VMware Boxer Admin Guide

Configuring and deploying Boxer

Workspace ONE UEM v9.6

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 VMware Boxer 3

Benefits of Using VMware Boxer 3
Audience of this Guide 3
Requirements to Deploy VMware Boxer 3
Components to Use with VMware Boxer 5
Supported Capabilities for VMware Boxer 5
Interoperability Features of Boxer 7

Chapter 2: Application Configuration 8

Deploy VMware Boxer with the AirWatch Console 8
Add VMware Boxer to Public Applications 8
Assign VMware Boxer with Email Settings 11
Configure Fingerprint Authentication 30

Chapter 3: Device Management 32

Enterprise Wipe 32
Device Wipe Considerations 32
Block Access to IBM Traveler Server 33
Work around for Third-Party Address Book (iOS Only) 33
Workaround for Sync and Policy Errors on Boxer using IBM Notes 34

Chapter 4: VMware Boxer Comparison Matrix 36

VMware Boxer Comparison Matrix for Microsoft Exchange 36
VMware Boxer Comparison Matrix for IBM Notes Traveler 41

Chapter 1:
Introduction to VMware Boxer

VMware Boxer is an email application that offers a consumer-centric focus on mobile productivity with enterprise-grade security in the form of AES 256-bit encryption. VMware Boxer app separates business data from personal data, providing access to enterprise email, calendar, and contacts across corporate-owned devices and bring your own devices (BYOD).

From release v4.9, Boxer supports IBM Notes Traveler v9.0.1 integration. IBM Notes Traveler integration introduces Email, Calendar, and Contacts capabilities in Boxer using ActiveSync protocol. Install the latest Boxer version for the optimum functioning of email, calendar, and other features. IBM Notes Traveler is not supported when you upgrade from Boxer v4.8 or older versions.

Benefits of Using VMware Boxer

VMware Boxer allows users to personalize the app with features like custom swipe gestures, contact avatars, custom smart folders, and account color preferences. The all-in-one app provides an intuitive user experience following native design paradigms on iOS and Android devices.

Audience of this Guide

This guide is intended for administrators looking to configure Boxer as part of their AirWatch deployment. Setting up Boxer involves configuring the various email settings and options you want to require or to make available to your end users.

Requirements to Deploy VMware Boxer

To deploy Boxer as part of your AirWatch deployment, Meet the following prerequisites related to the UEM console, operating system, and email servers.

Console Requirements

- For iOS, AirWatch Console v8.3.1 and higher.
- For Android, AirWatch Console v8.3 FP5 and higher.

Supported Agent Version

Android	iOS
AirWatch Agent v6.0.1 and higher AirWatch Container v3.0.1 and higher	AirWatch Agent v5.2 and higher

Supported Devices

Android	iOS
Android Version 5.0 and higher	iOS 9 and higher

Supported File Types

File Types			
iOS			
DOC	JPEG	JPG	MOV
PDF	VCF	DOCX	XML
PPT	EXCEL	MP3	SLX
TXT	HTML	MP4	EML
Android			
DOC	TXT	CSV	BMP
DOCX	ASC	PPT	DIB
DOT	JPG	PPS	WBMP
XLS	JPEG	PPSX	TIF
XLSX	GIF	POTX	EMF
XLTX	TIFF	PDF	PCX
HTP	MP3		

Supported Email Infrastructure

- Supports the following email infrastructures for Boxer integration:
  - **iOS** – Exchange ActiveSync 2007, 2010, 2013, 2016, Office 365, IBM Notes Traveler version 9.0.1.
  - **Android** – Exchange ActiveSync 2007, 2010, 2013, 2016, Office 365, IBM Notes Traveler version 9.0.1.
- Requires a Public trusted SSL certificate such as Symantec, GoDaddy, Verisign.

Components to Use with VMware Boxer

Integrate VMware Boxer with other components in your AirWatch deployment for more control of your enterprise email system.

Email Notification Service (iOS Only, Optional)

Deploy the Email Notification Service (ENS) to provide real-time email notifications.

The Email Notification Service (ENS) adds Apple Push Notification support to Exchange. On iOS, a third-party app can either receive notifications using Apple's background app refresh or Apple Push Notification Service (APNs) technologies. Background app refresh is used by default because each app may provide notifications at irregular intervals using this method. However, iOS attempts to balance the needs of all apps and the system itself.

To provide notifications quickly and consistently, Apple also provides APNs. APNs allows a remote server to send notifications to the user for that application, however Exchange does not natively support this APNs. ENS adds APNs support to your deployment to allow quick and consistent notifications about new items in your end users' email inboxes.

For more information on deploying Email Notification Service, see the AirWatch Online Help topic, **Introduction to Email Notification Service** at https://my.air-watch.com/help/9.1/en/Content/Expert_Guides/Email_Config_Guides/ENS/C/Introduction.htm.

AirWatch Mobile Email Management Models (Optional)

Configure one of the AirWatch email deployment models, either Secure Email Gateway (SEG) or PowerShell.

For more information on choosing a MEM deployment model, see the AirWatch Online Help topic **Protect Email Infrastructure** at https://my.air-watch.com/help/9.1/en/Content/Core_Guides/MEM/KS_MEM_Email_Infrastructure.htm.]

Supported Capabilities for VMware Boxer

Review the following notes and considerations before you configure and deploy VMware Boxer.

Enrollment

You can use VMware Boxer on devices enrolled and managed in AirWatch or on iOS and Android devices using standalone enrollment.

Typical enrollment uses the AirWatch Agent or the AirWatch Container to enroll the device into AirWatch. You can also enroll devices through Workspace ONE step-up enrollment.

Standalone enrollment is unique to VMware Boxer. This enrollment method allows end users to download the VMware Boxer app from the App Store or the Google Play Store without enrolling first. When the end user configures Boxer, they must provide their login credentials such as their user name, password, server URL, and group ID.

Standalone Enrollment supports (optional) AirWatch Autodiscovery that can be configured on the UEM console. Autodiscovery system allows end users to enroll devices to environments and organization groups (OG) using their email addresses.

For more information on Autodiscovery setup and configuration, see the **VMware AirWatch Mobile Device Management Guide**.

Note: The server URL and user group ID are pre-populated on the end-user devices from Autodiscovery Service during Standalone enrollment.

S/MIME

As an admin, you can upload S/MIME certificates from the UEM console (AirWatch v9.0+). End users can upload the certificates to Self Service Portal (SSP) or can send the certificates as email attachments for installation on their device. To allow users to decrypt and view emails that are encrypted using expired S/MIME encrypted emails, upload the expired certificate at **Accounts > User > Edit > Advanced > Certificates > old Encryption Certificate**. Once uploaded, the device users can view the expired certificate at **Boxer > Settings > Account > SMIME > Sign and/or Settings > Account > SMIME > Encrypt.**

Other Supported Capabilities

- **Certificate-Based Authentication** - VMware Boxer supports certificate-based authentication using Certificate Authority (CA) that is configured in AirWatch for iOS and Android platforms. SCEP is not supported for certificate-based authentication.
- **Information Rights Management** - VMware Boxer supports information rights management for both iOS and Android platforms.
- **VPP Application Deployment** - You can deploy VMware Boxer for iOS through Apple's Volume Purchase Program (VPP) from the UEM console. This deployment allows end users to download the app without the need to enter Apple ID. For more information on how to deploy applications through VPP, see the topic **Purchased Applications (Apple VPP) Feature Overview** at https://my.air-watch.com/help/9.1/en/Content/Core_Guides/MAM/KS_MAM_Purchased_Apps.htm.
- (Android Only) **Block Insecure Attachments** - Boxer for Android restricts opening and downloading insecure attachment types by default. The device user can allow downloading of insecure attachment by navigating to **Boxer > Settings > More mail settings** and select **Allow insecure attachments**. The following file types are restricted by Boxer:

Restricted File Types			
Common File Formats			
ADE	ADP	BAT	CHM
CMD	COM	CPL	DLL
EXE	HTA	INS	ISP
JSE	LIB	MDE	MSC
MSP	MST	PIF	SCR
SCT	SHB	SYS	VB
VBE	VBS	VXD	WSC
WSF	WSH		

Restricted File Types			
Common Container Formats			
ZIP	GZ	Z	TAR
TGZ	BZ2	XEN	APK

Interoperability Features of Boxer

Boxer URL Schemes

Boxer app extends the support for inter-app integration using URL schemes. AirWatch provides you with a set of URLs that can be used to access different Boxer menus and options from supported third-party applications. The URL schemes can be used with any application that supports URL formats, for example, browsers, email applications, and notes. You can save the URLs and open them to directly access a specific Boxer menu or option. For example, use *boxer://calendar* URL scheme to open Boxer calendar directly from any supported app.

URL Scheme	Description
boxer://messages	AirWatch Agent v5.2 and higher
boxer://calendar	Opens calendar
boxer://calendar/<unix timestamp>	Opens calendar for a specific date or time
boxer://calendar/create	Creates a calendar event
boxer://calendar/nextEvent	Opens the first upcoming event in the calendar
boxer://contacts	Opens contacts
boxer://contacts/create	Creates a contact
boxer://settings	Opens Boxer settings
Additional URL Schemes	
Pre-composed Email awemailclient://emailcompose?kAWEmailClientEmailTo=someone@domain.com,anotherone@domain.com&kAWEmailClientEmailCC=someelse@domain.com&kAWEmailClientEmailSubject=whatever&kAWEmailClientEmailBody=here's+the+body **Description** Opens a pre-composed email for single or multiple recipients with a subject and an email body. You can edit and save the URL to create multiple quick templates for frequent email interactions.	

Chapter 2:
Application Configuration

Deploy VMware Boxer with the AirWatch Console

Configuring the Boxer application involves adding it as a public application and assigning it with set email configurations to end users.

Smart Group Based Assignments

Create single or multiple smart group based assignments and deploy different Boxer email settings specific to a set of users in your organization. An assignment group is a representation of single or multiple smart groups that are assigned with same email configuration.

Procedure

There are two parts to configure the deployment of VMware Boxer to iOS and Android devices. You must perform both procedures.

1. Add VMware Boxer as a public application. See Add VMware Boxer to Public Applications on page 8 for information.
2. Assign the VMware Boxer to smart groups. See Assign VMware Boxer with Email Settings on page 11 for details.

For in-depth instructions on deploying public applications, see the AirWatch Online Help topic **Public Application Overview** at https://my.air-watch.com/help/9.1/en/Content/Core_Guides/MAM/KS_MAM_Public_Apps.htm.

Note: When you deploy Boxer as a public app in a PowerShell deployment, you must configure a device access rule on Exchange to allow Boxer users to access emails. For more information about configuring the device access rule, see Workaround for Boxer Flexible Deployment section of Mobile Email Management (MEM) Guide.

Add VMware Boxer to Public Applications

Add VMware Boxer as a public application to the UEM console. Adding applications through an app store enables AirWatch to manage applications by your settings in the console.

Note: In Apple App Store, Boxer Lite and Boxer Pro may also appear in the search results. These apps are consumer apps that do not offer AirWatch functionality.

1. Navigate to **Apps & Books > Applications > List View > Public**.
2. Select **Add Application**.
3. Configure the text boxes that display and select **Next**.

Setting	Description
Managed By	View the organization group where the application is uploaded.
Platform	Choose the appropriate platform. Only iOS and Android devices are supported currently.
Source	Select to search for the application in the app store or play store.
Name	Enter "VMware Boxer".

4. Locate and select the **VMware Boxer** app in the **Search** results screen.
5. Review the information that automatically populates in the **Details** tab.
6. Under the **Deployment** tab, choose the app delivery mode either as On-Demand or Automatic.

- **On Demand** – Deploys content to the App Catalog and lets the device user decide if and when to install it. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic.
- **Automatic** – Deploys content to a device upon enrollment. If the device is enrolled, this option immediately prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users.
- Under **Policies** settings, determine how your end users receive the app.

Setting	Description
Device must be MDM Managed to install this App	Enable this option if a device must be managed to install the Boxer app. ◦ If you enable this option, only the devices enrolled using Agent and Workspace ONE step up enrollment method receive the email configurations. ◦ If you disable this option, the devices enrolled using Container, Workspace ONE without step up enrollment, Workspace ONE with step up enrollment, and the Agent receive the email configurations.
App Tunneling **Apple iOS 7+**	This setting is not applicable to Boxer.
Remove On Unenroll **Apple iOS**	Select this option to remove the Boxer application when the device unenrolls from AirWatch.

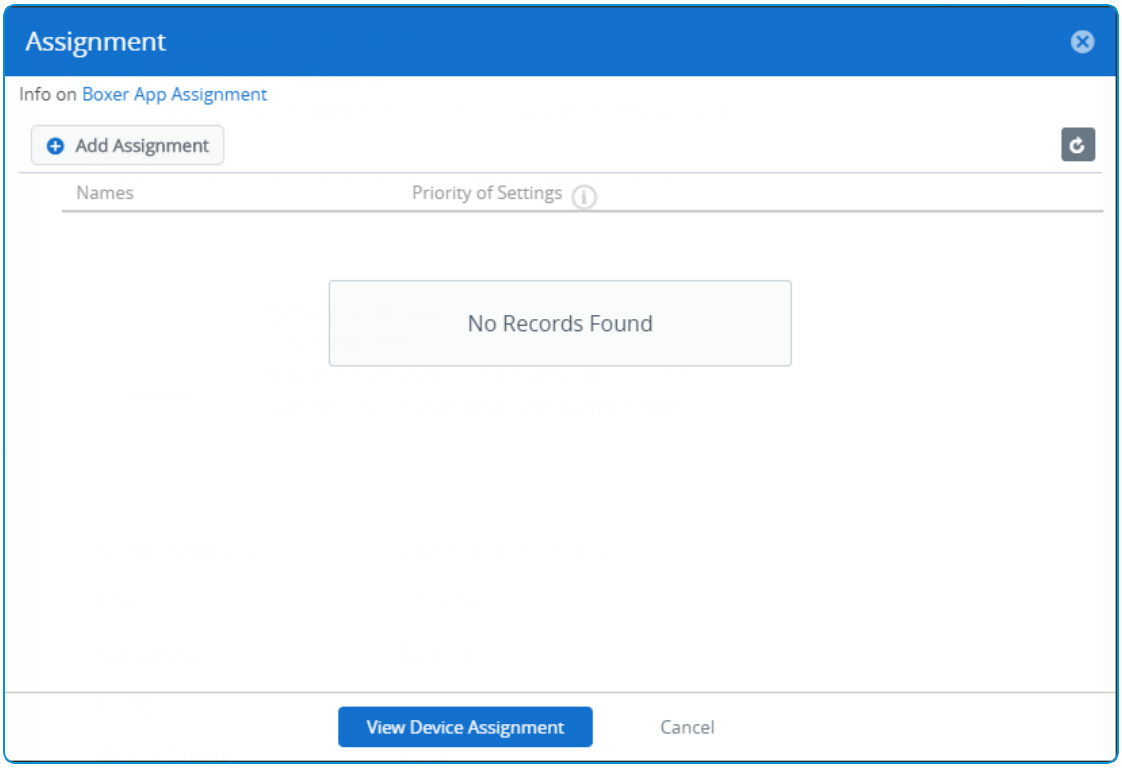
Setting	Description
Prevent Application Backup **Apple iOS**	This setting does not apply to Boxer, because the application is configured such that it prevents application backup.
Make App MDM Managed if User Installed **Apple iOS 9+**	Enable this setting if your end users download Boxer from the Store and you want to use the **Remove on Unenroll** setting. Otherwise, Boxer does not have to be MDM managed.
Application uses AirWatch SDK	Enable this setting to use the AirWatch SDK for additional functionality. If you are using Single Sign-On, you must enable this option.

7. Assign **Terms of Use**, which displays when users first access the application from the App Catalog.
8. Select **Save and Assign**.

Next Steps

You can add an assignment now or you can come back and add assignments later.

- **Add assignments now** - Select **Add Assignment** and follow the steps outlined in Assign VMware Boxer with Email Settings on page 11.
- **Add assignments later** - Select **View Device Assignment**. The console prompts for confirmation that you are not assigning the application. VMware Boxer displays in the **List View** and you can edit it later to assign it to devices as outlined in Assign VMware Boxer with Email Settings on page 11.



Assign VMware Boxer with Email Settings

Assign VMware Boxer to devices with the assignment feature known as flexible deployment. Configure the security and email management features within the assignment procedure so that they meet your organization's needs.

Task Considerations

Important: If Passcode is set to **None**, then the Boxer app is not encrypted. If you do not enforce an app-level passcode, then consider enforcing a device-level passcode using a device profile, which encrypts the iOS device.

- All attachment security, Data Loss Prevention (DLP), and encryption are handled from within the Boxer app itself.
- Enabling **DLP > Caller ID** settings cause an error if end users have deleted their local address book. See Work around for Third-Party Address Book (iOS Only) on page 33 for more information.
- For information on optional application configurations, see Application Configurations for VMware Boxer on page 15.

Procedure

1. Navigate with one of the following paths.
   - Select **Add Assignment** in the Assignment window.

     This navigation reflects adding an assignment immediately after adding the application to the public tab of the console.
   - Go to **Apps & Books > Public**, select the **VMware Boxer** application in the **List View**, select **Assign**, and choose **Add Assignment**.

     This navigation reflects adding an assignment later after adding the application to the public tab of the console.
2. Complete the settings on the **Email Settings** page.

Settings	Description
Assignment	
Assigned Smart Groups	Enter smart groups to receive the VMware Boxer flexible deployment assignment.
Is App Restricted to Silent Install (Android)	Enable to assign the application to those devices that support the silent install or the silent uninstall capability only.
Account Settings	
Account Name	Enter a description of the mail account.
Exchange ActiveSync Host	Enter your EAS server URL. For SEG deployments, enter the SEG URL instead.
Domain, User, Email Address	Enter the login information, including Domain name, user name, and Email Address. By default, the login information includes {EmailDomain}, {EmailUserName} and {EmailAddress} that are defined as lookup values in your directory service. If you need to override these values, you can use custom lookup values.

Settings	Description
Password (Android Only)	Enter the password to the email account or input the lookup value for pulling the password from the user account.
Email Sync Period	Set the number of past days of emails for Boxer to sync.
Calendar Sync Period	Set the number of past days of calendar events for Boxer to sync.
Email Signature	Specify an email signature to be used in emails that are sent using Boxer.
Authentication Type	Choose one of the following authentication types for end users to authenticate with Exchange using the AirWatch credentials: • **Basic** – Authenticates using a user name and a password. • **Certificate** – Authenticates using a certificate. ◦ Select the desired Certificate Authority and Certificate Template. • **Both** – Authenticates using a certificate to authenticate with network appliance and a password to authenticate with Exchange.
Passcode	
Setting an app-level passcode for Boxer also encrypts the application. Device users set their passcode on the device at the application level when they first access the application.	

Settings	Description
Type	• **None** – Does not require a passcode. • **Numeric** – Prompts the user with a numeric keyboard to set a passcode. ◦ (iOS only) **Biometric ID** - Enable this option to use fingerprint to authenticate the application. The user is asked to enable Touch ID settings on device the first time when they are asked for their passcode and NOT when they create their passcode during first-time setup. ◦ **Minimum Length** - Set the minimum number of numeric characters a user's passcode must contain. ◦ **Timeout Minutes** - Set the time in minutes until the application locks when idle. ◦ **Maximum Age** - Set the maximum allowed days for the passcode, after which passcode expires and has to be reset. When the set number of days exceeds, the client asks the end user to create a passcode. ◦ **History** - Determine the history of passcodes used to prevent the user from reusing passcodes. ◦ **Maximum Number of Failed Attempts** - Determine the maximum number of failed passcode attempts before the email data in the app are erased. • **Alphanumeric** – Prompts the user with alphanumeric keyboard to set a passcode. The list explains only those options that are different from the **Numeric** setting. ◦ **Minimum Number of Complex Characters** - Set the minimum number of character sets required for the passcode. ■ Character sets include uppercase letters, lowercase letters, numbers, and symbols. ■ For example, if you select 2, then a passcode must contain at least two of the character sets above. This can be a number and symbol: 3!$#!$, uppercase and lowercase: RtGfH, lowercase and symbol: p!$@!, and so on.
Data Loss Prevention	
Determine how your end users can access emails, email attachments, and hyperlinks by configuring the following settings.	

Settings	Description
Copy Paste	If restricted: • End users cannot copy and paste content from Boxer to other applications. • If personal accounts are enabled, end users can copy and paste between personal and work accounts. Therefore, consider disabling personal accounts to restrict copy and paste functionality completely. • Share and Define options are made unavailable in the application when selecting text.
Screenshots (Android Only)	If restricted, Android end users cannot take screenshots of the Boxer application.
Allow Email Widget (Android Only)	If enabled, Android end users can add the Boxer Email widget to their home screens.
Allow Calendar Widget (Android Only)	If enabled, Android end users can add the Boxer Calendar widget to their home screens.
Hyperlinks	If restricted, end users can only open hyperlinks in VMware Browser.
Sharing	Choose one of the following restrictions based whether the end user can open emails and their attachments in other applications: • **Preview Only** — Set this restriction for end users to preview emails and attachments within Boxer application only. End users cannot open attachments into any other applications. • **Whitelist** — Set this restriction and specify bundle IDs of the applications for emails and their attachments to open in those specified applications. The bundle IDs for Content Locker and Evernote are prepopulated. • **Unrestricted** — Set this restriction for end users to open emails and attachments in any applications.
Caller ID	Enable to provide Caller ID functionality for all Boxer contacts. By enabling this feature, Boxer exports names and phone numbers only to the native contacts app.
Personal and Work Separation	
You can allow end users to add multiple personal accounts and use local contacts by configuring the following settings on the UEM console.	
Personal Accounts	If restricted, end users can no longer add any additional accounts to the application. If end users already have Boxer on their device with personal accounts configured, then they are prompted whether they want to remove their existing personal accounts now or later. End users do not receive work email through Boxer until they remove all personal accounts.

Settings	Description
Personal Contacts	If restricted, end users can access contacts only from the email accounts in the app. If unrestricted, end users can access contacts from other apps on the device.
Optional	
Application Configuration	You can configure settings for your Boxer deployment using the Configuration Key and Configuration Value pairs provided by AirWatch. Application configurations are optional.

3. Select **Save**.

4. If you want to restrict copying and pasting of data from and to the Boxer and other supported apps, configure these settings at **Apps** > **Settings and Policies** > **Security Policies** > **Data Loss Prevention**. SSO must be enabled for these settings to be applied on the end user devices. These restrictions are applied accross all supported VMware applications.

Settings	Description
Enable Copy and Paste Out	When disabled, end users cannot copy and paste content from Boxer to other applications.
Enable Copy and Paste Into	When disabled, end users cannot copy and paste content from other applications into Boxer.

Application Configurations for VMware Boxer

You can configure settings for your Boxer deployment using the Configuration Key and Configuration Value pairs provided by AirWatch.

To configure these settings, enter the configuration key and the corresponding value into the Application Configuration setting during the app assignment.

Important: If Boxer is already installed on end-user device, it might take few minutes for Boxer to download the new profile settings.

Sync Period

Add this key value pair to configure the maximum number of past days of mail and calender to sync in the Boxer app. This setting allows you to hide the **No Limit** feature available in the Boxer app settings.

Configuration Key	Value Type	Configuration Value	Description
PolicyEmailMaxSyncPeriod	Integer	0 - sync all 1 - 1 day 2 - 3 days 3 - 1 week 4 - 2 weeks 5 - 1 month	Enter the number of days of past mail to sync.

Configuration Key	Value Type	Configuration Value	Description
PolicyCalendarMaxSyncPeriod	Integer	0 - sync all 4 - 2 weeks 5 - 1 month 6 - 3 months 7 - 6 months	Enter the number of days of past calendar events to sync.

Note: Set the key value pairs to block syncing of all old emails and calendar until new emails or calendar events are synced first. Removing 0 from the key values disables the **No Limit** option for PolicyEmailMaxSyncPeriod and PolicyCalendarMaxSyncPeriod.

Default S/MIME Signing and Encryption Algorithms

Add the following key value pairs to configure the default encryption algorithms for signing and encrypting S/MIME emails. When a default S/MIME algorithm is configured, Boxer sends the outgoing emails with the default configured algorithm. Boxer also checks the algorithms for the incoming emails. If the incoming emails are not configured with the default algorithm, a warning message is displayed in the conversation view.

Configuration Key	Value Type	Configuration Value	Description
PolicySMIMEDefaultEncryptionAlgorithm	String	Allowed Values: 3DES AES128 AES192 AES256 For example, PolicySMIMEDefaultEncryptionAlgorithm - [“3DES”]	Specify an encryption algorithm to use for incoming and outgoing emails. If a valid algorithm is not provided, the lowest supported algorithm is used (3DES).
PolicySMIMEDefaultSigningAlgorithm	String	Allowed values: SHA1 SHA256 SHA384 SHA512 For example, PolicySMIMEDefaultSigningAlgorithm - [“SHA1”]	Specify a default S/MIME signing algorithm to use for incoming and outgoing emails. If a valid algorithm is not provided, the lowest supported algorithm is used (SHA-1).

(Android Only) S/MIME Algorithms Compliance

Add the following key value pairs to configure the list of algorithms that Boxer checks for compliance when receiving a signed or encrypted S/MIME email. When set, only the configured algorithms are recognized by Boxer. Boxer displays non-compliance warning when accessing emails that are encrypted using any other algorithm, both strong or weak, than that are listed using the key value pairs.

Configuration Key	Value Type	Configuration Value	Description
PolicySMIMEConformingEncryptionAlgorithms	String	Supported Values: 3DES AES128 AES192 AES256 For example, PolicySMIMEConformingEncryptionAlgorithms = ["AES-128", "AES-256"]	Set the algorithms that are recognized by Boxer for encrypting S/MIME emails.
PolicySMIMEConformingSigningAlgorithms	String	Supported Values: SHA1 SHA256 SHA384 SHA512 For example, PolicySMIMEConformingSigningAlgorithms = ["SHA-256", "SHA-512"]	Set the algorithms that are recognized by Boxer for signing S/MIME emails.

ENSv2 Notification Policy

Add the following key value pair to configure the ENS Notification Policy for Boxer. When confgured, Boxer immediately re-subscribes to ENSv2 and notification policy is updated as per the set key value.

Configuration Key	Value Type	Configuration Value	Description
PolicyLimitNotificationText key	Integer	0 - sets notification to sender, subject and preview (not supported in ENSv1) 1 - sets notification to sender and subject 2 - sets notification to sender 3 - sets notification to generic message (new message) 4 - sets notification to none (only the badge is updated)	Configure the notification policy used by Boxer.

Boxer Plain Text Mode

Add the following key value pair to confgure Boxer plain text mode.

Configuration Key	Value Type	Configuration Value	Description
AppPlainTextMode	Boolean	False - disabled (default) True - enabled	Set to **True** to enable Boxer plain text mode. When set, Boxer retrieves only plain text from HTML mails when syncing. Boxer sends only plain text regardless of the email message format. The formatting controls in compose view is disabled and only text can be copied and pasted from rich or HTML content.

Policy Allow Metrics

Add this key to define the policy for allowing collection of anonymous usage data to improve user's Boxer experience. When enabled, a Data Sharing notice is displayed to user when Boxer is launched. The device user can enable or disable data sharing by navigating to Settings > Privacy > Data Sharing.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowMetrics	Boolean	True - enabled False - disabled	Set to **True** to enable data collection for Boxer experience improvement. The value of PolicyAllowFeatureAnalytics, when set from Custom SDK settings takes precedence over the value of PolicyAllowMetrics that is set from App Configuration Settings.

Policy Allow Crash Reporting

Add this key to define the policy for reporting Boxer crashes to VMware.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowCrashReporting	Boolean	True - enabled False - disabled	Set to **True** to report Boxer crashes to VMware. The value of PolicyAllowCrashReporting, when set from Custom SDK settings takes precedence over the value that is set from App Configuration Settings.

(iOS only) Allow Print

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowPrint	Boolean	True - enabled False - disabled	Set to **False** to disable printing of emails and attachments from Boxer.

(iOS only) Enforce HTTPS

From Boxer v4.13 for iOS, adding this key value pair blocks email content from unsecured connections in Boxer.

Configuration Key	Value Type	Configuration Value	Description
PolicyEnforceHTTPS	Boolean	False = disabled (default) True = enabled	When set to True, email content from unsecured HTTP connections are not loaded. Outgoing links (hrefs) are not affected since the outgoing links can be controlled using Browser policy.

(Android only) Limit Notification

Configuration Key	Value Type	Configuration Value	Description
PolicyLimitNotificationText	Integer	0 - Displays Sender, Subject, and Body Preview (Default) 1 - Displays Sender and Subject 2 - Displays Sender 3 - Generic notification (You've got a new email) 4 - No notification	Set configuration value to limit what is displayed in Boxer notification.

Mark External Addresses

Add the following keys to configure Boxer to warn the user when adding external recipients to emails.

Configuration Key	Value Type	Configuration Value	Description
AppDomainsInternal	String	Provide the list of internal domains. For example, [vmware.com, air-watch.com].	Define the domains that are internal or permitted. The user can disable the warning using the 'Confirm before sending' setting in Boxer when the internal domains are defined and AppDomainsWarning key is not set.
AppDomainsWarning	Boolean	True - enabled False - disabled (default)	Set to **True** to enable warning when the user enters recipients from external domains. If the domains are configured and the AppDomainsWarning value is set to True, the 'Confirm before sending' setting is unavailable to the users. When the warning is displayed, the user can either Accept and return to the Compose email menu or Ignore and continue sending the email to external recipients.

If the AppDomainsInternal key is enabled and the AppDomainsWarning key is disabled, then the ‘Confirm before sending emails’ setting is disabled and the device user can toggle the setting in the Boxer app as per requirement. If the 'AppDomainsInternal' key and 'AppDomainsWarning' key is disabled, then the 'Confirm before sending emails' setting is disabled and the device user can enable the setting in the Boxer app as per requirement. If both the AppDomainsInternal and AppDomainsWarning is set to true, then the ‘Confirm before sending emails’ setting is enabled and is unavailable to the device user.

Mobile Flows

Add the following keys to configure Mobile Flows for Boxer.

Configuration Key	Value Type	Configuration Value	Description
AppMobileFlowsEnabled	Boolean	True - enabled False - disabled	Set to **True** to enable Mobile Flows for Boxer.
AppMobileFlowsHost	String	Provide a valid URL for the Mobile Flows host. For example, http://acme.hero.acme1.com	Define the URL for the Mobile Flows host.
AppMobileFlowsvIDM	String	Provide a valid URL for authenticating the device users. For example, http://acme.vIDM.acme2.com	Defines the URL for the device user to authenticate.

Allow Local Contacts

Add this key to define the policy for local contacts in Boxer.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowLocalContacts	Boolean	True - enabled False - disabled	Set to **True** to enable local contacts in Boxer. If disabled, the Local Contacts option in Boxer is unavailable to the end users.

Allow Local Calendars

Add this key to define the policy for local calendars in Boxer.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowLocalCalendars	Boolean	True - enabled False - disabled	Set to **True** to enable local calendars in Boxer. If disabled, the Local Contacts option in Boxer is unavailable to the end users.

(iOS only) PolicyDerivedCredentials

Add this key to enable derived credentials authentication policy for Boxer. When enabled, the device users must install VMware PIV-D Manager app for enrolling into Boxer.

Configuration Key	Value Type	Configuration Value	Description
PolicyDerivedCredentials	Integer	1- enabled 0 - disabled	Set to 1 to enable derived credentials enrollment in Boxer.

Default Swipe Actions

Add this key to define the default swipe actions in Boxer.

Configuration Key	Value Type	Configuration Value	Description
AppSwipesLeftShortDefault	Integer	1 - actions grid 2 - archive 3 - delete 4 - move 5 - flag 6 - quick reply 7 - read or unread 8 - spam	Define the default swipe actions. User can customize swipe actions using the options provided in the Boxer app.
AppSwipesLeftLongDefault			
AppSwipesRightShortDefault			
AppSwipesRightLongDefault			

Default Conversation View

Add this key to define the default policy for converation view in Boxer.

Configuration Key	Value Type	Configuration Value	Description
AppConversationViewDefault	Boolean	True - enabled False - disabled	Set to **True** to enable conversation threading by default. When set to **False**, the conversation threading option is disabled for the users.

Default Avatar Policy

Add this key to define the default policy for avatars in Boxer.

Configuration Key	Value Type	Configuration Value	Description
AppAvatarsDefault	Boolean	True - enabled False - disabled	Set to **True** to enable avatars by default. User can change the Avatar setting using the options provided in the Boxer app.

(iOS only) Allow Custom Keyboards

Add this key to define the policy for allowing third-party keyboards with Boxer.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowCustomKeyboards	Boolean	True - enable (default value for unmanaged device) False - disable (default value for managed device)	Set to **True** to permit users to activate third-party keyboards within Boxer.

Export Contacts by Default

Add this key to enable or disable exporting of contacts by default.

Configuration Key	Value Type	Configuration Value	Description
AppDefaultCallerID	Boolean	True - enabled False - disabled	Set to **true** to enable the exporting of contacts by default. This setting requires the Caller ID option in the AirWatch Console to be set as Unrestricted.

Allow Caller ID (Contact Export for iOS)

Add this key to enable or disable Export Contact option in Boxer for end users.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowCallerID	Boolean	True - enabled False - disabled	Set to **true** to enable the exporting of contacts by the end users. This setting requires the AppDefaultCallerID configuration value set to 'enabled'. If disabled, the Export Contacts option in Boxer is unavailable for the end users.

Allow Archive

Add this key to enable or disable Archive action in Boxer for end users.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowActionArchive	Boolean	True - enabled False - disabled	Set to **true** to enable archive action by the end users. If disabled, the Archive option in Boxer is unavailable for the end users.

Allow Spam

Add this key to enable or disable Spam action in Boxer for end users.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowActionSpam	Boolean	True - enabled False - disabled	Set to **true** to enable spam action by the end users. If disabled, the Spam option in Boxer is unavailable for the end users.

Restricting Third-Party Attachments

Add these keys to restrict the device user from attaching files to emails from multiple third-party sources.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowDocProviders	Boolean	True - enable False - disable	Enables or disables attachments from external providers (iCloud, Dropbox, Google Drive, etc.) within Boxer.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowOpenIn	Integer	0 - not allowed 1 - allowed	Enables or disables attaching of files from other apps using open-in or share into Boxer. When open-in or sharing of attachments are disabled, the message 'Your administrator has restricted attachments from external applications' is displayed.
(iOS Only) PolicyAllowPhotoAttachment	Boolean	True - enable False - disable	Enables or disables attaching of images and media files from photo gallery and camera.

S/MIME

Use these key value pairs to configure S/MIME support.

Configuration Key	Value Type	Configuration Value	Description
PolicySMIME	Integer	0 - disabled (default) 1 - allowed 2 - required	Changes the status of S/MIME support.
PolicySMIMEEnableRevocationCheck	Integer	0 - disabled 1 - enabled	Enable or disable Online Certificate Status Protocol (OCSP).
PolicySMIMERevocationCheckUrl	String	Supported format: http://ocsp.acme.us/ ocsp:88	Configure the Revocation check URL.
PolicySMIMERevocationCheckType	Integer	0 - check entire chain 1 - check only user certificate	Configure the revocation check type.
PolicySMIMERevocationUseAIA	Integer	0 - disabled (don't use URL configured inside certificate for revocation status, use PolicySMIMERevocationCheckUrl only) 1 - enabled (use URL configured inside certificate for revocation status check, fall back to PolicySMIMERevocationCheckUrl if it is unavailable) 2 - required (only use URL configured inside certificate to check for revocation status, ignore PolicySMIMERevocationCheckUrl)	Define the revocation usage policy.

Configuration Key	Value Type	Configuration Value	Description
PolicySMIMERevocationEnforceNonce	Integer	0 - disabled (enforce nonce) 1 - enabled (do not use nonce)	Define the nonce usage policy.
PolicySMIMERevocationTTL	Integer	7 - Default value	Define the amount of time to retain the revocation data.
PolicySMIMETrustStore	Integer	0 - Device Trust Store (default) 1 - Boxer Trust Store	Define the Trust Store.

Refetch Empty Links

Add this key value pair to configure refetch policy for non-standard URL schemes.

Configuration Key	Value Type	Configuration Value	Description
AppRefetchEmptyLinksUsingMime	Boolean	True - Use MIME to fetch email body	For emails (fetched using HTML) that contain non-standard URL schemes, pointing to non-server domains, Exchange replaces the URL with two empty spaces. Enable the PolicyRefetchEmptyLinksUsingMime for the Boxer to detect this occurrence and re-download the affected body using MIME, which is not subject to the URL replacement error.

Modern Authentication

Add this key value pair to enable modern authentication for Office 365 accounts.

Configuration Key	Value Type	Configuration Value	Description
AccountUseOauth	Boolean	True - enable False - disable	Enables or disables modern authentication for Office 365 accounts. When enabled, during enrollment, users are redirected to the login page for entering email password.

Downloading Attachments

Add this key value pair to enable or disable downloading of attachments.

Configuration Key	Value Type	Configuration Value	Description
PolicyAllowAttachments	Boolean	True - enable False - disable	Enables or disables downloading of attachments.

Activate SSO

If SSO is enabled in the Security Policies, enable **Application uses AirWatch SDK** and assign the following application configuration keys and values to add SSO functionality for Boxer. For using SSO functionality in Boxer (iOS and Android) , you must have AirWatch Console version 9.0.5 or above.

Configuration Key	Value Type	Configuration Value	Description
AppForceActivateSSO	Boolean	True - enable False - disable	Enables or disables SSO for Boxer.

Browser Exception List

You can use the **AppDefaultBrowserExceptions** key to create exception lists for hyperlinks when hyperlinks are Restricted or Unrestricted in the AirWatch Console.

You can configure the key value pairs to support the following functionalities:

- If hyperlinks are restricted in the AirWatch Console, all links open in VMware Browser
- If hyperlinks are restricted, but has an exception list, all available browsers are displayed but only links in the exception list opens in the default browser
- If hyperlinks are unrestricted in the AirWatch Console, all available browsers are displayed and all links open in the default browser
- If hyperlinks are unrestricted in the AirWatch Console, but has an exception list, all available browsers are displayed and the links in the exception list only opens in VMware Browser

Configuration Key	Value Type	Configuration Value	Description
AppDefaultBrowserExceptions	String	AppDefaultBrowserExceptions = ["*.acme.com", "acme*.acme1.com", "source.acme.com", "acme.com"]	Create exception list to restrict and unrestrict specific links from opening in the default browser.

Security Classifications

Enable Email Classification Marking to assign security classifications to the emails sent from Boxer. Assign the following application configuration keys and values to enable Email Classification Marking feature:

Configuration Key	Value Type	Configuration Value	Description
PolicyClassMarkingsEnabled	Integer	0 - disable 1 - enable	Enables or disables classification markings.
PolicyClassMarkingsXHeader	String	x-header-name	(Optional) Enables and defines x-header for classification.
PolicyClassVersion	String	1.0	Version number for classification feature.
PolicyClassMarkingsRankEnabled	Integer	0 - disable 1 - enable	(Optional) Enables hierarchical classification ranking.
PolicyClassMarkingsDefaultClass	String	Confidential, Restricted, Protected, or Secret	(Optional) Set the default classification for emails. The value must match a display name from an entry in PolicyClassMarkings configuration value.

Configuration Key	Value Type	Configuration Value	Description
PolicyClassMarkings	String	PolicyClassMarkings Configuration Value on page 27	Defines the hierarchical list of classifications.

PolicyClassMarkings Configuration Value


```
[{
                        "Rank": 4,
                        "DisplayName": "Secret",
                        "Description": "This is secret...",
                        "Subject": "(Secret)",
                        "TopBody": "Classification: Secret",
                        "BottomBody": "Classification: Secret",
                        "XHeader": "Secret"
                        }, {
                        "Rank": 3,
                        "DisplayName": "Restricted",
                        "Description": "This is restricted...",
                        "Subject": "(Restricted)",
                        "TopBody": "Classification: Restricted",
                        "BottomBody": "",
                        "XHeader": "Restricted"
                        }, {
                        "Rank": 2,
                        "DisplayName": "Protected",
                        "Description": "This is protected...",
                        "Subject": "[Sec=Protected]",
                        "TopBody": "",
                        "BottomBody": "Classification: Protected",
                        "XHeader": "Protected"
                        }, {
                        "Rank": 1,
                        "DisplayName": "Confidential",
                        "Description": "This is confidential...",
                        "Subject": "(Confidential)",
                        "TopBody": "Classification: Confidential",
                        "BottomBody": "Classification: Confidential",
                        "XHeader": "Confidential"
                }]
```


Configure Privacy Settings for Boxer

Use the configuration keys in the UEM console to perform additional privacy disclosure and data collection practices. When Boxer is launched, a privacy notice is displayed to the end users who are upgrading to or using the latest Boxer version.

The privacy dialog screen lets the user know the following information:

- **Data collected by the app** – Provides a summary of data that is collected and processed by the application. Some of this data is visible to the administrators of the Workspace ONE UEM administration console.
- **Device Permissions** – Provides a summary of device permissions requested for the app to enable product features and functionality, such as push notifications to the device.
- **Company's privacy policy** – By default, a message is displayed to the user to contact the employer for more information. You can configure the privacy policy URL in the UEM console. Once configured, the user can access the employer's privacy policy from Boxer.

If you are using SDK Default settings:

1. Navigate to **Group & Settings** > **All Settings**.
2. From All Settings, navigate to **Apps** > **Settings & Policies** > **Settings**.
3. Select **Enable Custom Settings** and paste the configuration keys as per your requirement.
   For example, to enable Crash reporting, { "PolicyAllowCrashReporting": true}.
4. Select **Save**.

If you are using a custom SDK profile for Boxer:

1. Navigate to **Group & Settings** > **All Settings**.
2. If you have an existing custom profile, navigate to **Apps** > **Settings & Policies** > **Profiles** > **Custom Profile** > **Custom Settings**.
3. If you want to add a custom profile, navigate to **Apps** > **Settings & Policies**> **Profiles** > **Add Profile** > **SDK Profile** > **iOS**> **Custom Settings**.
4. From Custom Settings, select **Configure** and paste the following configuration keys as per your requirement.

Configuration Key	Value Type	Supported Values	Description
{ "DisplayPrivacyDialog" }	Integer	0 = disabled 1 = enabled (default)	When set to '1' (enabled), Boxer displays a privacy notice to the users about the data that is collected and the permissions that are required on the device for the optimal functioning of the app.

{ "PolicyAllowFeatureAnalytics" }	Integer	0 = disabled 1 = enabled (default)	When set to '1' (enabled), Boxer displays a notice to the users about the option to opt-in to anonymous feature usage analytics that help VMware improve product functionality and invent new product capabilities. When set to '0', the data sharing notice is not displayed and no data is collected from the device to optimize the app experience. The device user can enable or disable data sharing by navigating to **Settings > Privacy > Data Sharing**.
{ "PolicyAllowCrashReporting" }	Boolean	True = enabled False = disabled	When set to True, app crashes are reported to VMware.

{ "PrivacyPolicyLink" }	String	"https://www.acme.com"	Provide the Policy URL that you want your users to visit when *Your company's privacy policy* is selected from the Privacy notice.
Sample SDK configuration: {"PolicyAllowFeatureAnalytics":1, "PrivacyPolicyLink":"https://www.acme.com/privacypolicy", "PolicyAllowCrashReporting":true}			

5. Select **Save**.

Flexible Deployment Assignments and VMware Boxer

Assignment by flexible deployment enables mapping of your email settings to smart groups.

An assignment can contain single or multiple smart groups belonging to an Organization Group. Assignments with same email settings are grouped together. You can choose existing smart groups or create new smart groups from the Assigned Smart Groups field as per your requirement.

If you have multiple email settings that are assigned to different assignment groups, then the most recently created settings gets priority. If a device exists in multiple assignment groups that have been configured with different email settings, the device will receive the email settings from the assignment group with the highest priority.

Configure Fingerprint Authentication

VMware Boxer for Android and iOS supports fingerprint authentication. Configure the authentication method as part of your normal deploy and assign process.

Prerequisites

- VMware Boxer v4.5 for Android and VMware Boxer 4.2 for iOS
- AirWatch v9.0.5+

Procedure

To configure fingerprint authentication:

1. Navigate to **Groups & Settings > All Settings > Apps > Settings & Policies > Security Policies**.
2. Select **Override** to override any inherited settings.
3. Set the **Authentication Type** to **Passcode** or **user name and Password**. Passcode and Biometrics must be enabled for using the Fingerprint functionality with Boxer.
4. Expand the Authentication Type settings.

5. Enter a value greater than 0 for Authentication timeout.
6. Set **Biometric Mode** to **Fingerprint**.
7. Select **Save** at the bottom of the screen.
8. Configure the VMware Boxer app to use the AirWatch SDK. Use AirWatch SDK to customize your deployment with maximum security and stability.
   - If you have not added VMware Boxer as a public app to your UEM console, navigate to **Apps & Books > List View > Public > Add Application**. Follow the steps to add the app. Enable **Application uses AirWatch SDK**. You can use the default profile. For more information, see Add VMware Boxer to Public Applications on page 8.
   - If you have already added VMware Boxer to your UEM console, navigate to **Apps & books > List View > Public** and select the app. Select **Edit**. Select the Deployment tab and enable **Application uses AirWatch SDK**. You can use the default profile.
9. Navigate to **Apps & Books > Public Application**. Select the VMware Boxer app and select **Assign**. Select **Add Assignment**.

   Configure the Email Settings. For more information, see Assign VMware Boxer with Email Settings on page 11.

   You must configure the following settings for fingerprint authentication for both Android and iOS devices:

Setting	Description
Application Configuration	
Configuration Key	Enter the configuration key for the setting. For fingerprint authentication, enter **AppForceActivateSSO**.
Value Type	Select the type of value associated with the configuration key. For fingerprint authentication, select **Boolean**.
Configuration Value	Enter the configuration value. For fingerprint authentication, enter **true**.

10. Select **Save**.
11. Select **View Device Assignment** and select **Save & Publish**.

After the assigned devices receive the new settings, end users may enable fingerprint authentication in the device settings. Configuring fingerprint authentication includes adding a fingerprint on the device. If enabled, end users must enter a backup passcode or user name and password.

Chapter 3:
Device Management

You can remove access to business data through device management tools in the UEM console. The actions available depend on the enrollment method.

Enterprise Wipe

Perform an enterprise wipe to remove all business data from an enrolled device. Enterprise wipe also removes access to enterprise email accounts in VMware Boxer. While the action removes enterprise data, enterprise wipe does not remove personal data from the device. Devices must be enrolled through typical enrollment to use enterprise wipe. Standalone enrollment does not support enterprise wipe.

Performing an enterprise wipe also removes all personal accounts from Boxer. End users have to log in to those accounts again in Boxer and sync to restore email for their personal accounts. Enterprise wipe does the following:

- If the **Remove on Unenroll** setting was selected during the initial Boxer app configuration, Removes the Boxer application during unenrollment from AirWatch.
- Sends a sync request to the app to remove all Boxer data, including email, contacts, and calendar.

  Data is actually removed only after the application syncs. Syncing occurs when the app is active and performs a scheduled sync, or when the user starts the app. If an end user deletes the app before the sync, then the Boxer contacts remain on the device.

Device Wipe Considerations

Standalone enrolled Boxer devices are not managed through AirWatch and no device samples are sent back from device to the UEM console. The enrolled devices are always seen idle on the Device Details page of the UEM console.

You must remove compliance policies that rely on device status from smart groups using Standalone enrollment. If compliance policies are enabled, the UEM consolereports these devices as violating compliance policies and invokes any set actions such as device wipe.

Block Access to IBM Traveler Server

IBM Traveler server can be configured to allow access only to managed devices (AirWatch Agent, AirWatch Container, VMware Workspace One, Standalone Enrollment) using the Traveler's **notes.ini** configuration. This configuration can be edited to allow a client based on Boxer User Agent. Boxer can have a unique user agent string to identify the managed mode for communicating with Traveler server.

Procedure

1. Log onto your Traveler server and locate **notes.ini** configuration file.
2. Open **notes.ini** configuration file and find the `NTS_USER_AGENT_ALLOWED_REGEX` parameter.
3. Add `= AirWatch BoxerManaged` after the `NTS_USER_AGENT_ALLOWED_REGEX` parameter. For example, NTS_USER_AGENT_ALLOWED_REGEX = AirWatch BoxerManaged.
4. (Optional) If you want to allow Boxer managed and un-managed devices but block the native email client from accessing the Traveler server, add `= AirWatch Boxer` after the `NTS_USER_AGENT_ALLOWED_REGEX` parameter. For example, NTS_USER_AGENT_ALLOWED_REGEX = AirWatch Boxer.
5. Select **Save.**

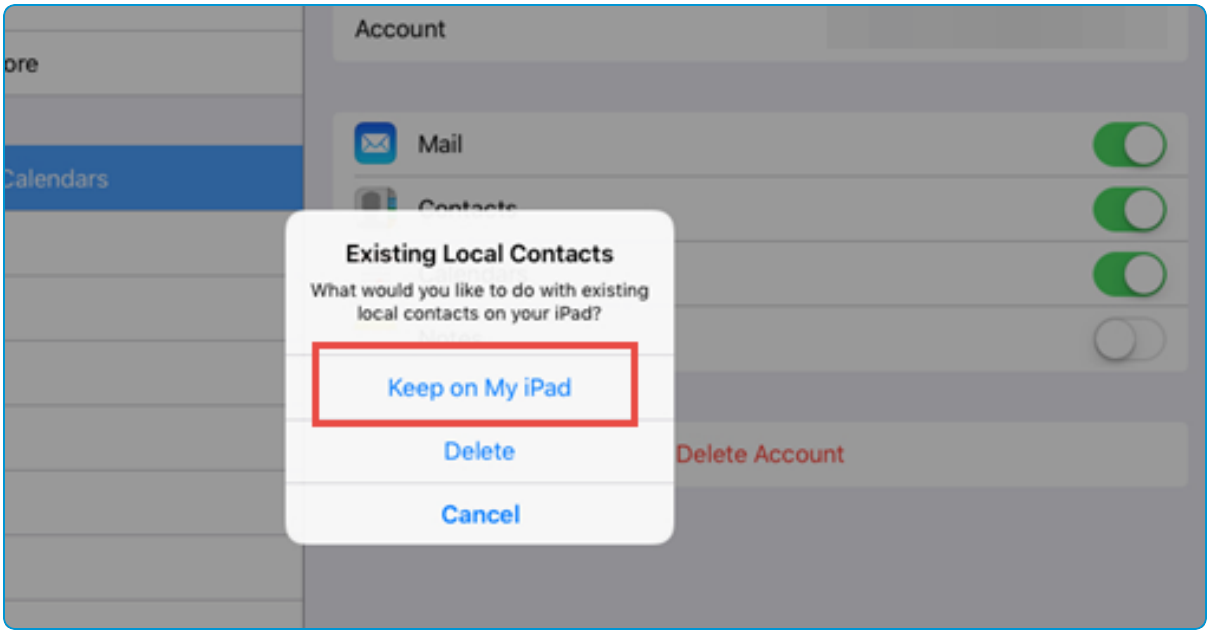
Work around for Third-Party Address Book (iOS Only)

When end users configure an email account using the native iOS Mail settings, they are prompted with a dialog asking what they would like to do with existing local contacts. One option is to **Delete**, which lets end users delete their local address books. If this happens, then the native iOS Address Book is deleted, where Boxer stores its contacts if **Caller ID** is enabled. As a result, end users cannot export Boxer contacts for Caller ID functionality.

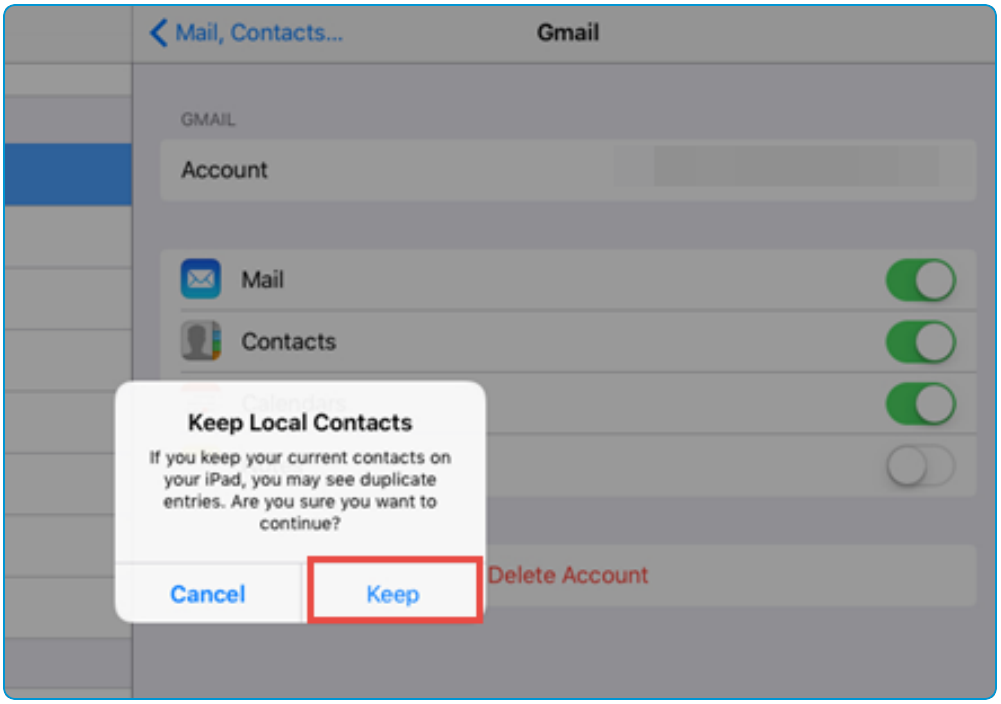
End users can use the following steps to resolve this issue:

1. Navigate to **Mail, Contacts, and Calendar** in **Settings** and turn off **Contacts** sync for all accounts.
2. Start the Boxer app and enable **Caller ID** in **Settings**.
3. Navigate back to the device's **Settings** and under **Mail, Contacts, and Calendar**, turn on **Contacts** sync for all accounts.

   End users are prompted with a dialog box asking them whether or not they want to delete local contacts.
4. Select **Keep on My iPad**.



5. Select **Keep**, when prompted that this may cause duplicates.



Workaround for Sync and Policy Errors on Boxer using IBM Notes

On AirWatch Console v9.2, sync and policy errors are observed on devices configured using email type as IBM Notes with SEG. If the Managed Device policy is set to *ON*, then the device is detected as an unmanaged device. As a result, mail sync is blocked until the next re-council (delta or complete sync). If the Managed Device policy is set to *OFF*, then the device is detected as an unmanaged device. In this case, mail sync is not blocked but the managed device SEG policies are not

applied on the Boxer. You can resolve this errors by changing the Email Type from Lotus Notes to Microsoft Exchange. The issue and workaround applies only for AirWatch Console v9.2.

Perform the following workaround to resolve the issues:

1. Navigate to **Console** > **Email** > **Email Setting** and select **Configure**.
   You can edit an existing MEM configuration if you are using it only for Boxer. If you are using the existing MEM configuration for AirWatch Inbox, you can create a duplicate configuration and apply the settings with the workaround for Boxer.
2. Select **Edit Email Configuration**. The Edit Email Configuration page is displayed.
3. From the Platform tab, select Email Type as **Exchange** and then select any **Exchange** version.
4. Select **Next** to navigate through the tabs and select **Save**.
5. Navigate to **Console** > **Email** > **Email Setting** and verify if the email server type is displayed as Microsoft Exchange.
6. Navigate to **Apps & Books** > **Applications** > **VMware Boxer**.
7. Select **Assign** and then select **Add Assignment**.
8. From Email Settings, select **Email Management**.
9. Choose the email setting configured with Exchange as the email server type.
10. Select **Save & Publish**. Email sync starts and policies are applied on Boxer.

Chapter 4:
VMware Boxer Comparison Matrix

This section provides information about the available features in VMware Boxer when configured with Microsoft Exchange and IBM Lotus Notes server.

VMware Boxer Comparison Matrix for Microsoft Exchange

The following features matrix compares the differences between the iOS and Android versions supported by VMware Boxer when configured with Microsoft Exchange.

Features and Functionality	iOS	Android
Remote Administrative Actions		
Configure email accounts	✓	✓
Wipe all enterprise data and settings	✓	✓
Clear passcode	x	x
Deployment Methods		
VMware AirWatch Container	✓	✓
VMware Workspace One	✓	✓
AirWatch Agent	✓	✓
Standalone Enrollment (email access only)	✓	✓
Application Passcode Policy		
Require Active Directory username and password	x	x
Enforce minimum length	✓	✓
Alphanumeric passcode	✓	✓
Require special characters	✓	✓
Set passcode timeout	✓	✓
Set maximum passcode age	✓	✓

Features and Functionality	iOS	Android
Enforce passcode history	✓	✓
Set maximum failed attempts	✓	✓
TouchID/Fingerprint Integration	✓	✓
Reset Forgotten Passcode	✓	✓
Share passcode across AirWatch apps	✓	✓
Data Loss Prevention		
AES 256-bit SSL encryption in transit	✓	✓
AES 256-bit encryption at rest	✓	✓
Enable or disable adding multiple accounts	✓	✓
Detect compromised devices	✓	✓
Enable or disable copy and paste	✓	✓
Enable or disable screenshots	x	✓
Enable or disable downloading attachments	x	x
Restrict which apps can open attachments	✓	✓
Prevent sending to blacklisted domains	x	x
Restrict sending to whitelisted domains	x	x
Force links to open in VMware Browser	✓	✓
Enable or disable Caller ID	✓	✓
Remote IT Policies		
Set default past days of mail to sync	✓	✓
Set past days of calendar to sync	✓	✓
Ignore SSL errors	x	x
Enable or disable calendar access	x	x
Enable or disable contacts access	x	x
Authenticate account using a certificate	✓	✓
Authenticate account using credentials	✓	✓
Authenticate account using credentials and certificate	✓	✓
Enable or Disable HTML Email	x	x
Configure default email signature	✓	✓
Enable or disable signature editing	x	x

Features and Functionality	iOS	Android
Set maximum attachment size	x	x
Application Settings		
Add multiple accounts	✓	✓
Configure default past days of mail to sync	✓	✓
Configure default past days of calendar to sync	✓	✓
Configure swipe gestures	✓	✓
Configure custom quick responses	✓	✓
Enable or disable displaying local calendars	✓	✓
Enable or disable displaying local contacts	✓	✓
Enable or disable conversation view	✓	✓
Configure undo duration	✓	✓
Configure auto-download of attachments over WiFi	x	✓
Configure week start day	✓	✓
Email Functionality		
Combined inbox for multiple accounts	✓	✓
Send availability	✓	✓
Email quick replies	✓	✓
Reply with event invitation	✓	✓
Predictive email move	✓	✓
Custom boxes (pin individual or combined subfolders)	✓	✓
View event conflicts in event invitations	✓	✓
Filter by flagged or starred	✓	✓
Filter by unread emails	✓	✓
Mark as read/unread/flagged	✓	✓
Bulk actions for emails	✓	✓
View email by conversations (threads)	✓	✓
Search by to/subject	✓	✓
View email sub-folders	✓	✓
Automatically sync email sub-folders	✓	✓
Search contacts in global address list	✓	✓

Features and Functionality	iOS	Android
Save email to drafts	✓	✓
Select all	✓	✓
Select all from sender	✓	x
Configure Out of Office automatic replies	✓	✓
Calendar Functionality		
Search by title or organizer	x	✓
Accept/decline/tentative calendar invites	✓	✓
Create events and send event invitations	✓	✓
Reply to event organizer/attendees	✓	✓
Forward calendar events	✓	✓
One click conference call dialing	✓	✓
View events by month or day	✓	✓
View calendar agenda	✓	✓
Mark meeting as private	✓	✓
View local device calendars	✓	✓
Configure your availability status for meeting (Show As)	✓	✓
Edit recurring event schedule	✓	✓
Respond to individual occurrences of a calendar event series	✓	✓
Respond to event invitation with comments	✓	✓
Configure calendars to display	✓	✓
Contacts Functionality		
Search contacts from global address list	✓	✓
Call and send messages to contacts	✓	✓
Caller ID contact sync	✓	✓
View recent contacts	✓	x
Manage favorite contacts	✓	✓
Create/edit/delete rich contacts	✓	✓
View contact photos from GAL	✓	✓
Information Rights Management		
Read rights managed email messages	✓	✓

Features and Functionality	iOS	Android
Add rights management to composed email messages	✓	✓
Restrict copy-paste (extract allowed)	✓	✓
Restrict printing	✓	✓
Restrict forward	✓	✓
Restrict reply	✓	✓
Restrict reply all	✓	✓
Prevent removing rights management on reply/forward	✓	✓
Restrict modifying recipients on reply/forward	✓	✓
Prevent programmatic access	x	x
Enforce email message content expiration	x	x
Restrict editing message contents (on reply/forward)	✓	✓
Preview rights management protected attachments	x	x
Notifications and Widgets		
Push email notifications (iOS requires email notification service)	✓	✓
Display notifications for calendar events	✓	✓
Enable or disable email widget	x	✓
Enable or disable calendar widget	x	✓
Configure notification preferences	✓	✓
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 previews	✓	✓
View locally saved attachments	✓	✓
Add links to files from Content Solutions	✓	✓
Add files from document providers	✓	✓
Attach from local attachments	✓	✓

Features and Functionality	iOS	Android
Troubleshooting and Diagnostics		
Send logs from application	✓	✓
View device's MDM and email connectivity status	✓	✓
Server Protocol Support		
Microsoft Exchange ActiveSync	✓	✓
IMAP (Personal Accounts Only)	✓	✓
Interoperability		
Microsoft Exchange 2016	✓	✓
Microsoft Exchange 2013	✓	✓
Microsoft Exchange 2010	✓	✓
Microsoft Exchange 2007	✓	✓
Microsoft Exchange 2003	x	x
Microsoft Office 365	✓	✓
Microsoft Office 365 with Modern Auth	✓	✓
IBM SmartCloud	x	x
IBM Lotus Notes 9.0	x	x
Google Apps	x	x

VMware Boxer Comparison Matrix for IBM Notes Traveler

The following features matrix compares the differences between the iOS and Android versions supported by VMware Boxer when configured with IBM Notes Traveler (Lotus Notes Traveler).

Features and Functionality	iOS	Android
Remote Administrative Actions		
Configure email accounts	✓	✓
Wipe all enterprise data and settings	✓	✓
Clear passcode	x	x
Deployment Methods		
VMware AirWatch Container	✓	✓
VMware Workspace One	✓	✓
VMware AirWatch Agent	✓	✓
Standalone Enrollment (email access only)	✓	✓

Features and Functionality	iOS	Android
Application Passcode Policy		
Require Active Directory username and password	x	x
Enforce minimum length	✓	✓
Alphanumeric passcode	✓	✓
Require special characters	✓	✓
Set passcode timeout	✓	✓
Set maximum passcode age	✓	✓
Enforce passcode history	✓	✓
Set maximum failed attempts	✓	✓
TouchID/Fingerprint Integration	✓	✓
Reset Forgotten Passcode	✓	✓
Share passcode across AirWatch apps	✓	✓
Data Loss Prevention		
AES 256-bit SSL encryption in transit	✓	✓
AES 256-bit encryption at rest	✓	✓
Enable or disable adding multiple accounts	✓	✓
Detect compromised devices	✓	✓
Enable or disable copy and paste	✓	✓
Enable or disable screenshots	x	✓
Enable or disable downloading attachments	x	x
Restrict which apps can open attachments	✓	✓
Prevent sending to blacklisted domains	x	x
Restrict sending to whitelisted domains	x	x
Force links to open in VMware Browser	✓	✓
Enable or disable Caller ID	✓	✓
Remote IT Policies		
Set default past days of mail to sync	✓	✓
Set past days of calendar to sync	✓	✓
Ignore SSL errors	x	x
Enable or disable calendar access	x	x

Features and Functionality	iOS	Android
Enable or disable contacts access	x	x
Authenticate account using a certificate	x	x
Authenticate account using credentials	✓	✓
Authenticate account using credentials and certificate	x	x
Enable or Disable HTML Email	x	x
Configure default email signature	✓	✓
Enable or disable signature editing	x	x
Set maximum attachment size	x	x
Application Settings		
Add multiple accounts	✓	✓
Configure default past days of mail to sync	✓	✓
Configure default past days of calendar to sync	✓	✓
Configure swipe gestures	✓	✓
Configure custom quick responses	✓	✓
Enable or disable displaying local calendars	✓	✓
Enable or disable displaying local contacts	✓	✓
Enable or disable conversation view	✓	✓
Configure undo duration	x	✓
Configure auto-download of attachments over WiFi	x	✓
Configure week start day	✓	✓
Email Functionality		
Combined inbox for multiple accounts	✓	✓
Send availability	✓	✓
Email quick replies	✓	✓
Reply with event invitation	✓	✓
Predictive email move	✓	✓
Custom boxes (pin individual or combined subfolders)	✓	✓
View event conflicts in event invitations	✓	✓
Filter by flagged or starred	✓	✓
Filter by unread emails	✓	✓

Features and Functionality	iOS	Android
Mark as read/unread/flagged	✓	✓
Bulk actions for emails	✓	✓
View email by conversations (threads)	✓	✓
Search by to/subject	✓	✓
View email sub-folders	✓	✓
Automatically sync email sub-folders	✓	✓
Search contacts in global address list	✓	✓
Save email to drafts	✓	✓
Select all	✓	✓
Select all from sender	✓	✓
Configure Out of Office automatic replies	✓	✓
Calendar Functionality		
Search by title or organizer	x	✓
Accept/decline/tentative calendar invites	✓	✓
Create events and send event invitations	✓	✓
Reply to event organizer/attendees	✓	✓
Forward calendar events	x	x
One click conference call dialing	✓	✓
View events by month or day	✓	✓
View calendar agenda	✓	✓
Mark meeting as private	✓	✓
View local device calendars	✓	✓
Configure your availability status for meeting (Show As)	✓	✓
Edit recurring event schedule	✓	✓
Respond to individual occurrences of a calendar event series	✓	✓
Respond to event invitation with comments	✓	✓
Configure calendars to display	✓	✓
Contacts Functionality		
Search contacts from global address list	✓	✓
Call and send messages to contacts	✓	✓

Features and Functionality	iOS	Android
Caller ID contact sync	✓	✓
View recent contacts	✓	x
Manage favorite contacts	✓	✓
Create/edit/delete rich contacts	✓	✓
View contact photos from GAL	✓	✓
Information Rights Management		
Support rights managed emails	x	x
Notifications and Widgets		
Push email notifications (iOS requires email notification service)	x	✓
Display notifications for calendar events	✓	✓
Enable or disable email widget	x	✓
Enable or disable calendar widget	x	✓
Configure notification preferences	✓	✓
S/MIME Functionality		
Support S/MIME signed messages	x	x
Attachment Functionality		
Built-in attachment previews	✓	✓
View locally saved attachments	✓	✓
Add links to files from Content Solutions	✓	✓
Add files from document providers	✓	✓
Attach from local attachments	✓	✓
Troubleshooting and Diagnostics		
Send logs from application	✓	✓
View device's MDM and email connectivity status	✓	✓
Server Protocol Support		
Microsoft Exchange ActiveSync	✓	✓
IMAP (Personal Accounts Only)	✓	✓
Interoperability		
Microsoft Exchange 2016	✓	✓
Microsoft Exchange 2013	✓	✓
Microsoft Exchange 2010	✓	✓
Microsoft Exchange 2007	✓	✓

Features and Functionality	iOS	Android
Microsoft Exchange 2003	x	x
Microsoft Office 365	✓	✓
IBM SmartCloud	x	x
IBM Lotus Notes 9.0.1.x	✓	✓
IBM Lotus Notes 8.5.3	x	x
Google Apps	x	x