VMware AirWatch Integration with Smart Glasses

Multiple AirWatch versions

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Overview

Introduction to Smart Glasses

Smart Glasses are headsets or head-mounted displays that enable an augmented reality experience.

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.

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

Before You Begin Deploying Smart Glasses

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

Supported Operating Systems

- AirWatch Admin Console v8.2+
- A PC or Mac computer equipped with Android Debug Bridge is needed for sideload staging.
- Google Glass only: Google Glass OS version EE13 or above.
    - 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 EExx. EE13 has the capability for AirWatch to push apps and is the minimum recommended version for customers. Contact Google to get information on how to upgrade your device.

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. Do not reuse Android (Legacy) mobile profiles.
- Enable Direct Prompt in Agent Settings to allow silent application install.

Chapter 2:
Smart Glasses Enrollment

All Smart Glasses in your deployment must be enrolled before it can communicate with AirWatch and access internal content and features. Enrollment is facilitated with the AirWatch Agent 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.

Create an Enrollment User

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.
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 AirWatch Agent .APF File for Smart Glasses

Upload the .apf file for your Smart Glasses deployment to enable a simplified enrollment. The Agent Package can be uploaded only in specific organization group types, for example, in organization groups of type 'Customer'. It is recommended to upload the Agent Package at the highest organization group. You can find the file specific to your OEM located in AirWatch Resources.

To upload an .apf file, follow the steps detailed below:

1. Navigate to **Devices > Staging & Provisioning > Components > Agent 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 agent 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 agent.
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.

To create the staging Wi-Fi profile:

1. Navigate to **Devices > Staging & 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 AirWatch Agent, and enroll Smart Glasses with minimal interaction.

To create a staging configuration, follow the steps outlined below:

1. Navigate to **Devices > Staging & Provisioning > Staging > Add Staging > Android (Legacy)**.
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.
Agent	Select the AirWatch Agent to download during staging. These agents are uploaded as an Agent Package. See how to Upload the AirWatch Agent .APF File for Smart Glasses on page 6

3. Select **Save**.

Generate a Sideload Staging Package

AirWatch 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.

To create a side staging package:

1. Navigate to **Devices > Staging & Provisioning > 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 agent folder saved to your computer and run the script from within the agent folder.
   b. The device should auto enroll into AirWatch.

> **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.

Chapter 3:
Smart Glasses Profiles

Overview

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.

Deploying Profiles with 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.

Create Wi-Fi Profile

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

To configure the Wi-Fi profile:

1. Navigate to **Devices > Profiles > List View > Add > Add Profile > Android (Legacy)**.
2. Configure the **General** profile settings as appropriate.

3. 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	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. • **Protocols** ◦ Use Two Factor Authentication ◦ SFA Type • **Authentication** ◦ 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.

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

Settings	Description
Credential Source	**Upload** a certificate from your local machine or define a **Defined Certificate Authority**, or upload a **User Certificate**. • If you choose to **Upload** a certificate, complete the following: ◦ **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: ◦ **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**.

5. Select **Save & Publish**.

Chapter 4:
Smart Glasses Device Management Overview

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, AirWatch Agent 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.

Add and 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.

Review instructions from platform sites about how to develop and package applications.

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.

Setting	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.

Setting	Description
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.
Version	Displays the internal version of the application set by the Workspace ONE UEM console.
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.
Description	Describe the purpose of the application. **Note:** 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.

Complete the options in the **Developer Information** area:

Setting	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.

Complete the options in the **Application Cost Information** area:

Setting	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.

   Review the file initially uploaded and upload auxiliary files to distribute internal applications.

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	Google Cloud Messaging (GCM) Token	This is an AirWatch SDK feature and does not apply to all Android applications. Some internal, Android applications support push notifications from the application to device-users. a. Select **Yes** for the **Application Supports Push Notification** option. b. Enter the **Server API** key in the **GCM Token (API Key)** option. Get this from the Google Developer's site. A developer codes a corresponding **SenderID** into the internal application. To use the feature, push the notification from the applicable device record in the console using the **Send** admin function on the **Devices** tab.

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 in the App Catalog for tablets.
Icon	Upload or drag and drop images of the application 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 AirWatch communicate securely.

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

   You cannot wrap an application that you previously saved in the AirWatch Console. You have two options:

   - Delete the unwrapped version of the application, upload it to AirWatch, 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 AirWatch to wrap internal applications.
App Wrapping Profile	Assign an app wrapping profile to the internal application.
Require encryption (Android)	Enable this option to use Data At Rest (DAR) encryption on Android devices. AirWatch uses the Advanced Encryption Standard, AES-256, and uses encrypted keys for encryption and decryption. 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. 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.

9. Select **Save & Assign** .

10. After adding Assignments, Click **Save & Publish**, then **Publish** to deploy the app to your Smart Glasses.

Smart Glasses Feature Matrix

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

	Atheer AiR Glasses	ODG R-7	Vuzix M100	Vuzix M300	Google Glass	RealWear HMT-1
Asset Tracking						
UDID	✓	✓	✓	✓	✓	✓
OS Version	✓	✓	✓	✓	✓	✓
Manufacturer	✓	✓	✓	✓	✓	✓
Model	✓	✓	✓	✓	✓	✓
Serial Number	✓	✓	✓	✓	✓	✓
Internal App Management						
Install Applications	✓	✓	✓	✓	✓	✓
Remove Applications	✓	✓	✓	✓	✓	✓
Update Applications	✓	✓	✓	✓	✓	✓
Push Services						
AWCM	✓	✓	✓	✓	✓	✓
Wi-FI						
WPA/WPA2	✓	✓	✓	✓	✓	✓
WPA/WPA2 Enterprise				✓	✓	

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