AirLift Configuration

VMware Workspace ONE UEM 2109
VMware Workspace ONE AirLift 2.1

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

VMware Workspace ONE AirLift Components and Requirements

1

VMware Workspace ONE AirLift is a server-side connector that simplifies and speeds your journey to modern management. Workspace ONE AirLift bridges administrative frameworks between Microsoft System Center Configuration Manager (ConfigMgr), Active Directory, and Workspace ONE UEM powered by AirWatch. Before you can use Workspace ONE AirLift to bridge ConfigMgr to Workspace ONE UEM, you must meet the prerequisites and requirements.

This bridge allows you to focus on moving workloads and applications to Workspace ONE UEM without redefining device and group memberships. Workspace ONE AirLift lets you export collections, apps, and policies to Workspace ONE UEM on a case-by-case basis.

The dashboard provides a visualization of the transition and shows the progress for devices and applications. The dashboard also displays top modern management workloads to show you what functionality you use on your devices. You can also see an enrollment history and percentage complete within ConfigMgr collections.

Admin Credentials in ConfigMgr

Workspace ONE AirLift communicates with ConfigMgr for collection mapping, app exporting, and enrollment. Workspace ONE AirLift requires an admin account with a minimum level of permissions in ConfigMgr.

Collections

Workspace ONE AirLift allows you to map your existing ConfigMgr device collections to Workspace ONE UEM smart groups. Workspace ONE AirLift dynamically monitors the device collections and keeps both platforms consistent. Workspace ONE AirLift uses Workspace ONE UEM tags to add devices to smart groups after enrollment. These tags use a naming scheme with the prefix **`co-mgt`** to clarify the source of the membership. This process is called ‘collection mapping’ and is accomplished in the Workspace ONE AirLift console. You can remove mappings once the transition to modern management is complete.

Enrollment

Workspace ONE AirLift allows you to enroll devices Workspace ONE UEM with a ConfigMgr enrollment application. Configure and create the enrollment application with a blueprint and the required software. Simplify and speed up the transition to modern management for proof of concepts, pilots, and production implementations using collection mapping and streamlined enrollment with Workspace ONE AirLift.

Applications

Workspace ONE AirLift also provides the means to export applications from ConfigMgr to Workspace ONE UEM. You can then deploy and manage applications from the Workspace ONE platform. Workspace ONE AirLift provides validations so you aware of any additional configuration applications might need. You can also create an app validation report for project plans that involve app rationalization or portfolio management. The CSV-format report allows you to target a specific list of apps and view and validations issues that need to be addresses before you export.

Policies

You can have a burdensome number of group policies in your current environment and want to transition some of these policies to modern management. Workspace ONE AirLift lets you map and export your existing GPO policies to the Workspace ONE UEM console. Workspace ONE UEM converts these exported policies into MDM policies with custom profiles based on Windows Configuration Service Providers.

Requirements

You must meet these requirements if you are a SaaS or on-premises customer.

Workspace ONE AirLift must communicate with different services depending on the features you plan to use.

- If you plan to use collection mapping, app export, and enrollment, you must configure Workspace ONE AirLift to communicate with ConfigMgr.
- If you plan to use policy mapping, you must configure Workspace ONE AirLift to communicate with your active directory.

Hardware Requirements

Ensure that your server meets the necessary hardware requirements before installing.

Hardware Requirements	Details
VM or Physical Server	2 CPU Core (2.0+ GHz) 4 GB RAM or more 1 GB disk space for the Workspace ONE AirLift application, operating system, and .NET Core runtime. Consider having 5 GB of disk space.

Software Requirements

Ensure that your server meets the software requirements before installing.

Software Requirement	Details
Browser	Workspace ONE AirLift supports the most recent versions of Chrome, Firefox, and Edge. Internet Explorer is not supported. To maximize automation, the Workspace ONE AirLift server must be online and able to retrieve software from Microsoft and Mongo.
Operating System	Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows 10 **Note** Workspace ONE AirLift does not support Windows Server 2012 R2 configured as domain controllers.
Remote Server Administration Tools	This requirement only applies if you plan on using policy mapping. You must install Remote Server Administration Tools (RSAT) on the Workspace ONE AirLift server. ■ Installing RSAT for Windows Server through Server Manager: ■ **Add Features and Roles > Features > Group Policy Management** ■ **Add Features and Roles > Features > Remote Server Administration Tools > Role Administration Tools > AD DS and AD LDS Tools** ■ Installing RSAT on Windows 10: ■ Download RSAT from Microsoft: https://www.microsoft.com/en-au/download/details.aspx?id=45520.

Network Requirements

Ensure that your server meets the network requirements before installing.

Network Requirement	Details
Domains	Microsoft System Center Configuration Manager (ConfigMgr) and Workspace ONE AirLift must be on the same domain.
Workspace ONE AirLift to SCCM communication	You must allow Workspace ONE AirLift the following access to the ConfigMgr server: ■ WinRM port (typically 5985) ■ Port 443 or the specified TLS port if Secure Connection is configured. ■ Interactive Log in Permissions - Ensure that AD user account settings or security policy settings do not deny local log in.
Workspace ONE AirLift to Workspace ONE UEM console	You must allow Workspace ONE AirLift the following access to the UEM console: ■ Access to the Console/API server using Port 443.
Workspace ONE AirLift to Active Directory	This requirement only applies if you plan on using policy mapping. You must allow Workspace ONE AirLift access to the SYSVOL directory. The directory must contain the PolicyDefinitions folder. To map third-party ADMX settings, you must include those ADMX files in the PolicyDefinitions folder. If there is no PolicyDefinitions folder in the SYSVOL location: 1 Log in to your AD server . 2 Copy the local PolicyDefinitions folder located in C:\Windows in the AD server. 3 Paste the folder to the Active Directory SYSVOL location. For example: `\\[company].com\SYSVOL\[company].com\Policies\PolicyDefinitions`

Workspace ONE UEM Requirements

Ensure your Workspace ONE UEM deployment meets the requirements before installing.

Workspace ONE UEM Requirements	Details
Version	Workspace ONE UEM 1903 or later
Admin account	Admin account with API-level permissions. For on-premises customers, the admin account cannot be a Global-level admin. Only use a child customer organization group admin account.

ConfigMgr Requirements

Ensure your ConfigMgr deployment meets the requirements before installing Workspace ONE AirLift.

ConfigMrg Requirements	Details
Version	Microsoft Systems Center Configuration Manager 2012 R2 or later
Admin Account	Workspace ONE AirLift requires an admin account with a minimum level of permissions. You must create an admin account with the listed permissions in ConfigMgr. ■ Basic permissions - Cannot create an enrollment app or enroll devices. ■ Application - Read ■ Collection - Read, Read Resource ■ Distribution Point - Read ■ Distribution Point Group - Read ■ Package - Read ■ To enroll devices: ■ Collection - Distribute Applications ■ To create an enrollment app: ■ Application - Create, Modify ■ To manage distribution: ■ Distribution - Copy to Distribution Point
Content Location	Workspace ONE AirLift requires an admin account with read access to the ConfigMgr content location. If you plan to create a Workspace ONE enrollment application, Workspace ONE AirLift needs write access to the content location.

Active Directory Requirements

Ensure that Active Directory deployment meets the requirements before installing Workspace ONE AirLift.

Active Directory Requirements	Details
Read permissions for group policy processing and policy definitions location.	This requirement only applies if you plan on using policy mapping.Workspace ONE AirLift requires a domain account with read permissions for any GPO you want to export.

Access Files

You can access the MongoDB MSI file at https://fastdl.mongodb.org/win32/mongodb-win32-x86_64-2008plus-ssl-3.6.5-signed.msi.

You can access the SQL Server EXE file at https://download.microsoft.com/download/E/F/2/EF23C21D-7860-4F05-88CE-39AA114B014B/SQLEXPR_x64_ENU.exe.

Workspace ONE AirLift Installation and Configuration 2

Installing Workspace ONE AirLift involves running the installation file on your server and configuring Workspace ONE UEM and Microsoft System Center Configuration Manager (ConfigMgr).

Retrieve the Workspace ONE UEM REST API Key

Before you configure Workspace ONE AirLift, retrieve the API key from the Workspace ONE UEM console.

1 In the Workspace ONE UEM console, navigate to **Groups & Settings > All Settings > System > Advanced > API > REST API**.

2 Copy the **APIserver** key for later use.

Install Workspace ONE AirLift

Run the Workspace ONE AirLift executable file on your application server and install Workspace ONE AirLift.

Prerequisites

Before you can install Workspace ONE AirLift, you must meet the prerequisites.

- Meet the Workspace ONE AirLift Prerequisites.
- Download the Workspace ONE AirLift executable file from My Workspace ONE (my.workspaceone.com).

Procedure

1 On the application server, navigate to the AirLiftSetup.exe file. Run the executable file. After installing the prerequisites, the Workspace ONE AirLift installer runs.

   This wizard installs the required SQL Server Express 2017 and MongoDB.

2 Complete the installation wizard.

Connect Workspace ONE AirLift to Workspace ONE UEM, ConfigMgr, and Active Directory

After installingWorkspace ONE AirLift, you must connect the server to the UEM console, ConfigMgr, and Active Directory. The connections required depend on which features you want to use.

1 Run Workspace ONE AirLift by selecting the Workspace ONE AirLift desktop icon. The icon opens http://localhost:5000 in your default browser.

2 Configure the Workspace ONE UEM connection information.

Settings	Description
API URL	Enter the URL for your Workspace ONE UEM API service.
Console Address	Select **Same as API** if your console and API service share an address. If the Workspace ONE UEM console does not share an address with the API service, select **No**. Enter the **Console URL**.
API Key	Enter the API key from the Workspace ONE UEM console.
User name	Enter the user name of the admin account created for Workspace ONE AirLift.
Password	Enter the password for the admin account created for Workspace ONE AirLift.

3 Select **Continue**.

4 Configure the ConfigMgr settings.

Setting	Description
ConfigMgr Server	Enter the server address for your ConfigMgr environment.
Site Code	Enter the ConfigMgr Site Code.
Secure Connection	This option is enabled by default. Disable if you do not have TLS properly configured on your SCCM server.
Domain	Enter the domain of your ConfigMgr server.
User name	Enter the user name of the admin account for Workspace ONE AirLift.
Password	Enter the password for the admin account created for Workspace ONE AirLift.

5 Configure the Active Directory settings. Enter the domain of your Active Directory in the **Active Directory Domain** field.

6 Select **Submit**.

Workspace ONE AirLift is now configured.

Schedule Sync

The **Schedule Sync** option allows you to schedule when Workspace ONE AirLift syncs with ConfigMgr for updates. You can set the schedule to the specific time and day you want.

Navigate to **Settings > Schedule Sync** to configure these settings.

Permissions

The **Permissions** settings allow you to grant additional users either **View Only** or **Admin** permissions for Workspace ONE AirLift.

Navigate to **Settings > Permissions** to configure these settings.

Web Proxy

In situations where your Workspace ONE AirLift server requires different web proxy settings you can change how Workspace ONE AirLift handles the system proxy settings. You can configure Workspace ONE AirLift to use the system-configured proxy settings, bypass the web proxy, or manually configure proxy settings.

The manual proxy server configuration settings only apply to communication with the Workspace ONE UEM API server. Other traffic such as Workspace ONE UEM console, ConfigMgr, and Customer Experience Improvement Program does not use these settings.

To configure the proxy settings, navigate to **Settings > Web Proxy**. Select the option that applies to you:

- Use the system-configure proxy server settings (default)
- Bypass web proxy
- Manually configure proxy settings

If you manually configure the settings, you must provide the following information:

Setting	Description
Web Proxy Host	Enter the web proxy host domain name or IP address.
Web Proxy Port	Enter the port used for the web proxy.
Use Authentication	If your proxy requires authentication select **Yes** and enter the **Username** and **Password**.

Support

If you encounter difficulties with Workspace ONE AirLift, you can simplify troubleshooting using the support bundle feature. The support bundle automatically gathers logs, SQL data, and environment information and creates a ZIP file. You can send this file to Workspace ONE support to facilitate fixing your issue.

The support bundle contains the following information:

- Collection data from MongoDB
- Workspace ONE AirLift logs
- Workspace ONE AirLift environment information, including OS version, environment variables, and so on.
- SQL data from the following tables:
  - ActiveDirectoryDataSources
  - AirWatchDataSources (no password)
  - AuditLogs
  - SccmDataSources (no password)
  - Settings
  - Tenants
  - TenantSettings
  - WindowsVersions

Navigate to **Settings > Support** and select **Generate Support Bundle** to get started.

Customer Experience Improvement Program

Select **Join the VMware Customer Experience Improvement Program** to contribute technical information related to the performance, configuration, and use of Workspace ONE AirLift. Your participation improves and benchmarks our products and services, fixes problems, and helps us to advise customers on the use of our software.

The data is used by VMware and its service providers strictly on an aggregated basis.

Navigate to **Settings > Feedback** to configure these settings.

Command Line Tools for Workspace ONE AirLift

Command Line Tools for Workspace ONE AirLift allow you to make system administrator changes to your Workspace ONE AirLift service. Use caution when using these tools as they can remove data.

The following tools allow you to complete admin tasks on your Workspace ONE AirLift server.

- Delete Workspace ONE AirLift data
  - This command line tool allows you to delete all data retrieved and generated after performing a synchronization of Airlift without deleting your existing settings. The tool deletes the data in SQL Server and MongoDB but keeps all configuration data in SQL Server and leaves appsettings.json untouched.

- Code:

```
--delete-data [--force|-f]
```

- Example:

```
Airlift --delete-data
```

- Factory reset Workspace ONE AirLift
  - This command line tool allows you to remove all Workspace ONE AirLift and any existing settings and configurations you have made. The tool deletes the data in SQL Server and MongoDB and restores appsettings.json file with appsettings.json.default.
  - Code:

```
--factory-reset [--force|-f]
```

  - Example:

```
Airlift--factory-reset -f
```

- Get MongoDB connection string
  - This command line tool allows you to obtain the MongoDB connection string which stores the cache data which Workspace ONE AirLift uses. You can use this connection string to authenticate and access MongoDB manually to read the cached data that Workspace ONE AirLift generated.
  - Code:

```
--get-mongo-connection
```

  - Example:

```
Airlift --get-mongo-connection
```

Workspace ONE AirLift Collections

3

Workspace ONE AirLift connects your ConfigMgr collections to Workspace ONE UEM smart groups. This connection allows you to map devices from your existing collections into Workspace ONE UEM.

Note Only collections and devices that match the following criteria are displayed:

- The collections contain at least one Windows 10 device
- The devices have a ConfigMgr client installed
- The devices are not marked as obsolete

Mapping a collection to a smart group allows you to begin enrolling devices into Workspace ONE UEM. The mapping honors the dynamic nature of device collections by adding and removing devices in the mapped Workspace ONE UEM smart group while the mapping exists. Mapping collections does not enable Workspace ONE UEM management functionality directly. You must enroll devices to begin using modern management. Mapping only creates a relationship between collections, organization groups, and smart groups.

Workspace ONE AirLift displays your ConfigMgr collections and their migration progress to modern management in Workspace ONE UEM.

If a collection mapping is removed or is the migration is completed and the ConfigMgr collection is no longer used, Workspace ONE AirLift does not display the collection as mapped. See the state of your collections in Workspace ONE AirLift in the Collections tab.

The **Management** column shows the management state of the collection.

- SCCM - ConfigMgr manages the collection.
- Co-existing - the collection is mapped to a Workspace ONE UEM smart group and enrollment into Workspace ONE UEM can begin.

The **Workspace Mapping** column shows which Workspace ONE UEM smart group the collection is mapped to. To open the smart group in the Workspace ONE UEM console, select the mapping.

The **Enrollment Progress** column shows the percentage of the collection that has completed the enrollment process.

Map a Collection to Workspace ONE UEM

To begin the transition to modern management, map your ConfigMgr collections to Workspace ONE UEM smart groups. This mapping connects ConfigMgr managed devices to Workspace ONE UEM while maintaining your device membership in ConfigMgr.

1 In Workspace ONE AirLift, navigate to the **Collections** tab. Select the check box next to the collection you want to map then select **Map**.

2 In the **Map to Workspace ONE** dialog, complete the settings.

Setting	Description
ConfigMgr Collection	(Display Only) This value is the collection you selected previously.
Workspace ONE Organization Group	Select the Organization Group that manages the smart group you want to map your collection to. This option allows you to create hierarchies in the Workspace ONE UEM console.
Workspace ONE Group	Select the Workspace ONE UEM smart group to which you want to map your collection. Manually entering a smart group creates a new smart group in Workspace ONE UEM.

3 Select **Save**.

The collection now displays a co-existing state.

Remove a Mapping from Workspace ONE AirLift

When the need arises, remove a mapping from a collection in Workspace ONE AirLift to break the relationship between a collection and a smart group.

1 In Workspace ONE AirLift, navigate to the **Collections** tab.

2 Select the collection that you want to remove the mapping from.

3 Select **Map**.

4 In the **Map to Workspace ONE** window, select **Remove**.

5 In the **Remove Mapping** prompt, select whether you want to keep any devices in their Workspace ONE UEM smart group.

   a If you select **Yes**, the device remains in the smart group.

   b If you select **No**, the device is removed from the smart group. The device remains in Workspace ONE UEM, but all profiles, applications, and tags associated with the smart group are removed.

6 Select **Remove**.

Workspace ONE AirLift now removes the relationship between the collection and the smart group.

Workspace ONE AirLift Enrollment

4

Workspace ONE AirLift enrollment allows ConfigMgr and Workspace ONE UEM to co-exist. This process moves the device to a co-existing state.

You must first map your ConfigMgr collections to Workspace ONE UEM smart groups.

Configure the Workspace ONE AirLift Enrollment Application

To enroll your Windows 10 devices into Workspace ONE UEM using Workspace ONE AirLift, you must configure the enrollment application. This process involves switching between Workspace ONE AirLift, Workspace ONE UEM, and ConfigMgr.

This task is only for those users who either do not have an enrollment application configured or want to create a new enrollment app.

Note Workspace ONE AirLift utilizes the provided ConfigMgr credentials to create the enrollment app programmatically. Advanced logging or monitoring of the ConfigMgr infrastructure may detect and log this usage and the credentials if configured to do so.

1 In Workspace ONE AirLift, navigate to **Settings** > **Enrollment**.

2 Set **Use Existing Enrollment Application** to **No**.

3 Configure the following settings:

Setting	Description
Application Name	Enter a name for the enrollment application
Organizational Group	Select an organizational group from the drop-down menu.
Staging User	Enter the staging user name.
Staging User Password	Enter the staging user password.
Enrollment Server URL	Enter your Workspace ONE UEM enrollment URL.
Include Workspace ONE App	Select to download the Workspace ONE app as part of enrollment.

Setting	Description
Include ConfigMgr Integration Client	If you are enrolling Windows 10 devices running a version of Windows 10 before 1709 and a version of ConfigMgr before 1709, select to download the ConfigMgr Integration Client as part of enrollment. Otherwise, do not select this option.
Workspace ONE Intelligent Hub Install Command Line	Select **Show** to display the command line.
Content Location	Enter the file path for the enrollment application.
Distribution Selection	Set the distribution selection to Auto or Manual.If you select manual, you must select the distribution servers or groups in ConfigMgr.

Your enrollment application is ready for use in Workspace ONE AirLift.

Enroll Collections into Workspace ONE AirLift

After creating an enrollment application, enroll your devices into Workspace ONE UEM. This enrollment process adds your Windows 10 devices to Workspace ONE UEM and enables them to receive profiles, apps, and more.

1 In Workspace ONE AirLift, navigate the **Collections** tab.

2 Select the collection you want to enroll and select **Enroll**. Only a collection that is mapped to a

3 Workspace ONE UEM smart group can enroll devices into Workspace ONE UEM.

4 Review the information displayed and select **Enroll**.

Enrollment into Workspace ONE UEM begins on the Windows 10 devices in the collection selected.

Workspace ONE AirLift Applications

5

Workspace ONE AirLift exports Microsoft System Center Configuration Manager (ConfigMgr) applications so you can add the applications toWorkspace ONE UEM. This export simplifies the process of migrating your applications to Workspace ONE UEM without the need for repackaging.

Workspace ONE AirLift displays your existing ConfigMgr applications and the relevant validation information. The applications display in the Applications list view with relevant information. These applications must be an .MSI or .EXE (using the script installer deployment type) file type. You can also use ZIP files. Workspace ONE AirLift supports file system and Windows Installer detection methods. If your application uses MST and MSP files, Workspace ONE AirLift includes those files in the export.

The Validation column displays the application validation status. If the install context of an application is set to both system and user install context, AirLift defaults to Device context in Workspace ONE UEM.

Consider exporting the applications with a green Validation status first. Apps with red or yellow statuses might require additional configuration.

The Status column displays the export status of your applications.

You can review the state of your application validation by selecting the **Report** button. This button download a .CSV file onto your machine that reviews the state of all your application validations.

The Workspace Application column displays the name of the application after it is added to Workspace ONE UEM.

Workspace ONE AirLift General Considerations

Exporting applications from Microsoft System Center Configuration Manager (ConfigMgr) requires specific considerations. Workspace ONE AirLift handles deployment types and detection methods based on rules.

Workspace ONE AirLift supports exporting apps with file, registry, and Windows installer based ditection criteria. Additionally, you can manually configure the app deployment options to set **When To Call Install Complete** in the Workspace ONE UEM console.

ConfigMgr application dependencies are not transferred as part of the application export function.

The Application Export page lists the corresponding Workspace ONE UEM application name if the exported application has a matching name. After a successful export, you can edit or rename the application as needed. This edit removes the linkage to the Workspace Application from the column in the Workspace ONE AirLift application export page.

Workspace ONE UEM stores each binary as a unique value to prevent multiple imports of the same application. This binary value also prevents a repeat app export of the same application. If you want to export an app again, consider deleting the application from Workspace ONE UEM and then exporting the application again from Workspace ONE AirLift. The application export feature involves transferring the application binaries and the configuration metadata which can take a significant amount of time depending on connectivity between Workspace ONE AirLift and Workspace ONE UEM.

You can only select and export apps one page at a time. This restriction increases the predictability and success of the app export function. Consider sorting the columns to target the list of application you want to export. Also consider using the activity log to track the progress of the application export process.

Apps with Multiple Deployment Types

Workspace ONE AirLift addresses applications with multiple deployment types by reviewing the specific OS requirements and platform support to select the right deployment type. Use the validation messages to see which deployment type Workspace ONE AirLift uses for the app export.

The validation process uses the following logic:

1 If any OS version information exists in the ConfigMgr requirements, Workspace ONE AirLift uses the application with the latest OS version.

2 If no OS version specifications exist, Workspace ONE AirLift looks for RuleID: `Windows/All_Windows_Client_Server`.

3 If there are multiple Windows 10 requirements, Workspace ONE AirLift choses the x64 version over x86 version.

4 If there is not a best choice or an acceptable choice in the deployment list, Workspace ONE AirLift selects nothing and reports there are no valid deployment types.

Export ConfigMgr Applications to Workspace ONE UEM

Export your ConfigMgr applications to Workspace ONE UEM through Workspace ONE AirLift. This process moves your existing application lists to Workspace ONE UEM to simplify moving to modern management.

1 In Workspace ONE AirLift, navigate to the **Applications** tab and select the application you want to export.

2 Select **Export**.

3 In the **Export Applications** dialog, select the **Workspace ONE Organization Group** you want to export the app to.The application export process begins. After the app has been exported, the status changes to **Exported**.

4 To open the **Applications Details View** in the Workspace ONE UEM console, select the **Workspace Application** hyperlink.

   Selecting the hyperlink opens the Workspace ONE UEM console. From the console, you can finish the app assignment.

Workspace ONE AirLift Policies

6

Workspace ONE AirLift connects your Active Directory policies to Workspace ONE UEM profiles. This connection allows you to create profiles based on existing policies your business uses.

Exporting Polices to Workspace ONE UEM

The Policies list view allows you to review your existing GPO policies and export them. Workspace ONE UEM combines the exported policies into a single custom profile using MDM policies. You must do all editing, deleting, assigning, and publishing of profiles in the Workspace ONE UEM console.

Workspace ONE AirLift Policies List View

The Policies list view automatically populates with existing Active Directory policies. From this page, you can select a policy name to see the existing settings and values of the policy.

Select a GPO name to filter the list view by that GPO.

The **Validation** column displays the validation status of the policies. This status reflects if the GPO policy has a corresponding MDM policy.

- **Success** - The GPO policy maps to a valid MDM policy. You can export a policy with a successful validation.
- **Error** - The GPO policy does not map to a valid MDM policy. You cannot export a policy with an error.
- **Warning** - The GPO policy maps to a valid MDM policy but has some additional information. This information can include warning you about limited support for policies based on OS version. You can export a policy with a warning.

The **Status** column displays the Workspace ONE UEM profiles that contain the GPO policy. If you select a link in this column, a new window opens with the profile in the Workspace ONE UEM console.

Organizing the Policy List View

To help organize your list of policies, you filter the list view based on the Windows 10 version you are using. This filter limits the displayed policies. Only those policies that map to MDM policies for the filtered OS version display. Use this filter to ensure that you export policies that work with your different device OS versions. The Exportable bar at the top of the list view shows the percentage of the displayed policies that you can successfully export. This bar changes based on your filters.

You can also hide policies you do not plan on exporting. To hide a policy, simply select the policy and then select **Hide**. You can review the hidden policies from the **Hidden** tab.

Export Workspace ONE AirLift Policies

Export Workspace ONE AirLift Policies to the Workspace ONE UEM console to create profiles based on MDM policies. This export allows you to ensure that your existing policies still apply to your devices after transitioning to Workspace ONE UEM.

Prerequisites

You must configure Workspace ONE AirLift to communicate with your Active Directory.

Procedure

1 In Workspace ONE AirLift, navigate to the **Policies** tab.

2 Select the policies you want to export and then select **Add to Export**.

3 Select the **Ready to Export** tab.

4 Select the policies you want to export together.

5 Select the **Export** button.

6 In the Export Policies dialog, configure the settings.

Settting	Desctiption
Profile Name	Enter the name for the profile in the Workspace ONE UEM console based on these policies.
Workspace ONE Organization Group	Select the organization group that manages the profile you are creating. This option allows you to create hierarchies in the Workspace ONE UEM console.
Profile Context	Select whether the profile applies to the user or the device. Device context applies the policies at the device level. User context applies the policies at the user level.

After you export GPO policies to the UEM console, Workspace ONE UEM converts the policy settings to MDM policies and creates a custom profile.

To edit, delete, version, assign, or publish a profile to your devices, you must use the UEM console.

Troubleshooting Workspace ONE AirLift 7

Occasionally you need to troubleshoot your Workspace ONE AirLift deployment. Issues can arise with the communication between services, transitions to modern management, and other areas.

When you are troubleshooting Workspace ONE AirLift, you should first look for the Workspace ONE AirLift log file. You can find the logs at `C:\ProgramData\VMware\VMware AirLift\Logs\`. You can also use the Support bundle feature in Workspace ONE AirLift to gather the logs, SQL data, and environment information automatically to expedite the troubleshooting process.

Profiles Created Using Workspace ONE AirLift Fail to Install on End-User Devices

Workspace ONE AirLift policies exported into profiles in Workspace ONE UEM occasionally fail to install on end-user devices.

Problem

Exported Policies occasionally fail to install on the end-user devices.

Cause

After exporting policies to Workspace ONE UEM to create profiles, the profiles sometimes fail to install on end-user devices.

Solution

1 In the Workspace ONE UEM console, navigate to the profile that failed to install.

2 Edit the profile.

3 Create a new version of the profile.

4 Unselect **Make Commands Atomic**.

5 Select **Save and Publish** this new version.

ADMX policies fail to display in the policies page in Workspace ONE AirLift

ADMX policies sometimes fail to display in Workspace ONE AirLift.

Problem

ADMX policies sometimes fail to display in Workspace ONE AirLift.

Cause

This issue could be related to a Microsoft Known issue releated to ADMX and ADML language files. For more information, see https://support.microsoft.com/en-au/help/2688272/wrong-error-message-for-missing-adml-files.

Solution

Ensure you have the ADML language files for any ADMX files you use.