

Smart Glasses

VMware Workspace ONE UEM 2001



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

Copyright © 2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

1	Smart Glasses Integration with Workspace ONE UEM	4
	Before You Begin Deploying Smart Glasses	4
2	Smart Glasses Enrollment	6
	Create an Enrollment User	6
	Upload the Workspace ONE Intelligent Hub .APF File for Smart Glasses	7
	Create Android (Legacy) Wi-Fi Profile for Staging Smart Glasses(Optional)	7
	Create a Staging Package for Smart Glasses	8
	Generate a Sideload Staging Package	9
	Enroll Google Glass Using QR Code Enrollment	10
3	Smart Glasses Profiles	11
	Create Wi-Fi Profile	12
4	Smart Glasses Device Management Overview	14
	Deploy Internal Applications as a Local File	14
	Add Assignments and Exclusions to Applications	19
	Smart Glasses Feature Matrix	22

Smart Glasses Integration with Workspace ONE UEM

1

Workspace ONE UEM powered by AirWatch™ provides you with a robust set of mobility management solutions for enrolling, securing, configuring, and managing your Smart Glasses deployment. Through the Workspace ONE UEM console, you have several tools and features at your disposal for managing the entire life-cycle of Smart Glasses.

The glasses display information in a hands-free smartphone-like format, and wearers communicate with the device using natural language voice commands. The voice-command feature of Smart Glasses allows users to prompt for instructions as they work without ever having to take their focus off of the equipment.

This chapter includes the following topics:

- [Before You Begin Deploying Smart Glasses](#)

Before You Begin Deploying Smart Glasses

Before deploying Smart Glasses, consider the following requirements from the Workspace ONE UEM team. Familiarizing yourself with the information available in this section helps prepare you for a successful deployment of devices.

Supported Operating Systems

- Workspace ONE UEM console v8.2+
- A PC or Mac computer equipped with Android Debug Bridge is needed for sideload staging.
- Google Glass only: 1st edition Google Glass OS version EE13-EE15 is deployed with Android (Legacy) settings.
 - First edition Google Glass runs a version of the Android OS, but not all features that are available on mobile devices are available on Google Glass. Google Glass OS versions are identified as EE x . Google Glass EE13-EE15 has the capability for Workspace ONE UEM to push apps and is the minimum recommended version for customers. Contact Google to get information on how to upgrade your device.
- Google Glass EE2 provides Android Work Managed Device Mode functionality. This documentation will include separate sections for Google Glass EE2 deployment.

Best Practices

- All Smart Glasses must be registered in the Workspace ONE UEM console in a separate Organization Group.
- Disable the following enrollment settings:
 - Terms of Use
 - Optional Prompts
- Create separate Android (Legacy) profiles for your Smart Glasses deployment with Google Glass EE15 or below. Do not reuse Android (Legacy) mobile profiles.
- Enable Direct Prompt in Hub Settings to allow silent application install.

Google Glass EE2 Best Practices

The latest version of Google Glass, Google Glass EE2, provides Android functionality that is highlighted in this section.

- Google Glass EE2 devices must be enrolled into an Organization Group that is enabled for Android. This is done by registering with Google under **Settings > Device & Users > Android > Android EMM Registration**.
- Create separate Android profiles for your Smart Glasses deployment with Google Glass EE2. Do not reuse Android mobile profiles.

Smart Glasses Enrollment

2

All Smart Glasses in your deployment must be enrolled before they can communicate with Workspace ONE UEM and access internal content and features. Enrollment is facilitated with the Workspace ONE Intelligent Hub for Android.

Important The Google Glass enrollment script in the staging package includes additional commands that can be manually enabled. If you plan on blocking adb access, please note that if adb needs to be re-enabled at a later time, it can only be done by a trusted computer. This will typically be the computer that was used to run the script in the first place, or any computer trusted previously by Google Glass prior to enrollment.

This chapter includes the following topics:

- [Create an Enrollment User](#)
- [Upload the Workspace ONE Intelligent Hub .APF File for Smart Glasses](#)
- [Create Android \(Legacy\) Wi-Fi Profile for Staging Smart Glasses\(Optional\)](#)
- [Create a Staging Package for Smart Glasses](#)
- [Generate a Sideload Staging Package](#)
- [Enroll Google Glass Using QR Code Enrollment](#)

Create an Enrollment User

Procedure

- 1 Navigate to **Devices > Users > List View > Add > Add User**.
- 2 From the **General** tab, enter the details for your user.

Setting	Description
Security Type	Choose Basic to add a basic user.
Username	Enter a username with which the new user is identified.
Password	Enter a password that the user can use to log in.
Confirm Password	Confirm the password.
Full Name	Complete the First Name, Middle Name, and Last Name of the user.

Setting	Description
Display Name	Enter a name to represent the user in the Workspace ONE UEM console.
Email Address	Enter or edit the user's email address.
Email Username	Enter or edit the user's email username.
Domain	Select the email domain from the drop-down field.

- 3 Select **Save**.

Upload the Workspace ONE Intelligent Hub .APF File for Smart Glasses

Upload the .apf file for your Smart Glasses deployment to enable a simplified enrollment.

The Hub Package can be uploaded only in specific organization group types, for example, in organization groups of type 'Customer'. It is recommended to upload the Workspace ONE Intelligent Hub Package at the highest organization group. You can find the file specific to your OEM located in MyWorkspace ONE.

Procedure

- 1 Navigate to **Devices > Provisioning > Components > Hub Packages** and select **Add**.
Make sure you are using the top level organization group.
- 2 Select **Upload** and **Choose File** to browse for the .apf file of the Workspace ONE Intelligent Hub version you want to upload.
- 3 Select the .apf file and select **Open** to choose the file.
- 4 Select **Save** to close the upload dialog.
- 5 Enter a **File Name**.
- 6 Enter a **Package Name**.
- 7 Enter a **Version** for the Workspace ONE Intelligent Hub.
- 8 Select **Save** to upload the .apf file to the Workspace ONE UEM console.

Create Android (Legacy) Wi-Fi Profile for Staging Smart Glasses(Optional)

The staging Wi-Fi profile connects a device to a Wi-Fi network used for enrollment if the device is not configured to a network.

Procedure

- 1 Navigate to **Devices > Provisioning > Components > Profiles > Add Profile > Android (Legacy)**.
- 2 Select the **General** profile option.

- 3 Set the Profile Scope of the Wi-Fi profile.
 - **Staging Wi-Fi Profile** – Connects a device to the Wi-Fi used for staging.
 - **Production Wi-Fi Profile** – Connects a device to the Wi-Fi used for everyday use. Production Wi-Fi profiles are under **Device > Profiles > List View > Add**. You must use auto deployment and publish the profile before staging a device with it.
 - **Both** – Connects the device to Wifi to be used for staging and continues use during production.
- 4 Navigate to **Wi-Fi > Configure**.
- 5 Provide the Service Set Identifier to name the network to which the device will connect.
- 6 Indicate if the Wi-Fi network is a Hidden Network.
- 7 Ensure the WiFi is setup as the Active Network.
- 8 Specify the Security Type of access protocol used and whether certificates are required.
- 9 Provide the Password required for the device to connect to the network.
- 10 Select **Save & Publish**.

Create a Staging Package for Smart Glasses

Create a staging package to configure your devices to connect to Wi-Fi, download the Workspace ONE Intelligent Hub, and enroll Smart Glasses with minimal interaction.

Procedure

- 1 Navigate to **Devices > Lifecycle > Staging > Add Staging > Android (Legacy)**.

Staging
✕

General
Manifest

Name*

Description

Owned By*

Enrollment User*

Password*

☐ Show Characters

Confirm Password*

Agent

LaunchAutoEnrollWinMo - 3.0
▼

Save
Cancel

- 2 Complete the required fields on the **General** tab.

Settings	Description
Name	Enter the name of the staging configuration.
Description	Enter the description of the staging configuration.
Enrollment User	Enter the username of the enrollment user.
Password	Enter the password for the enrollment user.
Confirm Password	Re-enter the password for the enrollment user.
Hub	Select the Workspace ONE Intelligent Hub to download during staging. These are uploaded as the Workspace ONE Intelligent Hub Package. See how to Upload the Workspace ONE Intelligent Hub .APF File for Smart Glasses

- 3 Select **Save**.

Generate a Sideload Staging Package

Workspace ONE UEM can create a sideload staging package that allows you to create one side staging enrollment for all devices and assign the device to an Organization Group as needed.

Procedure

- 1 Navigate to **Devices > Lifecycle > Staging > List View**.
- 2 Choose a previous staging package that you want to create a sideloaded staging package for. Select the **More** option and select **Staging Side Load** from the drop-down.
- 3 Choose the **Organization Group** to which this staging applies.
- 4 Select **Download** to start downloading the zip file of the staging sideload.
- 5 Download and install the Android Debug Bridge to the computer from which you will stage devices.
For more information, see <http://developer.android.com/tools/help/adb.html>.
- 6 Unzip the staging file and connect the Smart Glasses to the staging computer.
- 7 Ensure that the Android Debug Bridge is enabled and running on the staging computer.
- 8 Run the autoenroll script.
 - a Find the script from the Workspace ONE Intelligent Hub folder saved to your computer and run the script from within the Workspace ONE Intelligent Hub folder.

Note The auto-enroll script for Google Glass devices allows you to manually enable the following commands: Setting OTA server, Lock ADB access, Set an app into kiosk mode, and enable/disable camera.

The device should auto enroll into Workspace ONE UEM.

Enroll Google Glass Using QR Code Enrollment

The QR code enrollment method sets up and configures Google Glass smart glasses by scanning a QR code. The QR code contains a payload of JSON values with all the information needed for the device to be enrolled.

Note Various word processing applications use special characters for editing. Using copy/paste can pick up those characters, invalidating your JSON. Consider validating your JSON using any free online tool.

You can use any online QR Code generator, such as Web Toolkit Online, to create your QR code before beginning enrollment. The QR code includes the Server URL and Group ID information. You can also include the user name and password or the user has to enter their credentials. Here is the format of the text to paste into the QR Code generator:

```
{
  "COMPONENT": "com.airwatch.androidagent/com.airwatch.agent.DeviceAdministratorReceiver",
  "LOCATION": "https://discovery.awmdm.com/mobileenrollment/airwatch.apk", "NFC_MIME": "application/
com.airwatch.agent.enroll",
  "NFC_MIME": "application/com.airwatch.agent.enroll",
  "EXTRAS": "serverurl=https://EnrollmentURL/AirWatch\nngid=EnrollmentOG\nun=EnrollmentUserName
\npw=EnrollmentUserPassword"
}
```

Note QR Code enrollment is only applicable to Google Glass.

Procedure

- 1 Follow the steps to create an enrollment user. See [Create an Enrollment User](#) .
- 2 Create QR code using a QR code generator.
- 3 From your Google glasses, go to **Settings > Device Options > Provisioning** which launches the QR code reader.
- 4 Scan your QR code and follow the prompts.
- 5 Use the RunIntent File/Action to enable commands such as Setting OTA server, Lock ADB access, Set an app into kiosk mode, and enable/disable camera.

What to do next

Important To manage applications, the intent "install_non_market_apps" needs to be executed on the device first. Please see EE14 and EE15 documentation from Google for all of the intents that are now supported on Google Glass.

Smart Glasses Profiles

3

Device profiles ensure proper use of devices, protection of sensitive data, and workplace functionality. Profiles serve many different purposes, from letting you enforce corporate rules and procedures to tailoring and preparing Glass devices for how they are used.

The individual settings you configure are called payloads. Consider configuring only one payload per profile, which means you have multiple profiles for the different settings you want to push to devices. For example, you can create a profile to integrate with your email server and another to connect devices to your workplace Wi-Fi network.

The way profiles are deployed for Google Glass depends on the edition. The chart below explains the differences:

Table 3-1. Profiles for Smart Glasses

Edition	Profile Selection
Google Glass EE13	Android (Legacy)
Google Glass EE14	Android (Legacy)
Google Glass EE15	Android (Legacy)
Google Glass EE2	Android

Deploying Profiles with First Edition Google Glass

For Google Glass, if you use certificate-based Wi-Fi, ensure that Screen Lock is set up and enabled before enrollment or certificate installation fails. Screen Lock is a device passcode on Google Glass devices. Steps to configure screen lock are as follows:

- Recovery code needs to be configured. This is achieved by running the following adb command (in this example, 12345 is the recovery code).
 - `$ adb shell am broadcast -a com.google.glass.action.STORE_RECOVERY_CODE --el RECOVERY_CODE 12345`
- Navigate to **Settings > Device Options > Screen Lock** to configure this option.

Deploying Profiles with Second Edition Google Glass

Google Glass EE2 uses Android Work Managed Device mode functionality. In the steps for creating a profile for Google Glass, select Android platform. For Google Glass EE15 and lower and other smart glasses, use Android (Legacy) platform.

This chapter includes the following topics:

- [Create Wi-Fi Profile](#)

Create Wi-Fi Profile

Configuring a Wi-Fi profile lets devices connect to corporate networks.

Procedure

- 1 Navigate to **Devices > Profiles > List View > Add > Add Profile > .**
- 2 Select **Android (Legacy) > or > Android (Second Edition Google Glass Only).**
- 3 Configure the **General** profile settings as appropriate.
- 4 Select the **Wi-Fi** payload and configure the Wi-Fi settings.

Setting	Description
Service Set Identifier	Provide the name of the network the device connects to.
Hidden Network	Indicate if the Wi-Fi network is hidden.
Set as Active Network	Indicate if the device connects to the network with no end-user interaction.
Security Type	<p>Specify the access protocol used and whether certificates are required. Depending on the selected security type, the displayed fields will change. If None, WEP, or WPA/WPA 2 are selected; the Password field will display. If WPA/WPA 2 Enterprise is selected, the Protocols and Authentication fields display.</p> <ul style="list-style-type: none"> ■ Protocols <ul style="list-style-type: none"> ■ Use Two Factor Authentication ■ SFA Type ■ Authentication <ul style="list-style-type: none"> ■ Identity ■ Anonymous Identity ■ Username ■ Password ■ Identity Certificate ■ Root Certificate
Password	Provide the required credentials for the device to connect to the network. The password field displays when WEP, WPA/WPA 2, Any (Personal), WPA/WPA2 Enterprise are selected from the Security Type field.

- 5 Select the **Credentials** payload and configure certificate setup that will be used to authenticate.

Settings	Description
Credential Source	<p>Upload a certificate from your local machine or define a Defined Certificate Authority, or upload a User Certificate.</p> <ul style="list-style-type: none">■ If you choose to Upload a certificate, complete the following:<ul style="list-style-type: none">■ Credential Name – Enter the name of the credential or select on the information symbol to view acceptable lookup values like {EmailDomain} and {DeviceModel} to find the credential file to use.■ Certificate – Upload the new certificate or lookup values.■ If you choose to use a Defined Certificate Authority, complete the following:<ul style="list-style-type: none">■ Certificate Authority for the Defined Certificate Authority – Select the external or internal CA issuing encryption keys for the PKI.■ Certificate Template for the Defined Certificate Authority – Select the predefined template for the CA to use when requesting a certificate.■ If you choose upload a User Certificate, select either S/MIME Certificate or S/MIME Encryption Certificate.

- 6 Select **Save & Publish**.

Smart Glasses Device Management Overview

4

After your devices are enrolled and configured, manage the devices using the Workspace ONE™ UEM console. The management tools and functions enable you to keep an eye on your devices and remotely perform administrative functions.

You can manage all your devices from the UEM console. The Dashboard is a searchable, customizable view that you can use to filter and find specific devices. This feature makes it easier to perform administrative functions on a particular set of devices. The Device List View displays all the devices currently enrolled in your Workspace ONE UEM environment and their status. The **Device Details** page provides device-specific information such as profiles, apps, Workspace ONE Intelligent Hub version and which version of any applicable OEM service currently installed on the device. You can also perform remote actions on the device from the Device Details page that are platform-specific.

This chapter includes the following topics:

- [Deploy Internal Applications as a Local File](#)
- [Smart Glasses Feature Matrix](#)

Deploy Internal Applications as a Local File

Upload internal applications with local files to deploy them to your mobile network and to take advantage of the mobile application management features of Workspace ONE UEM.

For internal Apple iOS applications, you must provide a provisioning profile so that the internal application works when it is managed in Workspace ONE UEM. Obtain this file from your Apple iOS application developers.

Procedure

- 1 Navigate to **Apps & Books > Applications > Native > Internal** and select **Add Application**.
- 2 Select **Upload > Local File** to browse for the application file on the system.

- 3 Select **Continue** and configure the **Details** tab options. Not every option is supported for every platform.

Details Setting	Details Description
Name	Enter a name for the application.
Managed By	View the organization group (OG) that the application belongs to in your Workspace ONE UEM OG hierarchy.
Application ID	Represents the application with a unique string. This option is pre-populated and was created with the application. Workspace ONE UEM uses the string to identify the application in systems like application whitelists and blacklists.
Actual File Version	Displays the coded version of the application set by the application's developer.
Build Version	Displays an alternate "File Version" for some applications. This entry ensures Workspace ONE UEM records all version numbers coded for applications because developers have two places within some applications they can code a version number.
Version	Displays the internal version of the application set by the Workspace ONE UEM console.
Supported Processor Architecture	Select the bit-architecture value for applicable Windows applications.
Is Beta	Tags the application as still under development and testing, a BETA version.
Change Log	Enter notes in this text box to provide comments and notes to other admins concerning the application.
Categories	Provide a category type in the text box to help identify how the application can help users. You can configure custom application categories or keep the application's pre-coded category.
Minimum OS	Select the oldest OS that you want to run this application.
Supported Models	Select all the models that you want to run this application.
Is App Restricted to Silent Install-Android	Assigns this application to those Android devices that support the Android silent installation feature. The end user does not have to confirm installation activity when you enable this option. This feature makes it easier to uninstall many applications simultaneously. Only Android devices in the smart group that supports the silent uninstallation benefit from this option. These Android devices are also called Android enterprise devices.
Default Scheme	Indicates the URL scheme for supported applications. The application is packaged with the scheme, so Workspace ONE UEM parses the scheme and displays the value in this field. A default scheme offers many integration features for your internal applications, including but not limited to the following options: <ul style="list-style-type: none"> ■ Use the scheme to integrate with other platform and web applications. ■ Use the scheme to receive messages from other applications and to initiate specific requests. ■ Use the scheme to launch Apple iOS applications in the AirWatch Container.

Details Setting	Details Description
Description	Describe the purpose of the application. Do not use '<' + String in the Description, as you might encounter an Invalid HTML content error.
Keywords	Enter words that might describe features or uses for the application. These entries are like tags and are specific to your organization.
URL	Enter the URL from where you can download the application and get information about it.
Support Email	Enter an email to receive suggestions, comments, or issues concerning the application.
Support Phone	Enter a number to receive suggestions, comments, or issues concerning the application.
Internal ID	Enter an identification string, if one exists, that the organization uses to catalog or manage the application.
Copyright	Enter the publication date for the application.

Developer Information Setting	Developer Information Description
Developer	Enter the developer's name.
Developer Email	Enter the developer's email so that you have a contact to whom to send suggestions and comments.
Developer Phone	Enter a number so that you can contact the developer.

Log Notification for App SDK Setting - iOS	Log Notification for App SDK Description - iOS
Send Logs To Developer Email	Enable sending logs to developers for troubleshooting and forensics to improve their applications created using a software development kit.
Logging Email Template	Select an email template uses to send logs to developers.

Installer Package Deployment Setting - Windows Desktop MSI	Installer Package Deployment Description - Windows Desktop MSI
Command Line Arguments	Enter command-line options that the execution system uses to install the MSI application.
Timeout	Enter the time, in minutes, that the installer waits with no indication of installation completion before it identifies an installation failure. When the system reaches the timeout number, it stops monitoring the installation operation.

Installer Package Deployment Setting - Windows Desktop MSI	Installer Package Deployment Description - Windows Desktop MSI
Retry count	Enter the number of attempts the installer tries to install the application before it identifies the process as failed.
Retry interval	Enter the time, in minutes, the installer waits between installation attempts. The maximum interval the installer waits is 10 minutes.
Application Cost Setting	Application Cost Description
Cost Center	Enter the business unit charged for the development of the application.
Cost	Enter cost information for the application to help report metrics concerning your internal application development systems to the organization.
Currency	Select the type of currency that paid for the development, or the currency that buys the application, or whatever you want to record about the application.

- 4 Complete the **Files** tab options. You must upload a provisioning profile for Apple iOS applications and you must upload the architecture application files for Windows Desktop applications. If you do not upload the architecture application files, the Windows Desktop application does not function.

Platform	Auxiliary File	Description
All	Application File	Contains the application software to install and run the application and is the application you uploaded at the beginning of the procedure.
Android	Firebase Cloud Messaging (FCM) Token	<p>This is an Workspace ONE SDK feature and does not apply to all Android applications. Some internal, Android applications support push notifications from the application to device-users.</p> <ol style="list-style-type: none"> 1 Select Yes for the Application Supports Push Notification option. 2 Enter the Server API key in the FCM Token (API Key) option. Get this from the Google Developer's site. <p>A developer codes a corresponding SenderId into the internal application.</p> <p>To use the feature, push the notification from the applicable device record in the console using the Send admin function on the Devices tab.</p>
Apple iOS	<ul style="list-style-type: none"> ■ Provisioning Profile ■ APNs files for development or production 	<ul style="list-style-type: none"> ■ A provisioning profile authorizes developers and devices to create and run Apple iOS applications. See Apple iOS Provisioning Profiles for information about Workspace ONE UEM integration with this auxiliary file. <p>Ensure this file covers enterprise distribution and not app store distribution and that it matches the IPA file (Apple iOS application file).</p> <ul style="list-style-type: none"> ■ If the application supports Apple Push Notifications Services (APNs), this file enables messaging functionality. You must upload either the development or production APNs certificate.
macOS	Metadata file (pkginfo.plist)	<p>Create this file with a third-party utility tool like Munki or AutoPkgr.</p> <p>You can also use the VMware Admin Assistant to make this file. The file is available in the console when you upload an internal, macOS application.</p>

Platform	Auxiliary File	Description
Windows Desktop	Dependency files	Contains the application software to install and run the application for Windows Desktop.
Windows Phone	Dependency files	Contains the application software to install and run the application for Windows Phone.

5 Complete the options on the **Images** tab.

Setting	Description
Mobile Images	Upload or drag and drop images of the application to display in the app catalog for mobile devices.
Tablet Images	Upload or drag and drop images of the application to display for tablets.
Icon	Upload or drag and drop images to display in the app catalog as its icon.

Note To achieve best results for Mobile and Tablet Images, refer <https://help.apple.com/itunes-connect/developer/#/devd274dd925> for iOS and <https://support.google.com/googleplay/android-developer/answer/1078870?hl=en> for Android.

6 Complete the **Terms of Use** tab.

Terms of use state specifically how users are expected to use the application. They also make expectations clear to end users. When the application pushes to devices, users view a terms of use page that they must accept to use the application. If users do not accept, they cannot access the application.

7 Complete the **More > SDK** tab.

Setting	Description
SDK Profile	Select the profile from the drop-down menu to apply features configured in Settings & Policies (Default) or the features configured in individual profiles configured in Profiles .
Application Profile	Select the certificate profile from the drop-down menu so that the application and Workspace ONE UEM communicate securely.

8 Complete the **More > App Wrapping** tab.

You cannot wrap an application that you previously saved in the Workspace ONE UEM console. You have two options:

- Delete the unwrapped version of the application, upload it to Workspace ONE UEM, and wrap it on the App Wrapping tab.

- Upload an already wrapped version of the application, if you have one, which does not require deleting the unwrapped version.

Setting	Description
Enable App Wrapping	Enables Workspace ONE UEM to wrap internal applications.
App Wrapping Profile	Assign an app wrapping profile to the internal application.
Mobile Provisioning Profile - iOS	Upload a provisioning profile for Apple iOS that authorizes developers and devices to create and run applications built for Apple iOS devices.
Code Signing Certificate - iOS	Upload the code signing certificate to sign the wrapped application.
Require encryption - Android	<p>Enable this option to use Data At Rest (DAR) encryption on Android devices. Workspace ONE UEM uses the Advanced Encryption Standard, AES-256, and uses encrypted keys for encryption and decryption.</p> <p>When you enable DAR in App Wrapping, the App Wrapping engine injects an alternative file system into the application that securely stores all the data in the application. The application uses the alternative file system to store all files in an encrypted storage section instead of storing files in disk.</p> <p>DAR encryption helps protect data in case the device is compromised because the encrypted files created during the lifetime of the application are difficult to access by an attacker. This protection applies to any local SQLite database, because all local data is encrypted in a separate storage system.</p>

9 Select **Save & Assign** to configure flexible deployment options for the application.

What to do next

To assign and deploy internal applications, configure the flexible deployment options explained in [Add Assignments and Exclusions to Applications](#).

Add Assignments and Exclusions to Applications

To control the deployment of applications, add a single assignment or multiple assignments. Also, exclude groups from receiving the assignment.

If you add multiple assignments, prioritize the importance of the assignment by moving its place in the list up for most important or down for least important.

Note If you use APIs to assign applications, do not use the exclusions in the console. APIs for exclusions are in development at this time. If you want to use exclusions, assign applications through the console, do not use APIs for assignment.

Procedure

- 1 Navigate to **Apps & Books > Applications > Native > Internal** or **Public**.
- 2 Upload an application and select **Save & Assign** or select the application and choose **Assign** from the actions menu.

3 On the **Assignments** tab, select **Add Assignment** and complete the following options.

Setting	Description
Select Assignment Groups	Type a smart group name to select the groups of devices to receive the assignment.
App Delivery Method	<ul style="list-style-type: none"> ■ On Demand – Deploys content to a catalog or other deployment agent and lets the device user 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.
Display in App Catalog - Windows Desktop	<p>Select Show or Hide to display an internal or public application in the catalog.</p> <p>Note The Show or Hide option is applicable only to the Workspace ONE Catalog and not legacy VMware AirWatch Catalog.</p> <p>Use this feature to hide applications in the app catalog you do not want users to access.</p>
Desired State Management- macOS	<p>Currently when installing a macOS software, administrators have an option to enable or disable the Desired State Management settings based on the business needs.</p> <p>Desired State Management is enabled by default to enforce application management while installing a macOS software.</p> <p>If enabled, and if the end-user deletes the app, the application is automatically reinstalled on the next Workspace ONE Intelligent Hub sync.</p> <p>If disabled, and if the end-user deletes the app, the application is not automatically reinstalled, unless pushed from the Workspace ONE UEM console or Catalog.</p> <p>Also, as an administrator you have the flexibility to deploy applications as one-time configuration and provide end-users the facility to uninstall the application locally if needed.</p>
Deployment Begins On - Internal Apps	<p>Set a day of the month and a time of day for the deployment to start.</p> <p>The Priority setting governs which deployments push first. Workspace ONE UEM then pushes deployments according to the Effective configuration.</p> <p>To set a beginning date with enough bandwidth for successful deployment, consider the traffic patterns of your network.</p>
Policies - DLP <ul style="list-style-type: none"> ■ Android ■ iOS ■ Windows Desktop ■ Windows Phone 	<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 Devices > Profiles. Select Add > Add Profile and the platform.</p> <ul style="list-style-type: none"> ■ For Android and iOS devices, select Restrictions and enable options in the Data Loss Prevention section. ■ 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.

Setting	Description
Policies - Managed Access <ul style="list-style-type: none"> ■ Android ■ iOS 	<p>Enable adaptive management to set Workspace ONE UEM to manage the device so that the device can access the application.</p> <p>Workspace ONE controls this feature and is not supported by the AirWatch Catalog.</p>
Policies - Remove on Unenroll <ul style="list-style-type: none"> ■ Android ■ iOS 	<p>Set the removal of the application from a device when the device unenrolls from Workspace ONE UEM.</p> <p>If you choose to enable this option, supervised devices are restricted from silent app installation 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.</p> <p>If you choose to disable this option, provisioning profiles are not pushed along 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.</p>
Policies - Prevent Application Backup - iOS	<p>Prevent backing up the application data to iCloud.</p>
Policies - Make App MDM Managed if User Installed <ul style="list-style-type: none"> ■ iOS ■ Windows Desktop 	<p>Assume management of applications previously installed by users on their iOS devices (supervised and unsupervised) and Windows Desktop. MDM management occurs automatically regardless of the application delivery method and requires privacy settings to allow the collection of personal applications. For unsupervised iOS devices, the apps get converted to MDM managed only upon user's approval.</p> <p>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 application catalog version on the device.</p>
Policies - App Tunneling <ul style="list-style-type: none"> ■ Android ■ iOS 	<p>Configure a VPN at the application level, and select the Per-App VPN Profile. Users access the application using a VPN, which helps ensure that application access and use is trusted and secure.</p>
Policies - Application Configuration <ul style="list-style-type: none"> ■ Android ■ iOS 	<p>Send application configurations to devices.</p> <p>Upload XML (Apple iOS) – Select this option to upload an XML file for your iOS applications that automatically populates the key-value pairs. Get the configurations supported by an application from the developer in XML format</p>
App Attributes	<p>Configure key/value pairs of attributes for your application to leverage on iOS 13+ devices. These attributes can be used to specify values to be leveraged by the app for things such as associated domains for SSO extensions and universal links. To specify the Associated Domains for an app, provide the following key/value pair:</p> <ul style="list-style-type: none"> ■ Attribute Key: AssociatedDomains ■ Attribute Type: Array ■ Attribute Value: An array of strings for with the URLs of the domains you want to associate with this application.

- 4 Select **Add**.
- 5 Use the **Move Up** and **Move Down** options to order assignments if you have more than one. Place critical assignments at the top of the list.

This configuration displays as the **Priority**. The **Priority** setting takes precedence when there are conflicting deployments assigned to a single device.

- 6 Select the **Exclusions** tab and enter smart groups, organization groups, and user groups to exclude from receiving this application.
- The system applies exclusions from application assignments at the application level.
 - Consider the organization group (OG) hierarchy when adding exclusions. Exclusions at a parent OG do not apply to the devices at the child OG. Exclusions at a child OG do not apply to the devices at the parent OG. Add exclusions at the desired OG.
- 7 Select **Save & Publish**.

Smart Glasses Feature Matrix

This matrix summarizes specific functionality and configurations, as available by OEM.

Table 4-1. Smart Glass Supported Features - Asset Tracking

	Vuzix M100	Vuzix M300	Google Glass	RealWear HMT-1/1Z1
UDID	Supported	Supported	Supported	Supported
OS Version	Supported	Supported	Supported	Supported
Manufacturer	Supported	Supported	Supported	Supported
Model	Supported	Supported	Supported	Supported
Serial Number	Supported	Supported	Supported	Supported

Table 4-2. Smart Glass Supported Features - Internal App Management

	Vuzix M100	Vuzix M300	Google Glass	RealWear HMT-1/1Z1	
Install Applications	Supported	Supported	Supported	Supported	
Remove Applications	Supported	Supported	Supported	Supported	
Update Applications	Supported	Supported	Supported	Supported	

Table 4-3. Smart Glass Supported Features - Push Services

	Vuzix M100	Vuzix M300	Google Glass	RealWear HMT-1/1Z1	
AWCM	Supported	Supported	Supported	Supported	

Table 4-4. Smart Glass Supported Features - Wi-Fi

	Vuzix M100	Vuzix M300	Google Glass	RealWear HMT-1/1Z1	
WPA/WPA2	Supported	Supported	Supported	Supported	
WPA/WPA2 Enterprise		Supported	Supported	Supported	

Note System updates for Google Glass devices are handled by an OTA server. Please contact Google for more information.
