VMware Browser Admin Guide

Configuring and deploying the VMware Browser

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 the VMware Browser

Overview

The VMware Browser is a Workspace ONE UEM app created to provide your organization a manageable and secure alternative to device native web browsers. As a Workspace ONE UEM admin, you can configure this app in the Workspace ONE UEM console. The configurations you set determine the apps behavior once it deploys to end users. This guide explains the UEM console settings that apply to the VMware Browser, provides a brief explanation of how they impact the deployed apps behavior, and instructions on how to configure these settings.

Security and Encryption

The VMware Browser provides a secure browsing experience that you can tailor to enhance ease of use or security.

VMware Browser security works on multiple configurable levels:

- **Application Level** – Secure VMware Browser at the application level by requiring end users to authenticate with a passcode, biometerics, or Active Directory credentials. Alternatively, you can enable Single Sign On to facilitate ease of use.
- **Tunnel Level** – Use VMware Tunnel certificates to encrypt traffic. Only enrolled and compliant devices are given access to the VMware Tunnel.
- **Website Level** – Disable integrated authentication to require end users to authenticate when they access internal sites.

VMware Browser uses AES-256 for streaming and on disk encryption for downloaded files and browser settings.

Requirements

Meet the requirements listed below to ensure an optimum application deployment.

Supported Devices and Software

Platforms
• iOS 9+ • Android 5+
Broker Apps
• AirWatch Agent • AirWatch Container • Workspace One
Hardware
Samsung DeX (S8 and higher, Note8, and S9 and higher)
Recommended SDK Settings Requirements
App Tunnel
Prior to configuring the SDK, install VMware Tunnel, or integrate an existing third party equivalent with Workspace ONE UEM. Please see Choosing an App Tunnel for more information on meeting this requirement.

**Note: iOS 8 supports VMware Browser only through version 5.10.2. To take advantage of new features and versions, devices must update to iOS 9 or later.

Choosing an App Tunnel

Workspace ONE UEM supports a number of application tunneling (app tunneling) solutions that allow individual applications to authenticate and securely communicate with internal back-end resources. By enabling an app tunnel for a specific set of business applications, you can be certain that unauthorized or malicious apps do not have access to your network.

Supported Technologies

Workspace ONE UEM supports the following technologies for app tunneling using the **Settings and Policies** configuration.

App Tunnel	Description
Standard Proxy	Enables devices to rely on an existing HTTP or SSL Proxy to determine which content the VMware Browser can access.
VMware Tunnel	Accesses corporate content from within your network such as an intranet site. With the VMware Tunnel enabled, you can access internal corporate content on your device. For information on configuring the VMware Tunnel, please see the **VMware Tunnel Admin and Install Guide**.
F5 Proxy	Use to access your internal network as an alternative to the VMware Tunnel.

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
Restrictions	Block the native browser on devices using a restrictions payload to keep end users from using the native browser instead of the VMware Browser.	✓	✓

   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**.

Configure Browser Settings

Configure default SDK Settings to define behaviors that apply to the Browser. Configure browser specific System Settings to define unique application behavior.

1. Navigate to **Groups and Settings > All Settings > Apps > Browser**.
2. Select whether to **Inherit** or **Override** the displayed settings:
   - **Inherit** – Use the settings of the current organization group's parent OG.

- **Override** – Edit and modify the current OG's settings directly.

3. Configure the relevant settings on the **Browser Settings** tab:

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 appropriate profile from the drop-down menu that appears when you enable a **Custom Application Profile** to override default SDK settings.
Android SDK Profile	Select the appropriate profile from the drop-down menu that appears when you enable a **Custom Application Profile** to override default SDK settings.
Use Legacy Settings and Policies	Enable to configure settings and policies for legacy browsers only.
Disable Copy	(Legacy Browsers only) Enable this option to prevent copying from device. Configure this option under **Data Loss Prevention** in **Settings > Apps > Settings and Policies**.
Disable Printing	(Legacy Browsers only) Enable this option to prevent printing from device. Configure this option under **Data Loss Prevention** in **Settings > Apps > Settings and Policies**.
Force Downloads To Open in Content Locker	(Legacy Browsers only) Enable this option to open the force downloaded documents in Content Locker. Configure this option under **Data Loss Prevention** in **Settings > Apps > Settings and Policies**.
Enable AW Tunnel Proxy	(Legacy Browsers only) Enable AW App Tunnel Proxy to access internal network. Configure this option under **Data Loss Prevention** in **Settings > Apps > Settings and Policies**.
iOS SDK Profile (Legacy)	Select the appropriate iOS SDK profile from the drop-down menu for the legacy browser.
General	
Accept Cookies	**Enable** to accept cookies from websites viewed in the VMware Browser.
Clear Cookies Upon Exit	**Enable** to clear cookies when the app fully closes.
Clear Cookies and History if Idle	**Enable** to clear cookies and history if the Browser is idle for x minutes.

Clear Cookies and History if Idle for (mins)	Set the idle time in minutes to a value between 0.5 and 60 to ensure cookies and history are clear.
Remember History	**Enable** to keep track of the sites visited by the user.
Remember History From	Select the length of time you want the app to remember history to from the drop-down menu.
Caching	**Enable** to enhance web performance and reduce perceived lag time. **Disable** to protect browsing data on compromised devices.
Allow Connection to Untrusted Sites	**Disable** if navigating to untrusted sites is a security concern for your organization. **Enable** to give end users maximum navigation flexibility and ease of use.
Sync User Bookmarks	**Enable** this to sync bookmarks across various devices of the same user.
Default View Mode	Set the default view mode for VMware Browser. Select Desktop to set desktop as the default view mode. When selected, the VMware Browser renders the web pages in desktop mode if the websites supports the mode.
Mode	
Kiosk Mode	**Enable** for VMware Browser to function in **Kiosk Mode**. Kiosk Mode removes the navigation bar and limits browsing to the homepage and its available links.
Return Home After Inactivity	Direct the browser back to the home page after a period of **Inactivity (min)**. The values can be greater than or equal to 0.5 minutes.
Clear Cookies and History with Home	Prevent users from accessing the previous user's secure information after they finish using the Browser.
Enable Multiple Tabs Support	You can have multiple tabs opened within kiosk mode. This feature is supported only on iOS and Android devices.
Home Page URL	Define the URL displayed when the browser starts. Leave this field blank to display a 'Recently Visited' page by default.
Selection Mode	**Allow** to limit browsing to domains white listed in the **Allowed Site URLs** field. **Deny** to allow browsing to all sites except those blacklisted in the **Denied Site URLs** field.

Allowed/Denied Site URLs	Utilize the following recommendations to whitelist allowed domains and blacklist denied domains. • Define domain names without including full URLs. The browser filters by domain only, not by folder or page level. • Separate domains with a space, comma, or a new line. • Define wildcards as part of the domains; listing items from most general to specific. Example: *google.com is more general than http://yahoo.com. Entering *.google.com whitelists <text>.google.com, but it *does not* allow access to http://google.com. • Leave out the scheme (http:// or https://) to test the domain for both schemes. Include the scheme to limit testing to the specified scheme. • You can enter Port value separately. Restricted URL can contain the complete path, for example, http:// google.com:9191.
Allow IP Browsing	Select to whitelist IP addresses for browsing. A user can navigate to a whitelisted IP address even if the actual domain for the IP address was included in the Denied Site URL listing.
Allowed IP Addresses	Whitelist IP addresses using the following recommendations: • Enter values in IPv4 formatting with four octets each separated by a period. • Enter wildcards to whitelist octets. Adding an entry that includes a * in each octet allows browsing to any IP address.
Terms of Use	
Required Terms of Use	Select the appropriate agreement from the drop-down menu. For all internal Workspace ONE UEM apps, including the VMware Browser, you can implement a single Terms of Use Agreement for end users to accept. This agreement applies to all Workspace ONE UEM internal applications, and eliminates the need for end users to accept the same agreement multiple times, across apps. You can configure and manage your Terms of Use Agreements by navigating to **Groups and Settings > All Settings > System > Terms of Use.** For more information, please see the **VMware AirWatch Mobile Device Management Guide**.

4. Select the **Bookmarks** tab. Provide the following information to define and push a list of bookmarks to the VMware Browser:

Setting	Description
URLs for Predefined Bookmarks in Browser	Configure bookmarks to display as a URL address or with a friendly name.
Name	Provide text in this field to display as the friendly name. Leave this field blank to display the URL as the bookmark name.
URL	Provide the bookmark URL.

Setting	Description
Add Bookmark	Select to add additional bookmarks.

5. Do not configure any settings on the **Notifications** tab unless a Workspace ONE UEM representative provided you with configuration instructions.
6. Select **Save**.

Application Configurations for VMware Browser

You can configure Browser settings using the Configuration Key and Configuration Value pairs provided by AirWatch. To configure Browser settings, enter the configuration key and the corresponding value into the **Custom Settings** under **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.

Configuration Key	Value Type	Configuration Value	Description
{"BrowserDisableQRCode": "true"}	Boolean	True or False	(Available for Android and iOS) If the value is true, the QR Code scanner in VMware Browser URL bar is disabled. If the value is false, the QR Code scanner is displayed in the VMware Browser URL bar.
{“BrowserDisableUserAgentString” : "true”}	Boolean	True or False	(Available for Android only) If the value is true, the user agent string is disabled. However this also disables the ability to switch between desktop mode and mobile mode. If the value is false, the user agent string will be enabled and also enables the ability to switch between desktop mode and mobile mode.
{BrowserDisableAutoCloseTab": "true" }	Boolean	True or False	(Available for iOS only) If the value is true, VMware Browser does not auto-close the tab that launches an external application. If the value is false, VMware Browser auto-closes the tab that an external application.

Configuration Key	Value Type	Configuration Value	Description
{BrowserDisableWebclip":"true"}	Boolean	True or False	(Available for Android and iOS) By default, the Webclips are shown in the Browser Bookmarks. If the value is set to true, the Webclips do not appear in the Browser Bookmarks.

Admin Policies for Privacy and Data Collection

Use the configuration keys in the UEM console to perform additional privacy disclosure and data collection practices. End users who are upgrading or beginning to use the latest version (from v6.14 onwards on iOS and Android platform) are presented with new privacy dialog screen upon the application launch.

The privacy dialog screen lets the user know the following device information is fetched by the application:

- **Data collected by the app** – Provides a summary of data that is collected and processed by the application. Some of this data will be visible to 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 will be shown to the user to contact their employer for more information. We recommend customers to configure their privacy policy URL in the UEM console. Once configured, the user will be able to open the employer's privacy policy within the app.

Enter the configuration key and the corresponding value into the **Custom Settings** under **Groups & Settings > All Settings > Apps > Settings and Policies > Settings** to enable privacy and data collection policies.

Configuration Key	Value Type	Configuration Value	Description
{ "PolicyAllowFeatureAnalytics" }	Integer	0 - disabled 1 - enabled (default)	This is a Feature analytics data collection admin policy that controls whether the end users see the Data Sharing opt-in during configuration of the Browser. When set to 0, the data sharing screen is forced off to the user. When set to 1, the data sharing screen is displayed to the user. **Note:** Feature analytics data is collected for VMware to improve existing product features and invent new ones to make users even more productive.

{ "PolicyAllowCrashReporting" }	Boolean	True False	This is a Crash reporting data collection admin policy that controls the application reporting diagnostic data, which can be used to troubleshoot crash issues and provide support. If true, crash reports are reported back to VMware. If false, crash reports are not reported back to VMware. Thus impacting the efficiency in investigating and resolving any issues with the application.
{ "PrivacyPolicyLink" }	String	"https://www.url.com"	Provide the company or customer privacy policy URL that the users can view a specific privacy disclosure web page directly with the Browser. **Note:** This policy overrides the default company privacy policy URL.

SCEP Integrated Authentication

Use the integrated authentication with authentication type set to SCEP certificates in the UEM console by configuring the following key value pairs.

Configuration Key	Value Type	Configuration Value	Description
ScepPendingRetryTimeout	Integer	Min and max values	Provide the time duration after which the SCEP pending retry will timeout.
ScepPendingMaxRetryAttempts	Integer	Min and max values	Provide the maximum retry count for the SCEP certificate to update on the device.

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 July 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**.

(iOS Only) Configure Import Restriction in Content Locker

You can use the configuration keys in AirWatch Console to restrict import of content from third-party applications into the Content Locker. The configuration keys can be used to allow content import from only whitelisted set of native applications.

Use the following configuration keys to restrict or allow content import from third-party applications into Content Locker.

Configuration Key	Value Type	Supported Values	Description
{"ContentImportRestriction"}	Boolean	true = restriction enabled false = restirction disabled For example, {"ContentImportRestriction": true}.	When enabled, device users cannot import content from any non-whitelisted third-party applications including the native iOS applications into the Content Locker.
{"ContentImportAllowNativeApps"}	Boolean	true = import from native applications are allowed false = import from native applications are not allowed For example, {"ContentImportAllowNativeApps": true}	When enabled, the device users can import content from native applications when the import restriction is enabled.

The ContentImportRestriction and ContentImportAllowNativeApps configuration values can be used in combination to configure the import restriction as per your requirement. If you want to allow import of content from all native apps, enable the ContentImportAllowNativeApps key. The ContentImportAllowNativeApps key is enabled by default and allows import from all native apps such as iOS native Email, Files, Safari, AirDrop, and such. When enabled, the device users can open and import content from non-whitelisted apps into Content Locker using the web versions of the non-whitelisted applications (using Safari).

If you want to allow only specific applications, disable the ContentImportAllowNativeApps key and add the allowed applications in the whitelist.

If you want to restrict importing of content from specific native apps, disable the ContentImportAllowNativeApps key and add the allowed native applications in the whitelist.

Note: The Limit Documents to Open Only in Approved Apps option must be enabled in the Data Loss Prevention settings before enabling the configuration key values. Safari and AirDrop cannot be whitelisted as there is no associated bundle ID.

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 allow import only from native apps, { "ContentImportRestriction": true, "ContentImportAllowNativeApps": true}.
4. To allow importing from a specific list of apps (whitelist):
   a. Navigate to **Settings and Policies** > **Security Policies**.
   b. Select the **Allowed Applications List** text box and list the applications you want to allow the users to import content into the Content Locker.
5. Select **Save**.

If you are using a custom SDK profile for Content Locker:

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 configuration keys as per your requirement. For example to allow import only from native apps, { "ContentImportRestriction": true, "ContentImportAllowNativeApps": true}.
5. From the Restriction section, select **Restrict documents to be opened in following apps** and add the list of apps that you want to allow as per your requirement (whitelist).
6. Select **Save**.

(iOS Only) Configure PDF Autosave in Content Locker

From Content Locker v4.13.2, the device users can enable or disable the PDF Autosave functionality by using the Enable PDF Autosave setting in the Content Locker app. The PDF Autosave setting is disabled by default. The PDF Autosave function can be set to 30 seconds, 60 seconds, and 120 seconds respectively using the Autosave time in seconds setting in the Content Locker. The administrators can use the configuration key provided by VMware AirWatch in the AirWatch Console to force enable the PDF Autosave functionality in Content Locker. When enabled using the configuration key, the device users cannot disable the PDF Autosave function and the Enable PDF Autosave setting is unavailable in the Content Locker. When the PDF Autosave function is enabled, the changes made to a PDF file when an autosave is in progress are not saved. After every instance of an autosave, the PDF document is reloaded.

Use the following configuration key to enable PDF Autosave function is Content Locker:

Configuration Key	Value Type	Supported Values	Description
{ "ContentPDFAutoSaveEnabled" }	Boolean	true = enabled false = can be enabled or disabled by the device user	When set to True, the PDF Autosave functionality is enabled and the device users cannot disable the setting. The Enable PDF Autosave setting in the Content Locker is unavailable to the device users.

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 PDF Autosave, { "ContentPDFAutoSaveEnabled": true }.
4. Select **Save**.

If you are using a custom SDK profile for Content Locker:

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 configuration keys as per your requirement.
   For example, to enable PDF Autosave, { "ContentPDFAutoSaveEnabled": true }.
5. Select **Save**.

Expected Behavior for SDK Authentication

Enabling or disabling SSO determines the number of app sessions established, impacting the number of authentication prompts end users receive.

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:
VMware Browser Deployment

Overview

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 VMware Browser

Configure Browser app to deploy as a public application and utilize this simplified deployment workflow to seamlessly push Browser 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**.

Accessing SDK and Wrapped App Logs by Log File

After you Enable **Logging** in **Settings and Policies**, you can review collected logs from the **App Logs** page:

1. Navigate to **Apps & Books > Applications > Analytics > App Logs**.
2. Download or delete logs using the actions menu.

Accessing Logs by the View Logs Page

Use the View Logs feature from the actions menu to quickly access available log files pertaining to applications that use SDK functionality.

1. Navigate to **Apps & Books > Applications > Native** and select the **Internal** tab.
2. Select the application.
3. Select the **View Logs** option from the actions menu.

Accessing SDK Event Analytics for a Specific Application

After you Enable **Analytics** when you created your SDK profile in **Settings and Policies**, you can export analytics data for your Apple iOS applications built using the SDK or using SDK functionality.

1. Navigate to **Apps & Books > Applications > Native > Internal**.
2. Select the SDK application to display the Details View page.
3. Choose **View > Analytics** from the actions menu.

Accessing SDK Analytics Apps that Use SDK Functionality

This feature displays events and data usage information for applications that use SDK functionality. Workspace ONE UEM reports event analytics by the application ID and event name and data usage analytics by device.

Analytic Type	Description	How to Access
Event Analytics	These events are custom created and developers can code any process or behavior they want to track.	1. Navigate to **Apps & Books > Applications > Analytics > SDK Analytics**. 2. View events for SDK applications and retrieve data including application ID, the device on which it happened, and the event name.
Data Usage Analytics	These events are embedded in the PLIST file for the Apple iOS application by the developer. They track telecom usage for SDK developed applications.	1. Navigate to **Telecom > List View**. 2. Select devices that have the application installed and navigate to **Details View**. 3. View data for the SDK application on the **Telecom** tab and use the **Export** option to retrieve a .CSV version of the data.

Appendix:
VMware Browser Features Matrix

This section outlines the available VMware Browser features by platform, reflecting the app versions available as of July 2018.

VMware Browser Compatibility Matrix by Platform

Features	iOS	Android
Browsing Settings		
Restrict Access to Only Whitelisted Sites	✓	✓
Restrict Access Based on Blacklisted Sites	✓	✓
IP Browsing	✓	✓
Set Default Home Page URL with Support for Lookup Values	✓	✓
Kiosk Mode	✓	✓
Return Home after Configurable Inactivity Period	✓	✓
Clear Cookies and History with Home	✓	✓
Security Wi-Fi/Roaming Restrictions	✓	✓
Multiple Tabs Support	✓	
Security		
Data Loss Prevention		
Disable Cookies	✓	✓
Clear Cookies Upon Exit	✓	✓
Remember History	✓	✓
Clear Cookies and History if Idle for Predefined Period	✓	✓
"awb://" and "awbs://" Protocols Force Links to Open in VMware Browser	✓	✓
Enable caching	✓	✓
Limit Access Based on Network Connection		
Limit Access if Roaming		✓
Limit Access if using Cellular Network	✓	✓
Limit Access Based on SSID	✓	✓
Authentication		
Basic	✓	✓
AD/LDAP	✓	✓

Features	iOS	Android
Second Factor Passcode	✓	✓
Single Sign On	✓	✓
Biometrics	✓	✓
Encryption		
SSL Encryption in Transit	✓	✓
AES 256-Bit Encryption at Rest	✓	✓
Browser Interface		
Document Support		
Display PDF Documents	✓	✓ ***
Display MS Office Documents (PowerPoint, Word, Excel)	✓	✓ ***
Display MAC Documents (Keypoint, Pages, Numbers)	✓	✓ ***
Navigation and UI		
History	✓	✓
Bookmarks	✓	✓
Predefined Bookmarks	✓	✓
Friendly Name for Bookmarks	✓	✓
Universal Bar for Search and Navigation	✓	✓
See Allowed Sites (when whitelisting is enabled)	✓	✓
Tabbed Browsing	✓	✓
Javascript Popup Support	✓	✓
Browse HTML-based Websites (HTML, PHP, etc.)	✓	✓
HTML5, CSS3 & JavaScript	✓	✓
AJAX Support	✓	✓
W3C DOM	✓	✓
Request Desktop	✓	✓
Protocols		
Http/Https and Awb/Awbs Protocols	✓	✓
Ftp/Ftps Protocol	✓	
Market:// (Google Play Store)		✓
General		
Customizable Terms of Use	✓	✓
NTLM	✓	✓ **

*Clears only history, not cookies

**Due to platform limitations, Android Browser only supports NTLM v1.

***VMware Browser for Android uses VMware Content Locker to display PDF and MS Office documents. VMware Content Locker does not support MAC documents, hence other third party apps must be used to display MAC documents.

Chapter 5: 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	Browser	
	iOS	Android
Force Token For App Authentication: Enable	✓	✓
Passcode: Authentication Timeout	✓	✓
Passcode: Maximum Number Of Failed Attempts	✓	✓
Passcode: Passcode Mode Numeric	✓	✓
Passcode: Passcode Mode Alphanumeric	✓	✓
Passcode: Allow Simple Value	✓	✓
Passcode: Minimum Passcode Length	✓	✓
Passcode: Minimum Number Complex Characters	✓	✓
Passcode: Maximum Passcode Age	✓	✓
Passcode: Passcode History	✓	✓
Biometric Mode: Fingerprint	✓	✓

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

UI Label	Browser	
	iOS	Android
NAC: Wi-Fi Connection	✓	✓
Branding: Enable	✓	x
Branding: Toolbar Color	x	x
Branding: Toolbar Text Color	x	x
Branding: Primary Color	✓	x
Branding: Primary Text Color	✓	x
Branding: Secondary Color	x	x
Branding: Secondary Text Color	✓	x
Branding: Organization Name	✓	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	✓	✓
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.