

# VMware Browser Admin Guide

Configuring and deploying the VMware Browser

Workspace ONE UEM v9.4

**Have documentation feedback?** Submit a Documentation Feedback support ticket using the Support Wizard on [support.air-watch.com](https://support.air-watch.com).

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

# Table of Contents

---

<b>Chapter 1: Overview</b>	<b>3</b>
Introduction to the VMware Browser	4
Security and Encryption	4
Requirements	4
<b>Chapter 2: Initial Configurations</b>	<b>6</b>
Configure Profile Payloads	7
<b>Chapter 3: App Suite SDK Configurations</b>	<b>8</b>
Default vs Custom SDK Profiles	9
Custom SDK Profile Settings	9
Configure Default SDK Security Settings	10
Expected Behavior for SDK Authentication	16
Apply SDK Settings to the Android Agent	16
Apply SDK Settings to the iOS Agent	16
<b>Chapter 4: Application Configuration</b>	<b>18</b>
Configure Browser Settings	19
Application Configurations for VMware Browser	22
<b>Chapter 5: Application Deployment</b>	<b>23</b>
Overview of Workspace ONE UEM Application Deployment	24
Deploy Workspace ONE UEM Applications	24
Accessing SDK Event Analytics for a Specific Application	24
Accessing SDK Analytics Apps that Use SDK Functionality	25
<b>Appendix: VMware Browser Features Matrix</b>	<b>26</b>
SDK Profiles, Policies and Settings Compatibility	29

# Chapter 1:

## Overview

- Introduction to the VMware Browser .....4
- Security and Encryption .....4
- Requirements .....4

## Introduction to the VMware Browser

The VMware Browser is an Workspace ONE UEM app created to provide your organization a manageable and secure alternative to device native web browsers. As an 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, biometrics, 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
<b>Platforms</b> <ul style="list-style-type: none"> <li>• iOS 9+</li> <li>• Android 5+</li> </ul>
<b>Broker Apps</b> <ul style="list-style-type: none"> <li>• AirWatch Agent</li> <li>• AirWatch Container</li> <li>• Workspace One</li> </ul>
<b>Hardware</b> <p>Samsung DeX (S8 and higher, Note8, and S9 and higher)</p>
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 till v5.10.2. To take advantage of new features and versions, devices need to 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
<b>Standard Proxy</b>	Enables devices to rely on an existing HTTP or SSL Proxy to determine which content the VMware Browser can access.
<b>VMware Tunnel</b>	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 <b>VMware Tunnel Admin and Install Guide</b> .
<b>F5 Proxy</b>	Use to access your internal network as an alternative to the VMware Tunnel.

# Chapter 2:

## Initial Configurations

Configure Profile Payloads .....	7
----------------------------------	---

## 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
<b>Restrictions</b>	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**.

# Chapter 3:

## App Suite SDK Configurations

Default vs Custom SDK Profiles .....	9
Custom SDK Profile Settings .....	9
Configure Default SDK Security Settings .....	10
Expected Behavior for SDK Authentication .....	16
Apply SDK Settings to the Android Agent .....	16
Apply SDK Settings to the iOS Agent .....	16



## 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
<b>Implementation</b>	Share SDK profile settings across <i>all</i> applications set up at a particular organization group (OG) or below.	Apply SDK profile settings to a <i>specific</i> application, and override the Default Settings SDK profiles.
<b>Advantage</b>	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.
<b>Configure</b>	<b>Groups &amp; Settings &gt; All Settings &gt; Apps &gt; Settings and Policies &gt; Security Policies</b>	<b>Groups &amp; Settings &gt; All Settings &gt; Apps &gt; Settings and Policies &gt; Profiles</b>
<b>Read More</b>	Continue reading this section to learn which default SDK profiles apply to deployed apps.	Learn more about custom SDK profile settings in the <b>VMware Workspace ONE UEM Mobile Application Management Guide</b> .

## 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 settings 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
<b>Authentication Method</b>	Defaults to Single Sign-On. Ensure you require MDM enrollment so that Single Sign-On can function properly.
<b>iOS Profile</b>	Select a custom-created SDK profile from the drop-down list the settings profile for iOS devices.
<b>Android Profile</b>	Select a custom-created SDK profile from the drop-down list the settings profile for Android devices.

Setting	Description
<b>Use Legacy Settings and Policies</b>	Only enable legacy settings if directed to do so by an Workspace ONE UEM representative. Legacy settings do not leverage Shared SDK profile settings and should only be implemented in certain edge cases.
<b>Default Authentication Method</b>	Select the authentication method for the applications.
<b>Enable "Keep me signed in"</b>	Enable to allow end users to remain signed in between uses.
<b>Maximum Number of Failed Attempt</b>	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.
<b>Authentication Grace Period (min)</b>	Enter the time (in minutes) after closing the VMware Content Locker before reopening the VMware Content Locker will require users to enter credentials again.
<b>Prevent Compromised Devices</b>	Enable to prevent compromised devices from accessing VMware Content Locker.
<b>Enable Offline Login Compliance</b>	Enable to allow offline login compliance.
<b>Maximum Number of Offline Logins</b>	Enter the number of offline logins allowed before you have to go online.

## Configure Default SDK Security Settings

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

### Before You Begin

Not all platforms or Workspace ONE UEM applications support all available default SDK profile settings. A configured setting only expresses as a device side behavior when it has a full platform and app-side support. This also means that an enabled setting might not express 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
- Enrolled devices
- Workspace ONE UEM Inbox
- Workspace ONE UEM or wrapped apps
- VMware Content Locker
- SDK settings available as of April 2018.

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

Action	Description	Rec
<b>Authentication Type</b>		
<b>Passcode</b>	Prompt end users to authenticate with a user-generated passcode when the app first starts, and after an app session timeout. Enabling or disabling SSO determines the number of app sessions that get established.	–
<b>Username and Password</b>	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.	–
<b>Disabled</b>	Allow end user to open apps without entering credentials.	✓
<b>SSO</b>		
<b>Enabled</b>	Establish a single app session across all Workspace ONE UEM and Workspace ONE UEM wrapped apps.	✓
<b>Disabled</b>	Establish app sessions on a per app basis.	–

Action	Description	Rec
<b>Integrated Authentication</b>		
<b>Enabled</b>	Provide end users access to corporate sites without prompting for credentials. Choose the method of integrated authentication that works best with your organization's set up.	√
	<b>Enable Kerberos</b>	
	<b>Use Enrollment Credentials</b>	
	Access corporate resources listed in the <b>Allowed Sites</b> field with the SSO credentials.	
	<b>Use Certificate</b>	
	Perform any of the below options to access corporate resources listed in the <b>Allowed Sites</b> field with the integrated authentication. <ul style="list-style-type: none"> <li>• Upload the certificate</li> <li>• Set a <b>Defined Certificate Authority</b></li> <li>• Use a <b>User Certificate</b> (S/MIME signing cert)</li> <li>• Set to <b>Derived Credentials</b> and select the appropriate <b>Key Usage</b> based on how the certificate is used. Key Usage options are <b>Authentication</b>, <b>Signing</b>, and <b>Encryption</b>. For more information on Derived Credentials, refer <b>VMware Workspace ONE UEM PIV-D Manager Deployment Guide</b>.</li> </ul>	
	<b>Allowed Sites</b>	
	Enter systems in the field to control access to a specific set of sites and domains. You must complete this setting for <b>Integrated Authentication</b> to work. This setting ensures that Workspace ONE UEM does not expose credentials to non-trusted resources.	
<b>Disabled</b>	Require end users to authenticate each time their browser attempts to reach the corporate network.	–
<b>Compromised Protection</b>		
<b>Enabled</b>	Override MDM protection. App level Compromised Protection blocks compromised devices from enrolling, and enterprise wipes enrolled devices that report a compromised status.	√
<b>Disabled</b>	Rely solely on the MDM compliance engine for compromised device protection.	–

Action	Description	Rec
<b>Workspace ONE UEM App Tunnel</b>		
<b>Enabled</b>	Direct specified browser traffic through the App Tunnel, and send unspecified traffic through the internet.	√
	<b>App Tunnel Mode</b>	
	Workspace ONE UEM recommends that you complete tunnel installation, configuration, and integration prior to configuring the SDK. Then, select your organization's tunnel from the available options.	
	<ul style="list-style-type: none"> <li>• <b>VMware Tunnel</b> – Devices access corporate resources using the VMware Tunnel as a relay between mobile devices and enterprise systems.</li> <li>• <b>F5</b> – Devices access web services behind a firewall. The firewall's defined policies allow secure connections through your F5 components. Use to access your internal network as an alternative to the VMware Tunnel.</li> <li>• <b>Standard Proxy</b> – Filter device traffic using an existing HTTP or SSL Proxy.</li> </ul>	
	<b>App Tunnel Proxy</b>	
	Select from the menu the proxy you want to use to access your internal network.	
	<b>App Tunnel URLs</b>	
	Enter trusted resources or sites in the field to restrict communication to the listed set of tunnel domains. Users access these internal sites using the app tunnel while Workspace ONE UEM sends the rest of the traffic through the internet.	
	<ul style="list-style-type: none"> <li>• Disable Content Filter to send unlisted traffic directly to the internet.</li> <li>• Leave field blank to direct all traffic through the tunnel.</li> <li>• Use wildcards or the port number to allow access to any site with a domain subset and to access any port on that site. For example, <b>&lt;example&gt;.com*</b> or <b>&lt;example&gt;.com:8080</b>. <ul style="list-style-type: none"> <li>◦ If the site is accessed over a non-standard port, that is any port other than 80 or 443, the port number should be explicitly mentioned or a wildcard * must be added to the end of the domain.</li> </ul> </li> </ul>	
<b>Disabled</b>	Send all traffic through the internet.	–
<b>Content Filtering</b>		
<b>Enabled</b>	Ensure the security of <i>iOS device traffic</i> entering your network.	–
<b>Disabled</b>	Route traffic without the use of a third-party filter.	√
<b>Geofencing</b>		
<b>Enabled</b>	Restrict access to applications as defined at <b>Device &gt; Profiles &gt; Profile Settings &gt; Geofencing</b> . Enabling this setting limits the availability of your app suite.	–
<b>Disabled</b>	Maximize app accessibility.	√

Action	Description	Rec
<b>Data Loss Prevention</b>		
<b>Enabled</b>	Access and configure settings intended to reduce data leaks.	√
	<b>Enable Printing</b>	
	Allows an application to print from devices when set to <b>Yes</b> .	
	<b>Enable Camera</b>	
	Allows applications to access the device camera when set to <b>Yes</b> .	
	<b>Enable Composing Email</b>	
	Allows an application to use the native email client to send emails when set to <b>Yes</b> .	
	<b>Enable Copy And Paste Out</b>	
	Allows users to copy and paste data from Workspace ONE UEM applications (containerized applications such as Boxer, Browser, Content Locker) to external applications (non-containerized applications). Select <b>No</b> to allow copy and paste actions only between Workspace ONE UEM apps.	
	<b>Enable Copy And Paste Into</b>	
	Allow users to cut, copy, and paste data from external applications (non-containerized applications) into Workspace ONE UEM applications (containerized applications such as Boxer, Browser, Content Locker).	
	<b>Enable Data Backup</b>	
	Allows wrapped applications to sync data with a storage service like iCloud when set to <b>Yes</b> .	
	<b>Enable Location Services</b>	
	Allows wrapped applications to receive the latitude and longitude of the device when set to <b>Yes</b> .	
	<b>Enable Bluetooth</b>	
	Allows applications to access Bluetooth functionality on devices when set to <b>Yes</b> .	
	<b>Enable Screenshot</b>	
	Allows applications to access screenshot functionality on devices when set to <b>Yes</b> .	
	<b>Enable Watermark</b>	
	Displays text in a watermark in documents in the VMware Content Locker when set to <b>Yes</b> . Enter the text to display in the <b>Overlay Text</b> field or use lookup values. You cannot change the design of a watermark from the UEM console.	
	<b>Limit Documents to Open Only in Approved Apps</b>	
	Enter options to control the applications used to open resources on devices.	
	<b>Allowed Applications List</b>	
	Enter the applications that you allow to open documents.	

Action	Description	Rec
Disabled	Allow end user access to all device functions.	–
Network Access Control		
Enabled	Set cellular and wi-fi parameters that restrict device network access.	–
Disabled	Maximize usability and access.	✓

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 Workspace ONE UEM 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: <ul style="list-style-type: none"> <li>• <b>Error</b> – Records only errors. An error displays failures in processes such as a failure to look up UIDs or an unsupported URL.</li> <li>• <b>Warning</b> – Records errors and warnings. A warning displays a possible issue with processes such as bad response codes and invalid token authentications.</li> <li>• <b>Information</b> – Records a significant amount of data for informational purposes. An information logging level displays general processes as well as warning and error messages.</li> <li>• <b>Debug</b> – Records all data to help with troubleshooting. This option is not available for all functions.</li> </ul>	
	Send logs over Wi-Fi only	
	Select to prevent the transfer of data while roaming and to limit data charges.	
Disabled	Do not collect any logs.	–
Analytics		
Enabled	Collect and view useful statistics about apps in the SDK suite.	✓
Disabled	Do not collect useful statistics.	–
Custom Settings		
Enabled	Apply custom XML code to the app suite.	–
Disabled	Do not apply custom XML code to the app suite.	✓

6. **Save.**

## Expected Behavior for SDK Authentication

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
<b>Disabled</b>	Enabled	Single	Enrollment Credentials	Open apps without prompting end users to enter credentials.
<b>Passcode</b>	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.
<b>Username and Password</b>	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.
<b>Passcode</b>	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.
<b>Username and Password</b>	Disabled	Per App	Enrollment Credentials	Prompts on a per app basis, establishing individual app sessions. The next authentication prompt occurs when launching a new app, or an individual app session times out.

## Apply SDK Settings to the Android Agent

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

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

## Apply SDK Settings to the iOS Agent

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

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



<Organization Group>.

3. **Save** your settings.

# Chapter 4:

## Application Configuration

Configure Browser Settings .....	19
Application Configurations for VMware Browser .....	22

## Configure Browser Settings

Configure default SDK Settings to define behaviors that apply to all Workspace ONE UEM apps. Configure app 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
<b>Settings and Policies</b>	
<b>Application Profile</b>	<p>Select an application profile to apply SDK functionality to your app.</p> <ul style="list-style-type: none"> <li>• <b>Default</b> – Allow applications to use the default security policies and settings defined under <b>Apps and Books &gt; Settings &gt; Settings and Policies</b>.</li> <li>• <b>Custom</b> – Override default settings and apply custom profiles. Custom profiles use the security policies and settings defined under <b>Apps and Books &gt; Settings &gt; Settings and Policies &gt; Profiles</b>.</li> </ul>
<b>iOS SDK Profile</b>	Select the appropriate profile from the drop-down menu that appears when you enable a <b>Custom Application Profile</b> to override default SDK settings.
<b>Android SDK Profile</b>	Select the appropriate profile from the drop-down menu that appears when you enable a <b>Custom Application Profile</b> to override default SDK settings.
<b>Use Legacy Settings and Policies</b>	Enable to configure settings and policies for legacy browsers only.
<b>Disable Copy</b>	(Legacy Browsers only) Enable this option to prevent copying from device. Configure this option under <b>Data Loss Prevention</b> in <b>Settings &gt; Apps &gt; Settings and Policies</b> .
<b>Disable Printing</b>	(Legacy Browsers only) Enable this option to prevent printing from device. Configure this option under <b>Data Loss Prevention</b> in <b>Settings &gt; Apps &gt; Settings and Policies</b> .
<b>Force Downloads To Open in Content Locker</b>	(Legacy Browsers only) Enable this option to open the force downloaded documents in Content Locker. Configure this option under <b>Data Loss Prevention</b> in <b>Settings &gt; Apps &gt; Settings and Policies</b> .
<b>Enable AW Tunnel Proxy</b>	(Legacy Browsers only) Enable AW App Tunnel Proxy to access internal network. Configure this option under <b>Data Loss Prevention</b> in <b>Settings &gt; Apps &gt; Settings and Policies</b> .
<b>iOS SDK Profile (Legacy)</b>	Select the appropriate iOS SDK profile from the drop-down menu for the legacy browser.

General	
Accept Cookies	<b>Enable</b> to accept cookies from websites viewed in the VMware Browser.
Clear Cookies Upon Exit	<b>Enable</b> to clear cookies when the app fully closes.
Encrypt Cookies	Select <b>Disabled</b> for maximum app performance. <b>Enable</b> cookie encryption to add a further layer of security.
Clear Cookies and History if Idle	<b>Enable</b> 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	<b>Enable</b> 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	<b>Enable</b> to enhance web performance and reduce perceived lag time. <b>Disable</b> to protect browsing data on compromised devices.
Allow Connection to Untrusted Sites	<b>Disable</b> if navigating to untrusted sites is a security concern for your organization. <b>Enable</b> to give end users maximum navigation flexibility and ease of use.
Sync User Bookmarks	<b>Enable</b> 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	<b>Enable</b> for VMware Browser to function in <b>Kiosk Mode</b> . 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 <b>Inactivity (min)</b> . 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.

<b>Selection Mode</b>	<p><b>Allow</b> to limit browsing to domains white listed in the <b>Allowed Site URLs</b> field.</p> <p><b>Deny</b> to allow browsing to all sites except those blacklisted in the <b>Denied Site URLs</b> field.</p>
<b>Allowed/Denied Site URLs</b>	<p>Utilize the following recommendations to whitelist allowed domains and blacklist denied domains.</p> <ul style="list-style-type: none"> <li>Define domain names without including full URLs. The browser filters by domain only, not by folder or page level.</li> <li>Separate domains with a space, comma, or a new line.</li> <li>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 &lt;text&gt;.google.com, but it <i>does not</i> allow access to http://google.com.</li> <li>Leave out the scheme (http:// or https://) to test the domain for both schemes. Include the scheme to limit testing to the specified scheme.</li> <li>You can enter Port value separately. Restricted URL can contain the complete path, for example, http:// google.com:9191.</li> </ul>
<b>Allow IP Browsing</b>	<p>Select to whitelist IP addresses for browsing.</p> <p>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.</p>
<b>Allowed IP Addresses</b>	<p>Whitelist IP addresses using the following recommendations:</p> <ul style="list-style-type: none"> <li>Enter values in IPv4 formatting with four octets each separated by a period.</li> <li>Enter wildcards to whitelist octets. Adding an entry that includes a * in each octet allows browsing to any IP address.</li> </ul>
<b>Terms of Use</b>	
<b>Required Terms of Use</b>	<p>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.</p> <p>You can configure and manage your Terms of Use Agreements by navigating to <b>Groups and Settings &gt; All Settings &gt; System &gt; Terms of Use</b>. For more information, please see the <b>VMware Workspace ONE UEM Mobile Device Management Guide</b>.</p>

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

Setting	Description
<b>URLs for Predefined Bookmarks in Browser</b>	Configure bookmarks to display as a URL address or with a friendly name.

Setting	Description
<b>Name</b>	Provide text in this field to display as the friendly name. Leave this field blank to display the URL as the bookmark name.
<b>URL</b>	Provide the bookmark URL.
<b>Add Bookmark</b>	Select to add additional bookmarks.

- Do not configure any settings on the **Notifications** tab unless an Workspace ONE UEM representative provided you with configuration instructions.
- 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.

# Chapter 5:

## Application Deployment

Overview of Workspace ONE UEM Application Deployment	24
Deploy Workspace ONE UEM Applications .....	24
Accessing SDK Event Analytics for a Specific Application .....	24
Accessing SDK Analytics Apps that Use SDK Functionality ....	25

## Overview of Workspace ONE UEM Application Deployment

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

The **VMware Workspace ONE UEM Mobile Application Management (MAM) Guide** covers the process for deploying public applications in full detail. While the VMware Content Locker application is available in the public app store, your organization needs to purchase licenses per device to take advantage of the Workspace ONE UEM MCM solution. Please see <http://www.air-watch.com/pricing> or contact your AirWatch representative for more information.

## Deploy Workspace ONE UEM Applications

Configure Workspace ONE UEM Applications to deploy as public apps.

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

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

Setting	Description
<b>Managed By</b>	View the organization group the application uploads in.
<b>Platform</b>	Choose the appropriate platform.
<b>Name</b>	Enter a descriptive name in the field to help search for the application in an app store.
<b>Search App Store</b>	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 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
<b>Event Analytics</b>	These events are custom created and developers can code any process or behavior they want to track.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Apps &amp; Books &gt; Applications &gt; Analytics &gt; SDK Analytics</b>.</li> <li>2. View events for SDK applications and retrieve data including application ID, the device on which it happened, and the event name.</li> </ol>
<b>Data Usage Analytics</b>	These events are embedded in the PLIST file for the Apple iOS application by the developer. They track telecom usage for SDK developed applications.	<ol style="list-style-type: none"> <li>1. Navigate to <b>Telecom &gt; List View</b>.</li> <li>2. Select devices that have the application installed and navigate to <b>Details View</b>.</li> <li>3. View data for the SDK application on the <b>Telecom</b> tab and use the <b>Export</b> option to retrieve a .CSV version of the data.</li> </ol>

# Appendix:

## VMware Browser Features Matrix

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

### VMware Browser Compatibility Matrix by Platform

Features	iOS	Android
<b>Browsing Settings</b>		
Restrict Access to Only Whitelisted Sites	✓	✓
Restrict Access Based on Blacklisted Sites	✓	✓
IP Browsing	✓	✓
Set Default Home Page URL with Support for Lookup Values	✓	✓
<b>Kiosk Mode</b>	✓	✓
Return Home after Configurable Inactivity Period	✓	✓
Clear Cookies and History with Home	✓	✓
Security Wi-Fi/Roaming Restrictions	✓	✓
Multiple Tabs Support	✓	
<b>Security</b>		
<b>Data Loss Prevention</b>		
Disable Cookies	✓	✓
Enable/Disable Cookie Encryption		✓
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	✓	✓
<b>Limit Access Based on Network Connection</b>		
Limit Access if Roaming		✓
Limit Access if using Cellular Network	✓	✓
Limit Access Based on SSID	✓	✓
<b>Authentication</b>		
Basic	✓	✓

Features	iOS	Android
AD/LDAP	✓	✓
Second Factor Passcode	✓	✓
Single Sign On	✓	✓
Biometrics	✓	✓
<b>Encryption</b>		
SSL Encryption in Transit	✓	✓
AES 256-Bit Encryption at Rest	✓	✓
<b>Browser Interface</b>		
<b>Document Support</b>		
Display PDF Documents	✓	✓ ***
Display MS Office Documents (PowerPoint, Word, Excel)	✓	✓ ***
Display MAC Documents (Keypoint, Pages, Numbers)	✓	✓ ***
<b>Navigation and UI</b>		
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	✓	✓
<b>Protocols</b>		
Http/Https and Awb/Awbs Protocols	✓	✓
Ftp/Ftps Protocol	✓	
Market:// (Google Play Store)		✓
<b>General</b>		
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.

## 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
<b>Force Token For App Authentication:</b> Enable	x	x
<b>Passcode:</b> Authentication Timeout	✓	✓
<b>Passcode:</b> Maximum Number Of Failed Attempts	✓	✓
<b>Passcode:</b> Passcode Mode Numeric	✓	✓
<b>Passcode:</b> Passcode Mode Alphanumeric	✓	✓
<b>Passcode:</b> Allow Simple Value	✓	✓
<b>Passcode:</b> Minimum Passcode Length	✓	✓
<b>Passcode:</b> Minimum Number Complex Characters	✓	✓
<b>Passcode:</b> Maximum Passcode Age	✓	✓
<b>Passcode:</b> Passcode History	✓	✓
<b>Biometric Mode:</b> Fingerprint	✓	✓
<b>Username and Password:</b> Authentication Timeout	✓	✓
<b>Username and Password:</b> Maximum Number of Failed Attempts	✓	✓
<b>Single Sign On:</b> Enable	✓	✓
<b>Integrated Authentication:</b> Enable Kerberos	x	✓

UI Label	Browser	
	iOS	Android
<b>Integrated Authentication:</b> Use Enrollment Credentials	✓	✓
<b>Integrated Authentication:</b> Use Certificate	✓	** ✓
<b>Offline Access:</b> Enable	X	✓
<b>Compromised Protection:</b> Enable	✓	✓
<b>App Tunnel:</b> Mode	✓	✓
<b>App Tunnel:</b> URLs (Domains)	✓	✓
<b>Content Filtering:</b> Enable	✓	X
<b>Geofencing:</b> Area	✓	✓
<b>DLP:</b> Bluetooth	X	X
<b>DLP:</b> Camera	X	X
<b>DLP:</b> Composing Email	✓	✓
<b>DLP:</b> Copy and Paste Out	✓	✓
<b>DLP:</b> Copy and Paste Into	✓	✓
<b>DLP:</b> Data Backup	X	X
<b>DLP:</b> Location Services	X	X
<b>DLP:</b> Printing	✓	X
<b>DLP:</b> Screenshot	X	✓
<b>DLP:</b> Third Party Keyboards	X	X
<b>DLP:</b> Watermark	X	X
<b>DLP:</b> Limit Documents to Open Only in Approved Apps	✓	✓
<b>NAC:</b> Enable	✓	✓
<b>NAC:</b> Cellular Connection	✓	✓
<b>NAC:</b> Wi-Fi Connection	✓	✓
<b>Branding:</b> Enable	✓	X
<b>Branding:</b> Toolbar Color	X	X
<b>Branding:</b> Toolbar Text Color	X	X

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

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

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