Workspace ONE Web Admin Guide

VMware Workspace ONE UEM

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware Workspace ONE Web Admin Guide

1

VMware Workspace ONE Web admin guide highlights the features and capabilities of Web application. It describes the Workspace ONE UEM console settings that apply to Web and provides a brief explanation of how the settings impact the behavior of the application.

What is VMware Workspace ONE Web?

Workspace ONE Web is a mobile application that securely connects users to corporate networks and enhances their browsing experience across Intranet, Internet, and other web applications. It provides your organization with a manageable and secure alternative to device native web browsers. Workspace ONE Web runs on iOS and Android devices. You can deploy and customize Web through the Workspace ONE UEM console. The configurations set by you determine the behavior of the application when deployed on the users' devices.

Why VMware Workspace ONE Web?

Workspace ONE Web separates business data from personal data and manages security policies while keeping individual information private. With this application, users can:

- Instantly access your company's intranet without manually configuring a VPN.
- Find information quickly with pre-configured corporate bookmarks and home pages. Users can also edit and remove bookmarks or add them on their own.
- Scan QR codes.
- Securely access web links given in the business emails.
- Eliminate challenges with manually entering passwords to internal websites with built-in single sign-on.

How Secure is VMware Workspace ONE Web?

Workspace ONE Web offers a secure browsing experience by providing complete encryption of data at rest and in-transit with AES 256-bit encryption. It uses disk level encryption to protect the downloaded files and Web settings. You can configure Web to allow or disallow users to access specific web pages, enforce restrictions on copying or pasting content, enable or deactivate cookies.

Workspace ONE Web works on the following configurable levels.

- **Application Level** – Secure Web at the application level by requiring end users to authenticate with a passcode, biometrics, or Active Directory credentials. You can also enable single sign-on.
- **Tunnel Level** – Use the VMware Tunnel certificates to encrypt traffic. Only enrolled and compliant devices are given access to VMware Tunnel.
- **Website Level** – Deactivate integrated authentication to require end users to authenticate when they access internal sites.

Requirements to Deploy VMware Workspace ONE Web

For an optimum application deployment, meet the listed requirements

- Supported Platforms:
  - iOS 10 and later.
  - Android 8 and later.
- Supported Broker Apps:
  - VMware Workspace ONE Intelligent Hub
  - AirWatch Container
- Hardware requirements:
  - Samsung DeX (S8 and higher, Note8, and S9 and higher)
- SDK settings requirements

  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 more information on meeting this requirement.

Note

- iOS 8 supports Workspace ONE Web only through version 5.10.2. To take advantage of new features and versions, devices must update to iOS 9 or later.
- Workspace ONE WEB for Android does not support Kerberos authentication over HTTP. For more information, see Workspace ONE Web for Android withdrawal of support for Kerberos over HTTP.

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 Workspace ONE Web or other web can access.
VMware Tunnel - Proxy	Accesses corporate content from within your network such as an intranet site. With the VMware Workspace ONE Tunnel enabled, you can access internal corporate content on your device. For information on configuring the Workspace ONE Tunnel, please see the VMware Workspace ONE Tunnel Admin and Install Guide.
VMware Tunnel	Enables app-tunneling to both SDK-built applications and applications managed on MDM enrolled devices across major platforms. VMware Tunnel provides better speed and performance over VMware Tunnel - Proxy, more secure authentication and encryption utilizing certificates, TLS 1.2, and tighter network access control through domain filtering.
F5 Proxy	Use to access your internal network as an alternative to the Workspace ONE Tunnel.

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.

Note Workspace ONE console 1905 introduces a new "Allow all non-FQDN URLs through tunnel" option that gives you the option to deactivate the feature which is enabled by default.

Configuring Workspace ONE Web

2

This section explains the payloads applicable to Workspace ONE Web and the instructions for configuring Web.

You can use Mobile Device Management (MDM) to enhance the performance of Workspace ONE Web by configuring profile payloads. To do so, you first configure **General Settings** and then, define the type of restriction or setting to apply to the device by selecting a payload from the list. The payloads available and their configurable settings differ from platform to platform.

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

Payload	Description	iOS	Android	Windows 8
Restrictions	Block the native browsers on devices using a restrictions payload to keep end users from using the native web instead of the Workspace ONE Web.	✓	✓	✓
Exchange ActiveSync	This payload allows users to access corporate push-based email infrastructures and allows them to set the sync frequency for calendar and email systems.	✓	✓	✓

Payload	Description	iOS	Android	Windows 8
Credentials	Configure this payload with digital certificates to protect your corporate email, Wi-Fi, VPN, and other corporate assets.	✓	✓	✓
SCEP	With Credentials payload, you can also configure SCEP to handle digital certificates pushed to large-scale devices.	✓		

For step-by-step instructions on configuring a specific **Payload** for a particular platform, see the applicable **Platform Guide**, available on VMware Workspace ONE UEM Console Documentation.

5 Select **Save & Publish**.

Configure Workspace ONE Web Settings

Configure the default SDK settings to define behaviors that apply to the Workspace ONE Web. Configure Workspace ONE Web specific system settings to define unique application behavior.

1 Navigate to Groups and Settings > All Settings > Apps > Workspace ONE Web.

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 Web 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.

Setting	Description
Use Legacy Settings and Policies	Enable to configure settings and policies for legacy web only.
Deactivate Copy	(Legacy web only) Enable this option to prevent copying from device. Configure this option under Data Loss Prevention in Settings > Apps > Settings and Policies.
Deactivate Printing	(Legacy web 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 web 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 web 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 web.
General	
Accept Cookies	Enable to accept cookies from websites viewed in the Workspace ONE Web.
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 web 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. Deactivate to protect browsing data on compromised devices.
Allow Connection to Untrusted Sites	Deactivate 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 Workspace ONE Web. Select Desktop to set desktop as the default view mode. When selected, the Workspace ONE Web renders the web pages in desktop mode if the websites supports the mode.
Mode	
Kiosk Mode	Enable for Workspace ONE Web 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 Workspace ONE Web 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 Workspace ONE Web.

Setting	Description
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 web starts. Leave this field blank to display a 'Recently Visited' page by default.
Selection Mode	Allow to limit browsing to domains allow listed in the Allowed Site URLs field. Deny to allow browsing to all sites except those denied in the Denied Site URLs field.
Allowed/Denied Site URLs	Utilize the following recommendations to Allow allowed domains and denied domains. ■ Define domain names without including full URLs. The Workspace ONE Web 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 allowlists <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 Allow IP addresses for browsing. A user can navigate to a allowed IP address even if the actual domain for the IP address was included in the Denied Site URL listing.
Allowed IP Addresses	Allowed IP addresses using the following recommendations: ■ Enter values in IPv4 formatting with four octets each separated by a period. ■ Enter wildcards to allowed 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 Workspace ONE Web, 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 on docs. vmware. com.

Note Clear Cookies and History if idle is not supported in Kiosk Mode. You need to enable Return Home After Inactivity and Clear Cookies and History with Home under kiosk settings to achieve this functionality.

4 Select the Bookmarks tab. Provide the following information to define and push a list of bookmarks to the Workspace ONE Web.

Setting	Description
URLs for Predefined Bookmarks in Web	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.
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.

Obtain SDK and application logs from the UEM console

As an administrator, you can request SDK and Web app logs from a managed device through the UEM console. To do so, follow these steps:

1 Log in to the UEM Console as a system administrator.

2 Go to **DEVICES > List View**.

3 Select your device and go to **Apps** to see a list of apps installed on it.

4 Select Workspace ONE Web

5 Tap **Request Logs** and select **Upload Application logs currently available**.

6 Select **OK**

7 Go to **More > Attachments > Documents** and download the zip folder to get the logs.

Note You can retrieve logs from the device only when the Web application is active and not running in the background.

Enable users to upload files from Workspace ONE Content repositories

Workspace ONE WEB lets users to upload files or documents present in the Workspace ONE Content repositories or local storage to a web application opened in Web app. This feature requires the Content app admin to set the SDK custom setting PolicyEnableFileProvider to true when configuring the Content app. For more information, see the VMware Workspace ONE Content admin guide.

App Suite SDK Configurations

3

This section provides information of the custom and the default 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 that 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 your apps in a particular OG and its child groups.	Offers granular control for specific applications and overrides the Default Settings SDK profiles.

	Default	Custom
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** on docs.vmware.com.

Note Configuring client certificates to authenticate users is a part of the SDK security settings. For more information about how to configure the client certificate for the Web application, see the SDK and Managing Applications admin guide.

Custom SDK Profile Settings

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.

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 Workspace ONE Content is wiped from a device and the device is enterprise wiped.
Authentication Grace Period (min)	Enter the time (in minutes) after closing the Workspace ONE Content before reopening the Workspace ONE Content will require users to enter credentials again.
Prevent Compromised Devices	Enable to prevent compromised devices from accessing Workspace ONE Content.

Setting	Description
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.

Expected Behavior for SDK Authentication

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

Table 3-1.

Authentication Type	SSO	Sessions	Credentials	Expected Behavior
Deactivated	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.

Table 3-1. (continued)

Authentication Type	SSO	Sessions	Credentials	Expected Behavior
Passcode	Deactivate	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	Deactivate	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.

Configuring VMware Tunnel for Workspace ONE Web

4

Workspace ONE Web supports the ability to tunnel websites through the Tunnel gateway component, without the Tunnel Proxy component.

The Tunnel gateway provides stronger encryption and authentication, increased browsing speed, and more detailed traffic controls. This does not require the use of the Workspace ONE Tunnel App for SDK-built applications, but other third-party applications still need support from the Tunnel App.

To take advantage of the improved tunneling capabilities, make sure you have deployed the Tunnel gateway and are using Workspace ONE UEM Console 1905 or higher version.

Migrate Proxy App Tunnel URLs to Tunnel SDK

VMware Tunnel with the Per-App Tunnel (Tunnel SDK) provides a unique feature called Device Traffic Rules. You can set individual traffic policies for tunneling, blocking, and bypassing traffic for each of your apps with the Device Traffic Rules. For information on Device Traffic Rules, see Create Device Traffic Rules in VMware Tunnel

1. If you migrate from VMware Tunnel - Proxy to Tunnel SDK (Per-App Tunnel) and want to keep the domains that use the tunnel, enter the App Tunnel URLs from the Proxy to the Device Traffic Rules settings for Tunnel SDK.
2. Navigate to Groups & Settings > All Settings > Apps > Settings and Policies > Security Policies > App Tunnel Mode > VMware Tunnel - Proxy and record the entries in the App Tunnel URLs field.
3. Navigate to Groups & Settings > All Settings > System > Enterprise Integration > VMware Tunnel > Network Traffic Rules > Device Traffic Rules
4. Select the applicable SDK application (like Workspace ONE Web).
5. Add multiple applications. This configuration differs from the default SDK setting because you need to enter the domains to tunnel by the app rather than as a blanket entry for all SDK-built apps.
6. Select Tunnel for the Action.
7. Enter the app tunnel URLs from the VMware Tunnel - Proxy option in Destination Hostname.

8 Define a default policy for domains that do not match patterns with your destination host names.

9 Navigate to Groups & Settings > All Settings > Apps > Settings and Policies and select App Tunnel Mode and change from VMware Tunnel - Proxy to VMware Tunnel.

Configure App Tunnel for the Default SDK Profile

Use App Tunnel to allow an application to communicate through a VPN or reverse proxy to access internal resources, such as a SharePoint or intranet sites.

You must set up the menu items for VMware Tunnel-Proxy or VMware Tunnel before using them.

To set up configurations and device traffic rules for the VMware Tunnel - Proxy or the VMware Tunnel, see VMware Tunnel.

If you are replacing the VMware Tunnel - Proxy with Tunnel SDK, migrate the App Tunnel URLs entries. See Migrate Proxy App Tunnel URLs to Tunnel SDK.

Configuring VMware Cloud Web Security (CMS)

Workspace ONE Web supports routing all its traffic through VMware Cloud Web Security (CWS) to provide additional web security through CWS's capabilities like URL filtering, content filtering and more. Admins can configure Web's in-built tunnel to route the traffic through a Secure Access service instance and attach CWS security policy with that. For more information about CMS, see VMware Cloud Web Security Documentation.

Application Configurations for Workspace ONE Web

5

Configure Workspace ONE Web settings using the Configuration Key and Configuration Value pairs provided by Workspace ONE UEM.

To configure Workspace ONE Web 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 False	(Available for Android and iOS) If the value is true, the QR Code scanner in Workspace ONE Web URL bar is deactivated. If the value is false, the QR Code scanner is displayed in the Workspace ONE UEM URL bar.
{“BrowserDisableUserAgentString” : "true”}	Boolean	True False	(Available for Android only) If the value is true, the user Hub string is deactivated. However, this also disables the ability to switch between desktop mode and mobile mode. If the value is false, the user Hub string is enabled and also enables the ability to switch between desktop mode and mobile mode.
{"BrowserDisableAutoCloseTab": "true" }	Boolean	True False	(Available for iOS only) If the value is true, Workspace ONE Web does not auto-close the tab that runs an external application. If the value is false, Workspace ONE Web auto-closes the tab that runs an external application.

Configuration Key	Value Type	Configuration Value	Description
{"BrowserDisableWebclip":"true"}	Boolean	True False	(Available for Android and iOS) By default, the Webclips are shown in the Workspace ONE Web Bookmarks. If the value is set to true, the Webclips do not appear in the Workspace ONE Web Bookmarks. You can push webclips with awbf:// and awbfs:// protocols to open in full screen mode.
{ "BrowserDisableLongPressOnLinks":"true" }	Boolean	True False	(Available for Android only) When set to True, Workspace ONE Web deactivates the open in the new tab and add to bookmarks dialog (or prompt) box for links that are long pressed.
{ "DisableLongPressInKiosk": "true"	Boolean	True False	When set to True, Workspace ONE Web deactivates the long press option to prevent users to take any unintended actions on the website. This key applies only when Web is in kiosk mode.

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 prompt screen upon the start of the application.

The privacy prompt 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 are 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 is shown to the user to contact their employer for more information. VMware recommends users to configure their privacy policy URL in the UEM console. After configured, the users can open the employer's privacy policy within the application.

To enable privacy and data collection policies, enter the configuration key and the corresponding value in **Custom Settings** under **Groups & Settings > All Settings > Apps > Settings and Policies > Settings**.

Configuration Key	Value Type	Configuration Value	Description
{ "PolicyAllowFeatureAnalytics" }	Integer	0 - deactivate 1 - Activate (default)	Feature analytics data collection admin policy that controls whether the end users see the Data Sharing opt-in during configuration of the Workspace ONE Web. 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	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. It Impacts 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 Workspace ONE Web. **Note** This policy overrides the default company privacy policy URL.

Sample SDK configuration: {"PolicyAllowFeatureAnalytics":1, "PrivacyPolicyLink":"https://www.acme.com/privacypolicy", "PolicyAllowCrashReporting":true}

Configure Web Clips in Full Screen Mode

By default, web clips are displayed in normal mode in the Workspace ONE Web Bookmarks. If you want your user to view the web clips in full screen mode, set the URL prefix as awbf:// and awbfs://. For more information on the web clip configuration process, refer to the **Platform Guide**.

If you want to enforce full screen mode, you can configure Workspace ONE Web using the following configuration key. This key provides a more secure and restricted experience for your end users when using web clips in full screen mode. If configured, this key:

- Opens webclips in full screen mode without allowing users to exit.
- Hides the URL address bar, navigation controls, and other Web features to minimize user distractions.
- Prevents sensitive URLs from being exposed to end users for malicious or accidental misuse.

Configuration Key	Value Type	Configuration Value	Description
EnableForcedFullScreenWithAwbfs	Boolean	False (default) True	If the value is set to true, webclips that use awbfs are opened in full screen mode, which the user cannot exit. Such URLs are not added to bookmarks or history. When the value is set to false, webclips that use awbfs are opened in full screen mode and can be exited by the user. These URLs are added to bookmarks and history.

Enabling SDK logging on iOS Web

To enable the SDK logging on Web, use the following configuration key. This key provides a fallback if you want to log browser logs in the SDK logging framework.

Configuration Key	Value Type	Configuration Value	Description
BrowserEnableLoggingToSDK	Boolean	True False	Set this value to true to log browser logs in the SDK logging framework.

Enable Web Fullscreen mode

With Workspace ONE Web, users can browse content in the Fullscreen viewing mode. Fullscreen mode hides the URL and the navigation bar and displays only the content. Users can exit the fullscreen mode either by a long press on the screen or stop and relaunch the Web application.

By default, the fullscreen mode is enabled, and admin can deactivate this mode using the following KVP:

Configuration Key	Value Type	Configuration Value	Description
DisableFullscreenMode	Boolean	False (default) True	Set the value to true to deactivate the full screen mode view.

SCEP Integrated Authentication

Use the integrated authentication with an 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 time out.
ScepPendingMaxRetryAttempts	Integer	Min and max values	Provide the maximum retry count for the SCEP certificate to update on the device.

View Downloaded Files in Workspace ONE Content Application for Android Devices

To view the downloaded files in the Workspace ONE Content application, use this configuration key in the UEM console. Users must install and configure the Content application on their device to view the supported files. For more information about files supported by the Content application, see the *Matrix of Supported File Type by Platform* topic in the *Mobile Content Management* documentation.

Configuration Key	Value Type	Configuration Value	Description
BrowserAutoOpenInContent	Boolean	False (default) True	Set the key value to true, to automatically view the downloaded files in the Workspace ONE Content application.

Add a Custom String to the Browser User Agent

As an admin, you can pass an identifier to Workspace ONE Web that appends to the user agent string. This identifier is an optional parameter and applies to both mobile and desktop user agent. It does not support double byte characters and rich text.

Configuration Key	Value Type	Configuration Value	Description
BrowserUserAgentPostfix	String	"This is the appended string" Example: { "BrowserUserAgentPostfix": "This is the appended string" }	Set the string to append at the end of the user agent.

Configure Workspace ONE Web to Use a PAC File

You can configure Workspace ONE Web to use the Proxy Auto-Configuration (PAC) file to allow your web traffic to pass through the proxy server. A PAC file is a text file that directs a browser to a proxy server before it reaches the destination server.

Configuration Key	Value Type	Configuration Value	Description
BrowserPacURL	String	URL of the PAC file.	Set the PAC URL.

BrowserPacMode	Integer	1
		2
			Set the value to 1 to use a PAC file for URLs that are not tunneled through the tunnel proxy or VMware tunnel. For example:
			`{`
			`"BrowserPacURL":`
			`"https://`
			`mypac.mydomain.com/`
			`pacfile"`
			`"BrowserPacMode": 1`
			`}`
			Set the value to 2 to use a PAC file for URLs that are also tunneled through the VMware tunnel. For example:
			`{`
			`"BrowserPacURL":`
			`"https://`
			`mypac.mydomain.com/`
			`pacfile"`
			`"BrowserPacMode": 2`
			`}`

Enabling Print Option in Kiosk Mode

Use the following configuration key, to enable the print option in kiosk mode:

Configuration Key	Value Type	Configuration Value	Description
{"BrowserAllowPrintInKiosk" : "True"}	Boolean	False (default) True	Set the value to true, to enable printing in Kiosk Mode.
To enable the print option in Kiosk mode, ensure that printing is allowed under the SDK DLP settings,			

WebRTC Support in Workspace ONE Web (Android only)

With WebRTC, websites can easily access the camera and microphone in Workspace ONE Web for Web Real-Time Communication. To enable this feature, you must configure the Web application with the following KVP.

Configuration Key	Value Type	Configuration Value	Description
{ "BrowserEnableWebRTC": "True" }	Boolean	False (default) True	Set the value to true, to enable WebRTC in Workspace ONE Web.
This feature is supported only in Android 7 and higher versions.			

Workspace ONE Web lets the end users remember their choice to allow or block camera or microphone settings for individual websites by selecting **Remember my choice** setting. By selecting **Remember my choice** setting, they can conveniently load the websites next time without the pop-up dialog box asking for the same permissions again.

Redirect mailto: Links to your Favorite Email Clients

By default, Workspace ONE Web opens mailto: links in Workspace ONE Boxer or in the iOS native email application when the Data Loss Prevention (DLP) option is disabled. As an admin, you can change this behavior by configuring Web to open mailto: links in any configured third-party email client.

To apply the mailto: setting in Workspace ONE Web, you must add the following configuration in the **Custom Settings**. Before you configure, make sure that you have deactivated the **Enable Composing Email** option under the SDK DLP setting.

<table>
<tr><th>Configuration Key</th><th>Description</th></tr>
<tr><td><pre>
{
      "CustomSDKSettings": {
         "com_vmware_DLP_Redirection": {
                   "mailtoSchemeConfiguration": {
                             "mailto": "ms-
outlook",
                             "appName": "Outlook"
                     }
               }
        }
}
</pre></td><td>Add this configuration key to open mailto: links in any configured email client.
You must specify the target apps scheme as a value for the source scheme, and the application's name as a value for the appName.
<b>Note</b> Make sure that the email application configured by you must be installed on the iOS device.</td></tr>
</table>

Configure iOS Web to Support Shortened URLs

Use the shortened or non-FQDN (Fully qualified domain name) URLs to access the websites of your organization by adding the following Key-value pair. This Key eliminates the need to add HTTP or HTTPs to the URLs.

Configuration Key	Description
{"BrowserShortlinkPrefix": ["wmlink","vmware"]}	This KVP acts as a URL prefix. Any URL whose prefix matches this value is a non-FQDN URL. For example, wmlink treats wmlink, wmlink-clarity, wmlink-byod, wmlink-internal as non-FQDN URLs.

Set Up a Retention Period for Downloaded Files

Use the following key to configure a retention period for the downloaded files in Workspace ONE Web.

Configuration Key	Value Type	Configuration Value	Description
{"BrowserRetainDownloads": "day"}	String	Always (default) Day Week Month Always	This key removes the downloaded files from Web after the configured retention period expires. **Note** When configured, this key deletes all existing downloaded files if the time since the files where downloaded exceeds the retention period.

Automatically Open Downloaded Files (Android only)

Use the following key to configure Workspace ONE Web for Android to open the downloaded files automatically in a default application.

Configuration Key	Value Type	Configuration Value	Description
{"BrowserAutoOpenDownload": true}	Boolean	True (default) False	Set the value to true to open the downloaded files automatically in a default application.

Support for Android App Links

Configure Workspace ONE Web for Android to launch an intended application from an app link. You can use the following configuration key, to enable this behaviour of Web.

Configuration Key	Value Type	Configuration Value	Description
{"BrowserAllowAppLink": true}	Boolean	False (default) True	Set the value to true to allow an app link to open in the intended app.

Block Popup Windows in Web

Configure Workspace ONE Web to prevent JavaScripts from opening popup windows without any user interaction.

Configuration Key	Value Type	Configuration Value	Description
{ "BlockPopupWindows" : "true" }	Boolean	False (default) True	Set the value to true to prevent JavaScripts to open popups without any user interaction. **Note** In iOS Web, this key is applicable only in non-proxy scenario (WKWebView).

Enable WebSDK (iOS only)

Use the following key value pair to enable WebSDK in Workpsace ONE Web for iOS.

Configuration Key	Value Type	Configuration Value	Description
{"BrowseriOSDisableWebSDK": "true"}	Boolean	False (default) True	If the key value is set to True, Web continues to use its own webviews for rendering purposes. And If the value is set to False, Web uses the webviews provided by WebSDK to render websites.

Enable Secure Browsing

Configure Workspace ONE Web to provide secure browsing experience to the the end users. Use the following key value pair to use HTTPS protocol to load all URLs in Workpsace ONE Web for iOS and android.

Configuration Key	Value Type	Configuration Value	Description
{"BrowserForceHttps": "true"}	Boolean	false (default) true	If the key value is set to True, Web uses HTTPS protocol to load all URLs. And If the value is set to False, the Web honours the protocol provided by the user while entering the URL.

Customize the Display of the URL Address Bar in the Single Tab Kiosk Mode

Hide the URL address bar in single tab Kiosk mode to reduce user distraction. To do so, you must use the following key value pair.

Configuration Key	Value Type	Configuration Value	Description
{"HideURLBarInKioskMode": "false"}	Boolean	False (default) True	When the key value is set to true, the URL bar is hidden in the single tab Kiosk mode. When the value is set to false, the URL address bar is visible.

Customize the Display of the Navigation Controls in the Single Tab Kiosk Mode

Hide the navigation controls (which includes front or back navigation and home button) in single tab Kiosk mode to reduce user distraction. To do so, you must use the following key value pair.

Configuration Key	Value Type	Configuration Value	Description
{"HideNavigationControlsInKioskMode": "false"}	Boolean	False (default) True	When set to true, the navigation controls (includes front or back navigation, home button and print option if 'BrowserAllowPrintInKiosk' is true) are hidden in single tab Kiosk mode. When the value is set to false, the navigation controls become visible.

Scan URL QR codes in Kiosk mode

To activate and deactivate the QR scanning option in the URL address bar in Kiosk mode, use the following configuration key. This key is not applicable to multiple tab Kiosk mode.

,

Configuration Key	Value Type	Configuration Value	Description
{"EnableQRInKioskMode": "false"}	Boolean	False (default) True	When set to true, the the URL address bar must show the QR scanner in the single tab Kiosk mode.

VMware Workspace ONE Web Deployment

6

Deploy Workspace ONE Web to your end users and other security configurations from the UEM console.

Overview

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

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

Deploy Workspace ONE Web

Configure the Workspace ONE Web to deploy as a public application and utilize this simplified deployment workflow to seamlessly push it 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. 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 the UEM console or automatically push it to your devices.

7 Assign **Terms of Use**.

8 **Save and Publish**.

Accessing SDK and Wrapped App Logs by Log File

Review the collected logs from the App Logs page.

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

View the available log files that uses SDK functionality.

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

Access the SDK event analytics.

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 Select the **View Logs** option from the actions menu.

Accessing SDK Analytics Apps that Use SDK Functionality

Displays events and data usage information for applications that use SDK functionality. Workspace ONE Web reports event analytics by the application ID and event name and data usage analytics by device.

Access Event Analytics

Event Analytics are custom created to track specific events of an application. You can view events for the SDK application and access data such as application ID, the event name, and the device on which the event happened.

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.

Access Data Usage Analytics

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.

Make iOS Web as the Default Browser

Users can set Workspace ONE Web their default browser by following these steps:

1 Navigate to Web **Settings** and select**Default Browser App**, which opens the Web **Settings** in iOS settings app.

2 Select **Web** as your default browser app.

Trust Store for Self-Signed Certificates

7

Trust Store includes root certificates from trusted Certificate Authorities (CA) that are used to validate certificate presented by the server in SSL connection.

With the websites of self-signed SSL certificate, untrusted website warning messages appeared upon access. To avoid such error messages to appear in the users device, you can provide the trust store certificate with the SDK applications to support the trusting websites with the self-signed SSL certificates. Users can use self-signed SSL certificates for their websites without any untrusted site errors.

Push down certificates to unmanaged devices using SDK profiles.

Procedure

1 Navigate to **Groups and Settings** > > **All Settings** > **Apps** > **Settings and Policies** > **Profiles**.

2 Create an SDK profile, If not exist.

3 Select the SDK profile in which you want to push the self-signed certificate.

4 Navigate to **Credentials**.

5 Upload the Self-Signed Certificate.

6 Save the changes.

7 Navigate to **Groups and Settings** > > **All Settings** > **Apps** > **Workspace ONE Web**.

8 Select the SDK Profile in iOS or Android SDK Profile field and save.

Workspace ONE Web Features Matrix

8

This section outlines the available Workspace ONE Web features by platform, reflecting the latest app versions available in play store.

Table 8-1. Workspace ONE Web Compatibility Matrix by Platform

Features	iOS	Android
Browsing Settings		
Restrict Access to Only Allowed Sites	✓	✓
Restrict Access Based on Denied 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		
Deactivate 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 Workspace ONE Web	✓	✓
Enable caching	✓	✓
WebRTC	x	x
Limit Access Based on Network Connection		

Table 8-1. Workspace ONE Web Compatibility Matrix by Platform (continued)

Features	iOS	Android
Limit Access if Roaming		✓
Limit Access if using Cellular Network	✓	✓
Limit Access Based on SSID	✓	✓
Authentication		
Basic	✓	✓
AD/LDAP	✓	✓
Second Factor Passcode	✓	✓
Single Sign On	✓	✓
Biometrics	✓	✓
Encryption		
SSL Encryption in Transit	✓	✓
AES 256-Bit Encryption at Rest	✓	✓
Web 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	✓	✓
Tabbed Browsing	✓	✓
Javascript Popup Support	✓	✓
Browse HTML-based Websites (HTML, PHP, etc.)	✓	✓
HTML5, CSS3 & JavaScript	✓	✓

Table 8-1. Workspace ONE Web Compatibility Matrix by Platform (continued)

Features	iOS	Android
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

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

Workspace ONE Web for Andrid supports NTLM v1 and NTLM v2.

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. The following matrix shows support for Workspace ONE Web built with the Workspace ONE UEM SDK.

Table 8-2.

UI Label	Workspace ONE Web	
	Android	iOS
Force Token For App Authentication: Enable	✓	✓
Passcode: Authentication Timeout	✓	✓
Passcode: Maximum Number Of Failed Attempts	✓	✓
Passcode: Passcode Mode Numeric	✓	✓
Passcode: Allow Simple Value	✓	✓

Table 8-2. (continued)

Passcode: Minimum Passcode Length	✓	✓
Passcode: Minimum Number Complex Characters	✓	✓
Passcode: Maximum Passcode Age	✓	✓
Passcode: Passcode History	✓	✓
Biometric Mode: Fingerprint	✓	✓
Username and Password: Authentication Timeout	✓	✓
Username and Password: Maximum Number of Failed Attempts	✓	✓
Single Sign On: Enable	✓	✓
Integrated Authentication: Enable Kerberos	✓	✓
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

Table 8-2. (continued)

DLP: Watermark	x	x
DLP: Limit Documents to Open Only in Approved Apps	✓	✓
NAC: Enable	✓	✓
NAC: Cellular Connection	✓	✓
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	✓
Logging: Logging Level	x	✓
Logging: Send Logs Over Wi-Fi	x	✓
Custom Settings: Enable	x	x
SDK App Compliance: Enable	x	x
Compromised Protection: Enable	✓	✓
Offline Access: Enable	x	✓