer care center in connection with end users' use of the Solution.

AirWatch On-Premises MDM from AT&T – Pricing Table

Description of Charge	Monthly Charge	One-Time Charge	Annual Charge
Green Management Suite Device-Based License (includes maintenance)	\$3.25		
Green Management Suite User-Based License	\$6.25		
Green Management Suite Perpetual License; Device-Based License		\$50.00	
Green Management Suite Perpetual License Maintenance; Device-Based License			\$10.00
Green Management Suite Perpetual License; User-Based License		\$100.00	
Green Management Suite Perpetual License Maintenance; User-Based License			\$20.00
Green to Orange Management Suite Upgrade – Perpetual License; Device-Based License		\$22.00	
Green to Orange Management Suite Upgrade – Perpetual License Maintenance; Device-Based License		\$4.50	
Green to Blue Management Suite Upgrade – Perpetual License; Device-Based License		\$44.00	
Green to Blue Management – Perpetual License Maintenance; Device-Based License		\$8.75	
Green to Yellow Management Suite Upgrade – Perpetual License; Device-Based License		\$88.00	
Green to Yellow Management Suite Upgrade – Perpetual License Maintenance; Device-Based License		\$17.50	
Green Management Suite Perpetual Device License to Perpetual User-Based License		\$55.00	
Green Management Suite Perpetual Device License to User-Based License Upgrade Maintenance		\$11.00	
Orange Management Suite Device-Based License (includes maintenance)	\$4.00		
Orange Management Suite User-Based License	\$8.00		
Orange Management Suite Perpetual License; Device-Based License		\$70.00	
Orange Management Suite Perpetual License Maintenance; Device-Based License			\$14.00
Orange Management Suite Perpetual License; User-Based License		\$140.00	
Orange Management Suite Perpetual License Maintenance; User-Based License			\$28.00
Orange to Blue Management Suite Upgrade – Perpetual License; Device-Based License		\$22.00	
Orange to Blue Management Suite Upgrade – Perpetual License Maintenance; Device-Based License		\$4.50	
Orange to Yellow Management Suite Upgrade – Perpetual License; Device-Based License		\$66.00	
Orange to Yellow Management Suite Upgrade – Perpetual License Maintenance; Device-Based License		\$13.25	
Orange Management Suite Perpetual Device License to Perpetual User-Based License		\$77.00	
Orange Management Suite Perpetual Device License to User-Based License Upgrade Maintenance		\$15.50	
Blue Management Suite License (includes maintenance); Device-Based License	\$5.25		
Blue Management Suite User-Based License	\$10.50		
Blue Management Suite Perpetual License; Device-Based License		\$90.00	
Blue Management Suite Perpetual License Maintenance; Device-Based License			\$18.00

To learn more about AirWatch On-Premises Solutions from AT&T, visit www.att.com/emm or [have us contact you](#).

Share this with
your peers



Description of Charge	Monthly Charge	One-Time Charge	Annual Charge
Blue Management Suite Perpetual License; User-Based License		\$180.00	
Blue Management Suite Perpetual License Maintenance; User-Based License			\$36.00
Blue to Yellow Management Suite Upgrade – Perpetual License; Device-Based License		\$44.00	
Blue to Yellow Management Suite Upgrade – Perpetual License Maintenance; Device-Based License		\$8.75	
Blue Management Suite Perpetual Device License to Perpetual User-Based License		\$99.00	
Blue Management Suite Perpetual Device License to User-Based License Upgrade Maintenance		\$19.75	
Yellow Management Suite License (includes maintenance); Device-Based License	\$8.17		
Yellow Management Suite User-Based License	\$16.33		
Yellow Management Suite Perpetual License; Device-Based License		\$130.00	
Yellow Management Suite Perpetual License Maintenance; Device-Based License			\$26.00
Yellow Management Suite Perpetual License; User-Based License		\$260.00	
Yellow Management Suite Perpetual License Maintenance; User-Based License			\$52.00
Yellow Management Suite Perpetual Device License to Perpetual User		\$143.00	
Yellow Management Suite Perpetual Device License to User-Based License Upgrade Maintenance		\$28.50	
K12 EDU Management Suite Device-Based License – 1 Year (includes maintenance)		\$13.00	
K12 EDU Management Suite Device-Based License – 2 Years (includes maintenance)		\$25.00	
K12 EDU Management Suite Device-Based License – 3 Years (includes maintenance)		\$35.00	
K12 EDU with Teacher Tools Management Suite Device-Based License – 1 Year (includes maintenance)		\$16.00	
K12 EDU with Teacher Tools Management Suite Device-Based License – 2 Years (includes maintenance)		\$31.00	
K12 EDU with Teacher Tools Management Suite Device-Based License – 3 Years (includes maintenance)		\$43.00	
K12 EDU Management Suite Perpetual License; Device-Based License		\$24.00	
K12 EDU Management Suite Perpetual License Maintenance; Device-Based License			\$5.00
K12 EDU with Teacher Tools Management Suite Perpetual License; Device-Based License		\$29.00	
K12 EDU with Teacher Tools Management Suite Perpetual License Maintenance; Device-Based License			\$6.00
AirWatch On-Premises Basic Installation and Training		\$2,000.00	
AirWatch On-Premises Basic Plus Installation and Training		\$2,500.00	
AirWatch On-Premises Premium Installation and Training		\$3,000.00	
AirWatch On-Premises Premium Plus Installation and Training		\$5,500.00	
Mobile Content Management Collaborate Add-On Training		\$1,000.00	
AirWatch Video Configuration and Training		\$500.00	
AirWatch Advanced Telecom Configuration and Training		\$500.00	
AirWatch Video – Device-Based License	\$1.50		
AirWatch Video – User-Based License	\$3.00		
AirWatch Video Perpetual License – Device-Based License		\$30.00	
AirWatch Video Perpetual License – Device-Based License Maintenance			\$6.00
AirWatch Video Perpetual License – User-Based License		\$60.00	
AirWatch Video Perpetual License – User-Based License Maintenance			\$12.00
AirWatch Advanced Telecom – Device-Based License	\$1.00		
AirWatch Advanced Telecom – User-Based License	\$2.00		
AirWatch Advanced Telecom Perpetual License – Device-Based License		\$20.00	
AirWatch Advanced Telecom Perpetual License – Device-Based License Maintenance			\$4.00
AirWatch Advanced Telecom Perpetual License – User-Based License		\$40.00	
AirWatch Advanced Telecom Perpetual License – User-Based License Maintenance			\$8.00

To learn more about AirWatch On-Premises Solutions from AT&T, visit www.att.com/emm or [have us contact you](#).

Share this with
your peers



Description of Charge	Monthly Charge	One-Time Charge	Annual Charge
Teacher Tools – per Device License (includes maintenance)	\$0.50		
Teacher Tools – Perpetual; per Device License		\$20.00	
Teacher Tools – Perpetual Maintenance; per Device License			\$4.00
EMM Operations Training		\$1,500.00	
EMM Managed Service Health Check		\$1,750.00	
AirWatch PKI Integration and Identity Certificate Device Configuration		\$1,750.00	
Additional ACC Implementation and Configuration		\$500.00	
Additional SEG Implementation and Configuration		\$1,000.00	
Additional MAG Implementation and Configuration		\$1,000.00	
AirWatch Professional Services – 8 Hours		\$1,200.00	
AirWatch Software Upgrade for On-Premises Deployments		\$1,200.00	
AirWatch PS Custom – SOW		Custom Pricing	

User-based licenses may be applied on up to 3 devices.

All prices exclude applicable taxes, fees and surcharges.

Share this with
your peers



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

To learn more about AirWatch On-Premises Solutions from AT&T, visit www.att.com/emm or [have us contact you](#).

Important Information

General: AirWatch Hosted MDM from AT&T as described in this product brief (the "Solution") is available only to eligible customers with a qualified AT&T agreement ("Qualified Agreement") and a Foundation Account Number ("FAN"). The Solution is subject to (a) the terms and conditions found at http://www.air-watch.com/downloads/legal/AirWatch_ATT_Reseller_EULA_R-1.pdf, ("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.

Except for government customers, (i) Customer must accept the Additional Product Terms as the party liable for each user of a Customer owned device, and agrees in such case that each such user will comply with the obligations under the Additional Product Terms; (ii) Customer is responsible for providing each such user with a copy of the Additional Product Terms; (iii) Customer and each such user are individually and jointly liable under those terms; (iv) Customer may not enroll users of individually owned or subscribed devices ("Individual Users") in the Solution unless it has obtained and preserves proof that each Individual User has reviewed and accepted the terms and conditions of the Additional Product Terms; and (v) Customer shall indemnify and hold harmless AT&T against all claims by any Individual User relating to or arising from such use of the Solution if he or she has not accepted the terms and conditions of the Additional Product Terms. In addition, if and to the extent that 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/sq_customPreviewPDFPage?testid=0681A000002itjsQAA.

Requirements; Technical Information: A minimum of 20 Solution licenses is required for initial order. All fees paid for the Solution are non-refundable. Customers choosing the Annual License must pay in advance and there are no refunds. Customers choosing the Monthly License pay in arrears. The Solution is available for use with multiple network service providers. For 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. For users of the Solution with devices subscribed to non-AT&T wireless providers, customer is responsible for ensuring that customer, its applicable end users and the Solution comply 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 AirWatch 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. Customer will not permit any individually responsible user ("IRU") or BYOD user to register as a user of the Solution unless customer obtains and preserves proof that the IRU or BYOD user has accepted the Additional Product Terms. Upon reasonable request from AT&T, Customer will permit AT&T to review customer's records of users' acceptances. The Solution's functionality is limited to certain mobile devices and operating systems. A list of compatible devices and operating systems is available by contacting an AT&T Account Executive. Not all features are available on all devices. 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/sq_customPreviewPDFPage?testid=0681A000002itjsQAA, provided that Government customers shall not be subject to any such terms that are not allowable under applicable law.

AT&T reserves the right to perform 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. 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 will not instruct end users to call AT&T Customer Care at 611 or any other wireless carrier's customer care center in connection with end users' use of the Solution. Not all features are available on all devices. 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 shall pass through to Customer any warranties for the AirWatch software available from the licensor. AirWatch, not AT&T is responsible for any such warranty terms and commitments. ALL SOFTWARE IS OTHERWISE PROVIDED TO CUSTOMER ON AN "AS IS" BASIS.

Except for government Customers, Customer's sole and exclusive remedy for any damages, losses, costs and expenses arising out of or relating to use of the Solution will be termination of service.

Professional Services: Upon completion of any Professional Services, customer must either sign the acceptance document AT&T presents or provide within five (5) 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 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 will 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, the schedule, the Solution, and fees could be impacted.

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 Solution. 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, 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's 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.

*AT&T will perform 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 all diagnosis or remediation of authentication or authorization failures within the authentication, authorization and accounting (AAA) infrastructure

To learn more about AirWatch On-Premises Solutions from AT&T, visit www.att.com/emm or [have us contact you](#).

