

Application Management for Windows

VMware Workspace ONE UEM 2203

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

Copyright © 2022 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1** App Management for Windows in Workspace ONE UEM 4
- 2** Manage Applications with the Microsoft Store for Business 6
- 3** Flexera Software Vulnerability Manager Integration 11
- 4** Microsoft Intune App Protection Policies Integration 13

App Management for Windows in Workspace ONE UEM

1

Use Workspace ONE UEM powered by AirWatch to push Windows apps to Windows Desktop (Windows 10) devices. View what file types the system supports for each app type.

Application Types and Supported Platforms for Windows

Workspace ONE UEM classifies applications as internal, public, and Web and you can upload applications depending on the type. This topic describes the supported platforms and deployment for each of the application type.

Table 1-1. Application Types and Supported Platforms for Windows

Application Type	Supported Platforms
Internal	<p>Windows Desktop (Windows 10)</p> <ul style="list-style-type: none"> ■ APPX <p>Note Upload an APPX file, which can be x86, x64, or ARM. However, the APPX installs on only devices that use the same architecture. For example, if you use ARM, Workspace ONE UEM does not queue an installation command for the x64 and x86 architectures. It does not push the application to devices that use x64 or x86 architectures.</p> <ul style="list-style-type: none"> ■ EXE: Upload an EXE package of Win32 applications for Windows 10. ■ MSI: The MSI file, also called a Windows Installer, is a package that contains everything to install, maintain, and remove the software. ■ ZIP: Upload a ZIP package of Win32 applications for Windows 10.
Public (Free and Paid)	<p>The Microsoft Store for Business allows you to acquire, manage, and distribute applications in bulk. If you use Workspace ONE UEM to manage your Windows 10 devices, you can integrate the two systems. After integration, acquire applications from the Microsoft Store for Business and distribute the applications and manage their updated versions with Workspace ONE UEM. You can assign public applications imported from the Microsoft Store for Business to apply them to devices with the flexible deployment feature. You can also assign online and offline licenses depending on your license management strategy.</p>
Web Links	<p>The Workspace ONE UEM console supports Windows Desktop (Windows 10) to push and manage web links applications. A Web Clips Profile allows you to push URLs on to end-user devices for the easy access to important websites.</p> <p>You can add web links applications using two methods.</p> <ul style="list-style-type: none"> ■ As an application in the Resources section of the Workspace ONE UEM console. ■ As a Web clip device profile in the Devices section of the UEM console.

Manage Applications with the Microsoft Store for Business

2

The Microsoft Store for Business enables you to acquire, manage, and distribute applications in bulk. If you use Workspace ONE UEM to manage your Windows 10+ devices, integrate the two systems. After integration, acquire applications from the Microsoft Store for Business, distribute them, and manage their updated versions with Workspace ONE UEM. For information on Microsoft Store for Business processes, refer to <https://technet.microsoft.com/itpro/windows/manage/windows-store-for-business>.

Requirements common for both Offline and Online Licensing Model

- Windows 10+ Devices - Use Windows Desktop (Windows 10 devices) when assigning applications. The OG you select must be of a **customer** type.
- Azure Active Directory Services - Configure Azure Active Directory services in Workspace ONE UEM to enable the communication between the systems. This configuration enables Workspace ONE UEM to manage Windows devices and applications on these devices.

You do not need an Azure AD Premium account to integrate with the Microsoft Store for Business. This integration is a separate process from the automatic MDM enrollment.

Important Integration only works when the targeted organization group (OG) is a customer type OG where you configured Azure Active Directory Services.

- Microsoft Store for Business Admin Account with Global Permissions - Acquire applications with a Microsoft Store for Business admin account. Global permissions enable administrator to access all systems to acquire, manage, and distribute applications.
- File Storage is enabled for on-premises Workspace ONE UEM stores Microsoft Store for Business applications on a secure file storage system. On-premise environments must enable this feature in the Workspace ONE UEM console by adding the tenant identifier and tenant name on the Directory Services page. This requirement is part of the process to configure Azure AD Services.

Requirements for Online License Model

Azure Active Directory Device users must use Azure Active Directory to authenticate to content.

Requirements for Offline License Model

Workspace ONE UEM imports all the application packages and deactivates assignment actions while the process is in progress. When you re-import packages for purposes such as updates, Workspace ONE UEM downloads only those packages that changed. If you do not restrict the use of the app store on devices, then application updates push to devices from the Microsoft Store for Business. If you restrict the use of the app store on devices, then import updated applications in Workspace ONE UEM. Then, notify device users to install the updated version from the AirWatch Catalog.

Comparison of the Online and Offline Licensing Models of the Microsoft Store for Business

Online and offline models of the Microsoft Store for Business offer different capabilities. Select the model depending on how you want to manage your deployment. Capabilities include what system manages licenses, where app packages are stored, and what system authenticates to resources.

Table 2-1. Online and Offline Model Comparison - Different Capabilities

Feature	Online License Model	Offline License Model
License control	Licenses managed by the Microsoft Store for Business. Users can receive applications and claim licenses outside of your Workspace ONE UEM deployment.	Licenses managed by the enterprise. Use the offline licensing model to control application packages and updates. This model offers flexibility but requires attention to ensure that applications stay updated and licenses get renewed.
App package host	App package hosted by the Microsoft Store for Business.	App package hosted by the Workspace ONE UEM file storage for on-premises or in the Workspace ONE UEM SaaS environment.
Azure Active Directory	Devices must use your Azure Active Directory system to authenticate. Enable the Azure Active Directory system so Workspace ONE UEM and the Microsoft Store for Business can communicate.	Devices do not have to use the Azure Active Directory system to authenticate. However, you must enable the Azure Active Directory system so Workspace ONE UEM and the Microsoft Store for Business can communicate.
Restrict the app store	Devices cannot install applications because the restriction prevents the Microsoft Store for Business on the device.	Devices can still install applications because the app packages are hosted in the Workspace ONE UEM environment.

Table 2-2. Online and Offline Model Comparison - Same Capabilities

Feature	Online License Model	Offline License Model
Level where licenses are claimed	Licenses claimed by Workspace ONE UEM for the application at the user level.	Licenses claimed by Workspace ONE UEM for the application at the user level.
License reuse	Admins can revoke licenses through Workspace ONE UEM and reuse them.	Admins can revoke licenses through Workspace ONE UEM and reuse them.

Import Public Applications Acquired from the Microsoft Store for Business

You can import public applications acquired from the Microsoft Store for Business to Workspace ONE UEM console. The process is the same for the online and offline license models. For the offline license model, plan to import these applications when your corporate network is not busy. Due to the number of applications concerned, the import process can use more bandwidth than other Workspace ONE UEM systems.

- 1 Go to the organization group where you set your Azure Active Directory services.
- 2 Navigate to **Resources > Applications > Native > Public** and select **Add Application**.
- 3 Select the **Platform**.
- 4 Select **Import from BSP** and choose **Next**.
- 5 View a list of the applications that Workspace ONE UEM imports from your Microsoft Store for Business account. You cannot edit this list in the Workspace ONE UEM console.
- 6 Select **Finish**.
 - Offline license model - The system downloads applications to the remote file storage system.
 - Online license model - The system stores the applications in the Microsoft Store for Business and awaits an install command.

Deploy Public Applications acquired from the Microsoft Store for Business

You can assign public applications acquired from the Microsoft Store for Business to apply them to devices with the flexible deployment feature. You can assign online and offline licenses depending on your license management strategy.

- 1 Navigate to **Resources > Apps > Native > Public**.
- 2 Select the application and choose **Assign**.

3 Complete the **Add Assignment** options to add a rule.

Setting	Description
Assignment - Online Licenses	<p>Assign groups to the application with online licenses.</p> <p>If devices are part of your Azure Active Directory system and your deployment has online licenses available, devices receive the application.</p> <p>If you assign both online and offline licenses to the group, the system gives preference to online licenses.</p>
Assignment - Offline Licenses	<p>Assign groups to the application with offline licenses.</p> <p>If your deployment has offline licenses available, devices receive the application.</p> <p>If you assign both online and offline licenses to the group, the system gives preference to online licenses.</p>
Deployment - App Delivery Method	<p>View the delivery method. On demand deploys content to a deployment agent and lets the device user decide if and when to install the content.</p>
Deployment - DLP	<p>Configure a device profile with a Restrictions profile to set data loss prevention policies for the application.</p> <p>Select Configure. The system navigates to the Profiles area. Select Add > Add Profile > Windows > Windows Desktop > Device Profile > Restrictions. Enable options that apply to the data you want to protect</p>

4 Select **Add** and prioritize assignments if you have more than one assignment rule.

5 Deploy the application with **Save & Publish**.

Reclaiming and Reassigning your Application License

When you assign Microsoft Store for Business applications to devices, the assignment process claims the corresponding licenses before the system initiates the installation of the application. The details view provides you with the list of user devices and the associated, claimed license. You can also delete the application assignment to reclaim and reassign the licenses. Synchronizing the offline and online licenses in the application details view provides you with the corresponding users of the licenses.

You can navigate to **Resources > Applications > List View > Public** and select the Microsoft Store for the Business application. This action displays the details view. In this view, use the **Sync License** action to import the list of users that correspond to claimed licenses. To see the claimed licenses, select the **Licenses** tab.

Note Workspace ONE UEM also imports the license associations when you select the Import from BSP option upon the initial import of your Microsoft Store for Business applications. This sync is performed asynchronous to the application package sync.

You can reclaim and reuse the licenses displayed on the **Licenses** tab by deleting the assignment of the application to the user's device. Workspace ONE UEM includes several methods to delete assignments. Deletion results in the removal of the application from the device.

Table 2-3. Methods to Reclaim Licenses

Method	Description
Details View	Select the Delete Application function in the details view of the application. This action removes the application off devices in groups assigned to the application.
Device	Delete the applicable device from the console.
Organization Group	Delete the organization group. This action impacts all assets and devices in the organization group.
Assignment Group	Delete the smart or user group assigned to the application. This action impacts every device in the group.
User	Delete the applicable user account from the console.

Configure Azure AD Integration

To configure your Azure AD, use an Azure admin account to sign up with the store and to activate the Workspace ONE UEM management tool.

- 1 Create an Azure admin account for Workspace ONE UEM. Configure an admin account with global admin roles in your Default Directory in Microsoft Azure. Use this account to acquire applications in the Microsoft Store for Business. You do not need an Azure premium account to create an admin account for the Microsoft Store for Business.
 - a In Azure, navigate to your Azure Active Directory.
 - b Select **Users and groups** and **+ New user**.
 - c Configure the **Directory role** as **Global administrator**.
 - d Create a temporary password so you can log in to the Microsoft Store for Business.
- 2 Activate Workspace ONE UEM in the Microsoft Store for Business and acquire apps. Activate the Workspace ONE UEM management tool in the Microsoft Store for Business with your Azure admin account credentials. If you use offline licensing, enable the acquirement of offline license applications.
 - a Navigate to the Microsoft Store for Business and log in with your Azure admin account.
 - b Navigate to **Manage > Settings > Distribute > Management tools** and activate the Workspace ONE UEM by VMware tool.
 - c For offline licenses, go to **Manage > Settings > Shop > Shopping experience** and enable **Show offline licensed apps to people shopping in the store**.
 - d In the Store for Business, add applications to your inventory. You can add applications with either offline or online licenses depending on your license management strategy.

Flexera Software Vulnerability Manager Integration

3

Flexera Software Vulnerability Manager (seen sometimes abbreviated as SVM) includes many features and one of these features is providing a curated list of patches for thousands of apps along with their vulnerability scores. In Workspace ONE UEM, you can view, validate, and assign managed, Windows 10 apps according to their score as reported by Flexera Software Vulnerability Manager.

Requirements

- Use Flexera Software Vulnerability Manager v7.6.1.16 or 2021 R1.
- Use Workspace ONE UEM console v2101 or later.
- Use Windows 10 devices that are enrolled with Workspace ONE UEM and also have the Flexera Software Vulnerability Manager agent running.
- Use SVM Patch Daemon v5.0.381 or later.

How Do You Configure Integration?

Configure your SVM Patch Daemon and work with desired apps in Workspace ONE UEM.

- 1 Configure the SVM Patch Daemon with your Workspace ONE UEM credentials.
 - a Start the SVM Patch Daemon and select the **Workspace ONE** tab.
 - b Enter your Workspace ONE UEM instance credentials.
 - c Select the type of authentication.
 - d Provide the REST API key for the tenant hierarchy where you want to publish the patches.
The SVM Patch Daemon displays a list of Workspace ONE UEM organization groups.
 - e Select the applicable Workspace ONE UEM organization group for your integration.
 - f Test the connection and validate the logging level on the **SVM** tab.
- 2 Identify and publish vulnerabilities in Software Vulnerability Manager.
 - a In Software Vulnerability Manager, review the critical patches in the **SPS** section or in the **Vendor Patch** module.

- b Identify the vulnerability to patch, and right-click the selection to create a package.
 - c Configure the packaged vulnerability with the package wizard. Select **Patch Daemon** as the publishing mode.
 - d Publish the package and monitor its status on the **Patch Deployment Status** page.
 - e Confirm the Workspace ONE environment details.
- 3 View, validate, and assign apps in Workspace ONE UEM.

Note Consider pushing to a device test group before pushing this integration to production devices.

- a In the Workspace ONE UEM console, go to **Resources > Apps > Native** and select the app type to see the apps **List View**.
- b Filter the **List View** using the **Flexera SVM** attribute to see the app with its assigned criticality (vulnerability score).
- c Validate the metadata for the app. The metadata includes installation contingencies and detection criteria converted from the app's applicability rules in Software Vulnerability Manager.
- d Add flexible deployment assignments to the app to push to devices. The integration installs the **Flexera SVM** app to only those devices that match the metadata (converted applicability rules).

Microsoft Intune App Protection Policies Integration

4

VMware Workspace ONE[®] powered by AirWatch integration with Microsoft Intune[®] App Protection Policies removes the management of DLP policies for your Microsoft Intune App Protection policies in two consoles.

You can configure the data loss prevention (DLP) application policies for your Microsoft Intune App Protection in Workspace ONE UEM. After you integrate the two systems, manage the DLP application policies in the Workspace ONE UEM console so that the integration stays current.

Most Microsoft Intune App Protection Policies are available for the Android platform and the iOS platform.

Manage in the Workspace ONE UEM Console to Stay Synced

After you integrate the two systems, manage the DLP application policies in the Workspace ONE UEM console so that the integration stays current. Workspace ONE UEM does not receive changes that are made in other parts of the integration. The DLP application policies or security group assignments can get out of sync.

User Experiences on Android and iOS

The iOS and Android platforms have different and similar user experiences when users first access apps after a successful integration with Intune.

Experience on iOS

When the device user authenticates to Microsoft Office 365 applications on iOS devices, and the profile pushed successfully, the system displays a pop-up stating that your organization manages the application. There are no additional steps in the configuration.

Experience on Android

To manage Android and Android Enterprise devices, users must install the Intune Company Portal application. This application acts as a broker for the Intune App SDK the same way the Workspace ONE Intelligent Hub acts as a broker for Workspace ONE UEM applications.

Common Experience on iOS and Android

Both platforms must set Intune as the MDM Authority on the device. You can configure this setting on the device in **Azure Tenant > All Resources > Intune**. Enable **Intune MDM Authority** from the **Getting Started** notification.

Do These Actions in Azure to Integrate Microsoft Intune

For integration, create a user account and assign the user the listed Microsoft licenses.

Those environments that do not have the Azure AD integration in Directory Services in the Workspace ONE UEM console, you must add the **AirWatch by VMware** app in Azure. Access [Configure Workspace ONE UEM to Use Azure AD as an Identity Service](#) for details.

Important If you already have Out of the Box Enrollment (OOBE) set up with any other MDM provider other than Workspace ONE UEM, add **AirWatch by VMware** and do not enter or edit any other settings in Azure. If you do enter or edit configurations, you might break the existing enrollment process.

- Create a service account (a user) in Azure, and assign the user the proper roles.

Note These steps are general. For current details about configuring Azure, see Microsoft documentation.

- a Go to your Azure portal by entering **portal.azure.com** in your browser.
- b Create a user or sync a user with On-Premises Active Directory.
Deactivate MFA (multi-factor authentication) for this user's domain.
- c Assign this user the listed roles.
 - **Intune Administrator**
 - **Application Administrator**
 - **Directory Reader**
 - **Directory Writer**
- If you created a user in Azure AD, use this account to log in to Azure at **portal.azure.com**. Ensure that the password is valid and does not need updating.
- You must assign the user the listed licenses in Azure.
 - Microsoft Intune App Protection Policies
 - Microsoft Enterprise Mobility + Security E3 or E5

Configure Intune Settings

In the Workspace ONE UEM console, configure and apply data loss prevention (DLP) application policies to Microsoft Intune® App Protection applications and data. Configure the Authentication tab first so the systems can communicate. Then configure your DLP settings and assign them to groups.

Workspace ONE UEM does not directly enforce policies on applications. The Microsoft SDK controls and enforces the policies.

Note The warning alters for the Operating System version and the App version. The Android Patch version only notifies the user with a warning message. However, the warning alerts do not stop the end users from using the app.

Prerequisites

To configure and apply DLP application policies to Intune applications, you must have the privileges to configure app policies in Intune.

Procedure

- 1 Navigate to **Groups & Settings > All Settings > Apps > Microsoft Intune® App Protection Policies**.
- 2 Select the **Authentication** tab and enter the user name and password for the Azure admin.

Administrators can use Office 365 DLP application policies to protect Office 365 apps and data with Microsoft Graph APIs. To configure Office 365 DLP policies, you need admin credentials to connect your tenant to Workspace ONE UEM.

Setting	Description
User Name	Enter the user name that is used to configure your tenant to Workspace ONE UEM.
Password	Enter the password that is used to configure your tenant to Workspace ONE UEM.

Workspace ONE UEM uses these credentials to search and assign the DLP application policies to the Microsoft Security Groups.

- 3 Select the Data Loss Prevention tab and configure the preferred Microsoft Intune App Protection Policies DLP application policies. Configure DLP app policies for your managed Microsoft Intune App Protection Policies applications and data.

Settings for Data Relocation	Description
Prevent Backup	Prevents users from backing up data from their managed applications.
Allow Apps to Transfer Data to Other Apps	<ul style="list-style-type: none"> ■ All - Users can send data from managed applications to any application. ■ Restricted - Users can send data from their managed applications to other managed applications. ■ None - Prevents users from sending data from managed applications to any application.

Settings for Data Relocation	Description
Allow Apps to Receive Data from Other Apps	<ul style="list-style-type: none"> ■ All - Users can receive data from applications to their managed applications. ■ Restricted - Users can receive data from other managed applications to their managed applications. ■ None - Prevents users from receiving data from all applications to their managed applications.
Prevent "Save As"	Prevents users from saving managed Microsoft Intune App Protection Policies application data to another storage system or area.
Restrict Cut Copy Paste with Other Apps	<ul style="list-style-type: none"> ■ Any App - Users can cut, copy, and paste data between their managed applications and any application. ■ Blocked - Prevents users from cutting, copying, and pasting data between managed applications and all applications. ■ Policy Managed Apps - Users can cut, copy, and paste data between managed Microsoft Intune App Protection Policies applications. ■ Policy Managed Apps with Paste In - Users can cut and copy data from their managed applications and to paste the data into other managed applications. <p>Users can also cut and copy data from any application into their managed applications.</p>
Restrict Web Content to Display in Managed Browser	Forces links in managed applications to open in a managed browser.
Encrypt App Data	Encrypts data pertaining to managed applications when the device is in the selected state. The system encrypts data stored anywhere, including external storage drives and SIM cards.
Disable Contents Sync	Prevents managed applications from saving contacts to the native address book.
Disable Printing	Prevents users from printing data associated with managed applications.
Allowed Data Storage Locations	Admins can control where users can store managed application data.
Settings for Access	Description
Require PIN for Access	Requires users to enter a PIN to access managed applications. Users create the PIN during their initial access.
Number of Attempts before PIN Reset	Sets the number of entries users attempt before the system resets the PIN.
Allow Simple PIN	Users can create four-digit PINs with repeating characters.
PIN Length	Sets the number of characters users must set for their PINs.
Allowed PIN Characters	Sets the characters that users must configure for their PINs.
Allow Fingerprint Instead of PIN	Users can access managed applications with their fingerprints rather than PINs.
Require Corporate Credentials For Access	Users can access managed applications with their enterprise credentials.

Settings for Access	Description
Block Managed Apps from Running on Jailbroken or Rooted Devices	Prevents users from accessing managed applications on compromised devices.
Recheck The Access Requirements After (minutes)	<p>Sets the system to validate the access PIN, fingerprint, or credential information when the access session reaches one of the time intervals.</p> <ul style="list-style-type: none"> ■ Timeout - The number of minutes the access sessions for managed applications are idle. ■ Offline Grace Period - The number of minutes devices with managed applications are offline.
Offline Interval (days) before App Data is Wiped	Sets the system to remove managed application data from devices when devices are offline for a set number of days.

Settings for Android	Description
Block Screen Capture and Android Assistant	If Yes is selected, screen captures and Android Assistant app scanning are unavailable when using an Office app.
Minimum Operating System version required	Enter the required minimum Android OS version number that a user must have to gain secure access to the app.
Minimum Operating System version required (Warning alert only)	Enter the minimum Android OS version number that a user must have to gain secure access to the app.
Minimum App version required	Enter the required minimum App version number that a user must have to gain secure access to the app.
Minimum App version required (Warning alert only)	Enter the minimum App version number that a user must have to gain secure access to the app.
Minimum Android patch version required	Enter the oldest required Android security patch level a user can have to gain secure access to the app.
Minimum Android patch version required (Warning alert only)	Enter the oldest Android security patch level a user can have to gain secure access to the app.

- 4 Select the **Assigned Groups** tab and assign the DLP application policies to the Microsoft Security Groups. The security groups are previously configured in Azure.

Setting	Description
All Security Groups	<p>Enter the name of the security group and assign it to the DLP app policies. Select from the list the system displays after an entry.</p> <p>Select Add Group and assign the DLP app policies to the security group.</p>
Security Groups Assigned to O365 Policies	<p>Lists the security groups assigned to the DLP app policies.</p> <p>Select Remove Group and remove the assignment from the security group.</p>

Warning Messages for Deleted and Modified Policies

After the Microsoft Intune App Protection Policies load, Workspace ONE UEM console checks for deletions and modifications in Intune in the Azure portal. It is possible for managed policies to get out of sync with the deployed policies. To warn admins about possible deletions and modifications, the Workspace ONE UEM console displays warning messages based on the scenario.

- Policy was deleted on the Microsoft Intune Portal. Click Delete Settings to delete the policy settings from UEM.

The Workspace ONE UEM console displays this message after someone deletes one or both iOS and Android policies deployed in Intune. Selecting **Delete Settings** removes the settings of both policies from the Workspace ONE UEM console without modifying anything on the Azure side. The console page does not refresh automatically.

Users can deploy new iOS and Android policies to Azure without error.

Note If only one of the policies, iOS or Android, is deleted in Azure, the other policy still remains in Azure. Users must manually delete the other policy if they choose not to keep the past settings.

- Policy settings were updated on the Microsoft Intune portal and are out of sync with Workspace ONE UEM. Click Sync Settings to update this policy in UEM.

The Workspace ONE UEM console displays this message after someone modifies both iOS and Android policies in Intune in the Azure portal and the policy settings still match between the two policies. Selecting **Sync Settings** updates the settings of both policies in Workspace ONE UEM to match those pulled from the policies in Azure. The console page does not refresh automatically.

Note This scenario excludes settings that are specific to iOS or Android such as iOS SDK settings and Android Assistant settings.

- "Receive data between other apps" policy is different for Android policy and iOS policy in Azure Portal. This setting needs to be the same for Workspace ONE UEM to sync the Android and iOS policy. Contact IT administrator to resolve the issue.

"Receive data between other apps" and "Send org data to other apps" policies are different for Android policy and iOS policy in Azure portal. These settings need to be the same for Workspace ONE UEM to sync the Android and iOS policy. Contact IT administrator to resolve the issue.

"Prevent Backups", "Receive data between other apps", and "Send org data to other apps" policies are different for Android policy and iOS policy in Azure portal. These settings need to be the same for Workspace ONE UEM to sync the Android and iOS policy. Contact IT administrator to resolve the issue.

The Workspace ONE UEM console displays these messages after someone modifies both policies in Intune in the Azure portal but the policy settings do not match between the two policies. The messages list the setting discrepancies between the two policies in Azure. They also list the policy names listed in Azure and not the ones used by the Workspace ONE UEM console.

Resolve the conflicts listed in the messages before using the **Sync Settings** menu item in the Workspace ONE UEM console.

Note This scenario excludes settings that are specific to iOS or Android such as iOS SDK settings and Android Assistant settings.

The **Delete Settings** menu item and the **Sync Settings** menu item do not modify any settings in Intune in the Azure portal.