Reports and Analytics

VMware Workspace ONE UEM 2111

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

1 Workspace ONE UEM Reports 4

- New Reports 5
- Generate Reports 14
- Subscribe to an Old Report 16
- Manage Reports 18
- Troubleshooting Reports 18

2 File Storage 22

3 Reports Storage 25

Workspace ONE UEM Reports 1

Workspace ONE UEM lets you access detailed information about the devices, users, and applications in report form that you can analyze with Excel.

Custom Reports

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

For more information, see the VMware Workspace ONE Intelligence Products Guide.

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 XLSX or CSV (comma-separated values) format. You can view and analyze both file formats with Microsoft Excel.

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.

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

Reports Storage

Expand 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.

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 Chapter 3 Reports Storage.

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 Chapter 2 File Storage.

Reports for Workspace ONE Intelligence

For all procedures and information surrounding reports for Workspace ONE Intelligence, refer to the VMware Workspace ONE Intelligence documentation on docs.vmware.com.

This chapter includes the following topics:

- New Reports
- Generate Reports
- Subscribe to an Old Report
- Manage Reports
- Troubleshooting Reports

New Reports

The **New** tag in front of the report name in Workspace ONE UEM identifies new reports. These reports combine multiple legacy reports that have been deprecated.

Subscribe to a New Report

Subscribe to a new report to receive alerts from the **Monitor** 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.

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

1 Navigate to **Monitor > 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	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. 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.
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.

New Reports by Name

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

Workspace ONE UEM offers 21 new reports. The following table shows the available columns for each of these new reports.

Table 1-1. Admin Login History

Name	Browser
Core User	Platform
Login Date	Failure Reason
Source IP	Status

Table 1-2. 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	

Table 1-3. Application Details by Device

Organization Group ID	App Name
Organization Group Name	App Identifier

Table 1-3. Application Details by Device (continued)

Device ID	App Status
Friendly Name	App Assignment Status
User Name	Installation Status
Email Address	Last Action Taken
Device Platform	Last Action Timestamp
OS Version	App First Seen
Device Model	App Last Seen
Enrollment Status	Department
Last Seen	Custom Attribute 1
Ownership	Custom Attribute 2
Serial Number	Custom Attribute 3

Table 1-4. Certificate Near Expiration

Certificate Name	Profile Name
Issued To	Friendly Name
Issued By	Organization Group Name
CA Name	Effective Date
Status	Days until Expires

Table 1-5. Content Details by Device

This report shows both managed content set to download automatically and content set to be downloaded manually or on-demand. Admins typically use this data to evaluate unused documents to see which ones have the best traction with end users, then update or retire.

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

Table 1-5. Content Details by Device (continued)

Device Model	Expiration Date
OS Version	Last Modified Date
Ownership	Last Seen
Content Name	Days Offline

Table 1-6. Count of Active Devices

Organization Group Name	Total Number of Active Devices
Organization Group Type	Total Number of Inactive Devices
Organization Group ID Name	Total Number of Devices
Created On	

Table 1-7. Count of Active Devices by Users

Organization Group Name	User Name
Organization Group Type	Total Number of Active Devices
Organization Group ID Name	Total Number of Inactive Devices
Created On	Total Number of Devices

Table 1-8. Denylist or Non-Allowlist 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

Table 1-9. Device Battery Log

Device ID	Battery Flag
Friendly Name	Battery Life Percent
Organization Group ID	Battery Voltage
Organization Name	Battery Current

Table 1-9. Device Battery Log (continued)

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

Table 1-10. 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)
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

Table 1-10. Device Inventory (continued)

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

Table 1-11. Device Location Log

Organization Group Name	Email Address
Organization Group ID	Sample Time
Friendly Name	Latitude
Device ID	Longitude
User name	Elevation

Table 1-12. 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.
Is Compromised	Internal storage encryption is enabled.
MAC Address	SD Card encryption is enabled.
Wi-Fi IP Address	Offline Days

Table 1-12. Device Security Posture (continued)

Enrollment User Name	Device Group
Email Address	

Table 1-13. Device Usage Detail

Organization Group ID	Roaming End Date
Organization Group Name	Data Received (KB)
Device ID	Data Sent (KB)
Friendly Name	Total KB
Ownership	Roaming Data Usage
Device Platform	Data Usage (MB)
Device Model	Plan Name
OS Version	Cell Card Identifier
User name	Record Date
Email Address	Daily Peak Voice
Serial Number	Daily Off Peak Voice
IMEI	Daily Message
Phone Number	Message Limit
Last Seen	Daily Data Usage
Sim Card Number	Billing Cycle
Sample Time	Monthly Peak Voice
Home Carrier	Monthly Voice Percent Utilization
Current Carrier	Monthly Off Peak Voice
Country	Monthly message
Network IP Address	Monthly Message Percent Utilization
Cellular IP Address	Monthly Data Usage
Device Roaming	Monthly Data Percent Utilization
Roaming Start date	

Table 1-14. Device Wipe Log

Device ID or MAC Address	Organization Group ID
Friendly Name	Organization Group Name

Table 1-14. Device Wipe Log (continued)

Serial Number	User name
Device Type	Email Address
Device Model	Wipe Issued By.
OS Version	Wipe Type.
Ownership	Event Time
Device Platform	

Table 1-15. Devices with Application and User Details

Organization Group ID	Deployed By AirWatch
Organization Group Name	Managed App
Device ID	App Type
User Name	Installed Version
Email Address	Bundle Size(KB)
Serial Number	Dynamic Size(KB)
IMEI	Install Status.
Sim Card Number	Install Status Reason.
Device Platform	App First Seen
Device Model	App Last Seen
OS Version	Last Seen
Ownership	Device Capacity
Phone Number	Available Device Capacity
Department	Enrollment Date
Custom Attribute 1	Enrollment Status
Custom Attribute 2	Console App Name
Custom Attribute 3	Assigned Version
App Name	Last Action Taken
App Identifier	Last Action Timestamp

Table 1-16. Devices with User Details

Organization Group ID	User Status
Organization Group Name	Device Platform

Table 1-16. Devices with User Details (continued)

Friendly Name	Device Model
Device ID	OS Version
User name	Ownership
User Id	Serial Number
First Name	IMEI
Last Name	Enrollment Status
Email Address	Compliance Status
User Phone Number	Date Enrolled
Domain Type	Date Unenrolled

Table 1-17. 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

Table 1-18. Profile Details by Device

Organization Group ID	Model
Organization Group Name	OS Version
Friendly Name	C/E/S
User name	Profile
Email User name	Installed Version
Email Address	Latest Version
Serial Number	Installed Date
MAC Address	Installed

Table 1-19. SDK Analytics

Device ID	App Identifier
Friendly Name	Application Name

Table 1-19. SDK Analytics (continued)

Organization Group ID	Application Version
Organization Group Name	Event Name
User name	Event Data
Sample Time	

Table 1-20. Shared Device History

Organization Group ID	Last Name
Organization Group Name	Email Address
Device ID	Check-in Date
Device Name	Checkout Date
First Name	

Table 1-21. 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

Generate Reports

The reports and analytics solution in Workspace ONE UEM powered by AirWatch includes the ability to export data from many sections in the console. From the **Exports** page, you can

download the generated reports – once reports are successfully generated, links to download are available in the **Exports** grid.

Note

- The maximum size of a generated report is 4 GB.
- Reports sized in excess of 4 GB will not generate to completion. They are represented in the **Exports** grid with the status **File size exceeds limit**.
- Shared SaaS environments cannot change this 4 GB size limit.
- You can limit the number of records included in the generated report (and therefore reduce its size) by being more selective in the drop-down menu options of the report.
  - For example, when running a report on Applications, consider selecting specific apps instead of enabling the "Select All" check box.
  - You can also run multiple reports on smaller child OGs rather than a single report on the larger parent/Global OG.
- Dedicated SaaS and On-Premises environments can increase this 4 GB size limit by contacting support.

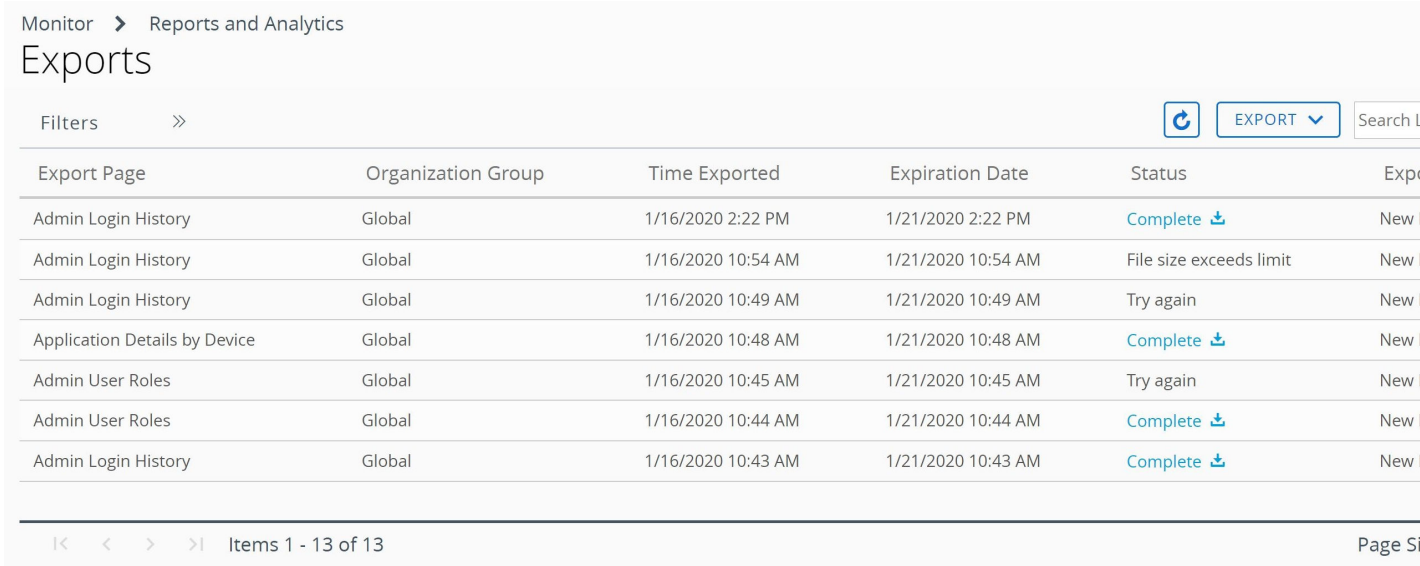
Procedure

1. Navigate to **Monitor > 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 **Monitor > Reports & Analytics > Exports** and select the desired report. Click **Complete** available under **Status** column against the selected report to download it.

Results

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



Note A **Try again** status indicates a server error during report generation.

What to do next

The comma-separated values (CSV) structured report is available for download in a ZIP format.

Subscribe to an Old Report

Workspace ONE UEM powered by AirWatch lets you subscribe to a report to receive alerts from the **Monitor**. Subscription enables you to access important information regarding use and other technical parameters.

Important Any subscriptions associated with a deprecated report continue to function. They are marked as deprecated. Consider using new reports and creating subscriptions to use them.

Procedure

1. Navigate to **Monitor > 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.

Setting	Description
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
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.
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.

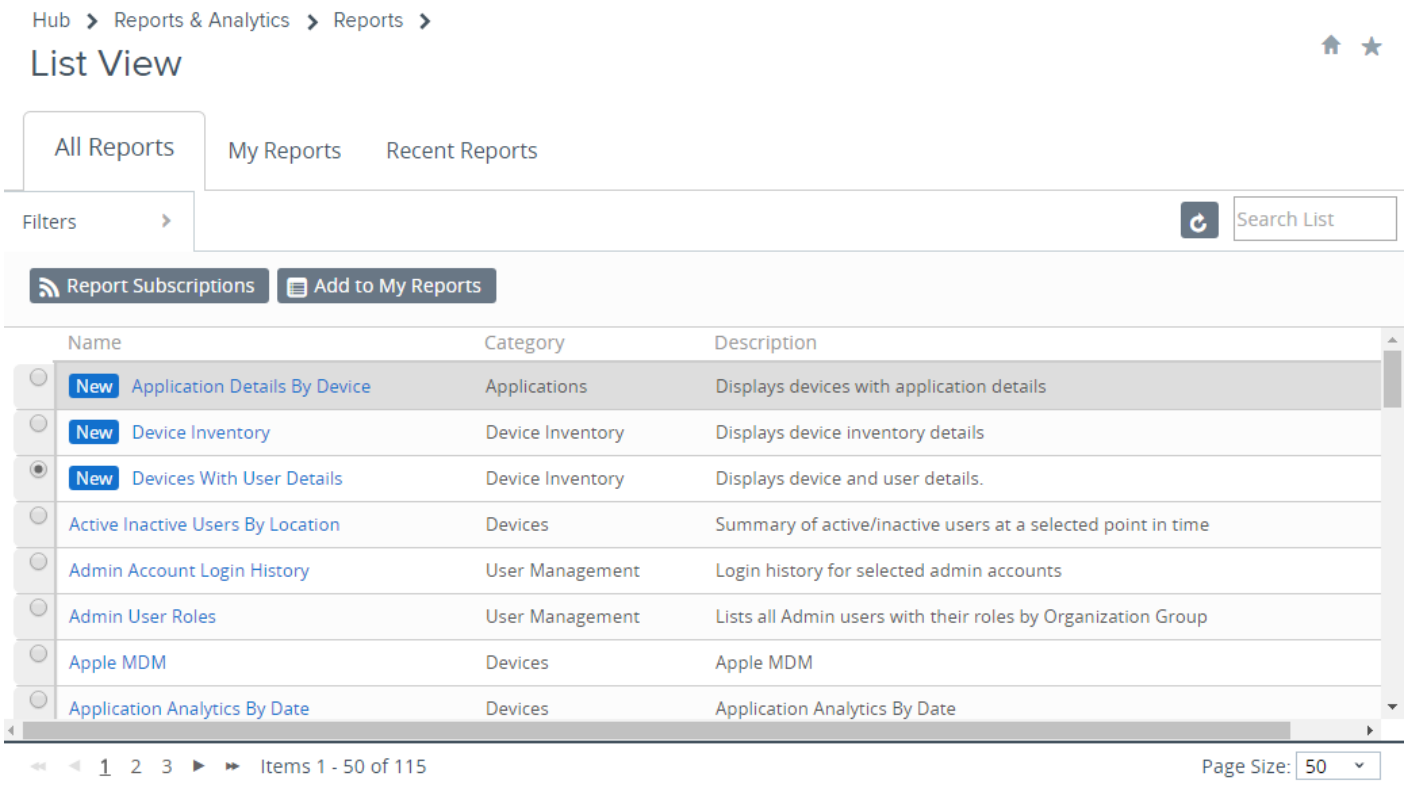
Setting	Description
Choose Role.	Select a role from the menu and click **Add to List** to add it to the distribution list.
Choose User.	Select individual users and click **Add to List** to add them to the distribution list.
Enter Email Address.	Enter the addresses of subscription recipients manually, if you know the address and click **Add to List** to add them to the distribution list.
Search List	Enter search parameters 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 **Monitor > 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.



Troubleshooting Reports

If you are having problems with the Reports feature, consider troubleshooting your problem before calling support. These troubleshooting steps address the most common problems with the Reports feature in Workspace ONE UEM.

Problem

Reports do not initiate.

Cause

The background processing service is not running.

Solution

Follow the instructions in the section below, entitled **Enable Background Processing Service**.

Problem

Errors occasionally occur during report processing.

Cause

Various causes.

Solution

Refer to the following logs.

- Web Console Logs – For troubleshooting purpose, refer to the 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
  ```

Problem

Reports fail to generate.

Cause

The size of the report exceeds the maximum size allowed of 4 GB.

Solution

Try to limit the size of the report by following the suggestions in Generate Reports.

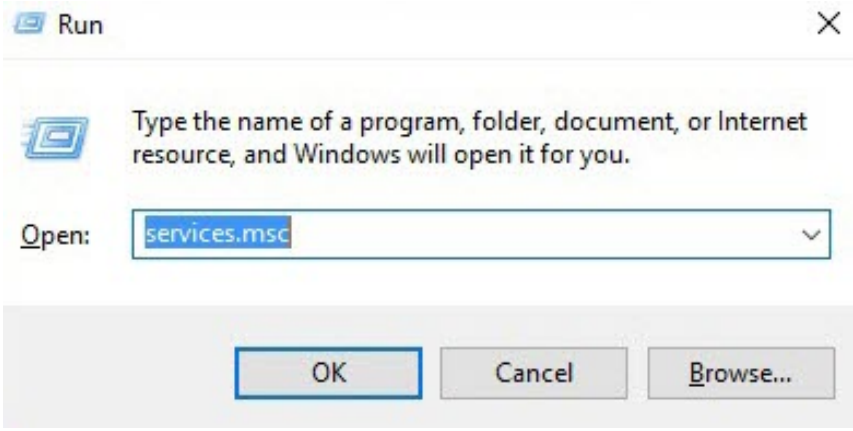
Enable Background Processing Service

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.

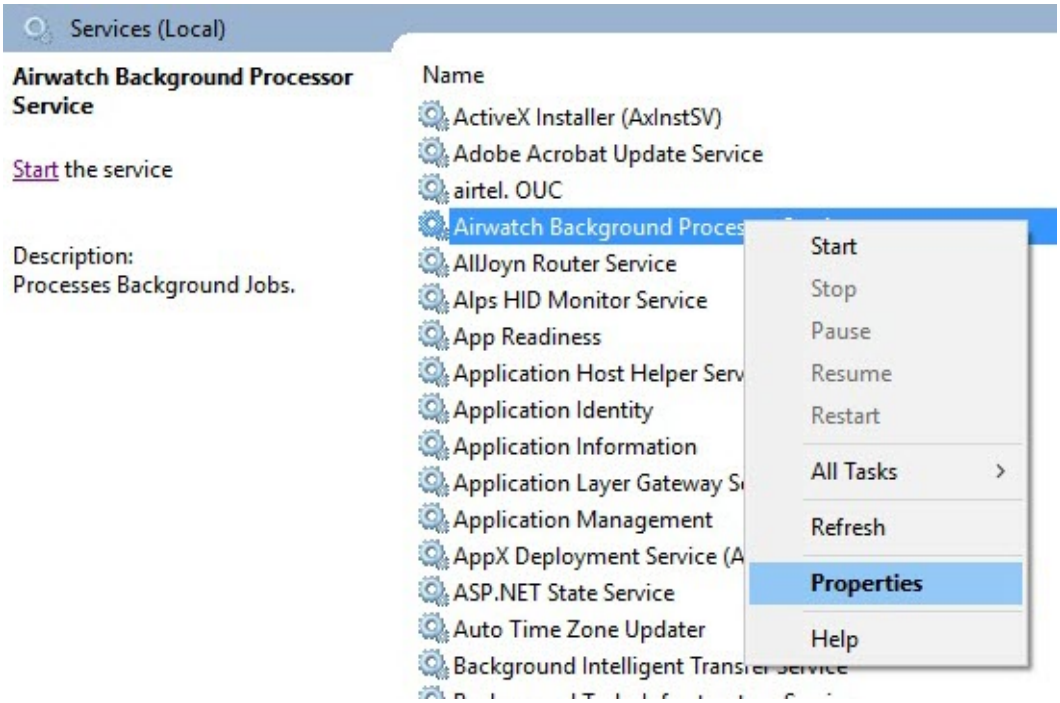
1 Press **Windows key + R** on the console server box.

2 Run the command "services.msc".



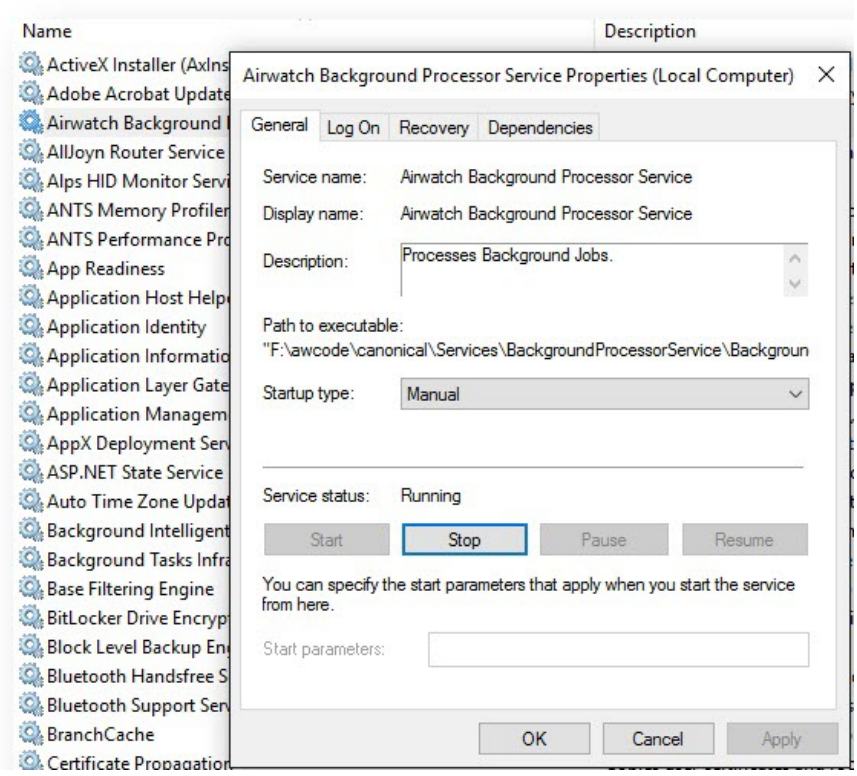
A screen displays listing all services running on the Console Server box.

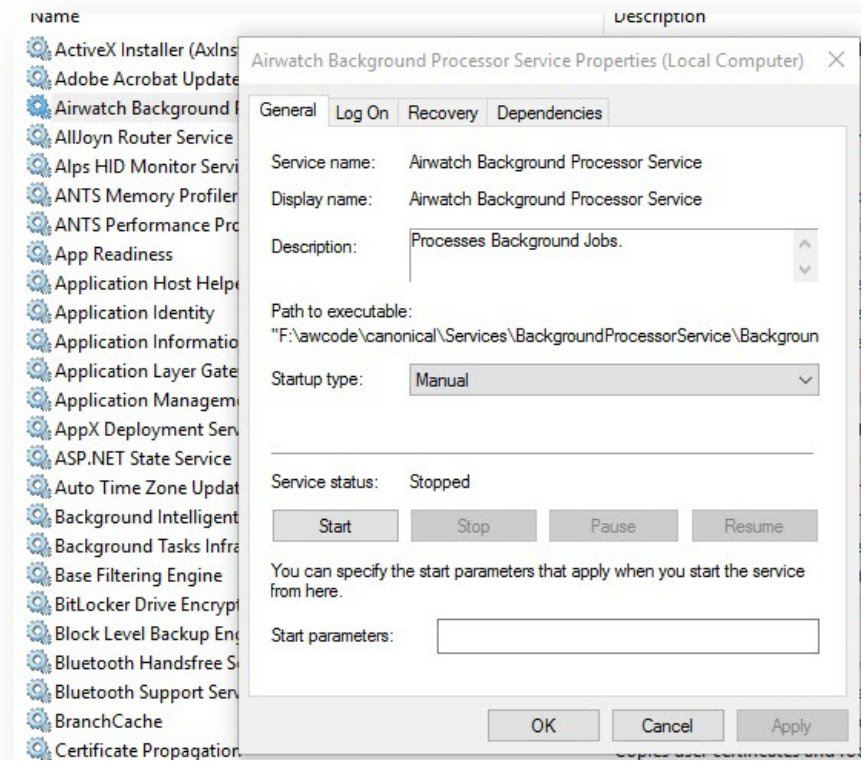
3 Locate **Airwatch Background Processor Service** and select **Properties**.



A screen displays showing if the service status.

4 Make sure that status of this service is **Running**. If status is **Stopped**, ensure to **Start** the service.


Name
Description
ActiveX Installer (AxInstSV)
Adobe Acrobat Update Service
Airwatch Background Processor Service
AllJoyn Router Service
Alps HID Monitor Service
ANTS Memory Profiler 2019.1
ANTS Performance Profiler 2019.1
App Readiness
Application Host Helper Service
Application Identity
Application Information
Application Layer Gateway Service
Application Management
AppX Deployment Service (AppXSVC)
ASP.NET State Service
Auto Time Zone Updater
Background Intelligent Transfer Service
Background Tasks Infrastructure Service
Base Filtering Engine
BitLocker Drive Encryption Service
Block Level Backup Engine Service
Bluetooth Handsfree Service
Bluetooth Support Service
BranchCache
Certificate Propagation
Airwatch Background Processor Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name: Airwatch Background Processor Service
Display name: Airwatch Background Processor Service
Description: Processes Background Jobs.
Path to executable:
"F:\awcode\canonical\Services\BackgroundProcessorService\Backgroun
Startup type: Manual
Service status: Running
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply


Name
Description
ActiveX Installer (AxInstSV)
Adobe Acrobat Update Service
Airwatch Background Processor Service
AllJoyn Router Service
Alps HID Monitor Service
ANTS Memory Profiler 2019.1
ANTS Performance Profiler 2019.1
App Readiness
Application Host Helper Service
Application Identity
Application Information
Application Layer Gateway Service
Application Management
AppX Deployment Service (AppXSVC)
ASP.NET State Service
Auto Time Zone Updater
Background Intelligent Transfer Service
Background Tasks Infrastructure Service
Base Filtering Engine
BitLocker Drive Encryption Service
Block Level Backup Engine Service
Bluetooth Handsfree Service
Bluetooth Support Service
BranchCache
Certificate Propagation
Airwatch Background Processor Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name: Airwatch Background Processor Service
Display name: Airwatch Background Processor Service
Description: Processes Background Jobs.
Path to executable:
"F:\awcode\canonical\Services\BackgroundProcessorService\Backgroun
Startup type: Manual
Service status: Stopped
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply

File Storage

2

Certain functionality in Workspace ONE UEM uses a dedicated file storage service to handle processing and downloads, which reduces the overall burden on the database and improves performance. Configuring file storage manually is only applicable to on-premises customers. It is configured automatically for SaaS customers.

It also includes certain 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.

Internal Applications

When you enable file storage, all internal application packages that you upload through the Workspace ONE 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 **Resources** area of the Workspace ONE 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.

File Storage Requirements for your Win32 Applications

If you have a lot of managed content taking up space in the database, Workspace ONE UEM offers you dedicated file storage. To set up file storage, you must determine the location and storage capacity, configure network requirements, and create an impersonation account.

Important File Storage is required for Windows 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 Workspace ONE UEM application servers in your internal network. It is only accessible to components that require access to it, such as Device Services, Console, and API servers.
- If the servers hosting Device Services, Console, & API servers, and the server hosting the shared folder are not in the same domain, then supply the domain when configuring the service account in the format <domain\username>. Domain Trust can also be established to avoid an authentication failure.

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 can vary depending on how you plan to use file storage. The file storage location must have enough space to accommodate the internal applications, managed content, or reports you intend to use. Take into the account the following considerations.

- If you enable caching for internal applications 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 must publish.
- 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, 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 in the domain of the shared storage directory.
- Give the local user read/write/modify permissions to the file share that is being used for the File Storage Path.
- Configure File Storage Impersonation User in Workspace ONE UEM with the domain account in the format <domain\username>.
- If the shared storage directory is not on a domain, create an identical local user and password on the server being used for File Storage, Device Services, Console, and API servers. In this case, supply the local user account in the format <username>.

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 Workspace ONE UEM Console.

Enable File Storage for Reports

Before you can enjoy the benefits of reports file storage in Workspace ONE UEM, you must enable and configure file storage.

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 deactivated 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	If you enable caching, consider accommodating for the amount of space needed on the server.
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.

Reports Storage

3

You can optimize the storage of your Workspace ONE UEM reports through reports storage. While the reports storage feature is separate from file storage, if you currently use file storage, you do not need to enable reports storage.

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 and see an improvement in reports performance in Workspace ONE UEM, 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 Device Services, Console, and API servers.

- If the servers hosting Device Services, Console, & API servers, 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, Console, and API 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 Workspace ONE 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 Device Services, Console, & API servers, 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 the performance of reports run in Workspace ONE UEM.

You must be in an on-premises environment.

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	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.
Report Storage Impersonation Enabled	Enabling this option adds a service account with the correct permissions.
Report Storage Impersonation user name	Enter the user name of a valid service account with both read, write, and modify permissions to the shared storage directory. Displays when **Report Storage Impersonation Enabled** is enabled.
Report Storage Impersonation Password	Enter the password of a valid service account with both read, write, and modify permissions to the shared storage directory. Displays when **Report Storage Impersonation Enabled** is enabled.

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