VMware AirWatch Inbox Admin Guide

Configuring and deploying AirWatch Inbox

Workspace ONE UEM v9.7

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Introduction to AirWatch Inbox

AirWatch Inbox is a fully containerized email management solution for iOS, Windows Desktop, Windows Phone, and Android devices. AirWatch Inbox enables you to remotely configure and manage enterprise email accounts while maintaining personal and enterprise data separately for end users. The application supports Exchange ActiveSync and offers encryption for email messages and attachments. Some of the application data loss prevention features are:

- Passcode setup to access the application.
- Configuration of restrictions such as disable copy/paste.
- Removal of email messages and attachments upon an enterprise wipe.

Security and Enhancements

AirWatch Inbox provides security measures and data loss prevention strategies across mobile devices using UEM console.

Using an AES 256-bit encryption algorithm, the AirWatch Inbox secures email content by encrypting message data such as email address and message text by storing it in a local database. The email database and attachments are stored in a protected app space that is inaccessible to third-party applications.

Note: AirWatch Inbox does not support AES encryption using SMIME.

Security Features

Following security features can be configured within the AirWatch email profile:

- **Account Information / Email Message Encryption**

  All device account information, including email password and message information such as the message body, are encrypted when written to the application database. The application database is not accessible on both rooted and non-rooted devices. Additionally, in rooted devices, the account information cannot be read as it is fully encrypted.

- **Email Attachment Encryption**

  With AirWatch Inbox, all saved attachments are downloaded to the encrypted internal application space to ensure protection. Inbox, along with SEG integration, encrypts the attachments once again which can later be opened from the VMware Content Locker. This ensures full end-to-end encryption.

- **SEG/PowerShell Support**

  When configured, the AirWatch Inbox automatically sends a unique EAS identifier to the AirWatch database. This EAS identifier is used to identify the device as a managed device through SEG or PowerShell commands. As a managed device, the administrator can create different email compliance policies using the SEG or PowerShell commands.

Requirements

Console Requirements

Platform	Console Version
iOS	AirWatch Console v7.0+
Android	AirWatch Console v6.5+
Windows Desktop	AirWatch Console v7.2+
Windows Phone	AirWatch Console v8.1+

Supported Devices and Software

Platform	Supported Devices and Software
iOS	iOS 7+** , iPhone, iPad (4, Air, Mini), AirWatch Agent v4.9.1110+
Android	Android 4.0+, AirWatch Agent v5.0+ or AirWatch Container v1.5+
Windows Desktop	Windows 8.1/Pro/Enterprise and higher or Windows Desktop 8.1+, AirWatch Agent v1.1.0.23+
Windows Phone	Windows Phone 8.1+

> ****Note:** iOS 7 and iOS 8 supports Inbox only till v2.5.9. To take advantage of new features and versions, devices need to update to iOS 9 or later.

Supported File Types

Platform	Supported File Types
iOS	.doc, .pdf, .ppt, .txt, .jpg, .gif, .png, .mp3, .html, .ics, .xml, and .xls
Android	.txt, .xls, .doc, .png, .jpg, .ppt, .mp4, .mp3, and .pdf
Windows Desktop	.txt, .png, .jpg, .pdf, .xls, .ppt, .doc, .gif, .html, .mp3, .mp4, and .xml
Windows Phone	.txt, .png, .jpg, .pdf, .xls, .ppt, .doc, .gif, .html, .mp3, .mp4, and .xml

Other Requirements

- **iOS**
  - Exchange ActiveSync 2003/2007/2010/2013/2016 or Office 365, Lotus Notes 9.0 email server
- **Android**
  - Exchange ActiveSync 2007/2010/2013/2016 or Office 365, IBM Lotus Notes 9.0 from Android Inbox v2.1 release onwards, Google Apps for Work from Android Inbox v2.3 release onwards

Two factor authentication in Android requires Exchange server credentials and certificate.

- **Windows Desktop**
  - Exchange ActiveSync 2007/2010/2013/2016 and Office 365
- **Windows Phone**
  - Exchange ActiveSync 2007/2010/2013/2016 and Office 365

Chapter 2:
Initial Configurations

Configure Profile Payloads

Use Mobile Device Management (MDM) functionality to enhance app performance by configuring a profile payloads in a two-step process. First, configure general settings. Then, specify the type of restriction or setting to apply to the device by selecting a payload from the list.

The available payloads and their configurable settings differ between platforms. This section provides a description of applicable payloads and brief instructions to help you get started.

1. Navigate to **Devices > Profiles > List View > Add** and select **Add Profile**.
2. Select the appropriate platform for the profile that you want to deploy.
3. Configure **General** settings to determine how the profile deploys, who receives it, and other overall settings.
4. Select and configure a **Payload**.

Payload	Description	iOS	Android	Windows Desktop	Windows Phone
Exchange ActiveSync	This payload allows users to access corporate push based email infrastructures and allows to set the sync frequency for calendar and email systems.	✓	✓	✓	✓
Credentials	Configure this payload with digital certificates to protect your corporate email, Wi-Fi, VPN, and other corporate assets.	✓	✓	✓	✓
SCEP	Along with Credentials payload, you can also configure SCEP to handle digital certificates pushed to large-scale devices.	✓			

For step-by-step instructions on configuring a specific **Payload** for a particular platform, please refer to the applicable **Platform Guide**.

5. Select **Save & Publish**.

Chapter 3:
App Suite SDK Configurations

Default vs Custom SDK Profiles

When you configure your application, you select a custom or a default application profile. This action applies an SDK profile to the application, giving deployed Workspace ONE UEM applications additional features.

To ensure your application configuration runs smoothly , it is helpful to:

- Know the difference between a Custom and Default SDK profile.
- Determine if a Custom or a Default SDK profile is more appropriate for your application.
- Ensure you have configured the SDK profile type that you want to apply.

Use the following chart to determine if you want to apply a **Default** or **Custom** SDK profile to your application, and to direct you to the configuration instructions for the profile you use.

You can define SDK profiles using two different profile types: **Default** or a **Custom** SDK application profile.

	Default	Custom
Implementation	Share SDK profile settings across *all* applications set up at a particular organization group (OG) or below.	Apply SDK profile settings to a *specific* application, and override the Default Settings SDK profiles.
Advantage	Provides a single point of configuration for all of your apps in a particular OG and its child groups.	Offers granular control for specific applications and overrides the Default Settings SDK profiles.
Configure	**Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**	**Groups & Settings > All Settings > Apps > Settings and Policies > Profiles**
Read More	Continue reading this section to learn which default SDK profiles apply to deployed apps.	Learn more about custom SDK profile settings in the **VMware Workspace ONE UEM Mobile Application Management Guide**.

Custom SDK Profile Settings

Workspace ONE UEM recommends using default settings for ease of maintenance and a consistent end user experience between Workspace ONE UEM and wrapped apps. However, Custom SDK setting are available to address cases where a single app needs to exhibit unique behaviors that differ from the rest of the app suite.

Enable **Custom Applications Settings** to override default SDK settings, and configure unique behaviors that only apply to a single app.

Setting	Description
Authentication Method	Defaults to Single Sign-On. Ensure you require MDM enrollment so that Single Sign-On can function properly.
iOS Profile	Select a custom-created SDK profile from the drop-down list the settings profile for iOS devices.
Android Profile	Select a custom-created SDK profile from the drop-down list the settings profile for Android devices.
Use Legacy Settings and Policies	Only enable legacy settings if directed to do so by a Workspace ONE UEM representative. Legacy settings do not leverage Shared SDK profile settings and should only be implemented in certain edge cases.
Default Authentication Method	Select the authentication method for the applications.
Enable "Keep me signed in"	Enable to allow end users to remain signed in between uses.
Maximum Number of Failed Attempt	Set the number of passcode entry attempts allowed before all data in the VMware Content Locker is wiped from a device and the device is enterprise wiped.
Authentication Grace Period (min)	Enter the time (in minutes) after closing the VMware Content Locker before reopening the VMware Content Locker will require users to enter credentials again.
Prevent Compromised Devices	Enable to prevent compromised devices from accessing VMware Content Locker.
Enable Offline Login Compliance	Enable to allow offline login compliance.
Maximum Number of Offline Logins	Enter the number of offline logins allowed before you have to go online.

Configure Default SDK Security Settings

Default SDK settings apply across AirWatch and wrapped applications, providing a unified user experience on devices. Because the configured SDK settings apply to all AirWatch and wrapped applications by default, you can configure the default SDK profile with the entire AirWatch and wrapped application suite in mind.

Before You Begin

Not all platforms or AirWatch applications support all available default SDK profile settings. A configured setting only works on the device when it is supported by the platform and app. This also means that an enabled setting might not work uniformly across a multi-platform deployment, or between applications. The SDK Settings matrix covers the available SDK profile settings and the apps and platforms they apply to.

Key Assumptions

The recommendations provided apply to an app suite that includes:

- VMware Browser
- AirWatch Inbox
- VMware Content Locker
- Enrolled devices
- AirWatch or wrapped apps
- SDK settings available as of September 2018.

1. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies**.
2. Configure **Security Policies**.

Action	Description	Rec
Authentication Type		
Passcode	Prompt end users to authenticate with a user-generate passcode when the app first launches, and after an app session timeout. Enabling or disabling SSO determines the number of app sessions that get established.	–
Username and Password	Prompt end user to authenticate by re-entering their enrollment credentials when the app first launches, and after an app session timeout. Enabling or disabling SSO determines the number of app sessions that get established.	–
Disabled	Allow end user to open apps without entering credentials.	√

SSO		
Enabled	Establish a single app session across all AirWatch and AirWatch wrapped apps.	√
Disabled	Establish app sessions on a per app basis.	–
Offline Access		
Enabled	Allow end users to open and use AirWatch and wrapped apps when disconnected from Wi-Fi. Offline AirWatch apps cannot perform downloads, and end users must return online for a successful download. Configure the Maximum Period Allowed Offline to set limits on offline access.	√
Disabled	Remove access to AirWatch and wrapped apps on offline devices.	–
Compromised Protection		
Enabled	Override MDM protection. App level Compromised Protection blocks compromised devices from enrolling, and enterprise wipes enrolled devices that report a compromised status.	√
Disabled	Rely solely on the MDM compliance engine for compromised device protection.	–
Data Loss Prevention		
Enabled	Access and configure settings intended to reduce data leaks.	**√**
Enable Copy And Paste		
Allows an application to copy and paste on devices when set to **Yes**.		
Enable Printing		
Allows an application to print from devices when set to **Yes**.		
Enable Camera		
Allows applications to access the device camera when set to **Yes**.		

Enable Composing Email	
Allows an application to use the native email client to send emails when set to **Yes**.	
Enable Data Backup	
Allows wrapped applications to sync data with a storage service like iCloud when set to **Yes**.	
Enable Location Services	
Allows wrapped applications to receive the latitude and longitude of the device when set to **Yes**.	
Enable Bluetooth	
Allows applications to access Bluetooth functionality on devices when set to **Yes**.	

Enable Screenshot	
Allows applications to access screenshot functionality on devices when set to **Yes**.	
Enable Watermark	
Displays text in a watermark in documents in the VMware Content Locker when set to Yes. Enter the text to display in the Overlay Text field or use lookup values. You cannot change the design of a watermark from the AirWatch Console	

Limit Documents to Open Only in Approved Apps		
Enter options to control the applications used to open resources on devices. (iOS only) You can use VMware AirWatch Configuration values to restrict users from importing files from third-party applications into Content Locker. For more information, see **Configure Import Restriction in Content Locker** section.		
Allowed Applications List		
Enter the applications that you allow to open documents.		
Disabled	Allow end user access to all device functions.	–

3. **Save**.

4. Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.

5. Configure **Settings**.

Branding		
Enabled	Apply specific organizational logo and colors, where applicable settings apply, to the app suite.	–
Disabled	Maintain the AirWatch brand throughout the app suite.	√
Logging		
Enabled	Access and configure settings related to collecting logs.	√
Logging Level		
Choose from a spectrum of recording frequency options: • **Error** – Records only errors. An error displays failures in processes such as a failure to look up UIDs or an unsupported URL. • **Warning** – Records errors and warnings. A warning displays a possible issue with processes such as bad response codes and invalid token authentications. • **Information** – Records a significant amount of data for informational purposes. An information logging level displays general processes as well as warning and error messages. • **Debug** – Records all data to help with troubleshooting. This option is not available for all functions.		
Send logs over Wi-Fi only		
Select to prevent the transfer of data while roaming and to limit data charges.		
Disabled	Do not collect any logs.	–
Analytics		
Enabled	Collect and view useful statistics about apps in the SDK suite.	√
Disabled	Do not collect useful statistics.	–
Custom Settings		
Enabled	Apply custom XML code to the app suite.	–
Disabled	Do not apply custom XML code to the app suite.	√

6. **Save**.

Expected Behavior for SDK Authentication

Authentication Type	SSO	Sessions	Credentials	Expected Behavior
Disabled	Enabled	Single	Enrollment Credentials	Open apps without prompting end users to enter credentials.
Passcode	Enabled	Single	Passcode	Prompts at first launch of first app, establishing a single app session. The next authentication prompt occurs after the session times out.
Username and Password	Enabled	Single	Enrollment Credentials	Prompts at first launch of first app, establishing a single app session. The next authentication prompt occurs after the session times out.
Passcode	Disabled	Per App	Passcode	Prompts on a per app basis, establishing individual app sessions. Note that each app may have a unique passcode. The next authentication prompt occurs when launching a new app, or an individual app session times out.
Username and Password	Disabled	Per App	Enrollment Credentials	Prompts on a per app basis, establishing individual app sessions. The next authentication prompt occurs when launching a new app, or an individual app session times out.

Apply SDK Settings to the Android Agent

Configure the AirWatch Agent to use the default SDK profile so that it can act as a 'broker application' for features such as single-sign on. If you do not set the AirWatch Agent to use the default SDK profile, then the system does not apply your **Settings and Policies** configurations to the agent.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Android > Agent Settings**.
2. Set the **SDK Profile V2** option in the **SDK PROFILE** section to the default profile by selecting **Android Default Settings @ <Organization Group>**.
3. **Save** your settings.

Apply SDK Settings to the iOS Agent

Configure the AirWatch Agent to use the default SDK profile so that it can act as a 'broker application' for features such as single-sign on. If you do not set the AirWatch Agent to use the default SDK profile, then the system does not apply your **Settings and Policies** configurations to the agent.

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Apple > Apple iOS > Agent Settings**.
2. Set the **SDK Profile V2** option in the **SDK PROFILE** section to the default profile by selecting **iOS Default Settings @ <Organization Group>**.
3. **Save** your settings.

Chapter 4:
Application Configuration

Configure Inbox Settings

Configure default settings to define behaviors that apply to AirWatch Inbox. Configure app specific system settings to define unique application behavior.

To configure AirWatch Inbox settings on the UEM console:

1. Navigate to **Groups and Settings > All Settings > Apps > Inbox**.
2. Select whether to **Inherit** or **Override** the displayed settings:
3. - **Inherit** – Use the settings of the current organization group's parent OG.
   - **Override** – Edit and modify the current OG's settings directly.
4. Configure the relevant settings on the **Inbox Settings** tab:

Setting	Description
Application Type	Leave the application type as **System** or select **Internal** to set system preferences. • **System** – Download this app type from an app store. • **Internal**– Upload this app type to the UEM console.
Application Name	Provide an app name for **Internal** applications. Navigate to **Apps & Books > Internal List View**and scan the list for an app name that matches the app name you entered. This list view only displays internal applications were uploaded with a matching APNs certificate.
Bundle ID	Enter the bundle ID of the application.

Setting	Description
Settings and Policies	
Application Profile	Select an application profile to apply SDK functionality to your app. • **Default** – Allow applications to use the default security policies and settings defined under **Apps and Books > Settings > Settings and Policies**. • **Custom** – Override default settings and apply custom profiles. Custom profiles use the security policies and settings defined under **Apps and Books > Settings > Settings and Policies > Profiles**.
iOS SDK Profile	Select the corresponding profile from the drop-down menu. This profile applies the default security policies and settings defined under **Settings & Policies** OR the custom security policies and settings defined under **Profiles**. This is an optional, advanced management feature. Instructions for configuring default SDK settings are available in the **VMware Workspace ONE UEM Mobile Application Management Guide**.

Note: Select the available behavior of child organization groups that exist below the currently selected organization group. Inherit only means child OGs will only be allowed to inherit these settings. Override only means they will override the settings, and Inherit or Override means you can choose to inherit or override settings in child OGs that exist below the currently selected OG.

5. Select **Save**.

Chapter 5:
Application Deployment

Overview of VMware Browser Deployment

Control how to deploy Browser to your end users and other security configurations from the UEM console. Once deployed, end users can download and use these apps.

For more information on the process for deploying public applications in full detail, refer the **VMware Workspace ONE UEM Mobile Application Management (MAM) Guide**.

Deploy Workspace ONE UEM Applications

Configure Workspace ONE UEM Applications to deploy as public apps.

Utilize this simplified deployment workflow to seamlessly push Workspace ONE UEM applications to end users.

1. Navigate to **Apps & Books > Applications > Native > Public**.
2. Select **Add Application**.
3. Configure the fields on the screen that appears:

Setting	Description
Managed By	View the organization group the application uploads in.
Platform	Choose the appropriate platform.
Name	Enter a descriptive name in the field to help search for the application in an app store.
Search App Store	Select to search for the application in the app store. In order to search the Google Play Store in an on-premises deployment, you must integrate a Google Account with the Workspace ONE UEM MDM environment.

4. Review the information that automatically populates in the **Info** tab.

5. Add smart groups from the **Assignment** tab.

6. Use the **Deployment** tab to determine how your end users receive the app. End users find and download recommended apps in the app store. To make finding and deploying it easier, you can recommend it through Workspace ONE UEM or automatically push it to your devices.

7. Assign **Terms of Use**, if desired.

8. **Save and Publish**.

Migrate from Other Clients

If you already have an AirWatch email profile deployed in your end user device, you can still migrate to AirWatch Inbox by publishing AirWatch Inbox profile.

Prior to publish and migrate to AirWatch Inbox profile, perform any one of the following task based on the type of email client in the device:

- To migrate from the NitroDesk TouchDown to the AirWatch Inbox, first publish the AirWatch Inbox profile. Users then receive notifications and prompts to use AirWatch Inbox.
- To migrate from the Native Mail Client to the AirWatch Inbox, you first need to deactivate the Native Mail Client profile and then publish the AirWatch Inbox profile.

Chapter 6: Troubleshoot AirWatch Inbox

Your end-users might experience some of the platform-specific common connection and usability issues. This section explains how to troubleshoot such issues when encountered.

For iOS

Not Configured Screen Display

Possible Cause	Solution
AirWatch Inbox did not authenticate	• Ask if the user is prompted with AirWatch Authentication Request. • Close or kill AirWatch Inbox and open it again. • Un-enroll the device and uninstall AirWatch Inbox application. Then, re-enroll the device and re-install AirWatch Inbox application.
Profile is not installed	• Verify that the profile configured is for AirWatch Inbox and not the Native Email Client. • Select **Try Again** option on device prompt. • Verify the profile configured is published and is set to **Pending Install**. • Verify that the user is enrolled. • Verify by re-pushing the profile to the device. • Verify the network connection problem to AirWatch Server (Device Services). • Verify by uploading enterprise cert. • Verify if the bundle ID of AirWatch Inbox matches the values set in the System Code table.
Login Error Message HTTP 401/403	
Possible Cause	**Solution**
Authentication Failed to Exchange	• Try a different username and password. • Verify an email exchange policy is not preventing access. • Verify SEG is not preventing access.
Login Error Message HTTP 502	
Possible Cause	**Solution**

Possible Cause	Solution
Unable to connect to the Exchange Server	• Verify the device network is connected to the email exchange server . • Verify the AirWatch enrollment user account has an email username.

Mailbox Sync Failure

Possible Cause	Solution
Unable to connect to the Exchange Server	• Verify the device network is connected to the email exchange server. • Collect logs and contact Workspace ONE Support.
Mail not Synchronizing properly	• Collect logs and contact Workspace ONE Support
No Messages Appear in AirWatch Inbox	
Possible Cause	**Solution**
EAS Mailbox Device Limit Reached	• Connect the device to a web debugging tool such as Fiddler. Evaluate Response Header. Messages such as the following indicate a problem with Exchange restrictions: ○ X-MS-ASError: Message = Collect logs and contact Workspace ONE Support. • Verify if the response obtained from Exchange/SEG is within 10 seconds of the request. A '-' indicates the client is waiting for a response.

For Android

Issue	Solution
AirWatch Email Client crashes upon initial config	Send a debug log to AirWatch from the **AirWatch Email Client Default** screen.
AirWatch Inbox crashes after config and mail sync	Send a debug log to AirWatch from the Inbox **Settings** screen.

Issue	Solution
HTTP 449 response when connecting to IBM Notes Traveler	Add the following flag to the **notes.ini** file on the Traveler server. `NTS_AS_PROVISION_EXEMPT_USER_AGENT_REGEX=(AirWatch*) | (Apple*; AWInbox*)` Adding this flag disables Traveler from enforcing any policies to the AirWatch Inbox Apps and AirWatch should be used to apply any policies. **Note:** Devices that are leveraging policies provisioned directly by Traveler (i.e not configured through AirWatch) will not be affected.

Debug logs

The **Debug** option available under **Settings > Debug** allows you to enable error logging and send error logs to AirWatch.

Enable Logging

Enable device level logging so that you can easily report issues. To enable logging,

1. Navigate to **Settings > Debug**.
2. Enable the following features:
   - **Enable extra debug logging** – Select the check box to enable sending email client UI logs through email.
   - **Enable Exchange parsser logging (extremely verbose)** – Select the check box to enable sending Exchange service logs through email.

Send Debug Logs to AirWatch

After enabling device level logging, you can send crash logs directly to AirWatch.

1. Tap **Menu** on the appropriate screen:
   - **AirWatch Email Client Default Screen** – Select **Menu** from this screen if your app crashes upon initial configuration.
   - **Settings Screen** – Select **Menu** from this screen if Inbox crashes after config and mail sync.

1. Select a debugging option from the appropriate menu:
   - **AWEC Default Screen Menu** – Select **Send Debug Logs**.
   - **Settings Screen Menu** – Select **Email Debug Logs**.

1. Select an email account from the options that display.
2. Complete the fields in the **Compose Message** window.

Settings	Description
To	Enter the default mail address. For example, **airwatch.android@gmail.com**. You can edit the 'To' address if required and then, tap **Send**.
Attachment	Attach a log file as an attachment in the email body.

Chapter 7:
SDK Profiles, Policies and Settings Compatibility

Workspace ONE UEM offers the ability to apply Workspace ONE UEM SDK functionality to Workspace ONE UEM applications using a default settings profile. View compatibility information for available Workspace ONE UEM SDK features for in the tables below.

> **Note:** The data in these tables describes the behaviors and support of the specific application and not for applications accessed using another application. For example, the data for the Workspace ONE UEM Container application references only the Workspace ONE UEM Container's behavior. It does not reference the behaviors for apps accessed using the Workspace ONE UEM Container.

Settings and Policies Supported Options for Workspace ONE UEM Applications

The following matrix shows support for Workspace ONE UEM applications built with the Workspace ONE UEM SDK. Inbox refers to Workspace ONE UEM Inbox, and not VMware Boxer, which is not built with the Workspace ONE UEM SDK. You can configure similar settings for Boxer when deploying the application.

UI Label	Inbox	
iOS	Android	
Force Token For App Authentication: Enable	x	x
Passcode: Authentication Timeout	x	✓
Passcode: Maximum Number Of Failed Attempts	x	✓
Passcode: Passcode Mode Numeric	x	✓
Passcode: Passcode Mode Alphanumeric	x	✓
Passcode: Allow Simple Value	x	✓
Passcode: Minimum Passcode Length	x	✓
Passcode: Minimum Number Complex Characters	x	✓
Passcode: Maximum Passcode Age	x	✓
Passcode: Passcode History	x	✓
Biometric Mode: Fingerprint	✓	x

UI Label	Inbox	
iOS	Android	
Username and Password: Authentication Timeout	X	X
Username and Password: Maximum Number of Failed Attempts	X	X
Single Sign On: Enable	✓	✓
Integrated Authentication: Enable Kerberos	X	X
Integrated Authentication: Use Enrollment Credentials	X	X
Integrated Authentication: Use Certificate	X	X
Offline Access: Enable	✓	X
Compromised Protection: Enable	X	X
App Tunnel: Mode	X	X
App Tunnel: URLs (Domains)	X	X
Content Filtering: Enable	X	X
Geofencing: Area	X	X
DLP: Bluetooth	X	X
DLP: Camera	X	X
DLP: Composing Email	X	X
DLP: Copy and Paste Out	X	X
DLP: Copy and Paste Into	X	X
DLP: Data Backup	X	X
DLP: Location Services	X	X
DLP: Printing	X	X
DLP: Screenshot	X	X
DLP: Third Party Keyboards	X	X
DLP: Watermark	X	X
DLP: Limit Documents to Open Only in Approved Apps	X	X
NAC: Enable	X	X
NAC: Cellular Connection	X	X

UI Label	Inbox	
iOS	Android	
NAC: Wi-Fi Connection	X	X
Branding: Enable	X	X
Branding: Toolbar Color	X	X
Branding: Toolbar Text Color	X	X
Branding: Primary Color	X	X
Branding: Primary Text Color	X	X
Branding: Secondary Color	X	X
Branding: Secondary Text Color	X	X
Branding: Organization Name	X	X
Branding: Background Image iPhone and iPhone Retina	X	X
Branding: Background Image iPhone 5 (Retina)	X	X
Branding: Background Image iPad and iPad (Retina)	X	X
Branding: Background Small, Medium, Large, and XLarge	X	X
Logging: Enable	X	X
Logging: Logging Level	X	X
Logging: Send Logs Over Wi-Fi	X	X
Custom Settings: Enable	X	X
SDK App Compliance: Enable	X	X
Compromised Protection: Enable	X	X
Offline Access: Enable	✓	X

*✓ This option is supported but is not configured using Settings and Policies.

**✓ This option requires Android Ice Cream Sandwich and KitKat.

Chapter 8:
AirWatch Inbox Comparison Matrix

The following features matrix compares the differences between the Android, iOS, Windows Desktop, and Windows Phone versions supported by AirWatch Inbox.

Features and Functionality	iOS	Android	Windows Desktop	Windows Phone
Remote Management				
Configure email accounts remotely	✓	✓	✓	✓
Wipe all data and settings	✓	✓	✓	✓
Clear passcode	✓	✓	✓	✓
Online compliance checks (MEM)	✓	✓	✓	✓
Trigger passcode lock	✓	✓	✓	✓
Deployment Methods				
Application Container Only	✓	✓	x	x
Device MDM Add-on	✓	✓	✓	✓
Core Feature Support				
Manage Email	✓	✓	✓	✓
Manage Calendar	✓	✓	✓	✓
Manage Contacts	✓	✓	✓	✓
Authentication and Passcode				
Require Active Directory username and password	✓	✓	✓	✓
Enforce minimum length	✓	✓	✓	✓
Require complex passcode	✓	✓	✓	✓
Require special characters	✓	✓	✓	✓
Set timeout for passcode lock	✓	✓	✓	✓
Set maximum passcode age	✓	✓	✓	✓
Enforce passcode history	✓	✓	✓	✓
Set maximum failed attempts	✓	✓	✓	✓
Auto-lock on device lock	✓	✓	x	x
TouchID/Fingerprint Integration	✓	x	x	x
Share passcode for multiple apps	✓	✓	x	x

Features and Functionality	iOS	Android	Windows Desktop	Windows Phone
Data Loss Prevention				
AES 256-bit SSL encryption (without SMIME) in transit	✓	✓	✓	✓
AES 256-bit encryption (without SMIME) at rest	✓	✓	✓	✓
FIPS 140-2 Compliant	✓	x	x	x
Enable/Disable adding multiple accounts	x	x	x	x
Offline compliance checks (Compromised Detection)	✓	✓	✓	✓
Enable/Disable copy/paste outside the container	✓	✓	✓	✓
Enable/Disable screenshots	x	✓	✓	✓
Enable/Disable downloading attachments	✓	✓	✓	✓
Restrict which apps can open attachments	✓	✓	x	x
Restrict attachments to VMware Content Locker only	✓	✓	✓	✓
Force attachment encryption (Requires VMware Content Locker)	✓	✓	x	x
Prevent sending to blacklisted domains	x	✓	✓	✓
Restrict sending to whitelisted domains	x	✓	✓	✓
Support for attachment stripping through the Secure Email Gateway	✓	✓	x	x
Open links in VMware Browser	✓	✓	✓	✓
Enable/Disable exporting contacts to native	✓	✓	x	x
Enforce Exchange ActiveSync Provisioning Policies	x	x	x	x
IT Policies				
Set past days of mail to sync	✓	✓	✓	✓
Set past days of calendar to sync	✓	✓	✓	✓
Ignore SSL errors	✓	✓	x	x
Enable/Disable calendar access	✓	✓	✓	✓
Enable/Disable contacts access	✓	✓	✓	✓
Authenticate account using a certificate	✓	✓	✓	✓
Authenticate account using credentials	✓	✓	✓	✓
Authenticate account using smart card credentials	x	x	x	x
Enable S/MIME using smart card certificates	x	x	x	x
Support two factor account authentication	x	✓	x	x

Features and Functionality	iOS	Android	Windows Desktop	Windows Phone
Enable/Disable HTML Email	✓	✓	✓	✓
Configure default email signature	✓	✓	✓	✓
Enable/Disable signature editing	✓	✓	✓	✓
Configure email subject classification rules	x	x	x	x
Application Settings				
Configure contacts sort order	x	✓	✓	✓
Modify account sync intervals	✓	✓	✓	✓
Configure new message notification preferences	✓	✓	✓	✓
Email Functionality				
Filter by flagged/starred	✓	✓	✓	✓
Filter by unread emails	✓	✓	✓	✓
Mark as read/unread/flagged	✓	✓	✓	✓
View email by conversations (threads)	x	x	x	x
Bulk actions for emails	✓	✓	✓	✓
Search by To, Subject	✓	✓	✓	✓
View email sub-folders	✓	✓	✓	✓
Automatically sync email sub-folders	x	✓	x	x
Add/Edit/Delete custom email folders	x	✓	✓	✓
Add contacts in bulk to new messages	✓	✓	✓	✓
Add contacts from recent/suggested contacts list	✓	✓	✓	✓
Search contacts in global address list	✓	✓	✓	✓
Save email to drafts	✓	✓	✓	✓
Configure Out of Office automatic replies	x	✓	✓	✓
Calendar Functionality				
Search by Title, Organizer	x	✓	✓	✓
Accept/Decline/Tentative calendar invites	✓	✓	✓	✓
Create events and send event invitations	✓	✓	✓	✓
Decline with response to organizer	✓	✓	✓	✓
Send message to event attendees	x	✓	x	x

Features and Functionality	iOS	Android	Windows Desktop	Windows Phone
Forward calendar events	✓	✓	✓	✓
One click conference call dialing	✓	✓	x	x
Lookup Free/Busy recipient information	x	x	✓	✓
View events by day	✓	✓	✓	✓
View events by month	x	✓	✓	✓
View a list of events	x	✓	✓	✓
Pending Event Invitations View	x	✓	✓	✓
Add event attendees as required or optional	x	x	x	x
View meeting room location availability	x	x	x	x
Mark meeting as private	✓	✓	✓	✓
Configure availability for meeting	✓	✓	✓	✓
Edit recurring event schedule	✓	✓	✓	✓
Respond to event invitation with comments	✓	✓	✓	✓
Contacts Functionality				
Automatically sync all users' contacts	✓	✓	✓	✓
Search contacts from global address list	✓	✓	✓	✓
Call and send messages to contacts	✓	✓	✓	✓
Create/edit/delete contacts	✓	✓	✓	✓
Export contact names and phone numbers to native app	✓	✓	x	x
Exchange ActiveSync Support				
Exchange 2016	✓	✓	✓	✓
Exchange 2013	✓	✓	✓	✓
Exchange 2010	✓	✓	✓	✓
Office 365	✓	✓	✓	✓
Google Apps	x	✓	x	x
IBM Lotus Notes 9.0	✓	✓	x	x
Information Rights Management				
Read rights managed email messages	✓	✓	x	x
Add rights management to composed email messages	✓	✓	x	x
Restrict copy-paste (extract allowed)	✓	✓	x	x

Features and Functionality	iOS	Android	Windows Desktop	Windows Phone
Restrict printing	✓	✓	x	x
Restrict forward	✓	✓	x	x
Restrict reply	✓	✓	x	x
Restrict reply all	✓	✓	x	x
Prevent removing rights management on reply/forward	x	x	x	x
Restrict modifying recipients on reply/forward	✓	✓	x	x
Prevent programmatic access	N/A	N/A	N/A	N/A
Enforce email message content expiration	x	x	x	x
Restrict editing message contents (on reply/forward)	x	x	x	x
Preview rights management protected attachments	x	x	x	x
Notifications				
Allow silencing work email notifications on-demand	x	✓	x	x
Push real-time email notifications	x	✓	✓	✓
Display notifications for calendar events	✓	✓	✓	✓
Display banner notifications for events on lock screen	✓	✓	✓	✓
Bandwidth/Roaming				
Set sync preferences while roaming	x	✓	x	x
Set email truncation size	x	x	x	x
Set maximum attachment size	✓	✓	✓	✓
Accounts				
Modify account sync intervals	x	✓	✓	✓
Configure new message notification preferences	x	✓	✓	✓
S/MIME Functionality				
Send S/MIME signed messages	✓	✓	✓	✓
Send S/MIME encrypted messages	✓	✓	✓	✓
Automatically fetch encryption certificates from GAL	✓	✓	✓	✓
Configure S/MIME options per email message	✓	✓	✓	✓
Decrypt S/MIME encrypted messages	✓	✓	✓	✓
View validity of S/MIME signed messages	✓	✓	✓	✓
Attachment Functionality				
Built-in attachment viewing	✓	x	✓	✓

Features and Functionality	iOS	Android	Windows Desktop	Windows Phone
Add links to files from Content Solutions	✓	✓	✓	✓
Add files from Document Providers	x	x	✓	✓
Troubleshooting and Diagnostics				
View device's MDM and email connectivity status	✓	✓	✓	✓
Server Protocol Support				
Exchange ActiveSync	✓	✓	✓	✓
IMAP	x	x	x	x