

VMware Workspace ONE UEM Reports Guide

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

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

Chapter 1: Introduction to Reports	3
Custom Reports	3
Workspace ONE UEM Reports	3
Reports Storage	3
Chapter 2: Reports for Workspace ONE Intelligence	4
Reports Background	4
Install the Reports Service	4
Reports Wizard	4
Manage Reports	5
Workspace ONE Intelligence Requirements	5
Install the Workspace ONE Intelligence Connector Service for On-Premises	6
Run the Reports Wizard	8
Reports Management	10
Chapter 3: Introduction to Reports	13
New Reports	14
Generate Reports	21
Subscribe to an Old Report	23
Manage Reports	25
Troubleshooting Reports	26
Chapter 4: File Storage	29
File Storage Requirements	30
File Storage Configuration	31
Chapter 5: Reports Storage	32
Reports Storage Requirements	32
Enable Reports Storage	33

Chapter 1:

Introduction to Reports

Workspace ONE™ UEM Reports provide access to reports on various sections of your Workspace ONE UEM solution. Use these reports to analyze patterns from the UEM console.

Custom Reports

Custom reports have moved locations. Navigate to **Hub > Intelligence**.

For more information, see [Reports for Workspace ONE Intelligence on page 4](#).

Workspace ONE UEM Reports

The reports functionality allows you to access detailed information about the devices, users, and applications in your Workspace ONE UEM solution. The exports of these reports are in CSV format.

For more information, see [Introduction to Reports on page 13](#).

Reports Storage

Optimize the storage of your Workspace ONE UEM Reports through reports storage. This storage feature increases the performance of Workspace ONE UEM Reports. Consider enabling reports storage if you see a performance impact on your Workspace ONE UEM database when using reports.

For more information, see [Reports Storage on page 32](#).

Chapter 2:

Reports for Workspace ONE Intelligence

Use Reports by Workspace ONE Intelligence to collate data in your Workspace ONE UEM deployment. Intelligence reporting uses a cloud-based report storage system to gather data and create the reports.

Reports Background

The Reports feature provides faster, easier access to critical business intelligence data than normal Workspace ONE UEM reports. Build reports using starter templates or customize canned reports. You can select from categories that include Apps, Devices, and OS Updates. These reports provide the latest data extracted from your Workspace ONE UEM environment.

Reports use a separate service to push data to a reports cloud service. This service captures data useful to administrators when trying to answer critical questions. The feature gathers an initial snapshot of your deployment and continues to capture ongoing changes.

Install the Reports Service

Before using Workspace ONE Intelligence features, you must install the Workspace ONE Intelligence Connector service (also known as the ETL installer) onto a separate server in your Workspace ONE UEM environment.

Each feature uses the Workspace ONE Intelligence Connector Service installed from the Workspace ONE Intelligence Connector Installer. The Workspace ONE Intelligence Connector service gathers the data from your Workspace ONE UEM console server and pushes it to the reports cloud service.

For more information, see [Workspace ONE Intelligence Requirements on page 5](#) and [Install the Workspace ONE Intelligence Connector Service for On-Premises on page 6](#).

Reports Wizard

The Reports wizard can create a customized report using a starter template or a new report. The wizard guides you through each step.

Reports use filters you can customize to gather data from apps and devices based on key attributes. Include as many filters as necessary to narrow the results of the report. Each filter added uses the "AND" operator. You then select the value for the value and the operator for each attribute.

For more information, see [Run the Reports Wizard on page 8](#).

Manage Reports

After creating a report, manage your reports from the Reports List View. From this screen, you can run reports, schedule reports to run, copy reports, and delete reports.

For more information, see [Reports Management on page 10](#)

Workspace ONE Intelligence Requirements

Before you can use Workspace ONE Intelligence features, you must turn on reports powered by Workspace ONE Intelligence (different from Workspace ONE UEM reporting). You must then install the Workspace ONE Intelligence Connector service (also known as the ETL installer).

How to Turn On Reports

- **Shared SaaS** customers work with their account representatives to access reports powered by Workspace ONE Intelligence. These deployments do not need to install their own Workspace ONE Intelligence Connector server.
- **Dedicated SaaS** customers work with their account representatives to access reports powered by Workspace ONE Intelligence. These deployments do not need to install their own Workspace ONE Intelligence Connector server. Review the instructions listed in this knowledge base article, <https://support.workspaceone.com/articles/115013381407>.
- **On-premises** customers work with their account representative to access reports powered by Workspace ONE Intelligence. These deployments must install their own Workspace ONE Intelligence Connector server.

Workspace ONE Intelligence Connector Server Requirements for On-Premises

You must install the Workspace ONE Intelligence Connector service on its own server before you can use Workspace ONE Intelligence features.

Requirement	Description
Hardware Requirements	
CPU	1 CPU
RAM	8 GB
Storage	50 GB
Software Requirements	
OS	Windows Server 2012 R2 or later
Java	Java 8

Requirement	Description
Network Requirements	
Outbound traffic from the Workspace ONE Intelligence Connector service	Port 443
Internal network access to the Workspace ONE UEM Database	The port used is based on your Workspace ONE UEM deployment.

Install the Workspace ONE Intelligence Connector Service for On-Premises

The Workspace ONE Intelligence Connector service collects data from your Workspace ONE UEM database and pushes it to the cloud-based report service.

Find the connector at <https://resources.workspaceone.com/view/88ymmbfft3zt9jbnc3gt/en>.

You must install it on its own server. For additional information about the installation process of other Workspace ONE UEM application servers, refer to the **VMware Workspace ONE UEM Installation Guide** on <https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/>.

Important: If you upgrade the Workspace ONE UEM database as part of the upgrade process, you must stop the Workspace ONE Intelligence Connector Service during the Workspace ONE UEM Database upgrade. You must then restart the service after finishing the upgrade process.

Important: If you must change the setting for **Deployment Region**, do not run the installer again.

To install the Workspace ONE Intelligence Connector Service, take the following steps.

1. Download the Workspace ONE Intelligence Connector installer on to the server you configured for the service.
2. Run the installer and select **Next**.
3. Accept the Terms of Use and select **Next**.
4. Ensure that the Workspace ONE Intelligence Connector Service is selected as a feature to install. Select **Next**.
5. The installer detects the version of Java installed on the application server. If the installer does not detect the required version, the required version installs. Select **Next**.
6. Enter the Database server settings.

Setting	Description
AirWatch Database Server	Select Browse next to the Database server text box and select your Workspace ONE UEM database from the list. If you are using a custom port, do not select Browse . Instead, use the following syntax: DBHostName,<customPortNumber> , then select Browse to select the database server. For example: db.acme.com, 8043

Setting	Description
Application Authentication	<p>Select one of the following authentication methods.</p> <ul style="list-style-type: none"> • Windows Authentication uses a service account on the Windows server to authenticate. You are prompted to enter the service account that you want to use. This service account is used to run all the application pools and Workspace ONE UEM-related services. The service account must have Workspace ONE UEM Database access. • SQL Server Authentication uses the SQL server authentication method. You are prompted to enter the user name and password.
AirWatch Database Name	Enter the name of the Workspace ONE UEM database or browse the SQL server and select it from a list.

Select **Next**.

7. Select the Destination Folder in which to install the Workspace ONE Intelligence Connector service. Select **Next**.
8. Configure the Workspace ONE Intelligence Connector Service settings.

Setting	Description
Deployment Region	<p>Select the region for your cloud service.</p> <p>Whitelist the api.ci.dpa0.org and the discovery.awmdm.com URLs for all regions. The installer calls these endpoints for a list of all supported regions.</p> <p>Each URL represents a region of the cloud service and is selected based on the location of your enterprise data. The United States (Sandbox) is for UAT environments.</p> <p>Ensure that the right region is selected. Do not run the installer again if you must change this region in the future.</p> <p>If you upgrade your Workspace ONE Intelligence Connector Service from a previous version, this screen does not display because you cannot change your region during an upgrade.</p> <p>Supported regions and URLs you might want to whitelist:</p>

Setting	Description
	<ul style="list-style-type: none"> • United States (UAT environment) <ul style="list-style-type: none"> ◦ api.sandbox.data.vmwservices.com ◦ eventproxy.sandbox.data.vmwservices.com ◦ sandbox.data.vmwareservices.com • United States (Production) <ul style="list-style-type: none"> ◦ api.na1.data.vmwservices.com ◦ eventproxy.na1.data.vmwservices.com ◦ na1.data.vmwservices.com • Frankfurt <ul style="list-style-type: none"> ◦ api.eu1.data.vmwservices.com ◦ eu1.data.vmwservices.com ◦ eventproxy.eu1.data.vmwservices.com • Ireland <ul style="list-style-type: none"> ◦ api.eu2.data.vmwservices.com ◦ eu2.data.vmwservices.com ◦ eventproxy.eu2.data.vmwservices.com • Sydney <ul style="list-style-type: none"> ◦ api.au1.data.vmwservices.com ◦ au1.data.vmwservices.com ◦ eventproxy.au1.data.vmwservices.com • Tokyo <ul style="list-style-type: none"> ◦ ap1.data.vmwservices.com ◦ api.ap1.data.vmwservices.com ◦ eventproxy.ap1.data.vmwservices.com
Installation Token	<p>Enter your Workspace ONE UEM Installation Token.</p> <p>This token is created as part of the Workspace ONE UEM Installation process. For more information, see the VMware AirWatch Installation Guide (VMware provides this document to you as part of the on-premises installation process).</p>

Select **Next**.

9. Select **Install** to install the Workspace ONE Intelligence Connector Service. After the installation finishes, select **Finish**.

Run the Reports Wizard

The reports wizard guides you through creating a customized report on your Workspace ONE UEM environment. The wizard has blank templates that you can use as a base for your reports, or you can customize canned reports.

For information about accessing the Workspace ONE Intelligence UI, see [Access Workspace ONE Intelligence on page 10](#).

To run the reports wizard, take the following steps.

1. Access the Workspace ONE Intelligence UI.
2. Go to **Reporting > Reports** and then select **Add Report**.
3. Select the report category: **Apps**, **Devices**, or **OS Updates**.
4. Select a template and select **Next**.

Setting	Description
Apps Templates	
Blank Report	Select to create a report from a blank template.

Setting	Description
Managed Apps	Select to create a report that shows a list of all managed apps on your devices.
All Apps	Select to create a report that lists all apps, managed or unmanaged, on your devices.
Workspace ONE UEM iOS and Android Agents	Select to create a report that lists all AirWatch Agent app details on your iOS and Android devices.
Device Templates	
Blank Report	Select to create a report from a blank template.
Enrolled devices	Select to create a report that lists all enrolled devices and their details.
Non-Compliant Devices	Select to create a report that lists all devices that violate your compliance policies.
OS Updates Templates	
Blank Report	Select to create a report based on a blank template.
All Windows OS Updates	Create a report on all (or filtered) updates to the Windows OS.
Critical Update Status	Create a report containing all (or filtered) critical updates to the OS.
Security Update Status	Create a report focused on security updates to the OS.
Service Pack Update Status	Create a report about service pack updates to the OS.

5. On the Customize screen, select **Add Filter** to add filters to your blank template or customize a starter template further. Each filter requires the following settings.

Setting	Description
Filter	Select an attribute that corresponds to the data you are trying to gather. For example, the Enrolled Devices template uses the Enrollment Status attribute to narrow results.
Selectors	Select an operator that applies to the value of the attribute. For example, if you are using the Device Organization Group GUID attribute, select the Includes selector to include all devices in the OG that match the value.
Value	Enter a value on which you want to receive data. For some selectors, you can select the value from a drop-down menu whereas others require an explicit entry. For example, if you are using the Enrollment Status attribute and the Includes selector, select Enrolled to receive a report on all enrolled devices. Conversely, if you are filtering devices by the Country attribute and the Include selector, you must enter in the name of the country you want to include in the report. You must Add Filter for each country you want to filter.

6. Under **Report Preview**, select **Edit Columns**. The **Edit Columns** screen displays.
7. Find the column that corresponds to the filter you have selected to see a preview of the report.

8. Select **Save** to return to the **Add Report** screen and select **Next**.
9. Enter a **Report Name** and **Report Description**.
10. Select **Run your report now** if you want to run the report after saving the customized report.
11. Optionally, you can select **Run report now** or you can create a schedule for the report at another time.
12. Select **Save** to save the report.

Access Workspace ONE Intelligence

Access the Workspace ONE Intelligence interface from the Workspace ONE UEM console. From the Workspace ONE Intelligence interface, you can use dashboards, automation, and reports (formerly custom reports).

Access the Workspace ONE Intelligence Interface

You must enter your credentials and opt-In to the service.

Access the reports by navigating to **Hub > Intelligence**, select **Opt-in**, and select **Launch** after installing the Workspace ONE Intelligence Connector service.

Return to the Workspace ONE UEM Console

To return to the Workspace ONE UEM console, follow these steps.

1. Select the square menu for VMware Services in the top right corner of the UI.
2. Select **Workspace ONE UEM** from the VMware Services menu.

Reports Management

After creating a report, you can manage your reports from the Reports List View. You can run reports, schedule reports to run, copy reports, and delete reports.

Run Reports

Select a report and select **Run** to run the report immediately. After the report finishes, you receive an email with a link directing you to your report.

Send Reports

Select a report and select **Send** to send the report to another Workspace ONE UEM administrator. They can then access the report through the link sent.

Schedule Reports

Select a report and select **Schedule** to schedule a report to run and to send an email containing a link to the report after it is finished.

The email contains a download link to the report. To access the report, users must have an admin account on the Workspace ONE UEM console to log in and authenticate before downloading.

In the **Schedule Report** screen, configure the following settings to schedule a report.

Setting	Description
Send To	Enter each recipient email address.
Recurrence	<p>Select from the drop-down menu the frequency the report runs.</p> <ul style="list-style-type: none"> • Hourly • Daily • Weekly • Monthly <p>The Recurrence value affects the available time settings.</p>
Hourly	
Every	Select the number of hours that must pass before the report runs again.
Starts At	Select the time of day the report runs.
Daily	
Time of the day	Select the time of day you want the report to run.
Weekly	
Days of the week	Select the days of the week and the time of day you want the report to run.
Starts At	Select the time of day the report runs.
Monthly	
Day of month	<p>Set the day of the month and the time of day you want the report to run.</p> <p>This setting displays when Recurrence is set to Monthly.</p>
Starts At	Select the time of day the report runs.
Ends	
Ends	If you want to stop the recurrence of a report, set the end date.
Subject	Enter a subject for the email sent after the report finishes. The email contains the link to access the report.
Message	Enter a message for the email sent after the report finishes.

You can view scheduled reports and their frequency by navigating to **Hub > Intelligence > Launch > Reporting > Scheduled Reports**.

Copy Reports

Select a report and select **Copy** to create a copy of the report. Use this action when you want different schedules for the same report. Copy also helps when you want to create a report that is based on an existing report without starting from the beginning.

Delete Reports

Select a report and select Delete to delete a report. Deleting a report removes the report and any associated subscriptions permanently.

Edit Reports

To edit the filters of a report, select a report and select **Edit**.

Chapter 3:

Introduction to Reports

The reports functionality allows you to access detailed information about the devices, users, and applications in your Workspace ONE™ UEM solution.

Use this information to troubleshoot your deployment and make informed decisions on what actions to take. The exports of these reports are in comma-separated values (CSV) format.

In version 9.0.2, Workspace ONE UEM added three new reports that appear the same as existing reports but use a revamped back-end framework. This new framework generates reports with improved features.

- More intuitive interface.
- Improved report generation reliability.
- Easier filter selection.
- Faster download times.
- Enhanced export status tracing capability.
- Streamlined reports subscription functionality.

The storage of your reports depends on the storage solution you use. By default, Workspace ONE UEM stores the reports in the database. The reports remain in the database until they expire. Once expired, the reports are automatically deleted. Depending on the size of your deployment, consider using a storage solution as an extension to your database to improve performance.

Extend your database with File Storage and Reports Storage.

- File Storage stores reports, content, and application in a separate file storage server.
- Reports Storage stores Workspace ONE UEM Reports in a dedicated file store separate from all other content.

To improve performance, consider enabling the reports storage. This storage uses a dedicated server to store all Workspace ONE UEM Reports and increase performance. For more information, see [Reports Storage on page 32](#).

Important: If you are using version 9.0.2 or 9.0.3, you must enable File Storage to use Workspace ONE UEM Reports. For more information, see [File Storage on page 29](#)

New Reports

The **New** tag in front of the report name in the UEM console identifies new reports. These reports combine multiple deprecated reports.

To see the new reports, navigate to **Hub > Reports & Analytics > Reports > List View**. To see the exported new reports, navigate to **Hub > Reports & Analytics > Exports**.

Workspace ONE™ UEM offers 20 new reports. The following table shows the available columns for each of these new reports.

New Reports	
Admin Login History	
Name	Browser
Core User	Platform
Login Date	Failure Reason
Source IP	Status
Admin User Roles	
Organization Group ID	Role
Organization Group Name	Role Description
User name	Last Login Date
Email	User Type
First Name	Primary
Last Name	
Application Details By Device	
Organization Group ID	Installed Version
Organization Group Name	Bundle Size (KB)
Friendly Name	Dynamic Size (KB)
Serial Number	Total Size
App Name	Install Status
App Identifier	Install Status Reason
Deployed By Workspace ONE UEM	App First Seen
Managed App	App Updated Date
Assigned Version	Device ID
Device Type	Device Model
OS Version	Ownership Type
Device Last Seen	User name
Email address	

New Reports	
Blacklist or Non-Whitelist Application Details By Device	
Organization Group ID	Device Model
Organization Group Name	OS Version
Device ID	Ownership
User name	Phone Number
Email Address	App Name
Serial Number	App Identifier
IMEI	App Version
Device Platform	App First Seen
Certificate Near Expiration	
Certificate Name	Profile Name
Issued To	Friendly Name
Issued By	Organization Group Name
CA Name	Effective Date
Status	Days until Expires
Content Details by Device	
Organization Group ID	Content Type
Organization Group Name	Content Installed
Device ID	Content Priority
Friendly Name	Content Importance
User name	Content Category
Email Address	Status
Serial Number	Content Version
IMEI	Content Size in KB
Device Platform	Effective Date
Device Model	Expiration Date
OS Version	Last Modified Date
Ownership	Last Seen
Content Name	Days Offline
Count of Active Devices	
Organization Group Name	Total Number of Inactive Devices
Total Number of Active Devices	Total Number of Devices

New Reports	
Count of Active Devices by Users	
Organization Group ID	Total Number of Inactive Devices
User name	Total Number of Devices
Total Number of Active Devices	
Device Battery Log	
Device ID	Battery Flag
Friendly Name	Battery Life Percent
Organization Group ID	Battery Voltage
Organization Name	Battery Current
Device Model	Battery Temperature
Device Platform	Battery mAh Consumed
OS Version	Battery Average Interval
Owner	Battery Average Current
AC Line Status	Backup Battery Lifetime
Sample Time	Backup Battery Full Life Time
Transmit Time	Backup Battery Life Percent
Battery Life Time	Backup Battery Flag
Battery Full Time	Backup Battery Voltage
Device Inventory	
Organization Group ID	Current Carrier
Organization Group Name	Device Roaming
Device ID	Roaming Start date
Friendly Name	Roaming End Date
User name	MAC Address
Email Address	Wi-Fi IP Address
First Name	IMEI
Last Name	Sim Card Number
Display Name	GPRS Connection
Serial Number	Device Capacity(GB)
Device Platform	Available Capacity(GB)
Device Model	Available Physical Memory (MB)
Phone Number	Total Physical Memory (MB)

New Reports	
Ownership	Battery Life Percent
OS Version	AC Power Sample Time
Enrollment Date	Device On AC Power
Compliance Status	Payload Removal Disallowed
Enrollment Status	Is Supervised
Unenrollment Date	EAS DeviceID
Managed By	Is Cloud Backup Enabled
Last Seen	Last iCloud Backup Date
Asset Number	Is Activation Lock Enabled
Is Compromised	Purchase Country
Find My iPhone	Estimated Purchase Date
Country	Warranty Status
MDM Managed	Registration Date
Device Identifier	Coverage Start Date
Home Carrier	Coverage End Date
Device Location Log	
Organization Group Name	Email Address
Organization Group ID	Sample Time
Friendly Name	Latitude
Device ID	Longitude
User name	Elevation
Device Security Posture	
Organization Group ID	IMEI
Organization Group Name	Data protection is enabled.
Device ID	Block level encryption is enabled.
Friendly Name	File level encryption is enabled.
Serial Number	Passcode is present.
Device Model	Passcode Compliant Y/N
Phone Number	Pending Installs
Ownership	All assigned profiles are installed.
OS Version	Passcode Compliant With Profiles
Last Seen	Encryption is compliant

New Reports	
Is Compromised	Internal storage encryption is enabled
MAC Address	SD Card encryption is enabled
Wi-Fi IP Address	Offline Days
Enrollment User Name	Device Group
Email Address	
Device Usage Details	
Organization Group ID	Roaming Data Usage
Organization Group Name	Data Usage (MB)
Device ID	Plan Name
Friendly Name	Cell Card Identifier
Ownership	Record Date
Device Platform	Daily Peak Voice
Device Model	Daily Off Peak Voice
OS Version	Daily Message
User name	Message Limit
Email Address	Daily Data Usage
Serial Number	Billing Cycle
IMEI	Monthly Peak Voice
Phone Number	Monthly Voice Percent Utilization
Last Seen	Monthly Off Peak Voice
Sim Card Number	Monthly message
Sample Time	Monthly Message Percent Utilization
Home Carrier	Monthly Data Usage
Current Carrier	Monthly Data Percent Utilization
Country	Call Start Date Time
Network IP Address	Call Duration Minutes
Cellular IP Address	Call Direction
Device Roaming	Call Answered State
Roaming Start date	Call End State
Roaming End Date	Call Connection State
Data Received (KB)	Call Roaming
Data Sent (KB)	Contact Name

New Reports	
Total KB	
Device Wipe Log	
Device ID or MAC Address	Organization Group ID
Friendly Name	Organization Group Name
Serial Number	User name
Device Type	Email Address
Device Model	Wipe Issued By
OS Version	Wipe Type
Ownership	Event Time
Device Platform	
Devices with User Details	
Organization Group ID	User Status
Organization Group Name	Platform
Friendly Name	Device Model
Device ID	OS Version
User name	Ownership Type
User Id	Serial Number
First Name	IMEI
Last Name	Enrollment Status
Email Address	Compliance Status
User Phone Number	Date Enrolled
Domain Type	Date Unenrolled
Profile Configuration Settings	
Organization Group	Device Model
Profile Name	Minimum Operating System Name
Profile Group Type	Maximum Operating System Name
Device Platform	Profile Setting Name
Description	Value
Assignment Type	Location Group Path
Profile Details by Device	
Organization Group ID	Model
Organization Group Name	OS Version

New Reports	
Friendly Name	C/E/S
User name	Profile
Email User name	Installed Version
Email Address	Latest Version
Serial Number	Installed Date
MAC Address	Installed
SDK Analytics	
Device ID	App Identifier
Friendly Name	Application Name
Organization Group ID	Application Version
Organization Group Name	Event Name
User name	Event Data
Sample Time	
Shared Device History	
Organization Group ID	Last Name
Organization Group Name	Email Address
Device ID	Check-in Date
Device Name	Checkout Date
First Name	
Terms of Use Acceptance Detail	
Organization Group Name	Phone Number
Organization Group ID	Terms of Use Name
User name	Version
First Name	Accepted Version
Last Name	Accepted
Email Address	Accepted On

Subscribe to a New Report

Subscribe to a new report to receive alerts from the **Hub** page of the UEM console. Subscription enables you to access important information regarding usage and other technical parameters.

For security reasons, the subscription email for new reports does not contain the report as a file attachment. The email provides a link to download the report. This link requires authentication to download. Only admins with valid credentials can access the reports.

Procedure

1. Navigate to **Hub > Reports & Analytics > Reports > List View > All Reports**.
2. Select a desired new report and select the **Report Subscriptions** icon.
3. On the **Parameters** tab, configure applicable settings to set criteria for the scope of the report. These settings vary depending on the report.
4. On the **Schedule** tab, configure the following settings.

Setting	Description
From	Specifies from whom the subscription is sent.
To	Specifies who receives the subscription.
Recurrence	Defines when the UEM console sends the subscription. Available options are once, daily, weekly, and monthly. You can also set the time of day for the report and the end of recurrence. If the recurrence is set to specific days of the month such as the 31st day of a month when the month only has 30 days, you do not receive a report for that month.
Date/Time	Specifies when to start sending subscriptions.
Subject	Specifies a subject to help identify the subscription when the UEM console delivers it.
Message	Defines the message to explain the subscription when the UEM console delivers it.

Important: Administrators with the appropriate role permissions and organization group access can view and edit other administrator's subscriptions.

Generate Reports

The Workspace ONE™ UEM reports and analytics solution includes the ability to export data from many sections in the UEM console. From the **Exports** page on the UEM console, you can download the generated reports – once reports are successfully generated, links to download are available in the **Export** grid.



To generate, view, and export a report, take the following steps.




1. Navigate to **Hub > Reports & Analytics > Reports > List View** and select the desired report.
2. On the report screen, complete the applicable settings. These settings vary depending on the report.
3. Click **Download** to export the report to the **Exports** page.
4. Navigate to **Hub > Reports & Analytics > Exports** and select the desired report. Click **Complete** available under **Status** column against the selected report to download it.

Note: The exported new reports are mentioned as **New Reports** and the existing reports are mentioned as **Reports** under **Export Type** column.

Hub > Reports & Analytics >

Exports

Filters >   Search List

Export Page	Organization Group	Time Exported	Expiration Date	Status	Export Type
Application Compliance	Global	1/23/2017 2:20 PM	1/28/2017 2:20 PM	Complete 	Reports
Application Compliance	Global	1/23/2017 2:18 PM	1/28/2017 2:18 PM	Complete 	Reports
Application Details By Device	Global	1/19/2017 3:35 PM	1/24/2017 3:35 PM	Complete 	New Reports

Note: From v9.0, the reports (in a comma-separated values (CSV) structure) are available for download in zipped format.

Subscribe to an Old Report

Subscribe to a report to receive alerts from the **Hub** page of the UEM console. Subscription enables you to access important information regarding usage and other technical parameters.

Important: Any subscriptions associated with a deprecated report should function as it is. Instead, they are marked as deprecated. Consider using new reports and creating subscriptions to use them.

Procedure

1. Navigate to **Hub > Reports & Analytics > Reports > List View > All Reports**.
2. Select a desired report and select the **Report Subscriptions** icon.
3. On the **General** tab, configure the following settings.

Setting	Description
Description	Defines a descriptive name for the subscription.
Render Format	Defines the format for the report. The default file format is comma-separated values (CSV).
Reply To	Specifies who receives the subscription.
Subject	Specifies a subject to help identify the subscription when the UEM console delivers it.
Message Body	Defines the message to explain the subscription when the UEM console delivers it.

4. On the **Parameters** tab, configure applicable settings to set criteria for the scope of the report. These settings vary depending on the report.
5. On the **Execution** tab, configure the following settings.

Setting	Description
Recurrence	
Once	Select this option to subscribe to this report a single time.
Daily	Select this option to receive the report every time a set number of days pass.
Weekly	Select this option to receive the report on specific days of the week.
Monthly	Select this option to receive the report on a specific day of the month. You can also set the schedule to First, Second, Third, Fourth, or Last weekday of the month. If the recurrence is set to a day that does not occur in the month, you do not receive a report. For example, if you set recurrence to the Fourth Friday of a month, and the month only has 3 Fridays, you do not receive a report for that month. This also applies to specific days of the month such as the 31st day of a month when the month only has 30 days.

Setting	Description
Range	
Date/Time	Set the specific day and time to receive the report.
Range	Set the end date for the subscription to the report.



6. On the **Distribution List** tab, use one or all the parameters to make a distribution list to receive the subscription.

Setting	Description
Choose Role	Select a role from the menu and click Add to List to add it to the distribution list.
Choose User	Select individual users and click Add to List to add them to the distribution list.
Enter Email Address	Enter the addresses of subscription recipients manually, if you know the address and click Add to List to add them to the distribution list.
Search List	Enter text to search the distribution list to find individual entries and to delete entries from the distribution list.
Distribution List	Define to whom Workspace ONE™ UEM sends the subscription. Create this list using the role, user, and email address entries.

Note: Admins can edit failed or inactive subscriptions and can save them again to fix the error.

Manage Reports

You can navigate to **Hub > Reports & Analytics > Reports > List View** page to view reports in the UEM console. You can export data in various formats and perform the following actions.



	Report Subscriptions – Configure a report to run on a specified interval with defined parameters.
	Add to My Reports – Add reports to the My Reports tab for quick access.

Hub > Reports & Analytics > Reports >

List View

All Reports | My Reports | Recent Reports

Filters

 Report Subscriptions  Add to My Reports

Name	Category	Description
<input type="radio"/> New Application Details By Device	Applications	Displays devices with application details
<input type="radio"/> New Device Inventory	Device Inventory	Displays device inventory details
<input checked="" type="radio"/> New Devices With User Details	Device Inventory	Displays device and user details.
<input type="radio"/> Active Inactive Users By Location	Devices	Summary of active/inactive users at a selected point in time
<input type="radio"/> Admin Account Login History	User Management	Login history for selected admin accounts
<input type="radio"/> Admin User Roles	User Management	Lists all Admin users with their roles by Organization Group
<input type="radio"/> Apple MDM	Devices	Apple MDM
<input type="radio"/> Application Analytics By Date	Devices	Application Analytics By Date

Items 1 - 50 of 115 Page Size: 50

Troubleshooting Reports

If you are having issues with the Reports feature, consider troubleshooting your issue before calling support. These troubleshooting steps address the most common issues with the Reports feature.

Problem

Reports do not initiate.

Cause

The background processing service is not running.

Solution

Follow the instructions in [Enable Background Processing Service on page 27](#)

Problem

Errors occasionally occur during report processing.

Cause

Various causes

Solution

Refer to the following logs.

- Web Console Logs – For troubleshooting purpose, refer to web console logs when any console error occurs. These logs can be referred for both new and existing reports. Logs can be found here:

```
\AirWatch\Logs\WebConsole\WebConsoleLog.txt
```

- Detailed error logs about new reports – Refer to logs found here:

```
\AirWatch\Logs\Services\BackgroundProcessorServiceLogFile.txt
```

- Detailed error logs about old reports – Refer to the reports server logs found here:

```
\Microsoft SQL Server\MSRS12.ABC\Reporting Services\LogFiles
```

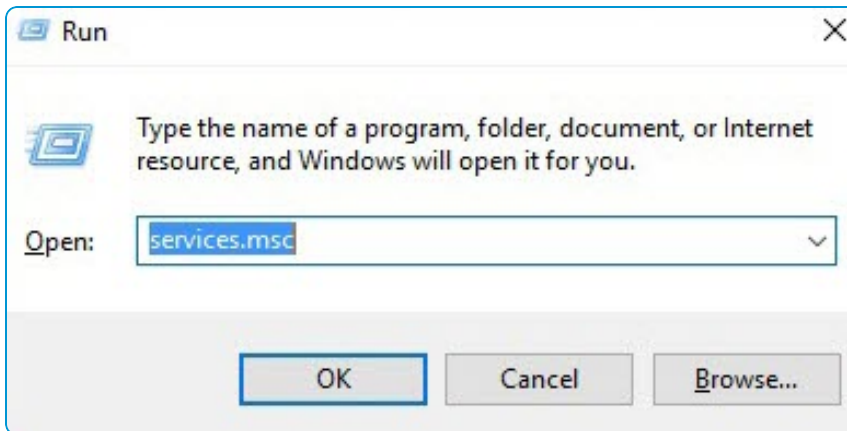
Enable Background Processing Service

Workspace ONE™ UEM Reports require the background processing service running on the UEM console server. The installation process enables this process but if it is not running, you must enable it to use Workspace ONE UEM Reports.

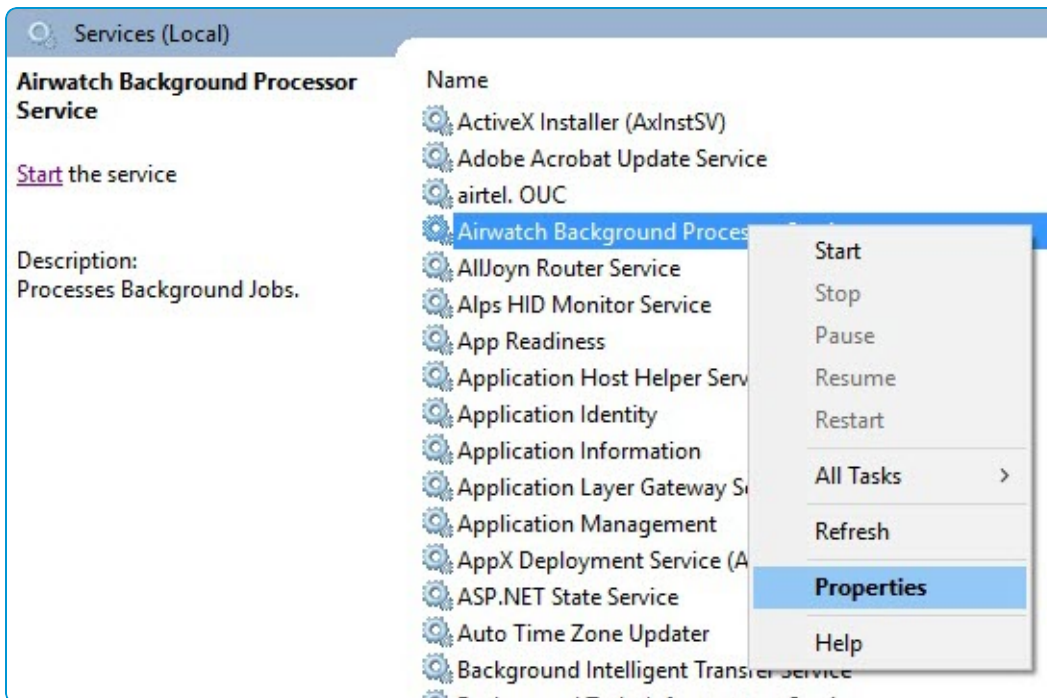
Each UEM console server requires the background processing service. Each server processes reports and writes them to their respective queue before sending them to the database, file storage, or reports storage.

To enable the background processing service, perform the following steps.

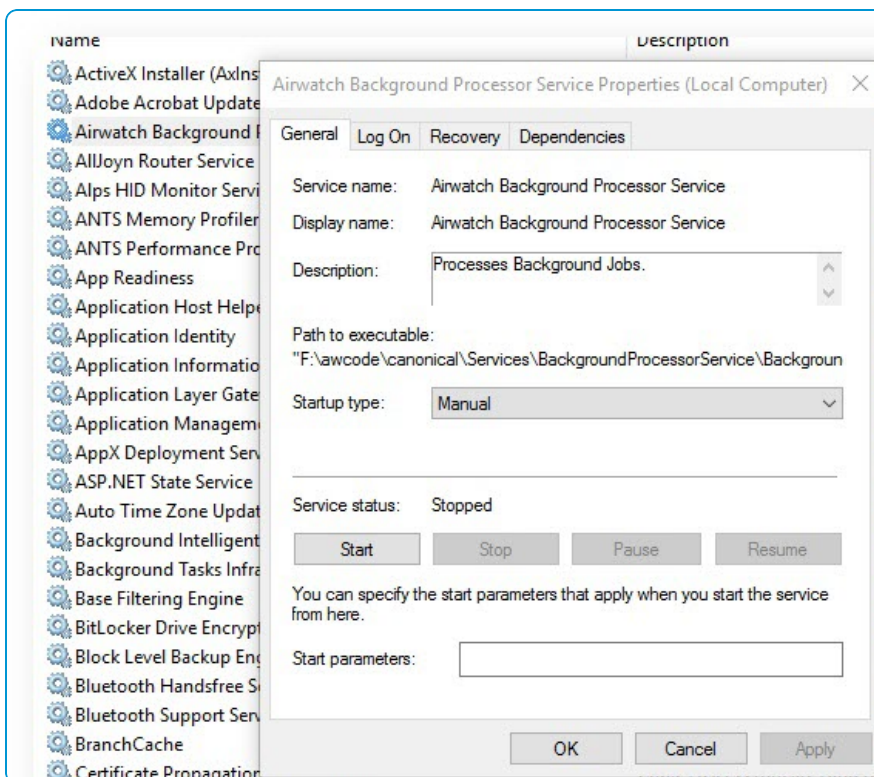
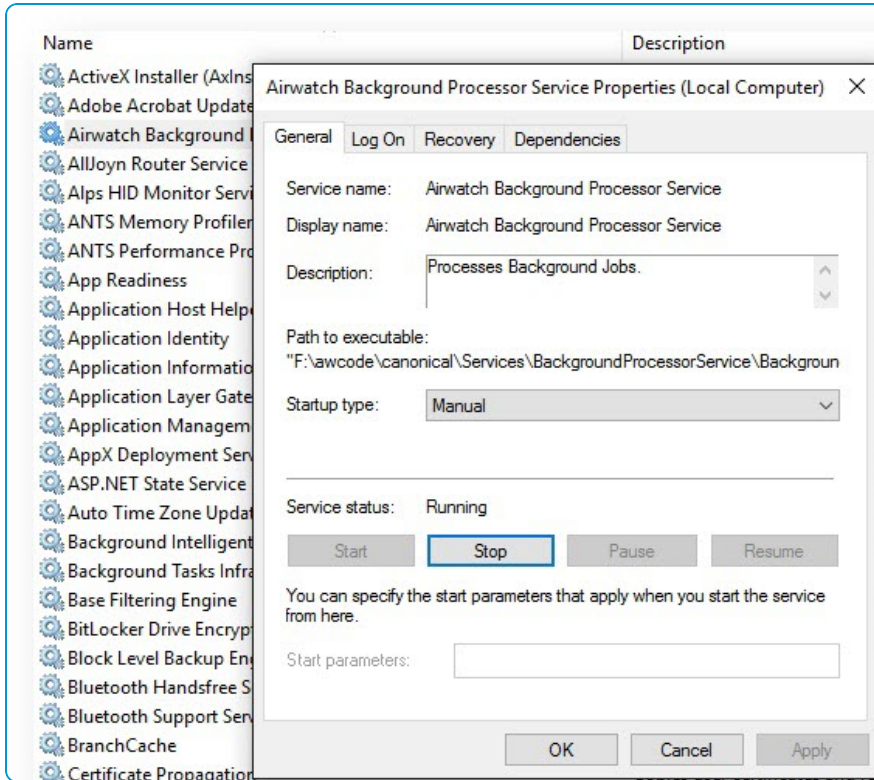
1. Press **Windows key + R** on the console server box.
2. Run the command "services.msc".



3. A screen appears listing all services running on the Console Server box. Locate **Airwatch Background Processor Service** and select **Properties**.



4. A screen appears showing if the service status. Make sure that status of this service is **Running**. If status is **Stopped**, ensure to **Start** the service.



Chapter 4:

File Storage

Certain Workspace ONE UEM functionality uses a dedicated file storage service to handle processing and downloads, which reduces the overall burden on your Workspace ONE UEM database and increases its performance. It also includes certain Workspace ONE UEM reports, internal application deployment, and Workspace ONE UEM-managed content. When you enable file storage for any of these functionalities, it is applied to the others automatically. Setting up file storage causes all reports, all internal applications, and all managed content to be stored there.

Configuring file storage manually is only applicable to on-premises customers. It is automatically configured for SaaS customers.

Workspace ONE UEM Reports

As of console version 9.0.2, three new reports were added that appear the same as existing reports but use a revamped back-end framework. This new framework generates reports with greater reliability and faster download times. To take advantage of these benefits, you must set up file storage.



For more information about these reporting updates, see the following Knowledge Base article: <https://support.air-watch.com/articles/115002346928>.

Internal Applications

When file storage is enabled, all internal application packages that you upload through the UEM console are stored in a file storage location.

File storage is required to deploy Win32 applications (IPA, PAK, APPX, MSI, EXE, and so on) and macOS applications (.dmg, .pkg, .mpkg, and so on) from the Apps & Books area of the UEM console. This feature is called software distribution.

Workspace ONE UEM Managed Content

You can separate the managed content from the Workspace ONE UEM database by storing it in a dedicated file storage location. Uploading large amounts of managed content might cause issues with database performance. In this case, on-premises customers can free up space in the database by moving the managed content to an integrated local file storage solution.

Personal content also moves to the file storage solution is enabled. By default, personal content is stored in the SQL database. If you have a Remote File Storage enabled, personal content is stored in the RFS and not in the file storage or SQL database.

File Storage Requirements

To set up local file storage, you must meet the following requirements.

Important: File Storage is required for Windows 10 Software Distribution.

Create the Shared Folder on a Server in Your Internal Network

- File storage can reside on a separate server or the same server as one of the other AirWatch application servers in your internal network. It is only accessible to components that require access to it, such as the Console and Device Services servers.
- If the Device Services server, Console server, and the server hosting the shared folder are not in the same domain, then establish Domain Trust between the domains to avoid the authentication failure. If the Device Services server or Console server is not joined to any domain, then supplying the domain during service account configuration is sufficient.

Configure the Network Requirements

- **If using Samba/SMB** – TCP: 445, 137, 139. UDP: 137, 138
- **If using NFS** – TCP and UDP: 111 and 2049

Allocate Sufficient Hard Disk Capacity

Your specific storage requirements may vary depending on how you plan to use file storage. The file storage location should have enough space to accommodate the internal apps, managed content, or reports you intend to use. Take into the account the following considerations.

- If you enable caching for internal apps or content, then a best practice is to size the Device Services server for 120 percent of the cumulative size of all the apps/content you need to publish.
- For storing reports, your storage requirements depend on the number of devices, the daily amount of reports, and the frequency with which you purge them. As a starting point, you should plan to allocate at least 50 GB for deployment sizes up to 250,000 devices running about 200 daily reports. Adjust these numbers based on the actual amount you observe in your deployment. Apply this sizing to your Console server as well if you enable caching.

Create a Service Account with Correct Permissions

- Create an account with read and write permissions to the shared storage directory.
- Create the same local user and password on the Console, Device Services, and the server that is being used for File Storage.

- Give the local user read/write/modify permissions to the file share that is being used for the File Storage Path.
- Configure the File Storage Impersonation User in AirWatch with the local user.

You can also use a domain service account instead of a local user account.

Configure File Storage at the Global Organization Group

Configure file storage settings at the Global organization group level in the UEM Console.

File Storage Configuration

Enable File Storage for Reports

Configure file storage using the following procedure.

1. At the Global organization group level, navigate to **Groups & Settings > All Settings > Installation > File Path** and scroll to the bottom of the page.
2. Select the **File Storage Enabled** slider and configure the settings. When file storage is enabled, you can configure an external repository in which files are stored. A disabled setting means that files are stored as binary large objects in the database.

Setting	Description
File Storage Path	Enter the path files are to be stored in the following format: \\{Server Name}\{Folder Name}, where Folder Name is the name of the shared folder you create on the server.
File Storage Caching Enabled	When enabled, files are cached locally on the DS server when accessed for the first time. Subsequent requests are served using the file cached on the DS server instead of streaming from the file storage location. If you enable caching, consider accommodating for the amount of space needed on the server. For more information, see File Storage Requirements on page 30 .
File Storage Impersonation Enabled	Select to add a service account with the correct permissions.
File Storage Impersonation Username	Provide a valid service account user name to obtain both read and write permissions to the shared storage directory.
Password	Provide a valid service account password to obtain both read and write permissions to the shared storage directory.

3. Select the **Test Connection** button to test the configuration.

Chapter 5:

Reports Storage

Optimize the storage of your Workspace ONE™ UEM Reports through reports storage. This storage feature increases the performance of Workspace ONE UEM Reports.

This storage is different than file storage used by reports, internal applications, and content. If you already use file storage, you do not need to enable reports storage. Consider enabling reports storage if you see a performance impact on your Workspace ONE UEM database when using reports. Reports storage applies to reports only, helping increase overall reports performance, and reducing the burden on your Workspace ONE UEM database.

If you enable both file storage and reports storage, reports storage overrides file storage when storing reports. Report storage requires a dedicated server to host the service and storage of the reports.

Reports Storage Requirements

To deploy the reports storage solution, ensure that your server meets the requirements.

Note: If you are already using File Storage, then Report Storage is available, but not required to run your deployment. If you configure Reports Storage alongside File Storage, the report files will prioritize report storage over file storage.

Create the Shared Folder on a Server in Your Internal Network

- Report storage can reside on a separate server or the same server as one of the other Workspace ONE™ UEM application servers in your internal network. Ensure only the components that require access to the server can access the report storage server, such as the Console and Device Services servers.
- If the Device Services server, Console server, and the server hosting the shared folder are not in the same domain, then establish Domain Trust between the domains to avoid an authentication failure. If the Device Services or Console servers are not joined to any domain, then supplying the domain during service account configuration is sufficient.

Configure Reports Storage at the Global Organization Group

Configure reports storage settings at the Global organization group level in the UEM console.

Create a Service Account with Correct Permissions

- Create an account with read and write permissions to the shared storage directory.
- Create the same local user and password on the Console, Device Services, and the server that is being used for report storage.
- Give the local user read/write/modify permissions to the file share that is being used for the Report Storage Path.
If you give the user modify permission, Workspace ONE UEM deletes old reports from the storage. If you do not give the user modify permissions, consider monitoring report storage to prevent running out of space.
- Configure the Report Storage Impersonation User in Workspace ONE UEM with the local user.

You can also use a domain service account instead of a local user account.

Allocate Sufficient Hard Disk Capacity

Your specific storage requirements can vary depending on how you plan to use reports storage. Ensure that the reports storage location has enough space to accommodate the reports you intend to use.

For storing reports, your storage requirements depend on the number of devices, the daily number of reports, and the frequency with which you purge them. As a starting point, plan to allocate at least 50 GB for deployment sizes up to 250,000 devices running about 200 daily reports. Adjust these numbers based on the actual amount you observe in your deployment. Also apply this sizing to your Console server if you enable caching.

Enable Reports Storage

Enable reports storage to store your reports on a dedicated server and improve performance.

To enable reports storage, take the following steps.

1. Navigate to **Groups & Settings > All Settings > Installation > Reports**.
2. Set **Report Storage Enabled** to **Enabled**.

3. Configure the report storage settings.

Settings	Description
Report Storage File Path	Enter the path reports are to be stored in the following format: \\{Server Name}\{Folder Name}, where Folder Name is the name of the shared folder you created on the server.
Report Storage Caching Enabled	<p>When enabled, files are cached locally on the DS server when accessed for the first time. Subsequent requests are served using the file cached on the DS server instead of streaming from the file storage location.</p> <p>If you enable caching, consider accommodating for the amount of space needed on the server. For more information, see Reports Storage Requirements on page 32.</p>
Report Storage Impersonation Enabled	Enabling this option adds a service account with the correct permissions.
Report Storage Impersonation user name	<p>Enter the user name of a valid service account with both read, write, and modify permissions to the shared storage directory.</p> <p>Displays when Report Storage Impersonation Enabled is enabled.</p>
Report Storage Impersonation Password	<p>Enter the password of a valid service account with both read, write, and modify permissions to the shared storage directory.</p> <p>Displays when Report Storage Impersonation Enabled is enabled.</p>

4. Select the **Test Connection** button to test the configuration.