Application Management for Windows

VMware Workspace ONE UEM 1909

vmware®

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

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Contents

Application Management for Windows 1

Use Workspace ONE UEM powered by AirWatch to push Windows public and internal applications, web apps and SaaS applications to Windows desktop and phone devices.

This chapter includes the following topics:

Application Types and Suported OS Versions for Windows

Workspace ONE UEMclassifies applications as native (internal, public, purchased), SaaS, and Web. You upload applications depending on the type. Workspace ONE UEM supports the following OS Versions for Windows applications based on the application type.

Table 1-1. Application Types and Supported OS Versions for Windows

Application Type	Supported Platforms
Internal	■ Windows Phone ■ Windows Desktop
Public (Free and Paid)	■ Workspace ONE UEM can manage free, public applications on Windows 10+ devices when you integrate with the Microsoft Store for Business. ■ Windows Desktop Workspace ONE UEM can manage free, public applications on Windows 10+ devices when you integrate with the Microsoft Store for Business.
Web Links	Windows Desktop
SaaS	Windows Desktop

Enable Workspace ONE UEM to Distribute Windows Desktop Internal Applications

Set the Workspace ONE UEM console to distribute approved Windows Desktop internal applications automatically with a side loading key. This process is not needed for Windows 10+.

Prerequisites

Before you can distribute internal applications to Windows Desktop devices, you must obtain two items from Microsoft.

- Side loading key (not needed for Windows 10+)

  Workspace ONE UEM sets a property to allow the side loading of applications on Windows 10 devices. This step occurs after the device enrolls with the Workspace ONE UEM system.

- Code signing certificate

Visit the Windows Dev Center for information about side loading keys and code signing certificates for Windows Desktop applications.

Important These settings affect devices enrolled after you have prepared the Workspace ONE UEM console for application distribution. If you change the side loading key after devices enroll, all devices must re-enroll to access internal applications.

Important The key provided by a Volume Licensing portal, such as https://www.Microsoft.com/licensing/servicecenter/default.aspx, might be limited to a specific number of device activations. Verify that there is a key available for your use. For more information, visit the Microsoft Developer Network site.

Procedure

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Desktop > Enterprise Apps**.
2. Complete the following options.

Setting	Description
Enable Enterprise Application Manager	Allows Workspace ONE UEM to push approved internal applications to Windows Desktop devices.
Side Loading Key	Enter the key provided by the Windows Dev Center. For example: ADQ2Z-6TP3W-4QGHK-PSDAW-8WKYR

3. Select **Save**.

   This process uploads the side loading key into the Workspace ONE UEM console and automatically enables corporate devices to install the enterprise internal application.

Root CA for Windows Desktop to Push Internal Applications

You can push internal applications made for the latest Windows Desktop version from Workspace ONE UEM with the root certificate authority (CA) of your company instead of with a third-party root CA.

Trusted Root CA

Make sure that your root CA is part of the trusted root CA list of the device. If it is not trusted, the Workspace ONE UEM system cannot deploy the application to Windows devices.

The Certificate Authorities (CA) settings page is used to configure integration with various certificate authorities and you can find it at **Groups & Settings > All Settings > System > Enterprise Integration > Certificate Authorities**.

Enable Workspace ONE UEM for Windows Phone Application Distribution

Distribute applications to devices using the Workspace ONE Intelligent Hub instead of a catalog. Set the Workspace ONE UEM console to distribute approved Windows Phone internal applications automatically with the AET you received when registering with the Windows Phone Dev Center.

Procedure

1. Navigate to **Groups & Settings > All Settings > Devices & Users > Windows > Windows Phone > Hub Settings**.
2. Select the **Enable Enterprise App Management** option in the **Enterprise App Management** section.
3. Select **Upload** in the **Upload Enterprise Token** text box to browse for the AET file and save your settings.

Register Applications With the Windows Phone Dev Center

Before you can distribute internal applications to Windows Phone devices, you must create, register, and gain approval from the Windows Phone Dev Center.

See the Windows Dev Center for current documentation on how to develop applications for Windows Phone and for prices to join the development center.

Procedure

1. **Register** a Microsoft account for your company with the Windows Phone Dev Center.

   There is a small fee to join, and the subscription enables your company to add applications to the Windows Phone Store. Registration creates a Windows account ID that you must use to obtain a Symantec authentication certificate. For more information about a Microsoft account, visit the Microsoft Developer Network site.

2. **Obtain** a Symantec Enterprise Mobile Code Signing Certificate for the internal application.

   Obtain an Enterprise Mobile Code Signing Certificate from Symantec with the Windows account ID. Use the certificate to sign and verify that your company built the application. Also, use the certificate to generate the application enrollment token (AET) used by each device to obtain a copy of the application.

3. **Build** and digitally sign the internal application.

   Develop and test the corporate application. When the application is ready for distribution, digitally sign the application by following the Precompile and Signature steps outlined in the Windows Phone Dev Center instructions.

4. **Generate** an AET for the internal application.

   Generate an AET that devices use to authenticate before installing the internal application. You can upload the AET to the Workspace ONE UEM console. This action automatically enables corporate devices to install the internal application. Generate an AET by following the AET generation walkthrough outlined by the Windows Phone Dev Center.

Installation Status of Windows 10 Applications in the Workspace ONE Catalog

Windows 10 device users can view the installation status of applications in their Workspace ONE catalog. This feature let's users know when installation of these large applications is complete and ready for use.

Reason

Applications for Windows 10 devices are often large and take several minuets to download. In the past, users did not have a visual representation of the application installation. If an installation took 10 minutes, a user might decide the installation had failed after five minutes and prematurely cancel the installation.

Workspace ONE now displays the installation status of applications so users can estimate when downloads complete and when applications are available for use.

Supported Application Types

Workspace ONE supports this feature for these file formats and application types.

Table 1-2. View Application Installation Status Support for Windows 10

Platform	Application Type	File Formats
Windows Desktop Windows Phone	Internal	XAP APPX Win32 (EXE, MSI, ZIP)
Windows Desktop Windows Phone	Public	XAP APPX

Required Components

Ensure that you configure the required components for the software distribution system. This system, also called software package deployment, is required because it communicates the installation status to Workspace ONE on devices. For software distribution requirements, see Requirements to Deploy Win32 Applications for Software Distribution.

Other components on devices include the following list.

- Workspace ONE v3.0
- Workspace ONE UEM App Deployment Agent v2.1 (available in the Workspace ONE UEM console v9.1.2+)

  The system deploys this agent when you enable the software package deployment.

Manage Applications with the Microsoft Store for Business

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 for Microsoft Store for Business Integration

Workspace ONE UEM supports the offline and online licensing models in the Microsoft Store for Business. Deploy Store for Business applications to Windows 10+ devices that communicate with your Azure Active Directory services.

Offline and Online License Model Requirements

- Windows 10+ Devices - Deploy to Windows 10+ devices because they are compatible with the bulk-acquirement and application deployment processes.

  Use the Windows Desktop or Windows Phone platforms when assigning applications.

You can deploy applications acquired through the bulk purchase process to older devices, like Windows 8 devices. The devices receive applications from Workspace ONE UEM through the regular process, and the system does not manage these applications.

- 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 you configure it in the same organization group 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 admins to access all systems to acquire, manage, and distribute applications.

Online License Model Requirements

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

Offline License Model Requirements

File Storage 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.

Comparison of the Online and Offline 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 1-3. 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.

Table 1-3. Online and Offline Model Comparison - Different Capabilities (continued)

Feature	Online License Model	Offline License Model
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 1-4. 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.

Configure Azure AD Identity Services Integration

Before you can use Azure AD to enroll your Windows devices, you must configure Workspace ONE UEM to use Azure AD as an Identity Service. Enabling Azure AD is a two-step process which requires the MDM-enrollment details to be added to Azure.

Prerequisites

You must have a Premium Azure AD P1 or P2 subscription to integrate Azure AD with Workspace ONE UEM. Azure AD integration with Workspace ONE UEM must be configured at the tenant where Active Directory (such as LDAP) is configured.

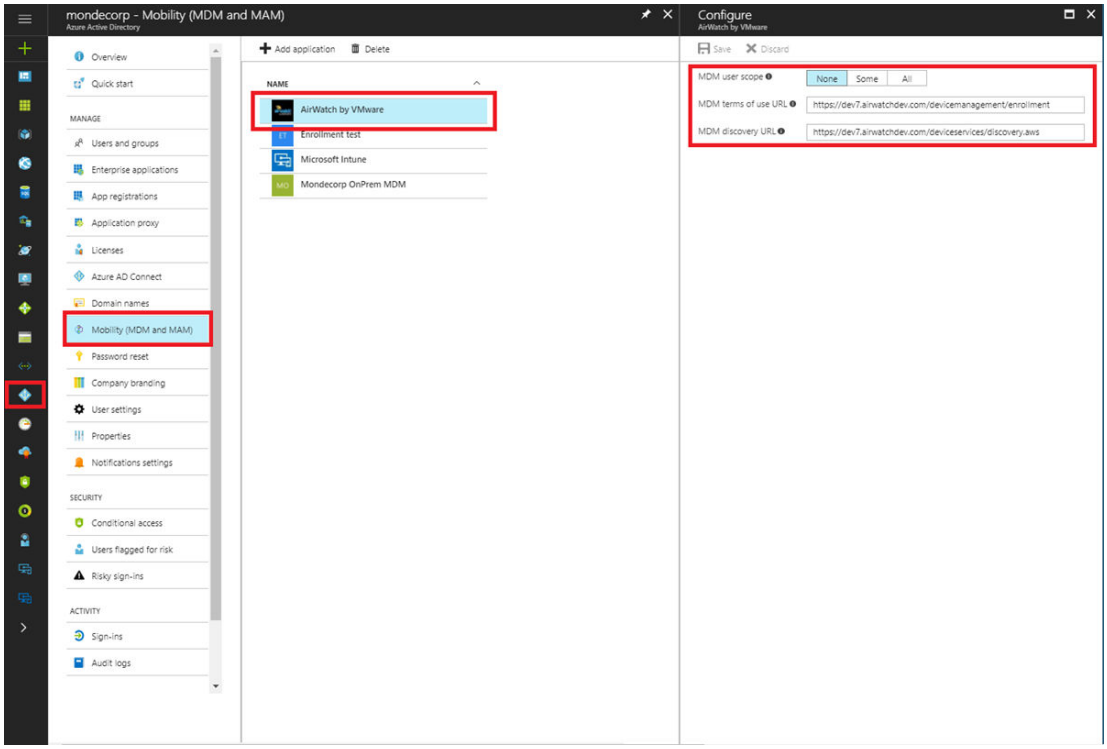
Important If you are setting the **Current Setting** to **Override** on the Directory Services system settings page, the LDAP settings must be configured and saved before enabling Azure AD for Identity Services.

Procedure

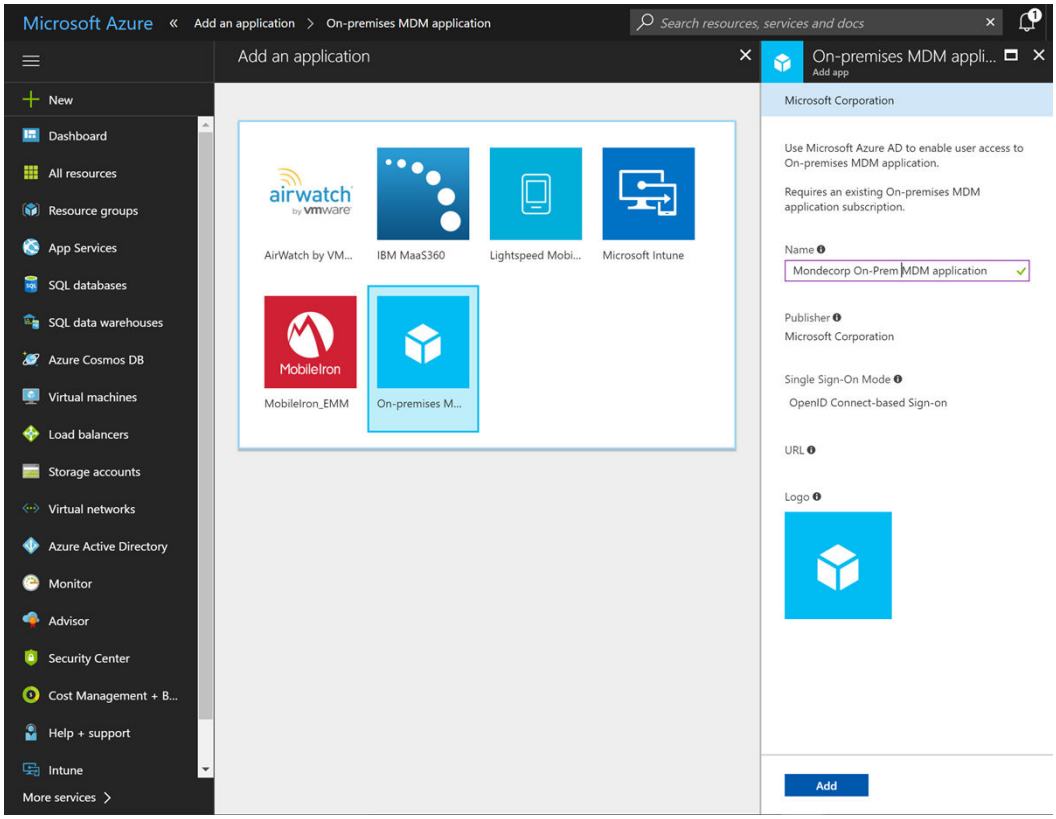
1. Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**.
2. Enable **Use Azure AD for Identity Services** under **Advanced** settings. Once enabled, take note of the MDM Enrollment and MDM Terms of Use URLs as they are needed when configuring the Azure directory.
3. Log in to the Azure Management Portal with your Microsoft account or organizational account.
4. Select your directory and navigate to the **Mobility (MDM and MAM)** tab. This tab was formerly the Applications tab.

5 Select **Add Application** and select the AirWatch by VMware application.

You can use the default URLs if the user scope is set to none. If needed, you can also use placeholder URLs.



6 Leave the AirWatch by VMware application on the default settings. Change the **MDM user scope** to **None**.



7 Select **Add Application** again and select the **On Premises MDM application**. You can rename the application when you add it.

8 Configure the On-Premises MDM application by entering the **MDM Enrollment URL** and **MDM Terms of Use** URLs from the Workspace ONE UEM Console.

9 Select **On-premises MDM application settings** then select **Required Permissions > Windows Azure Active Directory**.

10 Change the Application Permissions as follows:

   a Select **Read and write directory data**.

   b Select **Read and write devices**.

11 Change the Delegated Permissions as follows:

   a Select **Access the directory as the signed-in user**.

   b Select **Read directory data**.

   c Select **Sign in and read user profile**.

12 Select the Properties settings and enter your device services host in the **APP ID URI** text box.

   Use the same host that you used in the **MDM Enrollment URL** and **MDM Terms of Use** text boxes.

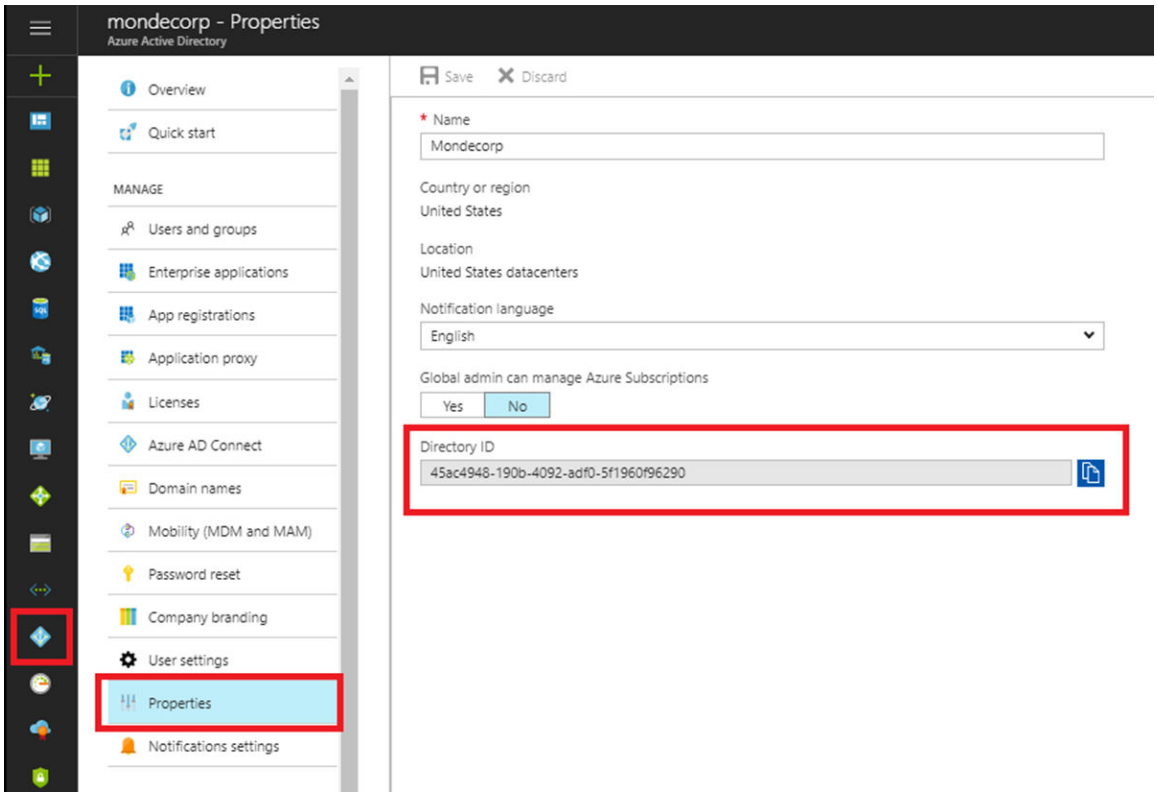
   https:// <MDM DS SERVER>

13 Set **MDM user scope** to **All** to apply these settings to all users.

You can also limit the OOBE enrollment to selected Azure AD groups by selecting **Some** and adding the preferred groups.

14 Select **Save** to continue.

15 Navigate to the Properties tab and find the Azure Directory ID. This setting was formerly called the **Tenant ID**.



16 Select **User Account Details** in the top right corner. The Azure **Tenant Name** is the name of your Azure Directory. You can find the name under the **Domain** tab.

17 Return to the UEM Console and select **Use Azure AD for Identity Services** to configure Azure AD Integration.

18 Enter the **Azure Directory ID** as the **Tenant Identifier**. Enter the default domain as your Azure Directory **Tenant Name**.

19 Select **Save** to finish the process.

Sign up and Acquire Applications From the Microsoft Store for Business for Offline and Online Licensing

For integration to work, use an Azure admin account to sign up with the store and to activate the VMwareWorkspace ONE UEM management tool.

See the Microsoft Store for Business portal for the most current documentation on creating an Azure admin account.

Procedure

1. Create an Azure sdmin 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.

Import Microsoft Store for Business Apps

Import public applications acquired from the Microsoft Store for Business to the 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.

Procedure

1. Go to the organization group where you set your Azure Active Directory services.
2. Navigate to **Apps & Books > Applications > Native > Public** and select **Add Application**.
3. Select the **Platform**, Windows Desktop or Windows Phone.
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.

What to do next

Follow the import by deploying applications outlined in Deploy Microsoft Store for Business Apps.

Package Downloads and Updates for the Offline License Model

Workspace ONE UEM imports all the application packages and disables assignment actions while the process is in progress. When you reimport 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.

Deploy Microsoft Store for Business Apps

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

For general information about the flexible deployment feature, how to prioritize assignments, and for setting descriptions, see Flexible Deployment to Assign Applications.

Procedure

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

2 Select the application and choose **Assign**.

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

Setting	Description
Assignment - Online Licenses	Assign groups to the application with online licenses. If devices are part of your Azure Active Directory system and your deployment has online licenses available, devices receive the application. If you assign both online and offline licenses to the group, the system gives preference to online licenses.
Assignment - Offline Licenses	Assign groups to the application with offline licenses. If your deployment has offline licenses available, devices receive the application. If you assign both online and offline licenses to the group, the system gives preference to online licenses.

Setting	Description
Deployment - App Delivery Method	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.
Deployment - DLP	Configure a device profile with a **Restrictions** profile to set data loss prevention policies for the application. Select **Configure**. The system navigates to **Devices > Profiles**. Select **Add > Add Profile** and the platform. ■ For Windows Desktop, select **Device Profile > Restrictions** and enable options that apply to the data you want to protect. ■ For Windows Phone, select **Restrictions** and enable options that apply to the data you want to protect.

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

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

Methods to Reclaim Licenses for Microsoft Store for Business Apps

Sync offline and online licenses with the details view of the application to view the corresponding users of the licenses. Choose a way to delete the assignment of the application off devices to reclaim and reassign licenses.

Sync Licenses to View Users and Claimed Licenses

When you assign Microsoft Store for Business applications to devices, the assignment process claims corresponding licenses before the system initiates the installation of the application. Use the details view to see the list of user devices and the associated, claimed license.

Navigate to **Apps & Books > 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.

Reclaim Licenses

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 1-5. 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.