Workspace ONE Notebook Admin Guide

VMware Workspace ONE UEM

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

https://docs.vmware.com/

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

Contents

About Workspace ONE Notebook

1

Workspace ONE Notebook is a mobile application focusing on the mobile productivity and enterprise content security.

Attention End of Support Life for VMware Workspace ONE Notebook

Workspace ONE Notebook application has reached End of Support Life starting February 2nd, 2024. For more information about this announcement, see Knowledge Base article.

You can connect to your Exchange account through Exchange Web Services (EWS) and manage the notes and tasks associated with that account using Workspace ONE Notebook. Administrators can ensure that DLP and application authentication policies are added to protect Notebook data. You can encrypt data at rest and in-flight, and manage on mobile devices through the Workspace ONE UEM console.

Workspace ONE Notebook application is supported on both Android and iOS platforms.

Features of Workspace ONE Notebook

You can use Workspace ONE Notebook to organize your business data. You can create, synchronize, annotate, and collaborate on documents in one place. Some of the features of this application are:

- Store information in one place and find it easily.
- Create notes using the rich text editor and manage them.
- Attach photos and audio recordings to notes.
- Access flagged emails in your task list.
- Set reminders to complete the high priority tasks.
- Attach and view Office documents as a part of notes.
- Support of editing and syncing of flagged tasks to the server.
- Support of special characters in email addresses through Exchange Authentication.

Requirements to Deploy Workspace ONE Notebook

Deploy Workspace ONE Notebook application as part of your Workspace ONE UEM deployment.

The access and authentication requirements are :

- Access to the endpoint Exchange Web Services is required. The application must access the EWS URL either directly or through the Secure Email Gateway or VMware Tunnel Per-App VPN.
- Notebook supports Exchange Server 2010 and later versions.
- Basic and NTLM authentication are supported.
- The Notebook application requires HTTPS protocol and port 443 to access EWS.

Console Requirements:

Workspace ONE UEM console 9.3 and later.

Supported Agent:

- VMware Workspace ONE
- VMware Workspace ONE Intelligent Hub

Supported Mobile Operating Systems - iOS 10 and later Android 5.1 and later

Supported File Types:

- iOS - DOC, DOCX, JPEG, JPG, PDF, MP4, MP3, PPT, PPTX, XLS, and XLSX
- Android - DOC, DOCX, JPEG, JPG, PDF, MP4, MP3, PPT, PPTX, XLS, and XLSX

Supported Workspace ONE Applications:

- Workspace ONE Boxer
- Workspace ONE Web
- Workspace ONE Content

Configuring VMware Workspace ONE Notebook

2

Notebook relies on the SDK profile for both general app settings (app passcode, SSO, DLP) and on the specific configurations.

The Notebook specific settings are configured in the “custom settings” payload of the SDK profile. These settings can either be set as a part of the default profile that might already be set up or as a part of a custom SDK profile that are assigned specifically to Notebook.

Only one SDK profile can be assigned to an application, so you must select either default or custom SDK profiles. The default profile is same for both iOS and Android, whereas the custom profiles are platform-dependent. A custom SDK profile can have an additional granularity as per requirements.

For more information on slecting default versus custom SDK profile, see the *App Suite SDK Configurations from Mobile Content Management* guide.

Configure a Default SDK Profile

The default SDK profile is already configured, if you have deployed other Workspace ONE applications, such as Intelligent Hub, Boxer, Web, or Content.

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

2 Configure **Security Policies**.

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

Activate	Establish a single app session across all Workspace ONE UEM and Workspace ONE UEM wrapped apps.
Deactivate	Establish app sessions on a per app basis.
Offline Access	
Activate	Allow end users to open and use Workspace ONE UEM and wrapped apps when disconnected from Wi-Fi. Offline Workspace ONE UEM apps cannot perform downloads, and end users must return online for a successful download. Configure the **Maximum Period Allowed Offline** to set limits on the offline access.
Deactivate	Remove access to Workspace ONE UEM and wrapped apps on offline devices.
Compromised Protection	
Activate	Override MDM protection. App level Compromised Protection blocks compromised devices from enrolling, and enterprise wipes enrolled devices that report a compromised status.
Deactivate	Rely solely on the MDM compliance engine for the compromised device protection.
Data Loss Prevention	
Activate	Access and configure settings intended to reduce data leaks.
	Enable **Copy And Paste**
	Allows an application to copy and paste on devices when set to **Yes**.
	Enable **Printing**
	Allows an application to print from devices when set to **Yes**.
	Enable **Camera**
	Allows applications to access the device camera when set to **Yes**.
	Enable **Composing Email**
	Allows an application to use the native email client to send emails when set to **Yes**.
	Enable Data Backup
	Allows wrapped applications to sync data with a storage service like iCloud when set to **Yes**.
	Enable **Location Services**
	Allows wrapped applications to receive the latitude and longitude of the device when set to **Yes**.
	Enable **Bluetooth**
	Allows applications to access Bluetooth functionality on devices when set to **Yes**.
	Enable **Screenshot**
	Allows applications to access screenshot functionality on devices when set to **Yes**.
	Enable **Watermark**

	Displays text in a watermark in documents in the VMware Workspace ONE Content when set to Yes. Enter the text to display in the Overlay Text field or use lookup values. You cannot change the design of a watermark from the UEM console.
	Limit Documents to Open Only in Approved Apps
	Enter options to control the applications used to open resources on devices. For more information, see *Configure Import Restriction in Workspace ONE Content* section. Enter options to control the applications used to open resources on devices. (iOS only) You can use Workspace ONE UEM Configuration values to restrict users from importing files from third-party applications intoWorkspace ONE Content. For more information, see Configure Import Restriction in Workspace ONE Content section.
	Allowed Applications List
	Enter the applications that you allow to open documents.
Deactivate	Allow end user access to all device functions.

3 **Save**.

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

5 Configure **Settings**. You must enter the Notebook specific application settings. See the Application Configurations for Workspace ONE Notebook section for more details on configuration options.

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

Enabled	Collect and view useful statistics about apps in the SDK suite.
Deactivate	Do not collect useful statistics.

6 **Save**.

Configure a Custom SDK Profile

You must configure the custom SDK profile if the Workspace ONE Notebook application has DLP or authentication requirements that differ from other Workspace ONE applications that may be using the default SDK profile. Otherwise the default SDK profiles are enough. For more information on how to select the right configuration type, see App Suite SDK Configurations in Workspace ONE Web Admin Guide.

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

2 Select **SDK Profile**.

3 Select the platform.

4 Configure the **General Settings**.

5 Configure the **Custom Settings** with the configuration keys listed on the Application Configurations for Workspace ONE Notebook page.

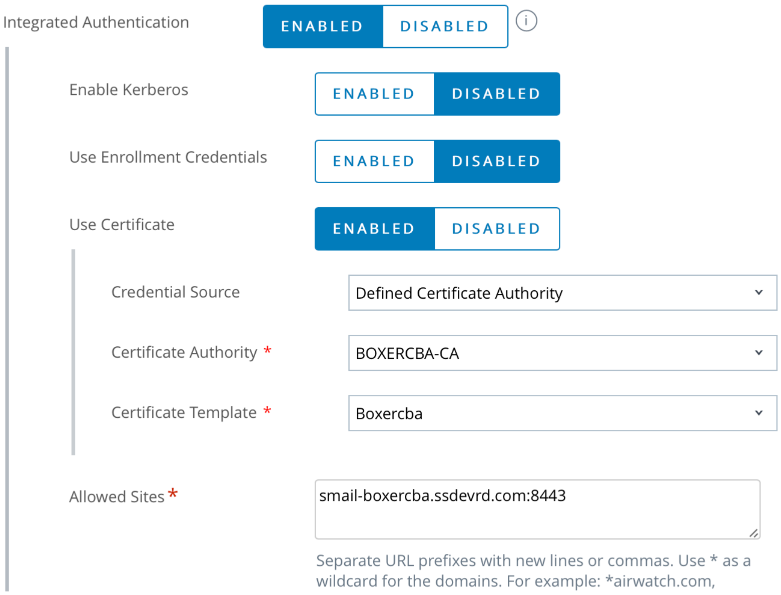
6 **Save** the profile.

Configure Workspace ONE Notebook using Certificate-Based Authentication (CBA) with Exchange

Configure Workspace ONE Notebook using the Certificate-Based Authentication (CBA) with Exchange to authenticate users.

1 If you are using a default SDK profile, perform the following steps:

   a In the Notebook SDK Profile, select the **Integrated Authentication** from the menu items.



Integrated Authentication [✓ ENABLED] DISABLED

Enable Kerberos ENABLED [✓ DISABLED]

Use Enrollment Credentials ENABLED [✓ DISABLED]

Use Certificate [✓ ENABLED] DISABLED

Credential Source: Defined Certificate Authority

Certificate Authority *: BOXERCBA-CA

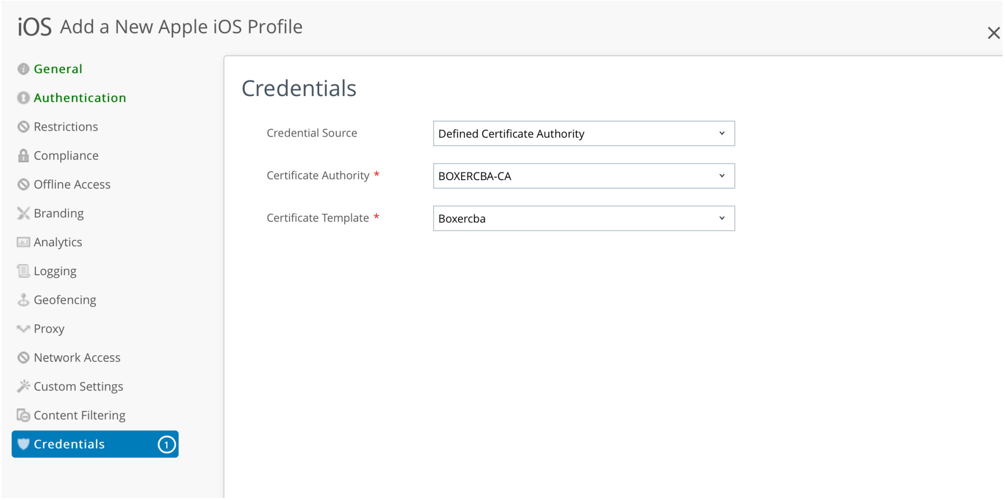
Certificate Template *: Boxercba

Allowed Sites *: smail-boxercba.ssdevrd.com:8443

Separate URL prefixes with new lines or commas. Use * as a wildcard for the domains. For example: *airwatch.com,

2 If you are using a custom SDK profile, perform the following steps:

   a Select the Certificate Authority and Template.



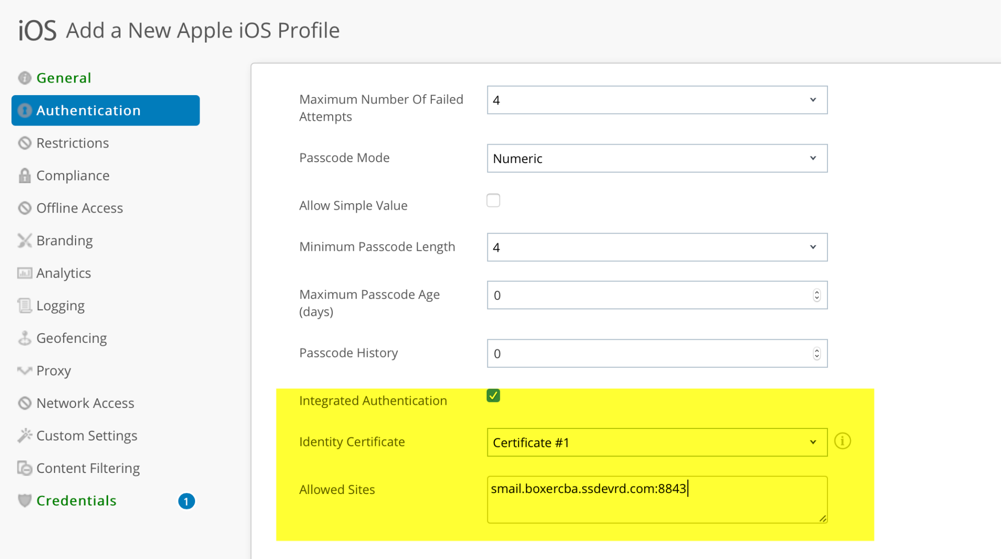
Credentials

Credential Source: Defined Certificate Authority

Certificate Authority *: BOXERCBA-CA

Certificate Template *: Boxercba

b List the Exchange URL in the allowlist URL text box.



Maximum Number Of Failed Attempts: 4

Passcode Mode: Numeric

Allow Simple Value: □

Minimum Passcode Length: 4

Maximum Passcode Age (days): 0

Passcode History: 0

Integrated Authentication: ☑

Identity Certificate: Certificate #1

Allowed Sites: smail.boxercba.ssdevrd.com:8843

3 Add KVPs such as AccountUseCBA and AccountUseDualAuth under the **Custom Settings** in the UEM console. For more information about the KVPs, see Application Configurations for Workspace ONE Notebook

Workspace ONE Notebook URL Schemes

Workspace ONE Notebook URL Schemes for Workspace ONE Notebook app extends the support for inter-app integration using URL schemes. Workspace ONE UEM provides you with a set of URLs that can be used to access different Workspace ONE Notebook menus and options from supported third-party applications. The URL schemes are compatible with any application that supports URL formats, such as browsers, email clients, and note-taking software. You can save the URLs and open them to directly access a specific Workspace ONE Notebook menu or option.

For example, use notebook://tasks URL scheme to open Workspace ONE Notebook tasks list directly from any supported app.

The following are the supported URL schemes:

- notebook://
- notebook://tasks
- notebook://notes
- notebook://favorites
- notebook://createnote
- notebook://createtask
- notebook://createnotefromtemplate

Deploying VMware Workspace ONE Notebook

3

Deploy Workspace ONE Notebook with security configurations to your end users from the Workspace ONE UEM console.

You can also configure Workspace ONE Notebook with Secure Email Gateway (SEG). To know how to configure SEG, see the Secure Email Gateway admin guide.

Note To enable SEG support when you are configuring Notebook version 1.4 using the Workspace ONE UEM console version 2003 and below, you must add the EasDeviceIdentifier key to the Notebook application configuration.

You can add the Workspace ONE Notebook app as a public application to the Workspace ONE UEM console.

Use this simplified deployment workflow to push the Workspace ONE Notebook app to the end users.

1 In the Workspace ONE UEM console navigate to **Apps & Books >Applications > Native > List View >Public**.

2 Select Add Application.

3 Configure **Add Application**.

Setting	Description
Managed By	Select the organization group.
Platform	Select an appropriate platform.
Name	Enter Workspace ONE Notebook.
Search App Store	(iOS only) Search App Store Select to make the application available in the App Store.
Enter URL	Enter the URL of the app.
Import from Play	Select to make the application available in the Play Store. It is applicable for the Android platform. 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 Select the Workspace ONE Notebook application.

5 **(Optional)** Assign the custom SDK profile to Workspace ONE Notebook. Only complete this step if you have selected to use a custom SDK profile instead of the default SDK profile.

6 Navigate to the SDK tab. It is the custom SDK profile.

7 Select the SDK profile you created during the Notebook configuration steps.

8 Select **Save and Assign**.

9 Select **Add Assignment** from the updated assignment page and enter the name of assignment group in the **Select Assignment Groups** text box.

10 Select **Add**.

11 Select **Save and Publish**.

Install Workspace ONE Notebook on a mobile device that is registered or enrolled using Workspace ONE Intelligent Hub or Workspace ONE app. Users must enter their Exchange credentials after the initial run to synchronize the Exchange content.

Configure Workspace ONE Notebook with Derived Credentials (PIV-D)

Create and configure an SDK profile with Derived Credential and assign the profile to the Notebook application. The SDK profile enables Notebook to fetch the Derived Credential certificates from the Workspace ONE PIV-D Manager application so that the device can use the certificates to access resources securely.

A Derived Credential is a client certificate that is generated (or issued) on a mobile device after end users prove their identity using their existing smart card (CAC or PIV) during the enrollment process.

When you set the Credential Source as Derived Credential on the Credential payload, Notebook imports the authentication, signing, and encryption certificates from the PIV-D application. The PIV-D certificate is then used to authenticate users against the Exchange Server through CBA and dual authentication in Notebook.

For more information on the PIV-D application, see *Workspace ONE PIV-D Manager Admin Guide*.

1 Configure the SDK Profile:

   a Navigate to **Groups & Settings > All Settings > Apps > Settings and Policies > Profiles select Add Profiles**.

   b Select **SDK Profile**.

   c Select the desired platform.

   d Configure the profile's **General Settings**.

   e Select the **Credentials payload** and select **Configure**.

   f Set the **Credential Source** to **Derived Credentials**.

g Select the **Key Usage** based on how the certificate is used. Select **Authentication**, **Signing**, or **Encryption**.

h To add additional certificates, use the plus sign at the bottom of the profile window.

i Select **Save and Publish**.

2 Assign the SDK Profile to Notebook:

a Navigate to **Apps & Books** > **Native** > **Public** > **Add Application** and add Workspace ONE Notebook.

b If the Notebook application has already been added, you can skip the preceding step.

c Select **Edit**.

d Navigate to the **SDK** tab and set the SDK profile to the one configured with the derived credential source and key usage.

e Select **Save and Assign**.

Assign and Configure Workspace ONE Notebook Using the App Assignment

Configure Workspace ONE Notebook using the App Policies.

The steps provided in this page are applicable to assign the Notebook application for versions 1.4 and higher using the console versions of 2004 and higher. For older versions of assigning Notebook, see Application Configurations for Workspace ONE Notebook.

These configurations are set as a part of the SDK profile that you are planning to use for Notebook. If you are using the default SDK profile, set the application configurations by navigating to **Groups & Settings** > **All Settings** > **Apps** > **Settings and Policies** > **Settings**.

You can upload Notebook as a public or an internal application to Workspace ONE UEM console.

1 Navigate to **Apps & Books** > **Applications** > **Native** > **List View** > **Public**.

2 Select the **Assign** link under the **Install Status** column for the Notebook application. Alternatively, you can also select the edit icon and then select **Save & Assign**.

3 On the Assignment page, select **Add Assignment** and complete the options.

a In the Distribution tab, enter the following information:

Settings	Description
Name	Enter the assignment name.
Description	Enter the description for the assignment.

Settings	Description
Assignment Groups	Enter the smart group name to which you want to assign the application. As you enter the smart group name, options are displayed and you can select the appropriate smart group from the list. If necessary, you can add more assignment groups.
App Delivery Method	■ **On Demand** – Deploys content to a catalog or other deployment agent. The device user can decide if and when to install the content. This option is the best choice for content that is not critical to the organization. Allowing users to download the content when they want helps conserve bandwidth and limits unnecessary traffic. ■ **Automatic** – Deploys content to a catalog or other deployment Hub on a device upon enrollment. After the device enrolls, the system prompts users to install the content on their devices. This option is the best choice for content that is critical to your organization and its mobile users.

4 In the Restrictions tab, enter the following information:

Settings	Description
Remove on Unenroll	Set the application to be removed from a device when the device unenrolls from Workspace ONE UEM. Workspace ONE UEM enables this setting by default. If you enable this setting, supervised devices are restricted from silent app installation. This is because the device is locked and the provisioning profile installation is in the command queue which requires a device to be unlocked to complete the installation. If you deactivate this setting, provisioning profiles are not pushed with the installed application. That is, if the provisioning profile is updated, the new provisioning profile is not automatically deployed to devices. In such cases, a new version of the application with the new provisioning profile is required.
Prevent Application Backup	Disallow backing up the application data to iCloud. However, the application can still back up to iCloud.
Make App MDM Managed if User Installed	Assume management of applications previously installed by users on their devices, whether applications are supervised or unsupervised. Enable this feature so that users do not have to delete the application version installed on the device. Workspace ONE UEM manages the application without having to install the AirWatch Catalog version on the device.

5 In the **Tunnel & Other Attributes** tab, enter the following information:

Per App VPN Profile	Select a VPN profile that you want to use for the application. Users access the application using a VPN, which helps ensure that application access and use is trusted and secure.
Other Attributes	App attributes provide device-specific details for applications to use. For example, when you want to set a list of domains that are associated to a distinct organization.

6 In the **Application Configuration** tab, enter the following information:

Settings	Description
UPLOAD XML	You can upload an XML file that contains the key value pairs supported by the application for the app configuration.

7 Select **Add Assignment**, to add more assignments for your publication.

8 In the **Exchange Settings**, enter the following information:

Table 3-1.

Settings	Descriptions
Exchange URL	Enter the Exchange URL. **Note** If you are using SEG then insert the SEG URL here.
Exchange User Name	Enter the Exchange user name.
User Email	Enter the user's email address.
Authentication Type	Select the type of authentication. **Note** For certificate authentication, configure and upload certificate in SDK profile.

9 In the **App Policies**, enter the following information:

Table 3-2.

Settings	Descriptions
Allow Gallery	Enables or deactivate access and use of the device image gallery.
Allow Voice Recordings	Enables or deactivate the use of audio recording.
Allow Document Scanner	(iOS Only) Enables or deactivate the document scanning feature.
Allow Hyperlinks	(iOS Only) Allow users to enter hyperlinks.

Table 3-2. (continued)

Settings	Descriptions
Allow Annotation	(iOS Only) Allows the use of handwriting and highlighter tools.
Allow Attachments	Enables or deactivate note attachments feature. When deactivate, no attachment types are allowed.

10 Select **Create**.

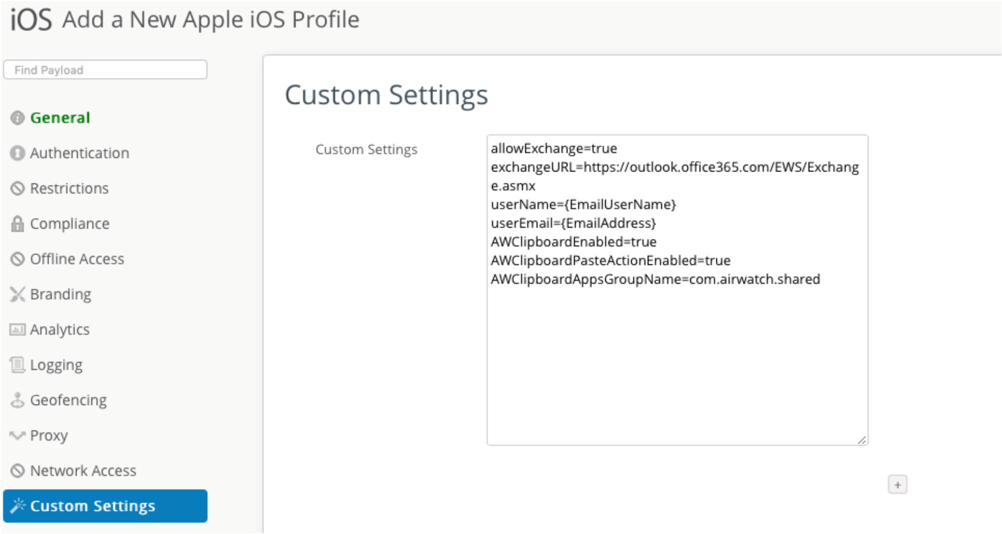
Application Configurations for Workspace ONE Notebook

4

Configure Workspace ONE Notebook settings using the configuration key and configuration value pairs. The steps provided in this page are applicable to assign the Notebook application for verisons 1.3 and below using the console versions of 2001 and below.

These configurations are set as a part of the SDK profile that you are planning to use for Notebook. If you are using the default SDK profile, set the application configurations by navigating to **Groups & Settings** > **All Settings** > **Apps** > **Settings and Policies** > **Settings**.

For example:



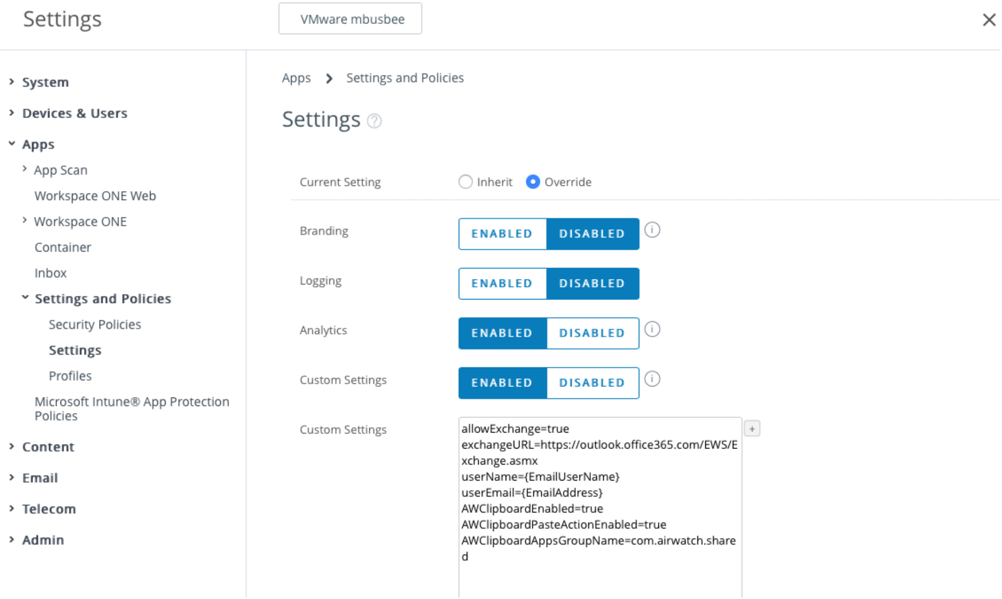
Custom Settings

Custom Settings

```
allowExchange=true
exchangeURL=https://outlook.office365.com/EWS/Exchange.asmx
userName={EmailUserName}
userEmail={EmailAddress}
AWClipboardEnabled=true
AWClipboardPasteActionEnabled=true
AWClipboardAppsGroupName=com.airwatch.shared
```

If you are using the custom SDK profile, **Groups & Settings** > **All Settings** > **Apps** > **Settings and Policies** > **Profiles** and choose the profile(s) that you have created for iOS and Android Notebook.

For example:



Current Setting ○ Inherit ● Override

Branding ENABLED [✓ DISABLED]

Logging ENABLED [✓ DISABLED]

Analytics [✓ ENABLED] DISABLED

Custom Settings [✓ ENABLED] DISABLED

Custom Settings

```
allowExchange=true
exchangeURL=https://outlook.office365.com/EWS/E
xchange.asmx
userName={EmailUserName}
userEmail={EmailAddress}
AWClipboardEnabled=true
AWClipboardPasteActionEnabled=true
AWClipboardAppsGroupName=com.airwatch.share
d
```

Account & Key Settings

Configuration Key	Value Type	Configuration Value	Description
{"exchangeURL":" URL"}	string	Specify the EWS URL. Use this format: https://server.domain.com/EWS/Exchange.asmx.	This configuration key is required. Allows user to synchronize notes with Exchange server.
{"userEmail": "{EmailAddress}" }	string	Provide a valid user email.	Enter the email address. This configuration key is required. The {EmailAddress} lookup value is supported.
{"userName": "{EmailDomain}\\{EmailUserName}" }	string	Enter the domain or username.	Provide a username for exchange server authentication. The {EmailUserName} lookup value is supported. Lookup value is available for Domain/Username as {EmailDomain}\\{EmailUserName} OR {EmailAddress}. **Note** For NTML auth it's specified in Domain\UserName format.
{"PolicyAllowLogging":"true"}	Boolean	True - enabled False - deactivate	This is a crash reporting data collection admin policy that controls the application reporting diagnostic data, which can be used to troubleshoot crash issues and provide support. If set to true, privacy manager allows the user to activate reporting.

Configuration Key	Value Type	Configuration Value	Description
{"PolicyAllowMetrics":"true"}	Boolean	True - enabled False - deactivate	Set to True to enable data collection for Workspace ONE Notebook experience improvement.
("PrivacyPolicyLink":"true"}	string	Example: https://www.acme.com	Provide the Policy URL that you want your users to visit when your company's privacy policy is selected from the privacy notice.
{"DisplayPrivacyDialog":1}	Integer	1 - enabled (default) 0 - deactivate	When set to 1 (enabled), Workspace ONE Notebook displays a privacy notice to the users about the data that is collected and the permissions that are required on the device for the app to function. If you do not set this configuration key, by default the privacy dialog will be shown.

OAuth-based Authentication

Add the following key value pair to enable the OAuth-based authentication with Exchange server.

Configuration Key	Value Type	Configuration Value	Description
{"AccountUseOauth":"true"}	Boolean	False - deactivate (default) True - enabled	Set to true to activate the OAuth-based authentication support with Exchange server.

Modern Authentication through WKWebView

Configuration Key	Value Type	Configuration Value	Description
{"AccountUseWebviewForOauth":"true"}	Boolean	True - activated False - deactivated	When set to True, the oauth flow is presented using a WKWebView instead of SFSafariViewController. **Note** The AccountUseWebviewForOauth key can be applied for managed accounts on Exchange server On- Premise or Office 365.

Configure Certificate-Based Authentication with Exchange

To activate CBA with Exchange Server, add the following key under the **Custom Settings** in the UEM console.

Configuration Key	Value Type	Configuration Value	Description
{"AccountUseCBA":"true"}	Boolean	False - deactivated (default) True - activated	Set this vale to true to activate Certificate Based Auth
{"AccountUseDualAuth":"true"}	Boolean	False - deactivated (default) True - activated	Set this value to true to activate Dual authentication (CBA and Basic).

Kerberos Authentication

Add the following key, to enable Kerberos authentication.

Configuration Key	Value Type	Configuration Value	Description
{"enableKerberos":"true"}	Boolean	False - deactivated (default) True - activated	Set this value to true to enable Kerberos authentication.

App Features

If a configuration key is not set, the default value listed below will be reflected in the Notebook application behavior.

Configuration Key	Value Type	Configuration Value	Description
{"allowGallery":"true"}	Boolean	True - activated (default) False - deactivated	Enables or deactivates access and use of the device image gallery
{"allowVoiceRecordings":"true"}	Boolean	True - activated (default) False - deactivated	Enables or deactivates the use of audio recording.
{"allowDocumentScanner":"true"}	Boolean	True - activated (default) False - deactivated	(iOS only) Enables or deactivates the document scanning feature.
{"allowHyperlinks":"true"}	Boolean	True - activated (default) False - deactivated	(iOS only) Allow users to enter hyperlinks.
{"allowAnnotations":"true"}	Boolean	True - activated (default) False - deactivated	(iOS only) Allows the use of handwriting and highlighter tools.
{"allowAttachments":"true"}	Boolean	True - activated (default) False - deactivate	Enables or deactivates note attachments feature. When deactivated, no attachment types are allowed.

Enable Support for SEG

If you are configuring Notebook version 1.4 using the console version 2003 or below, you must add the following key to the Notebook's application configuration to support SEG.

Configuration Key	Value Type	Configuration Value	Description
{"EasDeviceIdentifier":"EasDeviceIdentifier"}	String	{EasDeviceIdentifier}	Device identifier to allowlists traffic by SEG and traffic proxied.

Note Android Notebook versions 21.01 and 21.02 do not support SEG.

Workspace ONE Notebook Features Matrix

5

Table 5-1. Workspace ONE Notebook compatibility Matrix by Platform

Features	iOS	Android
Deployment Methods		
VMware Workspace ONE	✓	✓
VMware Workspace ONE Intelligent Hub	✓	✓
'Data Loss Prevention		
Activate or deactivate copy paste	✓	✓
Activate or deactivate clip board	✓	✓
Application Settings		
Synchronize notes with Exchange server	✓	✓
Allow annotation compression	✓	✓
App Features		
Allow camera	✓	✓
Allow gallery	✓	✓
Allow document scanner	✓	x
Allow hyperlinks	✓	x
Allow attachments	✓	✓