Table of Contents

This document reflects the Service Guide in effect as of June 12, 2020

AirWatch On-Premises MDM from AT&T

Section Effective Date: 13-Sep-2019

Grandfathering Statement: As of September 13, 2019, AirWatch On-Premises MDM from AT&T ("Solution") and all of the Service Components associated with the Solution are grandfathered and no longer generally available for purchase by new customers.

AirWatch On-Premises MDM from AT&T ("Solution") is a Customer premises deployed mobile enterprise management software application solution for compatible smartphones, tablets, laptops, and rugged devices. The Solution can be used to provide mobile device, mobile content and mobile application management capabilities depending on the suite selected.

This Service Guide consists of the following parts:

- Service Description (SD)

- Pricing (P)

- Country Specific Provisions (CSP)

In addition, General Provisions apply.

Service Description (SD)

SD-1. General

Section Effective Date: 17-May-2016

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.

SD-1.1. AirWatch On-Premises Mobile Device Management (MDM)

Section Effective Date: 19-Dec-2014

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 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 using the same user name and password.

AirWatch On-Premises MDM can be deployed to manage both Customer owned, individually owned, and shared devices. Benefits of the Solution include the ability to:

- Gain real-time visibility into the mobile devices in Customer environments

- Manage the entire lifecycle of mobile devices

- Administer consistent policies across devices

- Enforce enterprise security and compliance standards

- Increase the security of data transmitted to and from devices

- Implement highly secure enterprise Data Loss Prevention (DLP) programs

- Automate processes and issue trouble resolutions

- Analyze and report critical device information

SD-1.2. Mobile Application Management (MAM)

Section Effective Date: 19-Dec-2014

AirWatch MAM 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 one central console (the "AirWatch Admin Console").

Benefits of MAM include:

- A centralized web-based console to manage applications

- Simplified application distribution

- Improved maintenance through automatic mobile application updates and crash reports

- Support for end user feedback and ratings for applications

SD-1.3. AirWatch Container

Section Effective Date: 17-Sep-2015

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 internally 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.

Benefits of AirWatch Container include:

- Supports device choice for employees

- Separates Customer and personal data

- Manages only Customer data on devices

SD-1.4. AirWatch App Catalog

Section Effective Date: 19-Dec-2014

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

SD-1.5. Management Suites

Section Effective Date: 13-Sep-2016

The Solution is offered in four 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. All additional features are described in the Software Features section below.

SD-1.5.1. Green Management Suite

Section Effective Date: 17-Sep-2015

The Green Management Suite includes AirWatch On-Premises MDM, AirWatch MAM, AirWatch Container, and AirWatch App Catalog.

SD-1.5.2. Orange Management Suite

Section Effective Date: 15-Nov-2016

The Orange Management Suite includes the Green Management Suite, AirWatch Inbox, and/or AirWatch Boxer.

SD-1.5.3. Blue Management Suite

Section Effective Date: 15-Nov-2016

The Blue Management Suite includes the Orange Management Suite plus Application Wrapping, AirWatch Browser, VMware Identity Manager, and Mobile Content Management View.

SD-1.5.4. Yellow Management Suite

Section Effective Date: 17-Sep-2015

The Yellow Management Suite includes the Blue Management Suite, Advanced Telecom, and Mobile Content Management Collaborate.

SD-1.5.5. K-12 EDU Management Suite

Section Effective Date: 21-Apr-2017

The K-12 EDU Management Suite includes AirWatch On-Premises MDM, AirWatch MAM, AirWatch Container, AirWatch App Catalog, AirWatch Inbox and/or AirWatch Boxer, AirWatch Browser, VMware Identity Manager, and Mobile Content Management View. This suite is only available to primary and secondary educational institutions.

SD-1.5.6. K-12 EDU with Teacher Tools Management Suite

Section Effective Date: 21-Apr-2017

The K-12 EDU with Teacher Tools Management Suite includes the K-12 EDU Management Suite and AirWatch Teacher Tools. This suite is only available to primary and secondary educational institutions.

SD-1.6. Important Information

Section Effective Date: 21-Apr-2017

- A minimum of 20 Solution licenses is required for initial order.

- The Solution is only available to companies located in the US whose servers managing the Solution are installed at a US location.

- 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.

- Billing begins as of Effective Date of applicable order.

- All amounts paid for the Solution are non-refundable.

- The Solution is available only to Customers with a qualified AT&T business or government agreement and a Foundation Account Number ("FAN").

- The Solution is available for use with multiple network service providers. Both Company Responsibility Users ("CRUs") and Individual Responsibility Users ("IRUs") are eligible to participate in the Solution. With respect to CRUs and IRUs 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 and AirWatch, Inc. ("AirWatch") software is required.

- With respect to use 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.

- User-Based licenses may be applied to up to 3 devices.

- 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 performance with such customized settings and/or updates.

- Customer is responsible for any required hardware associated with the Solution.

- Customer is responsible for the configuration of the appropriate DNS prior to AT&T installation activities.

- AT&T reserves the right to conduct work remotely and 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 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.

- Additional hardware, software, service and/or network connection may be required to access the Solution. Customer's responsibilities relating to MDM deployment are set forth in the Installation of MDM Software (Required) section below.

- Availability, security/privacy, delivery and timeliness of information are not guaranteed by AT&T.

- The Solution is subject to the terms and conditions of applicable enterprise agreement between AT&T, Customer, an AirWatch End User License Agreement ("EULA") and the VMware Identity Manager Terms of Service ("TOS") if Customer subscribes to VMware Identity Manager, which are described in the AirWatch EULA; VMware Identity Manager TOS section below.

- 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.

SD-1.7. AirWatch EULA; VMware Identity Manager TOS

Section Effective Date: 15-Nov-2016

Customer must enter into a separate EULA with AirWatch in order to access and use the Solution and must enter into the separate VMware Identity Manager TOS with VMware Inc., ("VMware") if Customer subscribes to VMware Identity Manager. The EULA and TOS are agreements between Customer and AirWatch and VMware, respectively, to which AT&T is not a party. AirWatch and VMware are solely responsible for all items provided pursuant to these agreements. The EULA and TOS must be accepted before Customer's first use. If Customer does not accept the terms of the EULA and TOS, Customer must not use the licensed material. Customer must accept the EULA and TOS as the party liable for each CRU, and agrees in such case that the CRU will comply with the obligations under the EULA and TOS, including but not limited to the limitations of use in certain countries. Customer is responsible for providing each CRU of an enabled mobile device with a copy of the EULA and VMware Identity Manager TOS. The Customer and the CRU shall be individually and jointly liable under the EULA and TOS. A copy of the EULA is found at: http://www.air-watch.com/downloads/legal/AirWatch_ATT_Reseller_EULA_R-1.pdf, and the VMware Identity Manager TOS is found at http://www.vmware.com/download/eula/identity-manager-terms-of-service.html.

SD-1.8. Data Privacy

Section Effective Date: 07-Mar-2014

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 in this Service Guide, 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

This document reflects the Service Guide in effect as of June 12, 2020

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

SD-2. Offer Elements (Service Components)

Section Effective Date: 19-Dec-2014

The Solution includes Software Licenses, optional features, and Professional Services.

SD-2.1. Licenses (Software)

Section Effective Date: 19-Dec-2014

AT&T will provide the Solution software to Customer as described in the applicable Pricing Schedule or other ordering documents.

SD-2.2. Software Features

Section Effective Date: 21-Apr-2017

The following optional features are available as part of the relevant Orange, Blue, Yellow, K-12 EDU, and K-12 EDU with Teacher Tools management suites.

SD-2.2.1. AirWatch Application Wrapping (grandfathered)*

Section Effective Date: 15-Nov-2016

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 ("SSIDs").

- Control offline access to applications.

- Redirect traffic using App Tunneling with the AirWatch Mobile Access Gateway ("MAG"). (Requires purchase of MAG Installation Professional Service)

*AirWatch Application Wrapping is no longer available to be ordered a la carte by new or existing Customers as of September 13, 2016.

SD-2.2.1.1. AirWatch Software Developer Toolkit (Requires App Wrapping) (grandfathered)*

Section Effective Date: 15-Nov-2016

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 Wrapped, and other AirWatch applications.

Note: SDK technical support is available directly from AirWatch and 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 Software Developer Toolkit is no longer available to be ordered a la carte by new or existing Customers as of September 13, 2016.

SD-2.2.2. AirWatch Inbox (grandfathered)*

Section Effective Date: 15-Nov-2016

AirWatch Inbox is a fully containerized email management solution for iOS, Windows 8 RT/Pro, 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 can be used to encrypt email messages and attachments. 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 Inbox uses an AES 256-bit encryption algorithm to encrypt message data such as email addresses, message text, and email subject and store the content in a local database. The email database and attachments are stored in an application space that blocks access to undesirable third-party applications.

Android Device Requirements

- AirWatch Admin Console v6.5 and higher

- Android 4.0 devices and higher

- AirWatch Android MDM Agent v4.0.1010 or higher

- Exchange ActiveSync 2003/2007/2010/2013, Office 365, or Google Apps iOS Device Requirements

- AirWatch Admin Console v7.0 and higher

- iPhone, iPad, iPad Air, and iPod Touch devices running iOS 6 and higher

- AirWatch iOS MDM Agent v4.9.1110 or higher

- Exchange ActiveSync 2007/2010/2013 or Office 365

Windows 8/RT Device Requirements

- AirWatch Admin Console v7.0 and higher.

- Windows 8.1/Pro/Enterprise and higher or Windows RT 8.1 and higher.

- AirWatch Windows MDM Agent v1.1.0.23 and higher.

- Exchange ActiveSync 2007/2010/2013, or Office 365.

*AirWatch Inbox is no longer available to be ordered a la carte by new or existing Customers as of September 13, 2016.

SD-2.2.3. AirWatch Boxer

Section Effective Date: 15-Nov-2016

AirWatch Boxer is a fully containerized email management solution for iOS and Android devices. AirWatch Boxer enables administrators to remotely configure and manage enterprise email accounts while keeping end users' personal and enterprise data separated. It supports Exchange ActiveSync and can be used to encrypt email messages and attachments. AirWatch Boxer functionalities include the ability to:

- Set a passcode required to access applications

- Restrict personal accounts from being added to the application

- Configure usage restrictions such as disabling copy/paste

- Restrict hyperlinks to only open in AirWatch Browser

- Restrict attachments to be previewed only in AirWatch Boxer or opened in any whitelisted application and provide attachment encryption using Secure Email Gateway (SEG)

AirWatch Boxer uses an AES 256-bit encryption algorithm to encrypt message data such as email addresses, message text, and email subject and store the content in a local database. The email database and attachments are stored in an application space that blocks access to undesirable third-party applications.

Android Device Requirements

- AirWatch Admin Console v8.3.5 and higher

- Android 4.2 devices and higher

- AirWatch Android MDM Agent v6.0.1 or higher

- Exchange ActiveSync 2003/2007/2010/2013 or Office 365

iOS Device Requirements

- AirWatch Admin Console v8.3.1 and higher

- iPhone, iPad, iPad Air, and iPod Touch devices running iOS 8 and higher

- iOS 9+ for Touch ID support

- AirWatch iOS MDM Agent v5.2 or higher

This document reflects the Service Guide in effect as of June 12, 2020

- Exchange ActiveSync 2007/2010/2013 or Office 365

SD-2.2.4. AirWatch Browser (grandfathered)*

Section Effective Date: 15-Nov-2016

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 the two browsing options described below:

Restricted Mode

This mode affects 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. Restricted Mode can apply a blacklist or a whitelist to specific domains, and it supports wildcard entries, allowing Customers to whitelist or blacklist a comprehensive range of URLs.

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 Browser is no longer available to be ordered a la carte by new or existing Customers as of September 13, 2016.

SD-2.2.5. Teacher Tools*

Section Effective Date: 13-Sep-2016

AirWatch Teach for teachers and AirWatch Learn for students give 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, enabling them to help manage all devices in a classroom.

The AirWatch Teacher Tools include the following features:

- App Lock/Content Lock: Provides teachers with 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:

AirWatch Teach and AirWatch Learn are supported for:

- 1st and 2nd generation iPad minis

- 2nd, 3rd and 4th generation iPads

- 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:

  o Have an administrator account in the AirWatch Admin Console

  o Have the AirWatch Teach app installed on the 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 AirWatch Admin Console to defined groups. All other compatible apps must also be pushed from the AirWatch Admin Console.

*Available in the EDU Management Suite with Teacher Tools or can be added a la carte to any Management Suite.

SD-2.2.6. VMware Identity Manager

Section Effective Date: 15-Nov-2016

VMware Identity Manager is identity management for the mobile cloud that delivers one-touch access to nearly any app, from subscribed devices, as optimized by the conditioned access provided by the AirWatch solution. Users have access to a self-service app store, and IT managers have a central place from which to manage user provisioning and access policies that support directory integration, identity federation and user analytics. Features include:

Enterprise Single Sign-On ("SSO")

An identity provider (IDP) is included, or SSO can be integrated with existing on-premises identity providers to aggregate SaaS (Software-as-a-Service) and Native Mobile and Windows 10 apps into a single catalog.

Self-Service App Store

Supports a Customer branded self-service app store that enables users to subscribe to applications across devices with automated or manual provisioning.

Identity Management with Adaptive Access

Establishes trust between users, devices and the hybrid cloud, providing conditional access controls that leverage AirWatch device enrollment and SSO.

SD-2.2.7. AirWatch Mobile Content Management from AT&T

SD-2.2.7.1. AirWatch Mobile Content Management View (grandfathered)*

Section Effective Date: 15-Nov-2016

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 View is no longer available to be ordered a la carte by new or existing Customers as of September 13, 2016.

SD-2.2.7.2. AirWatch Mobile Content Management Collaborate from AT&T (grandfathered)*

Section Effective Date: 15-Nov-2016

AirWatch Mobile Content Management Collaborate from AT&T 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 available. 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 users with highly secure access to corporate content on their personal computers. The web-based self-service portal allows users to add, manage and share personal content.

*AirWatch Mobile Content Management Collaborate from AT&T is no longer available to be ordered a la carte by new or existing Customers as of September 13, 2016.

SD-2.2.8. AirWatch Video*

Section Effective Date: 13-Sep-2016

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. AirWatch Video enables Customers to:

- 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 multitenant architecture

- Define granular user access through dynamic smart groups

- Enforce Wi-Fi only downloads to control data costs

- Encrypt downloaded data stored on the device (Android only)

- Restrict application access if device is noncompliant

- Custom brand the app to meet Customer's standards

This document reflects the Service Guide in effect as of June 12, 2020

*AirWatch Video is only available a la carte, and can be added to any Management Suite. Professional Services charges apply.

SD-2.2.9. AirWatch Advanced Telecom*

Section Effective Date: 13-Sep-2016

AirWatch Advanced Telecom includes all 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.

*AirWatch Advanced Telecom is available in the Yellow Management Suite, or can be added a la carte to any Management Suite. Professional Services charges may apply.

SD-2.3. Professional Services

SD-2.3.1. Basic Configuration and Training for On-Premises Installation (Required for AirWatch Core MDM Server)

Section Effective Date: 21-Apr-2017

AT&T will provide implementation services connected with the purchase of the associated AirWatch software licenses. The deployment will be conducted remotely for the Customer's on-premises environment with optional integration supported by an on-premises AirWatch Cloud Connector ("ACC") in the Customer's data center(s). This project includes the following meetings, all to be conducted remotely unless agreed upon by the parties:

Meeting 1: Kick-Off

This meeting is approximately 60 minutes and includes the AT&T Project Manager and a Managed Services professional. The meeting is designed to provide an overview of the implementation activities related to the technical setup and the functional configuration for installation of system components, on the scope of the features available/recommended, and on pre-installation expectations for the Customer's infrastructure/environment.

This meeting is subject to a cancellation fee of up to $500.00 if Customer cancels less than 24 hours before the scheduled meeting.

Meeting 2: Readiness Call

This meeting is approximately 30 minutes and is designed to ensure all pre-installation requirements have been met prior to initiating installation of all software.

Meeting 3: Configuration, Training and Deployment

- This meeting is approximately 240 minutes and is designed to install the MDM application, configure the application to integrate with the Customer's domain, test connectivity to the MDM service and to deploy an initial pilot set of devices. The meeting is also used for the optional installation and configuration of one ACC.

- This meeting is subject to a cancellation fee of up to $500.00 if Customer cancels less than 24 hours before the scheduled meeting.

Meeting 1: Kick-Off		
AT&T Deliverables	**Notes**	**Responsible Party**
Review Customer's number and type of devices to be enrolled (iOS or Android only)		AT&T
Review AirWatch Cloud Connector ("ACC") server hardware, software, and port requirements (optional component for Active Directory Integration)		AT&T
Review Apple ID requirements for APNS certificate		AT&T
Review Active Directory service account needed for directory lookups		AT&T
Review Customer workbook with Customer	Policy creation is the Customer's responsibility	AT&T
Provide available dates/times for configuration and training call	Established at the end of the kick-off call	Customer

Pre-Work for Meeting 2: Customer to Complete Prior to Meeting 2		
Customer Responsibilities	**Notes**	**Responsible Party**
Procure virtual and/or physical servers for connection to cloud for ACC Installation	Reviewed during Meeting 1	Customer
Configure firewall, DNS and service accounts for integration	Reviewed during Meeting 1	Customer
Complete Pre-Installation Checklist /Configuration requirements	Customer to send completed Pre-Installation Requirements Worksheet checklist to AT&T	Customer
Complete AirWatch Academy: "Associate Level Certification" training course	Recommended, but not required	Customer
Complete and return Policy Workbook	Customer to send completed recommended configuration worksheet.	Customer

Meeting 2: Customer Readiness		
Customer Responsibilities	**Notes**	**Responsible Party**
Validate all pre-installation requirements have been met	Reviewed during Meeting 1	Customer

Meeting 2: Customer Readiness		
Customer Responsibilities	**Notes**	**Responsible Party**
Schedule the third meeting for installation and Training	Reviewed during Meeting 1	Customer

Meeting 3: Basic Configuration and Training Deliverables		
AT&T Deliverables	**Notes**	**Responsible Party**
Installation of AirWatch MDM software on server(s)		AT&T led with Customer
Assistance uploading APNS certificate for iOS device management	Required only for iOS devices. Customer must have Apple ID for APNS certificate.	AT&T led with Customer
Assist with setting up default Organization Groups with a Group ID. Assist creating up to 2 additional child organization groups if applicable.		AT&T
Demonstration of Console Navigation		AT&T
Assistance in configuring Active Directory Integration		AT&T
User management: 　Assist with creating up to 3 users 　Assist with creating up to 2 administrators 　Assist with adding one user group		AT&T
Assist with enrolling up to 5 devices total (iOS or Android)	Customer must bring devices to this meeting	AT&T led with Customer
Basic device management: 　Enterprise wipe 　Device wipe 　Clear passcode 　Locate device		AT&T
Assist with creation one of each of the following profiles (if applicable): 　Passcode 　Restrictions 　Exchange email 　Wi-Fi		AT&T

This document reflects the Service Guide in effect as of June 12, 2020

Meeting 3: Basic Configuration and Training Deliverables		
AT&T Deliverables	**Notes**	**Responsible Party**

Assist creating App Groups (If applicable):
   Required apps
   Blacklisted apps
   Whitelisted apps
		AT&T

Assist creating one of each of the following Policies (if applicable):
   Compromised Status
   Encryption
   Application List
		AT&T

Assist with loading one of each of the following application types (if applicable):
   Public Application
   Internal Application
		AT&T

Branding the solution (i.e. color schemes, logo)	Optional	AT&T
Assist with configuring one Report Subscription		AT&T
AT&T sends Customer survey and Customer is transitioned to Application Service Desk		AT&T

Additional Service Notes

AT&T will assist with up to 3 different device types/operating systems (iOS, WindowsPhone 8, Android) for configuration and setup that are not shared devices. Configuration Secure Launcher and Management of Rugged Devices, Windows CE and Laptops are out of scope

- AT&T will assist with an initial deployment of up to 5 devices.

- AT&T will integrate only 1 corporate e-mail infrastructure's active directory for an un-managed server (e.g. Secure Email Gateway).

- Alignment of all enterprise mobility management ("EMM") configurations and policy design with Customer's requirements is the responsibility of Customer. AT&T will provide recommendations and assistance.

- Procurement, configuration and installation of hardware is the responsibility of Customer. AT&T will provide recommendations and assistance.

- Simple Certificate Enrollment Protocol ("SCEP") and Certificate usage for authentication is out-of-scope. Customer can purchase the associated Advanced Authentication service offering to incorporate certificate usage for authentication.

- All work, documentation and work product(s) will be conducted during typical, U.S. local business hours and will be provided in English.

- All work must be completed within one calendar year.

This document reflects the Service Guide in effect as of June 12, 2020

- AT&T will not configure the AirWatch Cloud Connector ("ACC") to integrate with Domino Directory or other LDAP directory solutions other than Microsoft Active Directory. (Blackberry BES and GroupWise email solutions are out-of-scope)

- AirWatch SEG and MAG are excluded.

The following AirWatch special feature configuration activities are excluded:

- AirWatch Browser blacklist or whitelist configuration

- AirWatch Content Management configuration

- AirWatch Secure App Launcher for Android configuration

- AirWatch Android Inbox email application configuration

- AirWatch Boxer email application configuration

- VMware Identity Manager configuration

- Use of Apple Configurator for supervised iOS devices

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the project. 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. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order.

SD-2.3.2. Basic Plus Configuration and Training for On-Premises Installation (Required for AirWatch Core MDM Server with Shared Android Devices)

Section Effective Date: 15-Nov-2016

The Basic Plus Installation and Training includes all the features in the Basic Installation and Training plus the configuration of the AirWatch Secure Launcher feature for Android devices.

SD-2.3.3. Premium Installation and Training of MDM Software (Required for the Installation of AirWatch Enterprise Mobility Software, AirWatch Cloud Connector and a Secure Email Gateway)

Section Effective Date: 21-Apr-2017

Premium Installation and Training for On-Premises Servers

AT&T will provide implementation services connected with the purchase of the associated AirWatch software licenses. The services will be provided remotely and include installation of components located on the Customer's premise, including the AirWatch Console, an optional Cloud Connector ("ACC") and either a Secure Email Gateway ("SEG") or PowerShell integration for email management. These services include a total of four meetings, all to be conducted remotely unless otherwise agreed upon by all parties.

The AT&T Business Service Guide is subject to change by AT&T from time to time.
See http://serviceguidenew.att.com for current version.

This document reflects the Service Guide in effect as of June 12, 2020

The four meetings are as follows:

Meeting 1: Kick-Off

This meeting is approximately 30 – 60 minutes and includes the AT&T Project Manager and an AT&T Managed Services professional. The meeting is designed to provide an overview of the implementation activities for both technical setup and functional configuration of the deployment. The topics to be covered will focus on preparation for the technical installation of system components, determining the scope of the features available/recommended, based on the Customer's requirements, and discussing the Customer's infrastructure.

This meeting is subject to a cancellation fee of up to $500.00 if Customer cancels less than 24 hours before the scheduled meeting.

Meeting 2: Readiness

This meeting is approximately 30 minutes and is designed to ensure the Customer has completed the pre-installation requirements for the system components.

This meeting is subject to a cancellation fee of up to $500.00 if Customer cancels less than 24 hours before the scheduled meeting.

Meeting 3: Installation

This meeting is approximately 120 minutes and is designed to install the technical components necessary to deploy the AirWatch Solution in the Customer's infrastructure.

This meeting is subject to a cancellation fee of up to $500.00 if Customer cancels less than 24 hours before the scheduled meeting.

Meeting 4: Configuration, Training and Deployment

This meeting is approximately 180 minutes and is designed to configure the recommended features for the Customer's installation and to deploy an initial pilot set of devices. AT&T will also provide basic administrator training during this call.

This meeting is subject to a cancellation fee of up to $500 if Customer cancels less than 24 hours before the scheduled meeting.

Meeting 1: Kick-Off

Meeting 1: Kick-Off		
AT&T Deliverables	**Notes**	**Responsibility Party**
Review the number and type of devices to be enrolled (iOS, Android, or Windows Phone 8 only)		AT&T
Identify which components will be installed (ACC, SEG or PowerShell)	Not all components are applicable for every Customer.	AT&T
Review server hardware, software, and port requirements for the components identified above.		AT&T
Review Apple ID requirements for APNS certificate		AT&T

Meeting 1: Kick-Off		
AT&T Deliverables	**Notes**	**Responsibility Party**
Review Active Directory service account for directory lookup and PowerShell service account (if needed).	AT&T reviews with Customer	AT&T
Review Customer Workbook with Customer	Policy creation is the Customer's responsibility	AT&T
Provide available dates/times for readiness call.	Established at the end of the Kick-Off call	Customer

Pre-Work for Meeting 2: Customer to Complete PRIOR to Meeting 2		
Customer Deliverables	**Notes**	**Responsible Party**
Procure virtual and/or physical servers for connection to cloud	Reviewed during Meeting 1	Customer
Configure firewall, DNS and service accounts for integration	Reviewed during Meeting 1	Customer
Complete pre-installation checklist/configuration requirements.	Customer to send completed Pre-Installation Requirements Worksheet checklist to AT&T	Customer
Complete AirWatch Academy: "Associate Level Certification" training course	Recommended, but not required	Customer
Complete and return the Policy Workbook	Customer to send completed recommended configuration worksheet.	Customer

Meeting 2: Readiness	
AT&T Deliverables	**Responsible Party**
Validate all items in pre-installation checklist	AT&T
Schedule Installation	AT&T/Customer

Meeting 3: Installation		
AT&T Deliverables	**Notes**	**Responsible Party**
Installation of AirWatch Enterprise Mobility Management Software on server(s)	Customer will participate via teleconference with AT&T during the installation process	AT&T
Install one ACC (if required)		AT&T

The AT&T Business Service Guide is subject to change by AT&T from time to time.
See http://serviceguidenew.att.com for current version.

This document reflects the Service Guide in effect as of June 12, 2020

Meeting 3: Installation		
AT&T Deliverables	**Notes**	**Responsible Party**
Configure LDAP integration (if required)		AT&T
Install one SEG OR configure PowerShell integration with one Exchange endpoint.		AT&T

Meeting 4: Configuration and Deployment		
AT&T Deliverables	**Notes**	**Responsible Party**
Assist with obtaining and uploading APNS certificate	Required only for iOS devices	AT&T
Demonstrate Console navigation		AT&T

Assist in configuring Active Directory integration:
    Assist with creating up to 5 users
    Assist with creating up to 5 administrators
    Assist with adding one user group
    Register email domain for auto-discovery
		AT&T

Register email domain for auto-discovery		AT&T
Assist with enrolling up to 10 devices for up to three different supported device Operating Systems (OS)		AT&T
Create one Telecom Plan and one Dynamic Assignment Plan for telecom usage.		AT&T

Assist with creation one of each of the following profiles (if applicable):
    Passcode
    Restrictions (i.e. Siri, Encrypted Backups, etc.)
    Exchange (using Native client or AirWatch Inbox, and/or AirWatch Boxer)
    Wi-Fi
		AT&T

Assist in creating one of each of the following Compliance Policies (if applicable):
    Compromised Status
    Email Compliance Policy (i.e. Unmanaged Devices, Compromised Devices, Encryption, etc.
    Encryption
    Application List
    Telecom Data usage
		AT&T

Meeting 4: Configuration and Deployment		
AT&T Deliverables	**Notes**	**Responsible Party**

Assist with loading one of each of the following application types (if applicable):
  Public Application
  Internal Application
  VPP Application
		AT&T

Branding the Solution (i.e. color schemes, logo)		AT&T
Assist with configuring one Report Subscription		AT&T
AT&T sends Customer survey and Customer is transitioned to Application Service Desk		AT&T

Additional Service Notes

- AT&T will assist with up to 3 different device types/operating systems (iOS, Windows Phone 8 and Android). Configuration and Management of Rugged Devices, Windows CE, and laptops are out of scope.

- AT&T will assist with enrolling an initial deployment of up to 10 devices.

- AT&T will integrate one Customer email infrastructure.

- AT&T will integrate one Active Directory infrastructure.

- AT&T will provide recommendations and training during the implementation. Further configuration to meet Customer's full requirements, and additional device enrollment beyond those implemented during the installation is Customer's responsibility.

- Procurement and installation of hardware is the Customer's responsibility. Upon request, AT&T will provide recommendations, but all decisions are to be made by Customer.

- Simple Certificate Enrollment Protocol ("SCEP") and certificate usage for authentication is out-of-scope. Customer may purchase the Advanced Authentication Service offering to incorporate certificate usage for authentication.

- All work, documentation and work product(s) will be conducted during typical, local business hours and will be provided in English.

- All work must be completed within one calendar year.

- AT&T will not configure the AirWatch Cloud Connecter ("ACC") to integrate with Groupwise or LDAP directory solutions other than Microsoft Active Directory and IBM Notes Traveler.

- AT&T will not configure the AirWatch Secure Email Gateway ("SEG") or PowerShell to integrate with email solutions other than Microsoft Exchange. (Blackberry BES, Lotus Traveler email solutions are out-of-scope)

- The following special feature configuration activities are excluded:

This document reflects the Service Guide in effect as of June 12, 2020

- o AirWatch Content Management Configuration.

- o AirWatch Browser (whitelisting/blacklisting, secure browsing).

- o App Wrapping.

- o Use of Apple configurator for supervised iOS devices.

- o Multiple SEGs.

- o VMware Identity Manager configuration.

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete these projects. The mandatory software installation and configuration is estimated to take place over 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. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order.

SD-2.3.4. Premium Plus Installation and Training for Use of MDM Software (Required for the Installation of AirWatch Enterprise Mobility Software and a Secure Email Gateway and a Mobile Access Gateway)

Section Effective Date: 15-Nov-2016

AT&T will provide implementation services connected with the purchase of the associated AirWatch software licenses. The services will be provided remotely and include installation of components located on the Customer's premises, including the AirWatch Console, an optional Cloud Connector ("ACC"), either a Secure Email Gateway ("SEG") or PowerShell integration for email management, and a Mobile Access Gateway for Content Management or Secure Browsing, and AT&T will provide implementation services for VMware Identity Manager. These services consist of a total of four meetings, all conducted remotely unless otherwise agreed upon by the parties

*For new Customers after November 15, 2016, the two required meetings for VMware Identity Manager will be integrated into the four meetings below.

The four meetings are as follows:

Meeting 1: Kick-Off

This meeting is approximately 30 minutes and includes the AT&T Project Manager and an AT&T Managed Services professional. The meeting is designed to provide an overview of the implementation activities related to both the technical setup and the functional configuration of the Customer's installation. The topics covered are focused on preparation for the technical installation of system components, determining the scope of the features available/recommended based on the Customer's requirements, and discussing the Customer's infrastructure.

This meeting is subject to a cancellation fee of up to $500.00 if the Customer cancels less than 24 hours before the scheduled meeting.

Meeting 2: Readiness

This meeting is approximately 30 - 60 minutes and is designed to ensure the Customer has completed the pre-installation requirements.

This meeting is subject to a cancellation fee of up to $500.00 if the Customer cancels less than 24 hours before the scheduled meeting.

Meeting 3: Installation

This meeting is approximately 180 minutes and is designed to install the necessary technical components to deploy the AirWatch Solution in the Customer's infrastructure.

This meeting is subject to a cancellation fee of up to $500.00 if the Customer cancels less than 24 hours before the scheduled meeting.

Meeting 4: Configuration, Training and Deployment

This meeting is approximately 240 minutes and is designed to configure the recommended features for the Customer's installation and to deploy an initial pilot set of devices. AT&T will also provide basic administrator training during this call.

This meeting is subject to a cancellation fee of up to $500.00 if the Customer cancels less than 24 hours before the scheduled meeting.

Meeting 1: Kick-Off		
AT&T Deliverables	**Notes**	**Responsible Party**
Review Customer's number and type of devices to be enrolled (iOS, Android, or Windows Phone 8 only)		AT&T
Identify which components will be installed (ACC, MAG, SEG, VMware Identity Manager, or PowerShell)	Not all components are applicable for every Customer. *See VMware Identity Manager Professional Services for details on deliverables and responsibilities.	AT&T
Review server hardware, software, and port requirements for the components identified above.		AT&T
Review Apple ID requirements for the APNS certificate		AT&T
Review the Active Directory service account for directory lookup and the PowerShell service account (if needed).	AT&T reviews with Customer	AT&T
Review Customer Workbook with Customer	Policy creation is the Customer's responsibility	AT&T

This document reflects the Service Guide in effect as of June 12, 2020

Meeting 1: Kick-Off		
AT&T Deliverables	**Notes**	**Responsible Party**
Provide available dates/times for readiness call.	Established at the end of the Kick-Off call	Customer

Pre-Work for Meeting 2: Client to Complete PRIOR to Meeting 2		
Customer Deliverables	**Notes**	**Responsible Party**
Procure virtual and/or physical servers for connection to cloud	Reviewed during Meeting 1	Customer
Configure firewall, DNS and service accounts for integration	Reviewed during Meeting 1	Customer
Complete pre-installation checklist/configuration requirements.	Customer to send completed Pre-Installation Requirements Worksheet checklist to AT&T	Customer
Complete AirWatch Academy: "Associate Level Certification" training course	Recommended, but not required	Customer
Complete and return the Policy Workbook	Customer to send completed recommended configuration worksheet.	Customer

Meeting 2: Readiness	
AT&T Deliverables	**Responsible Party**
Validate all items in pre-installation checklist	AT&T
Schedule Installation	AT&T/Customer

Meeting 3: Installation		
AT&T Deliverables	**Notes**	**Responsible Party**
Installation of AirWatch Enterprise Mobility Management Software on server(s)	Customer will participate via teleconference with AT&T during the installation process	AT&T
Configure LDAP integration (if required)		AT&T
Install one SEG OR configure PowerShell Integration with one Exchange endpoint.		AT&T
Install one MAG (if required)		AT&T

Meeting 4: Configuration and Deployment		
AT&T Deliverables	**Notes**	**Responsible Party**
Assist with obtaining and uploading APNS certificate	Required only for iOS devices	AT&T
Demonstrate Console navigation		AT&T
Assist in configuring Active Directory integration: Assist with creating up to 5 users Assist with creating up to 5 administrators Assist with adding one user group		AT&T
Register email domain for auto-discovery		AT&T
Assist with enrolling up to 10 devices using up to three different supported device Operating Systems (OS)		AT&T
Create one Telecom Plan and one Dynamic Assignment Plan for telecom usage.		AT&T
Assist with creation one of each of the following profiles (if applicable): Passcode Restrictions (i.e. Siri, Encrypted Backups, etc.) Exchange (using Native client, AirWatch Inbox, and/or AirWatch Boxer) Wi-Fi		AT&T
Assist in creating one of each of the following Compliance Policies (if applicable): Compromised Status Email Compliance Policy (i.e. Unmanaged Devices, Compromised Devices, Encryption, etc.) Encryption Application List Telecom Data usage		AT&T
Assist in creating one Content Category		AT&T
Assist in deploying one document via the console.		AT&T
Assist in configuring one Content Repository		AT&T
Assist in configuring Browser Settings		AT&T
Enable Personal Content Storage		AT&T
Assist in deploying Content Locker (as a public app)		AT&T
Assist in configuring Bookmarks		AT&T

This document reflects the Service Guide in effect as of June 12, 2020

Meeting 4: Configuration and Deployment		
AT&T Deliverables	**Notes**	**Responsible Party**
Assist with loading one of each of the following application types (if applicable): Public Application Internal Application VPP Application		AT&T
Branding the Solution (i.e. color schemes, logo)		AT&T
Assist with configuring one Report Subscription		AT&T
AT&T sends Customer survey and Customer is transitioned to Application Service Desk		AT&T

Additional Service Notes

- AT&T will assist with up to 3 different device types/operating systems (iOS, Windows Phone 8 and Android). Configuration and Management of Rugged Devices, Windows CE, and laptops are out of scope.

- AT&T will assist with enrolling an initial deployment of up to 10 devices.

- AT&T will integrate one Customer email infrastructure.

- AT&T will integrate one Active Directory infrastructure.

- AT&T will provide recommendations and training during the implementation. Further configuration to meet Customer's full requirements and additional device enrollment beyond those implemented during the installation is the Customer's responsibility.

- Procurement and installation of hardware is Customer's responsibility. AT&T will provide recommendations, but all decisions are to be made by Customer.

- Simple Certificate Enrollment Protocol ("SCEP") and certificate usage for authentication is out-of-scope. Customer may purchase the Advanced Authentication Service to incorporate certificate usage for authentication.

- All work, documentation and work product(s) will be conducted during typical, local business hours and will be provided in English.

- All work must be completed within one calendar year.

- AT&T will not configure the AirWatch Cloud Connecter ("ACC") to integrate with Groupwise or LDAP directory solutions other than Microsoft Active Directory and IBM Notes Traveler.

- AT&T will not configure the AirWatch Secure Email Gateway ("SEG") or PowerShell to integrate with email solutions other than Microsoft Exchange. (Blackberry BES, Lotus Traveler email solutions are out-of-scope)

- The following special feature configuration activities are excluded:

  o Use of Apple configurator for supervised iOS devices.

    o   Multiple SEGs or multiple MAGs

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the project. The mandatory software installation and configuration is estimated to take place over a three day period 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. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order.

SD-2.3.5. VMware Identity Manager Professional Services

Section Effective Date: 21-Apr-2017

AT&T will provide implementation services for VMware Identity Manager as part of the Premium Plus Installation and Configuration. *The deployment will be conducted in an existing AirWatch On-Premises environment. This project has two meetings conducted remotely.

*Customers who purchased Blue and/or Yellow Management Suite licenses prior to November 15, 2016 must separately purchase VMware Identity Manager Professional Services at the rate listed in the Rate Table.

Meeting 1: Kick-Off

This meeting is approximately 60 minutes and includes the AT&T Project Manager and an AT&T Managed Services professional. The meeting is designed to provide an overview of the implementation activities related to both technical setup and functional configuration for the Customer's installation. The topics covered are focused on preparation for technical installation of system components, determining the scope of the features available/recommended based on Customer's requirements, and discussing the Customer's infrastructure.

This meeting is subject to a cancellation fee of up to $500.00 if the Customer cancels less than 24 hours before the scheduled meeting.

Meeting 2: Configuration, Training and Deployment

This meeting is approximately 180 - 240 minutes and is designed to activate and configure VMware Identity Manager. AT&T will provide training on basic administration and usage of these features.

This meeting is subject to a cancellation fee of up to $500.00 if Customer cancels less than 24 hours before the scheduled meeting.

Meeting 1: Kick-Off		
AT&T Deliverables	**Notes**	**Responsible Party**
Review Customer's number and type of devices that will use VMware Identity Manager	AT&T reviews with Customer	AT&T
Capture Customer admin and email domains to be included in the AirWatch implementation	AT&T reviews with Customer	AT&T
Verify that the Customer has a VMware Identity Manager instance and AirWatch instance provisioned and has received admin credentials	AT&T reviews with Customer	AT&T
Review AirWatch SAML capabilities	AT&T reviews with Customer	AT&T
Review high level SAML integration with AirWatch	AT&T reviews with Customer	AT&T
Schedule Configuration	Established at the end of the kick-off call	AT&T/Customer

Customer Pre-Work for Meeting 2	
Customer Deliverables	**Responsible Party**
Customer provisions a Windows Server intended for the AirWatch Cloud Connector	Customer
Customer creates firewall rules for the AirWatch Cloud Connector as needed	Customer
Customer creates an Active Directory service account for AirWatch Active Directory integration	Customer

Meeting 2: Configuration and Deployment	
AT&T Deliverables	**Responsible Party**
Install/Configure AirWatch Cloud Connector	AT&T
Configure Directory services within the AirWatch portal	AT&T
Integrate the Customer's AirWatch portal to the Customer's VMware Identity Manager portal	AT&T
Configure Email Domain Auto Discovery within the VMware Identity Manager portal	AT&T
Add VMware Identity Manager app(s) to the AirWatch Apps and Books portal	AT&T
Set up AirWatch admin portal cloud app within the VMware Identity Manager portal	AT&T
Assist Customer with deploying up to 2 non-AirWatch SAML applications via VMware Identity Manager	AT&T

This document reflects the Service Guide in effect as of June 12, 2020

Meeting 2: Configuration and Deployment	
AT&T Deliverables	**Responsible Party**
Enroll up to 3 devices within AirWatch, deploy VMware Identity Manager app, and verify user is able to login to AirWatch via VMware Identity Manager.	AT&T

Additional Service Notes

- AT&T will assist with only iOS and Android devices.

- AT&T will assist with adding one User Group to the AirWatch Solution.

- SAML settings (endpoint URLs, parameters, etc.) which are individually different for non-AirWatch apps must have been provided by the Customer.

- AT&T will provide recommendations and training during the implementation. Further configuration to meet Customer's additional requirements, and device enrollment beyond what has been implemented during the installation is the Customer's responsibility.

- All work, documentation and work product(s) will be conducted during typical, local business hours and will be provided in English.

- All work must be completed within one calendar year.

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the project. 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. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order.

SD-2.3.6. Mobile Content Management Collaborate Add-On Installation and Training (Add-On to Premium Plus)

Section Effective Date: 17-Sep-2015

AT&T will provide implementation services connected with the purchase of the associated AirWatch software licenses. The deployment will be conducted in Customer's on-premises environment, with integration provided by an existing Mobile Access Gateway. This service consists of two meetings, each conducted remotely unless otherwise agreed upon by the parties.

The two meetings are as follows:

Meeting 1: Kick-Off

This meeting is approximately 30 minutes and includes the AT&T Project Manager and an AT&T Managed Services professional. The meeting is designed to provide an overview of the implementation activities related to the technical setup and the functional configuration for the Customer's installation. The topics covered are focused on preparation for the technical installation of system components, determining the scope of the features that are available/recommended based on Customer's requirements, and discussing the Customer's infrastructure.

This meeting is subject to a cancellation fee of up to $500.00 if the Customer cancels less than 24 hours before the scheduled meeting.

Meeting 2: Configuration, Training and Deployment

This meeting is approximately 180 - 240 minutes and is designed to activate and configure the recommended features for Collaborate and Content Locker. AT&T will provide training on basic administration and usage of these features.

This meeting is subject to a cancellation fee of up to $500.00 if Customer cancels less than 24 hours before the scheduled meeting.

Meeting 1: Kick-Off		
AT&T Deliverables	**Notes**	**Responsible Party**
Review Customer use case and determine the number and type of devices to be included in Content Locker/Collaborate.		AT&T
Determine MAG configuration	The optional MAG service is required for Collaborate	AT&T
Provide available dates/times for next call.	Established at the end of the Kick-Off call	Customer

Meeting 2: Configuration and Deployment	
AT&T Deliverables	**Responsible Party**
Deploy Content Locker as a public app (if required)	AT&T
Create one Content Category (if required)	AT&T
Deploy one document via the Content Locker. (if required)	AT&T
Configure one content repository (if required)	AT&T
Configure and enable personal content in the console.	AT&T
Enter Editing/Annotation license key.	AT&T
Demonstrate the use of Collaborate and Content Locker on up to two client devices.	AT&T

Additional Service Notes

AT&T will provide recommendations and training during the implementation. Further configuration to meet Customer's additional requirements and additional device enrollment beyond those implemented during the installation is Customer's responsibility.

Installation of a Mobile Access Gateway ("MAG") (required for Collaborate) is not included. The MAG must be purchased and configured separately.

Procurement and installation of hardware is Customer's responsibility. AT&T will provide recommendations, but all decisions are to be made by Customer.

All work, documentation and work product(s) will be conducted during typical, local business hours and will be provided in English.

All work must be completed within one calendar year.

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the project. 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. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise ("Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order.

SD-2.3.7. Customer Responsibilities Relating to EMM Deployment

Section Effective Date: 17-May-2016

This section identifies the Customer actions required to prepare for EMM deployment. A brief telephone call is strongly recommended in advance of the installation start date to review server configuration and reach agreement on which specific features should be implemented.

At a high level, these actions include:

- Both virtual and physical servers are supported and must be built to the specifications provided, including all additional Windows features and roles. The AirWatch installation files must be downloaded directly from AirWatch and be available on each server to be used in the Solution's implementation.

- Allocating IP addresses and Fully Qualified Domain Names ("FQDNs") for the platform. The IP addresses and FQDNs must be publicly accessible so mobile devices can access these platforms over the Internet.

- Ensuring access to Simple Mail Transfer Protocol ("SMTP") and Domain Name System ("DNS") servers.

- If Lightweight Directory Access Protocol ("LDAP") operation is desired, providing credentials for a system account allowing directory lookups.

- Opening required TCP and UDP ports on the firewall and communicating the necessary details during the pre-installation call with AT&T.

This document reflects the Service Guide in effect as of June 12, 2020

- Acquiring and/or preparing required certificates, including the certificate for Apple Push Notification Service ("APNS").

- If using virtual machines ("VMs"), configuring VMs that meet the provided specifications and uploading the AirWatch installation file(s) to the VM data store(s).

- Providing AT&T's technical consultant remote access to the installation environment.

- Access to the fee based Apple Developer Program is required for creation of the application signing certificate.

SD-2.3.8. AirWatch Secure Email Gateway (SEG) Implementation and Configuration (Optional)

Section Effective Date: 17-Sep-2015

AT&T will install, configure, and test the AirWatch Secure Email Gateway or configure and test the SEG physical appliance to integrate the appliance with an existing AirWatch appliance.

Add-On-AirWatch SEG Implementation and Configuration	
Activity - Configuration	**Deliverables**
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) e-mail environment. For high-availability environments, configuration of the network load balancer cluster and monitoring for cluster member management is the sole responsibility of Customer.	AT&T to remotely install the AirWatch software on the Customer-provided hardware or VM guest container AT&T to remotely configure the SEG basic networking parameters. AT&T to implement SEG configuration. AT&T to perform a simple Exchange ActiveSync pass-through connectivity test only. Failover testing is the exclusive responsibility of Customer.

No travel expenses are required or included in this project.

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the project.   Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted.   In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order form.

SD-2.3.9. AirWatch Mobile Access Gateway (MAG) Implementation and Configuration (Optional)

Section Effective Date: 19-Dec-2014

Add-On-AirWatch MAG Implementation and Configuration	
Activity - Configuration	**Deliverable**
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.	AT&T to remotely install the AirWatch software on the Customer-provided hardware or VM guest container. AT&T to remotely configure the MAG basic networking parameters. AT&T to implement MAG configuration. AT&T to perform a simple MAG mobile device to end-point pass-through connectivity test.

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the project. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order form.

SD-2.3.10. AirWatch Cloud Connector (ACC) Implementation and Configuration

Section Effective Date: 17-Sep-2015

Add-On AirWatch ACC Implementation and Configuration	
Activity - Configuration	**Deliverable**
AT&T will remotely configure and integrate one AirWatch Cloud Connector on the Customer's premise. Setup will include integration to one Active Directory server. Customer is responsible for provisioning a server on its premises in accordance with the configuration checklist provided.	AT&T to remotely install the AirWatch software on the Customer-provided hardware or VM guest container. AT&T to remotely configure the ACC basic networking parameters. AT&T to perform a simple ACC connectivity test to ensure that the integration is complete between the AirWatch hosted console and the Customer's existing Active Directory Server.

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the project. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order form.

SD-2.3.11. AirWatch Advanced Telecom Professional Services

Section Effective Date: 17-Sep-2015

AT&T will provide implementation services connected with the purchase of the associated AirWatch software licenses. The deployment will be conducted in an existing AirWatch On-Premises environment. This project accounts for a total of one meeting conducted remotely.

The meeting is defined as follows:

Meeting 1: Configuration and Deployment

This meeting is approximately 60 minutes and includes the AT&T Managed Services professional. The meeting is designed to provide an overview of the implementation activities related to technical setup and functional configuration for the deployment, as well as the actual configuration of Advanced Telecom in the Customer's existing infrastructure.

This meeting is subject to a cancellation fee of up to $500.00 if Customer cancels less than 24 hours before the scheduled meeting.

Meeting 1: Configuration and Deployment	
AT&T Deliverables	**Responsible Party**
Assist with configuration of one "per device" or "pooled" telecom plan.	AT&T
Assist with configuration of one dynamic assignment rule	AT&T
Assist with configuration of one Telecom-based compliance rule (Roaming, data usage, etc.)	AT&T
Assist with configuration of Agent settings for supported platforms to enable collection of Telecom data	AT&T
Assist with configuration of privacy settings to enable collection of Telecom data	AT&T

Additional Service Notes

- Installation of any hardware or software is beyond the scope of this engagement.

- AT&T will provide recommendations and training during the implementation. Further configuration to meet Customer's additional requirements, and telecom plan deployments above and beyond what has been implemented during the installation is the Customer's responsibility.

- All work, documentation and work product(s) will be conducted during typical, local business hours and will be provided in English.

- All work must be completed within one calendar year.

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the project. 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. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes

This document reflects the Service Guide in effect as of June 12, 2020

in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order.

SD-2.3.12. AirWatch Video Professional Services

Section Effective Date: 17-Sep-2015

AT&T will provide implementation services connected with the purchase of AirWatch Video. The deployment will be conducted in an existing AirWatch On-Premises environment. This project includes one meeting conducted remotely.

The meeting is defined as follows:

Meeting 1: Configuration, and Deployment

This meeting is approximately 60 minutes and includes the AT&T Managed Services professional. The meeting is designed to provide an overview of the implementation activities related to the technical setup and functional configuration for the deployment, as well as the actual configuration of AirWatch Video in the Customer's existing on-premises infrastructure.

This meeting is subject to a cancellation fee of up to $500.00 if Customer cancels less than 24 hours before the scheduled meeting.

Meeting 1: Configuration and Deployment	
AT&T Deliverables	**Responsible Party**
Assist with obtaining and entering Wistia CDN token.	AT&T
Assist with configuration of up to three video channels.	AT&T
Assist with importing or uploading up to two videos.	AT&T
Assist with configuring the AirWatch video application for deployment to supported platforms.	AT&T
Verify functionality in the AirWatch Video client.	AT&T

Additional Service Notes

- Obtaining an appropriate Wistia account is the responsibility of the Customer.

- Installation of any hardware or software other than the AirWatch Video app is beyond the scope of this engagement.

- AT&T will provide recommendations and training during the implementation. Further configuration to meet Customer's additional requirements and video deployments beyond what has been implemented during the installation is the Customer's responsibility.

- All work, documentation and work product(s) will be conducted during typical, local business hours and will be provided in English.

- All work must be completed within one calendar year.

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the project. 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. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order.

SD-2.3.13. EMM Operations Training (Optional)

Section Effective Date: 15-Nov-2016

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 the five AirWatch features below:

- AirWatch Inbox and/or AirWatch Boxer 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.

All server software installation must have been completed prior to this training. Software upgrades are not offered with this service. These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the project. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fees could be impacted. In the event any Change(s) affect the schedule, devices and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order.

SD-2.3.14. EMM Managed Service Health Check

Section Effective Date: 17-May-2016

AT&T will remotely inspect and review the current state of the EMM 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.

No travel expenses are required or included in this project. No hardware or software installation will be done on the Customer's premises. Any changes in scope that arise from discovery during the health check will be addressed via a separate Professional Service engagement.

EMM Managed Service Health Check	
Health Check System Validation Components	**Deliverables**
Methodological review of an existing AirWatch MDM core server implementation and up to two SEGs. Review AirWatch MDM core server configurations and settings within the AirWatch console. Review configuration policy definitions for errors and completeness. Policies are not reviewed for security efficacy. Review Device Status (pending, verified and wiped) and document outstanding devices that should be under management. Not included: Assessment of the state of the identity (Active Directory), collaboration (Exchange), or public key (certificates/SCEP) infrastructures, and implementation of any remediation recommended by the review.	Summary report describing any identified variants in the current state implementation and configuration from a combined AT&T and vendor baseline. Summary of recommended remediation to correct identified variants. Teleconference question and answer session with AT&T technical consultant to review findings and recommendations.

SD-2.3.15. Logistics

Section Effective Date: 19-Dec-2014

Managed Health Check and System validation is provided remotely by one AT&T consultant. No hardware or software installation will be done on the Customer's premises.

Estimated project duration is 2 days of offsite work. The Services provided hereunder shall be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time. AT&T has made every attempt to accurately estimate the time required to successfully complete the health check project. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fess could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order.

SD-2.3.16. Policy Reviews for Customization (Optional)

Section Effective Date: 19-Dec-2014

Mobility Policy Reviews are available on a custom basis through AT&T Professional Services.

SD-2.3.17. AirWatch Public Key Infrastructure (PKI) Integration and Identity Certificate Device Configuration (Optional)

Section Effective Date: 17-May-2016

PKI Integration and Identity Certificate Device Configuration (Optional)	
Activity - Remote Configuration	**Deliverables**
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.	One Certificate Authority integration configuration and one certificate template will be created in AirWatch representing the Customer's desired type of identity certificate. AT&T will also define one device profile for Exchange ActiveSync auto-configuration using an AirWatch-managed identity certificate, one device profile for VPN client auto-configuration using an AirWatch-managed identity certificate, and one device profile for preferred Wi-Fi network auto-configuration using an AirWatch-managed identity certificate. If required by the Customer, AT&T will configure the service accounts in Active Directory (User or Computer object) for Kerberos authentication delegation, create service principal names ("SPNs") if necessary, and configure the email proxy service to request Kerberos delegated credentials on behalf of device users for mailbox access.

Activity - Testing	**Deliverable**
AT&T will assist with the testing of each device profile on a single supported device.	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 authorization or authorization failures within the authentication, authorization and accounting (AAA) infrastructure.

These services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., local time in the Continental U.S. Travel and Expense to perform the workshop are not included. AT&T has made every attempt to accurately estimate the time required to successfully complete the project. Customer acknowledges and agrees that if impediments, complications, or Customer requested changes in scope arise (the "Changes"), these factors are out of the control of AT&T, and the schedule, services and fess could be impacted. In the event any Change(s) affect the schedule, services and fees, the parties will modify the Customer's Service Agreement accordingly by executing a Change Order form.

SD-3. Post-Contract Support Requirements

Section Effective Date: 19-Dec-2014

- AT&T will assign a designated AT&T Project Manager to interface directly with Customer's designated Project Manager. AT&T and Customer shall cooperate to define an agreeable Project Plan. AT&T and Customer shall use commercially reasonable efforts to meet the timelines in the Project Plan. If AT&T or Customer cannot meet a date specified in the Project Plan, that party shall notify the other party, and the parties will agree upon revised

dates for the Project Plan. Delays in Customer deliverables, including requirements, shall extend AT&T's due dates for AT&T deliverables on a day-for-day basis.

- The Customer Project Manager shall represent Customer regarding selected work activities. The Customer Project Manager is responsible for overall project management and must have the authority to direct Customer's personnel and Customer's vendors (collectively "Customer Project Team") to provide the information and to participate in, and perform, the activities required by AT&T in support of its performance under the Customer's Service Agreement. The AT&T Project Manager shall lead the AT&T Project Team, receive Change Requests and facilitate resolution of all inter-team issues encountered by the Customer Project Team or AT&T Project Team, whether arising from the performance of the parties under the Customer's Service Agreement or a Change Request.

- Customer shall designate, within 24 hours of the Effective Date of the applicable Pricing Schedule or other ordering document, Customer's relevant management, staff and vendors who may be called upon to provide information to AT&T regarding the: (i) operational and technical specifications of the Solution (ii) definition of operational requirements; (iii) deployment of applications; and (iv) general business planning as applicable to the development of the project.

- 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.

- The AT&T Project Team may consist of an AT&T Technical Project Manager.

- The AT&T and Customer Project Managers shall participate in all phases of the project. They shall initiate the project, prepare reports, and manage project staffing, deployment, and overall delivery assurance. The AT&T Project Manager's responsibilities are as follows:

  o Conduct a formal project kick-off meeting ("Project Kick-off Meeting") which will include, among other things, concurrence from all as to the scope of the installation project. The AT&T Project Manager will work with the Customer Project Manager to create a communication plan that identifies both AT&T and Customer resources required for the project.

  o Serve as the primary interface to the Customer through the Customer's Project Manager.

  o Coordinate the site installation priorities and the installation schedules with the Customer Project Manager. The AT&T Project Manager will create an installation project timeline draft and submit the draft to Customer via hardcopy or electronic format. Customer and AT&T will mutually agree to the project timeline, and once that occurs, the project timeline will be considered final and subject to changes only through a Change Request.

  o Function as the escalation point for issues arising from the ordering and installation of the Solution.

  o Provide, at the Customer's request, email or telephone status updates as to the progress of the implementation.

o   Participate in and schedule regular status and project planning meetings as required. The audience for such status meetings may include AT&T personnel, third party vendors or Customer-designated team members.

o   Develop, manage and track project schedules and all change control processes.

o   Develop and maintain any contact list and communication plan and track and monitor prioritized action items and an issues list.

o   Manage the Test and Turn-up of the Production Environment.

SD-3.1. Responsibilities of the Parties

Section Effective Date: 30-Sep-2013

AT&T and Customer shall have the following responsibilities:

Responsibilities of the Parties		
Task/Function	**AT&T**	**Customer (or Customer's Third-Party)**
Conduct a formal project kick-off meeting. During the meeting AT&T and Customer will: introduce key people at Customer and AT&T; exchange contract information for regular reporting and emergencies; review scope of services; review communication, notification and issue escalation procedures; discuss other specific Customer requests and rules for engagement (e.g., period during which AT&T should not perform testing); and discuss the involvement of Customer's technical staff in the project for the purpose of knowledge transfer and security.	R	R
Overall project plan and milestones	R	C
Provide a project manager to serve as a single point of contact	R	R
Provide points of contact as requested including a designated decision-maker and company org chart		R
Provide a hand-off package upon Customer acceptance that includes AT&T Support information	R	
Provide completed questionnaires: SSL certificate, network, and DNS		R
Prepare server environment for SEG/MAG	C	R
Install the SEG and MAG and configure the SEG, MAG and On-Premise AirWatch MDM server.	R	
Install, configure, and maintain licenses that Customer has procured through AT&T as part of the Solution	R	
Provide administrator education and implement policy administration of end user groups within the AirWatch Console	R	
User acceptance testing prior to environment go-live	C	R
Notes:		

Responsibilities of the Parties		
Task/Function	**AT&T**	**Customer (or Customer's Third-Party)**
		R = Responsible and C = Consult

SD-3.2. Change Control

Section Effective Date: 30-Oct-2012

AT&T and Customer will manage all changes through a written change request process ("Change Control Process"). Either Party must submit change requests in writing to the other party via AT&T's required process.

The party requesting the change must submit a written change request to the other party and the receiving party shall issue a written response to the change request, including whether the receiving party accepts or rejects the request.

SD-3.3. Post Installation Technical Support

Section Effective Date: 19-Dec-2014

Post installation technical support is provided directly by AirWatch Technical Support services.

SD-4. Advanced Authentication using Certificates and Kerberos Delegation

Section Effective Date: 03-May-2013

Certificate authentication enables enterprises to verify end user identity without requiring end users to enter usernames and passwords on their mobile devices to access corporate resources, such as Exchange ActiveSync, VPN or Corporate Wi-Fi.

SD-4.1. Service Scope

Section Effective Date: 19-Dec-2014

AT&T will implement and configure the integration settings to enable the Solution to issue certificates to mobile devices from a supported interface to the Customer's Certificate Authority. In completing the Certificate Authority integration AT&T will:

- 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 MDM-issued identity certificate,

- Define one device policy profile for VPN Customer auto-configuration using an identity certificate,

- Define one device policy profile for preferred Wi-Fi network auto-configuration using an identity certificate

The AT&T Business Service Guide is subject to change by AT&T from time to time.
See http://serviceguidenew.att.com for current version.

This document reflects the Service Guide in effect as of June 12, 2020

- Configure the service accounts in Active Directory (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.

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.

SD-5. AT&T Enterprise Mobility Management (EMM) Administration Support (Optional)

Section Effective Date: 17-May-2016

AT&T's EMM consultants will perform advanced security and EMM policy analysis and provide recommendations based on industry best practices for Enterprise Mobility Management design, implementation and administration based upon Customer's use of the AirWatch platform. Services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., Customer's local time. All Services are provided in English.

SD-5.1. EMM Environment Discovery

Section Effective Date: 17-Sep-2015

AT&T will remotely perform an inventory of the of the Customer's existing EMM environment. The purpose of the inventory is to document the current state of the Customer's EMM environment and the environment's configuration and settings. This discovery effort will generate a report and provide a baseline for consulting. The inventory is performed remotely and there are no travel expenses required or included. Services will be performed Monday through Friday during mutually agreed hours and must be completed within 30 days of order placement. Customer must provide AT&T access to its EMM environment and ensure that appropriate resources with access to that environment are made available during the entire inventory process.

SD-5.2. Consulting and Advisory Services

Section Effective Date: 17-Sep-2015

AT&T will assign a consultant familiar with the Customer's baseline report and expertise in the Customer's EMM environment. The Consulting Services will be provided for the Customer's current EMM environment and includes best practices and consulting on how to perform EMM administration or system configuration changes such as the following:

- Organizational strategies and structure of users within the EMM environment

- User management strategies

- Security policy configuration and options

- Device configuration profiles

- Connectivity configuration profiles (e.g., Wi-Fi, VPN)

This document reflects the Service Guide in effect as of June 12, 2020

- Application management and distribution

- Content management and distribution

- Growing and scaling the EMM platform and user base

- Additional integration into the Customer's environment (LDAP, Exchange, Certificates)

- New EMM features and functionality

Access to the assigned Consultant must be scheduled in advance and is available Monday through Friday at mutually agreed upon times during Customer's normal business hours. The Consultant will be accessible via telephone and email. A designated backup will be assigned in appropriate situations. The Consultant will interface with up to two authorized Customer representative(s), who are typically IT or Security personnel responsible for the Customer's EMM production environment. AT&T will report hours used through the Consulting Service on a monthly basis.

The following is not in scope for Consulting Services:

- Consultants will not access or have logon credentials to the Customer's EMM environment. Access will be facilitated by and performed in conjunction with authorized Customer personnel.

- Consulting on new mobile OSs or EMM features before they are made generally available.

- Consulting on EMM vendors or products not supported by AT&T or not in production in the Customer's environment.

- Installing EMM hardware.

- Support or troubleshooting for third party applications.

- Documenting of Customer processes or support guides.

- Configuring or reconfiguring end user devices for deployment or redeployment.

Customer is responsible for providing the following:

- Access to its EMM environment for the AT&T Consultant via agreed upon web conferencing.

- Installation of EMM hardware that meets the minimum requirements as published by the EMM vendor and purchase and availability of EMM software.

- Day to day EMM administration including but not limited to, the following: Device Lock, Wipe, and Passcode Reset; Addition/Deletion of Users and Groups; Device Enrollment; Application of Customer Policies and Profiles; Addition/Updating of Applications and Content; and Reporting.

- EMM technical support, including troubleshooting and resolving end user issues.

- Providing AT&T up to two technical contacts authorized to interface with the AT&T consultant.

Consulting hours are valid for a 6 month period from initial consultant engagement. After 6 months, all unused hours will expire.

Overage time will not be provided unless supported by a written request from an authorized Customer representative

- All prices exclude applicable taxes, fees and surcharges.

- Billing and tracking for hours will be in 1 hour increments. Consulting time for each engagement is rounded up to the next whole hour.

- Services will be performed Monday through Friday, 9:00 a.m. to 5:00 p.m., Customer's local time.

- Prices do not include expenses for AT&T travel to Customer's facilities. If Customer requires onsite support, all reasonable travel expenses will be billed to the Customer in accordance with the AT&T Global Travel and Expense Policy.

- All Services are provided in English.

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 Consulting Services.

SD-6. Glossary

Section Effective Date: 15-Nov-2016

Glossary of Terms	
Acronym	**Description/Definition**
CRU	Corporate Responsibility User – An Employee receiving service under Customer's account.
DNS	Domain Name System
EMM	Enterprise Mobility Management
EULA/TOS	End User License Agreement/Terms Of Service - An agreement between AirWatch/VMware and Customer to which AT&T is not a party and pursuant to which AirWatch/VMware assumes all obligations and liabilities to Customer for the items provided thereunder.
IDC	Internet Data Center
IRU	Individual Responsibility User – An Employee receiving service under an individual account in accordance with a sponsorship program.
LDAP	Lightweight Directory Access Protocol
MAG	Mobile Access Gateway
MDM	Mobile Device Management
MRC	Monthly Recurring Charge
NRC	Non-Recurring Charge
NTP	Network Time Protocol
SEG	Secure Email Gateway
SLA	Service Level Agreement
SLO	Service Level Objective

The AT&T Business Service Guide is subject to change by AT&T from time to time.
See http://serviceguidenew.att.com for current version.

This document reflects the Service Guide in effect as of June 12, 2020

Glossary of Terms	
Acronym	**Description/Definition**
SMTP	Simple Mail Transfer Protocol
VPN	Virtual Private Network

Pricing (P)

P-1. Billing

Section Effective Date: 21-Apr-2017

- Billing for the Solution shall be on a non-recurring (one-time) and recurring basis and begins as of Effective Date of applicable order.

- Licenses for the Green, Orange, Blue, and Yellow are available (i) on a one-time (perpetual) basis with annual charges for maintenance or (ii) on a recurring monthly subscription basis, with maintenance included or (iii) on an annual subscription basis, with maintenance included.

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

- The K12 Management Suites are available on a one, two, three year term, or on a one-time (perpetual) basis with recurring annual charges for maintenance.

- Professional Services are invoiced on a non-recurring basis upon Acceptance or based on mutually agreed upon milestones.

- All prices exclude applicable taxes, fees and surcharges.

- All amounts paid are non-refundable.

Applies to EMMS Professional Services:

- Billing for Services shall be on a non-recurring (one-time basis) and issued upon acceptance of Customer's order.

- Billing and tracking for hours will be in one (1) hour increments. Consulting time for each engagement is rounded up to the next whole hour.

- Prices do not include expenses for AT&T travel to Customer's facilities. If Customer requires onsite support, all reasonable travel expenses will be filled to the Customer in accordance with the AT&T Global Travel and Expense Policy.

P-2. Rate Table AWOP-SUBSCR-CHRGS: Subscriptions (includes maintenance) – Monthly, 1 Year, 2 Year and 3 Year Charges

Section Effective Date: 21-Apr-2017

Rate Table AWOP-SUBSCR-CHRGS: Subscriptions (includes maintenance) - Monthly Charge and 1 Year, 2 Year and 3 Year Charges				
Description of Charges	**Monthly Charge**	**1 Year**	**2 Years**	**3 Years**
Green Management Suite Device-Based Subscription	$3.25	$39.00	$78.00	$117.00
Green Management Suite User-Based Subscription	$6.50	$78.00	$156.00	$234.00
Orange Management Suite Device-Based Subscription	$4.00	$48.00	$96.00	$144.00
Orange Management Suite User-Based Subscription	$8.00	$96.00	$192.00	$288.00
Blue Management Suite Device-Based Subscription	$5.25	$63.00	$126.00	$189.00
Blue Management Suite User-Based Subscription	$10.50	$126.00	$252.00	$378.00
Yellow Management Suite Device-Based Subscription	$8.17	$98.00	$196.00	$294.00
Yellow Management Suite User-Based Subscription	$16.33	$196.00	$392.00	$588.00
K-12 EDU Management Suite Device-Based Subscription		$13.00	$25.00	$35.00
K-12 EDU with Teacher Tools Management Suite Device-Based Subscription		$16.00	$31.00	$43.00
AirWatch Video - Device-Based Subscription	$1.50			
AirWatch Video - User-Based Subscription	$3.00			
AirWatch Advanced Telecom - Device-Based Subscription	$1.00			
AirWatch Advanced Telecom - User-Based Subscription	$2.00			
Teacher Tools - Device-Based Subscription	$0.50			

P-3. Rate Table AWOP-PERPLM-OTAC: Perpetual Licenses and Maintenance – One-Time and Annual Charges

Section Effective Date: 21-Apr-2017

Rate Table AWOP-PERPLM-OTAC: Perpetual Licenses and Maintenance - One-Time and Annual Charges		
Description of Charges	**One-Time Charge**	**Annual Charge**
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 Suite Upgrade - 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 - 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	

Rate Table AWOP-PERPLM-OTAC: Perpetual Licenses and Maintenance - One-Time and Annual Charges		
Description of Charges	**One-Time Charge**	**Annual Charge**
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 Maintenance Suite Upgrade - Perpetual License; Device-Based License	$66.00	
Orange to Yellow Maintenance 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 - Perpetual License; Device-Based License	$90.00	
Blue Management Suite - Perpetual License Maintenance; Device-Based License		$18.00
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 - Perpetual License; Device-Based License	$130.00	
Yellow Management Suite - Perpetual License Maintenance; Device-Based		$26.00

The AT&T Business Service Guide is subject to change by AT&T from time to time.
See http://serviceguidenew.att.com for current version.

This document reflects the Service Guide in effect as of June 12, 2020

Rate Table AWOP-PERPLM-OTAC: Perpetual Licenses and Maintenance - One-Time and Annual Charges		
Description of Charges	**One-Time Charge**	**Annual Charge**
License		
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	
K-12 EDU Management Suite - Perpetual License; Device-Based License	$24.00	
K-12 EDU Management Suite - Perpetual License Maintenance; Device-Based License		$5.00
K-12 EDU with Teacher Tools Management Suite Perpetual License; Device-Based License	$29.00	
K-12 EDU with Teacher Tools Management Suite Perpetual License Maintenance; Device-Based License		$6.00
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 - 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
Teacher Tools - Perpetual; per Device License	$20.00	
Teacher Tools - Perpetual Maintenance; per Device License		$4.00

The AT&T Business Service Guide is subject to change by AT&T from time to time.
See http://serviceguidenew.att.com for current version.

This document reflects the Service Guide in effect as of June 12, 2020

P-4. Rate Table AWOP-PSVCS-OTC: Professional Services – One-Time Charge

Section Effective Date: 21-Apr-2017

Rate Table AWOP-PSVS-OTC: Professional Services - One-Time Charge		
Description of Charges	**One-Time Charge**	**Notes**
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	
VMware Identity Manager Configuration and Training	$1,800.00	
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		<ICB>
Notes:		
	All prices exclude applicable taxes, fees and surcharges.	
<ICB>	Rates are provided on an individual case basis.	

P-5. Rate Table AWOP-GRAND-RATES: Grandfathered Rates

Section Effective Date: 21-Apr-2017

Rate Table AWOP-GRAND-RATES: Grandfathered Rates				
Description of Charge	**Monthly Charge**	**One-Time Charge**	**Annual Charge**	**Notes**
MDM License Only (includes maintenance) per License	$3.25			<GRAND>
MDM License - Perpetual per License		$50.00		<GRAND>
MDM Perpetual License Maintenance (annual) per License			$10.00	<GRAND>
AirWatch Inbox - per License (includes maintenance); per License	$1.00			<GRAND1>
AirWatch Browser - per License (includes maintenance); per License	$1.00			<GRAND1>
AirWatch Additional 15GB Content Storage; per License	$6.00			<GRAND1>
AirWatch Additional 15GB Content Storage; per License			$72.00	<GRAND1>
AirWatch Additional 25GB Content Storage (per Environment)			$500.00	<GRAND1>
Notes:				
<GRAND>	Not available for new Customers as of February 2, 2015.			
<GRAND1>	Not available for new Customers as of September 13, 2016.			

Country Specific Provisions (CSP)

CSP-1. General Country Provisions

Section Effective Date: 07-Mar-2014

To the extent that Customer or its end users downloads or uses the MDM software on devices in a country other than the U.S., the following additional terms and conditions shall apply:

CSP-1.1. Prohibited Countries; Restricted Countries; Permitted Countries; Other Countries

CSP-1.1.1. Prohibited Countries

Section Effective Date: 17-May-2016

The server software for the Solution may not be deployed and device software for the Solution may not be downloaded onto devices by end users who permanently reside in any of the following countries (the "Prohibited Countries"): Cuba, Iran, North Korea, Pakistan, Russia, Sudan, Syria and Turkey, and any countries subject to a US trade embargo at any time.

AT&T may make changes to the Prohibited Countries from time to time.

CSP-1.1.2. Restricted Countries

Section Effective Date: 17-May-2016

The server software for the Solution may not be deployed in the following countries (the "Restricted Countries"): China, Kuwait, Qatar, Saudi Arabia, United Arab Emirates and any countries subject to a US trade embargo at any time.

AT&T may make changes to the list of Restricted Countries from time to time.

CSP-1.1.3. Permitted Countries

Section Effective Date: 17-May-2016

Subject to any future embargo restriction as described in the Prohibited Countries section of this Service Guide, server software for the Solution may be deployed and device software for the Solution may be downloaded by permanent residents of the following countries (the "Permitted Countries").

AT&T may make changes to the list of Permitted Countries from time to time.

Permitted Countries		
Argentina	Germany	Panama
Australia	Greece	Peru
Austria	Guatemala	Philippines
Bahamas	Hong Kong	Poland
Bahrain	Hungary	Portugal
Belgium	India	Puerto Rico
Bermuda	Indonesia	Romania
Brazil	Ireland	Singapore
British Virgin Islands	Israel	Slovakia
Bulgaria	Italy	Slovenia
Canada	Japan	South Africa
Cayman Islands	Latvia	South Korea

This document reflects the Service Guide in effect as of June 12, 2020

Permitted Countries		
Chile	Lithuania	Spain
Colombia	Luxembourg	Sweden
Costa Rica	Macau	Switzerland
Croatia	Malaysia	Taiwan
Cyprus	Malta	Thailand
Czech Republic	Mauritius	United Kingdom
Denmark	Mexico	Uruguay
Dominican Republic	Monaco	Venezuela
Ecuador	Morocco	Vietnam
El Salvador	Namibia	
Estonia	Netherlands	
Finland	New Zealand	
France	Norway	

CSP-1.1.4. Other Countries

Section Effective Date: 17-May-2016

Customers wishing to deploy server software for the Solution in countries other than those identified in the Permitted Countries section of this Service Guide or to have device software for the Solution downloaded by permanent residents of countries other than those identified in the Permitted Countries sections of this Service Guide should contact an AT&T Sales Representative.

CSP-1.2. Device and Software Selection

Section Effective Date: 03-May-2013

Customer is solely responsible for selecting the mobile devices and software/apps (including specifications of associated configuration) that it and its end users may use.

CSP-1.3. Data Protection

Section Effective Date: 28-Jun-2013

- Customer shall (a) notify, obtain and keep current consents from end users that are required by law for the use or processing of end users' Customer Personal Data, including consents for the transfer to and processing of such data in a country(ies) other than where such individuals are permanently located, (b) shall give end users the opportunity to opt-in or opt-out to such data transfers and the use of geo-location and cookie functionalities of the Solution; and (c) comply at all times with local language laws to ensure end users have provided informed consent as required by law.

- Customer will only make accessible or provide Customer Personal Data to AT&T and or its contractors or agents when it has the legal authority to do so.

- Upon not less than thirty (30) days' written notice to Customer, AT&T may review Customer's practices to implement compliance with this section.

CSP-1.4. Vendor Software License Agreement

Section Effective Date: 15-Nov-2016

Customer shall (i) accept for itself and flow down to end users the terms and conditions of the AirWatch EULA found at: http://www.air-watch.com/downloads/legal/AirWatch_ATT_Reseller_EULA_R-1.pdf and, if applicable, the VMware Identity Manager TOS found at http://www.vmware.com/download/eula/identity-manager-terms-of-service.html, as it/they may be amended from time to time and (ii) be responsible to ensure that the agreement between Customer and end users containing such flow-down terms (the "Flow Down Agreement") (a) is enforceable in all relevant jurisdiction(s); and (b) requires end users to seek remedies solely and exclusively from Customer with regard to that agreement. Customer shall have in place the required consents from end users regarding their use of the Solution and all of its functionalities before AT&T is required to deliver the Solution.

CSP-1.5. Encryption Technology

Section Effective Date: 28-Jun-2013

Customer represents that it knows and understands the laws governing the cross-border transfer and use of encryption technology, including compliance with trade embargoes, in each country where the Solution will be used. Customer agrees that the duty to comply with laws and regulations governing the importation and use of encryption technology in each country where it uses the Solution - including the requirement to obtain licenses and comply with on-going reporting obligations - rests solely and exclusively with Customer.

CSP-1.6. Filters, Interception, Monitoring

Section Effective Date: 03-May-2013

Customer shall notify and obtain consents from end users for Customer's filtering, interception, and/or monitoring of e-mail and Internet use, and Customer's related processing of Customer Personal Data.

CSP-1.7. Compliance with Laws

Section Effective Date: 10-Oct-2013

- Without limiting the generality of any other provision of the Master Agreement between Customer and AT&T regarding the Parties' respective obligations to comply with applicable law, as between Customer and AT&T it is Customer's and its affiliates' responsibility to obtain and remain in compliance with the authorizations, licenses, consents and permissions required by law for use of the Solution in each country where Customer uses the Solution, and Customer and Customer's affiliates will comply with such laws in respect of their use of the Solution. If and to the extent the applicable laws of any country or portion thereof require information regarding or relating to the Solution to be provided to end users

in a language other than English, Customer and Customer's affiliates shall be responsible for providing such information in the required language.

- Upon request by AT&T, Customer will provide and will ensure that its end users will provide, to AT&T all assistance reasonably required to enable AT&T and/or its suppliers to comply with the requests or requirements of any regulator, authority or other competent governmental body in a country where Customer uses the Solution, including in regard to, but not limited to, lawful interception of communications and data retention.

CSP-1.8. Discontinuance

Section Effective Date: 17-Apr-2014

AT&T may discontinue the Solution and/or require Customer and its end users to discontinue the use of the Solution in any country or jurisdiction without liability at any time on thirty (30) days' notice; provided that it may discontinue the Solution immediately if required by a regulatory authority to do so. If AT&T discontinues the Solution for a reason other than default or breach by Customer, AT&T will provide a pro rata refund.

CSP-1.9. Taxes

Section Effective Date: 10-Oct-2013

AT&T shall charge and collect taxes based on the delivery of the Third-Party Software, Maintenance, and AT&T Services to the address provided in the applicable Pricing Schedule or Order form for Customer. For the avoidance of doubt, Customer acknowledges and agrees that it will be responsible for all taxes (including associated interest and penalties) arising from or relating to any distribution or delivery of the Third-Party Software, Maintenance, or AT&T Services by Customer to (or otherwise any use by) any Affiliate or User of Customer.

CSP-1.10. Additional Indemnification

Section Effective Date: 21-Apr-2017

To the extent allowed by applicable law, in addition to Customer's indemnity obligations in the Enterprise Agreement, Customer shall defend, indemnify, and hold harmless AT&T, AT&T Affiliates, and their respective agents, directors, employees, and officers against any loss, damage, liability, action, demand, or claim arising out of or relating to Customer's failure to comply with any of its duties and/or obligations as set forth in Sections CSP-1.1 through CSP-1.9 above, including but not limited to those related to downloads or transmissions of device software in violation of export/import laws and U.S. and multi-lateral trade sanctions.

End of Service Guide