Application Management for Windows

VMware Workspace ONE UEM

vmware®

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

Introduction to Managing Windows Applications

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 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	Windows Desktop ■ APPX **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. ■ 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. For more information, seeSoftware Distribution of Win32 Applications. Windows Phone ■ APPX **Note** Upload a single APPX file, which can be x86, x64, or ARM.
Public (Free and Paid)	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. For more information, see Manage Applications with the Microsoft Store for Business.
Web Links	The Workspace ONE UEM console supports Windows Desktop 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. You can add web links applications using two methods. ■ As an application in the **Apps & Books** section of the Workspace ONE UEM console. ■ As a Web clip device profile in the Devices section of the UEM console.

Configure Workspace ONE UEM to Distribute Windows Desktop Internal Applications

You can 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.

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.

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.

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.

1 Navigate to **Groups & Settings** > **All Settings** > **Devices & Users** > **Windows** > **Windows Phone** > **Agent 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.

Installation Status of Windows 10 Applications in the Workspace ONE Catalog

Applications for Windows 10 devices are often large and take several minuets to download. Workspace ONE displays the installation status of applications so you 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	Win32 (EXE, MSI, ZIP) APPX
Windows Desktop Windows Phone	Public	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 Software Distribution for Win32 Application Deployment Requirements.

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 common for both Offline and Online Licensing Model

- 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.

Requirements for Online License Model

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

Requirements for Offline License Model

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.

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.

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 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.
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.

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**, 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.

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** > **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.
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**.

Reclaiming and Reassigning your Applicaton 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 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.

Configure Workspace ONE UEM to Use Azure AD as an Identity Service

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.

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.

1 Navigate to **Groups & Settings > All Settings > System > Enterprise Integration > Directory Services**.

2 Enable **Use Azure AD for Identity Services** under **Advanced** settings. Copy the **MDM Enrollment URL** and the **MDM Terms of Use URL** because you must enter them in to Azure.

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.

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

6 Select the **AirWatch by VMware** app that you added to change the **MDM user scope** to **All**.

7 Paste your **MDM Terms of Use URL** from the Workspace ONE UEM console into the **MDM terms of use URL** text box in Azure. Paste your **MDM Enrollment URL** from the Workspace ONE UEM console into the **MDM discovery URL** text box in Azure.

8 Add an on-premises app by selecting **Add Application > On Premises MDM application**, and then selecting **Add**.

9 Select the **On Premises MDM application** again and configure the on-premises MDM application. Set the **MDM user scope** to **All** or **Some** and select a group of users.

10 Enter the Workspace ONE UEM console URLs to the **On Premises MDM application** and save the settings.

- Paste your **MDM Terms of Use URL** from the Workspace ONE UEM console into the **MDM terms of use URL** text box in Azure.
- Paste your **MDM Enrollment URL** from the Workspace ONE UEM console into the **MDM discovery URL** text box in Azure.

11 Select **On-premises MDM application settings > Expose an API**.

Note You no longer need to use the On-premise MDM application for this step if you are unable to save the application URI and are in a Shared Saas Environment.

12 Select **Edit** for **Application ID URI** and enter your Device Services URL in the **Application ID URI** text box. **Save** the settings.

13 You can select and assign premium licenses in Azure.

- In the Microsoft Azure console, select **Azure Active Directory > Licenses** and select **All Products**. Select the proper license in the list.

- Select **Assign**, select the users or groups for the license, and select **Assign**.

14 Copy the **Directory ID** and the primary domain to enter into the Workspace ONE UEM console.

- Navigate to the **Properties** tab and find the Azure **Directory ID** and copy it.
- Select **Custom domain names** and copy the **Name** that is listed as the primary domain.

15 Return to the Workspace ONE UEM console and select **Use Azure AD for Identity Services** to configure Azure AD Integration.

16 Enter the directory ID you copied to the **Directory ID** text box.

17 Enter the primary domain you copied in **Tenant Name** text box.

18 To finish the process, select **Save**.

Configure Azure AD Identity Services Integration

To configure your Azure AD Identity Services Integration, 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.