

# Reports and Analytics

VMware Workspace ONE UEM 1902



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

- 1 Introduction to Reports** 4
- 2 Reports for Workspace ONE Intelligence** 5
  - Workspace ONE Intelligence Requirements 6
  - Install the Workspace ONE Intelligence Connector Service for On-Premises 8
  - Run the Reports Wizard 10
    - Access Workspace ONE Intelligence 11
  - Reports Management 12
- 3 Workspace ONE UEM Reports Overview** 14
  - New Reports 15
    - Subscribe to a New Report 21
  - Generate Reports 21
  - Subscribe to an Old Report 22
  - Manage Reports 24
  - Troubleshooting Reports 24
    - Enable Background Processing Service 25
- 4 File Storage** 28
  - File Storage Requirements 29
  - Enable File Storage for Reports 30
- 5 Reports Storage** 31
  - Reports Storage Requirements 31
  - Enable Reports Storage 32

# 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 **Monitor > Intelligence**.

For more information, see [Chapter 2 Reports for Workspace ONE Intelligence](#).

## 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 [Chapter 3 Workspace ONE UEM Reports Overview](#).

## 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 [Chapter 5 Reports Storage](#).

# Reports for Workspace ONE Intelligence

# 2

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 Workspace ONE Intelligence Connector 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](#) and [Install the Workspace ONE Intelligence Connector Service for On-Premises](#).

## 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](#).

## 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](#)

This chapter includes the following topics:

- [Workspace ONE Intelligence Requirements](#)
- [Install the Workspace ONE Intelligence Connector Service for On-Premises](#)
- [Run the Reports Wizard](#)
- [Reports Management](#)

## 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 Access 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.
- **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.

### Required Workspace ONE UEM Console Version

Workspace ONE Intelligence requires Workspace ONE UEM console v9.6+.

### Required Database Permissions

To install the Workspace ONE Intelligence Connector, the person installing needs permissions for the following roles for the console and directory services servers.

- DBOwner for the Workspace ONE UEM database
- DBDatareader for the MSDB
- SQLAgentUserRole for the MSDB

## 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.

**Table 2-1. Hardware Requirements by Number of Devices**

Component	5000 Devices	25,000 Devices	50,000 Devices	100,000 Devices
Server	1	1	1	1
CPUs	2 (2 GHz Intel processor)			
Memory	4 GB	8 GB	8 GB	8 GB
Storage	25 GB	25 GB	25 GB	25 GB

**Table 2-2. Software Requirements**

Component	Requirement
Java	Java 8
OS	Windows Server 2012 R2 or later

**Table 2-3. Network Requirements**

Component	Requirement
Outbound traffic from the Workspace ONE Intelligence Connector service	Port 443
Protocol for outbound traffic from the Workspace ONE Intelligence Connector service	HTTPS
Internal network access to the Workspace ONE UEM Database	The port used is based on your Workspace ONE UEM deployment.

## Whitelist Regions of the Cloud Service for On-Premises

On the server for the Workspace ONE Intelligence Connector, whitelist specific URL destinations so that the connector installer can call the endpoints for a list of all supported regions. Also, whitelist other URL destinations depending on your region.

For the list, see the topic *URLs to Whitelist for On-Premises by Region* in the **VMware Workspace ONE Intelligence Guide**.

For an outline of what region resides in what part of the world, see the topic *Workspace ONE UEM SaaS Environment Location Mapped to a Workspace ONE Intelligence Region* in the **VMware Workspace ONE Intelligence Guide**.

## Proxy

If you use a proxy server and want to use it with the Workspace ONE Intelligence Connector, make sure you have whitelisted specific destinations. If you do not whitelist the listed destinations, the installation can fail.

For more information, see the topic *URLs to Whitelist for the Use of a Proxy Server in On-Premises Deployments* in the **VMware Workspace ONE Intelligence Guide**.

## 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/88ymbbfft3zt9jbnc3gt/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.

---

### Prerequisites

Ensure you have whitelisted the applicable URLs so the connector installation process can communicate with the correct cloud-based reports service. For the list of URLs, see the topic **URLs to Whitelist for On-Premises by Region** in the **Workspace ONE Intelligence User Guide**.

If you use a proxy server and want to use it with the Workspace ONE Intelligence Connector, make sure you have whitelisted specific destinations. If you do not whitelist the listed destinations, the installation can fail. See the topic *URLs to Whitelist for the Use of a Proxy Server in On-Premises Deployments* in the **Workspace ONE Intelligence User Guide**.

### Procedure

- 1 Ensure you have met the hardware, software, and network requirements outlined in the **Workspace ONE Intelligence User Guide**.
- 2 Download the Workspace ONE Intelligence Connector installer on to the server you configured for the service.
- 3 Run the installer and select **Next**.
- 4 Accept the Terms of Use and select **Next**.

- 5 Ensure that the Workspace ONE Intelligence Connector Service is selected as a feature to install. Select **Next**.

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.

- 6 Enter the Database server settings.

Setting	Description
Database server that you are installing to	Select <b>Browse</b> next to the <b>Database server</b> text box and select your Workspace ONE UEM database from the list.  If you are using a custom port, do not select <b>Browse</b> . Instead, use the following syntax: <b>DBHostName,&lt;customPortNumber &gt;</b> , then select <b>Browse</b> to select the database server.For example: db.acme.com, 8043
Connect using	Select one of the following authentication methods. <ul style="list-style-type: none"> <li>■ <b>Windows Authentication</b> 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.</li> <li>■ <b>SQL Server Authentication</b> uses the SQL server authentication method.  You are prompted to enter the user name and password.</li> </ul>
Name of database catalog	Enter the name of the Workspace ONE UEM database or browse the SQL server and select it from a list.

- 7 Select the Destination Folder in which to install the Workspace ONE Intelligence Connector service.
- 8 Configure the Workspace ONE Intelligence Connector Service settings.
  - a Select the deployment region for your cloud service. Ensure that the right region is selected.  
  
Do not run the installer again if you must change this region in the future.  
  
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.
  - b Enter your Workspace ONE UEM Installation Token.  
  
This token is created as part of the Workspace ONE UEM Installation process.
- 9 (Optional) Enter proxy information.  
  
Find this information in the Workspace ONE UEM console in **Groups & Settings > All Settings > Installation > Proxy > Console Proxy Settings**.
- 10 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](#).

## Procedure

- 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**.
  - Apps Templates

Setting	Description
Apps Starter Template	Select to create a report from a blank template.
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 Workspace ONE Intelligent Hub app details on your iOS and Android devices.

- Devices Templates

Setting	Description
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.
Device Starter Template	Select to create a report from a blank template.

- OS Updates Templates

**Table 2-4. OS Updates Templates**

Setting	Description
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.

**Table 2-4. OS Updates Templates (continued)**

Setting	Description
Service Pack Update Status	Create a report about service pack updates to the OS.
OS Updates Starter Template	Select to create a report based on a blank template.

- On the Customize screen, select the add filter icon (+) to add filters to your blank template or customize a starter template further.

Each filter requires the following settings.

Setting	Description
<b>Filter</b>	Select an attribute that corresponds to the data you are trying to gather. For example, the Enrolled Devices template uses the <b>Enrollment Status</b> attribute to narrow results.
<b>Selectors</b>	Select an operator that applies to the value of the attribute. For example, if you are using the <b>Device Organization Group GUID</b> attribute, select the <b>Includes</b> selector to include all devices in the OG that match the value.
<b>Value</b>	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 <b>Enrollment Status</b> attribute and the <b>Includes</b> selector, select <b>Enrolled</b> to receive a report on all enrolled devices. Conversely, if you are filtering devices by the <b>Country</b> attribute and the <b>Include</b> selector, you must enter in the name of the country you want to include in the report. You must <b>Add Filter</b> for each country you want to filter.

- Under **Report Preview**, select **Edit Columns**.  
The **Edit Columns** screen displays.
- Find the column that corresponds to the filter you have selected to see a preview of the report.
- Select **Save** to return to the **Add Report** screen and select **Next**.
- Enter a name and a description for the report.
- Select **Run report now** if you want to run the report after saving the customized report.
- (Optional) Select **Run report now** or create a schedule for the report at another time.
- 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).

To access the Workspace ONE Intelligence interface, you must enter your credentials and opt-In to the service.

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

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

### Procedure

- 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. Select a single report and use the management actions, the scheduler, and the audit logs.

### List View

The list view for Reports, **Reporting > Reports**, lets you select multiple reports and take actions with one selection.

- **Add Report** - Opens the Reports wizard to create a new report.
- **Edit** - Edits the filters of a report.
- **Run** - Runs the report immediately. After the report finishes, you receive an email with a link directing you to your report.
- **Share**- Sends the report to a single administrator or multiple administrators. They can then access the report through the link sent.
- **Schedule** - Schedules a report to run and to send an email containing a link to the report after it is finished. To access the report, users must have an admin account on the Workspace ONE UEM console to log in and authenticate before downloading.
- **Copy** - Creates 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** - Deletes a report and removes it and any associated subscriptions permanently.

### Single Report View

Select a report to access the **Overview**, **Schedules**, and **Audit Log** tabs.

- **Overview** - The **Overview** tab for a report contains management actions.
  - Edit
  - Run
  - Share

- Delete
- **Schedules** - The **Schedules** tab contains management actions for scheduling reports.
 

Select to add, edit, or delete a report. Add a report and configure the wizard settings. After the report runs, the system sends an email to the contacts configured in the wizard. 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** wizard, configure the following settings to schedule a report.

**Table 2-5. Settings to Schedule Reports**

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

You can view scheduled reports and their frequency by navigating to **Reporting > Scheduled Reports**. The Scheduled Reports page has **Edit** and **Delete** actions to manage schedules.

- **Audit Log** - The **Audit Log** tab lists events for a report. Find out when an event occurred, who caused it, and what happened. The log lists the following data.
  - Date and time
  - Admin account
  - Event name
  - Action

# Workspace ONE UEM Reports Overview

# 3

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.

- 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 [Chapter 5 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 4 File Storage](#)

---

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 the UEM console identifies new reports. These reports combine multiple deprecated reports.

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 20 new reports. The following table shows the available columns for each of these 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	Ownership
Organization Group Name	Serial Number
Device ID	App Name
Friendly Name	App Identifier
User Name	App Install Status
Email Address	Install Status
Device Platform	Install Status Reason
OS Version	Installed Version
Device Model	Managed App
Enrollment Status	App First Seen
Last Seen	App Last Seen
	App Type

### 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**

This report shows what content users are choosing to download. This report assumes that all the content admin has selected to auto download (via the "Download Type" deployment configuration option) is already on the device. Filtering such data up front allows a focus on only those documents a user must request/manually download. 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
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

**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)
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
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 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	
<b>Device Wipe Log</b>	
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	
<b>Devices with User Details</b>	
Organization Group ID	User Status
Organization Group Name	Device Platform
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

**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
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 **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.

### Procedure

- 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
<b>From</b>	Specifies from whom the subscription is sent.
<b>To</b>	Specifies who receives the subscription.
<b>Recurrence</b>	<p>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.</p> <p>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.</p>
<b>Date/Time</b>	Specifies when to start sending subscriptions.
<b>Subject</b>	Specifies a subject to help identify the subscription when the UEM console delivers it.
<b>Message</b>	Defines the message to explain the subscription when the UEM console delivers it.

## 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.

**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.

**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 <a href="#">↓</a>	Reports
Application Compliance	Global	1/23/2017 2:18 PM	1/28/2017 2:18 PM	Complete <a href="#">↓</a>	Reports
Application Details By Device	Global	1/19/2017 3:35 PM	1/24/2017 3:35 PM	Complete <a href="#">↓</a>	New Reports

**What to do next**

**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 **Monitor** 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 **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
<b>Description</b>	Defines a descriptive name for the subscription.
<b>Render Format</b>	Defines the format for the report. The default file format is comma-separated values (CSV).
<b>Reply To</b>	Specifies who receives the subscription.
<b>Subject</b>	Specifies a subject to help identify the subscription when the UEM console delivers it.
<b>Message Body</b>	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
<b>Once</b>	Select this option to subscribe to this report a single time.
<b>Daily</b>	Select this option to receive the report every time a set number of days pass.
<b>Weekly</b>	Select this option to receive the report on specific days of the week.
<b>Monthly</b>	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.
<b>Date/Time</b>	Set the specific day and time to receive the report.
<b>Range</b>	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
<b>Choose Role</b>	Select a role from the menu and click <b>Add to List</b> to add it to the distribution list.
<b>Choose User</b>	Select individual users and click <b>Add to List</b> to add them to the distribution list.
<b>Enter Email Address</b>	Enter the addresses of subscription recipients manually, if you know the address and click <b>Add to List</b> to add them to the distribution list.

Setting	Description
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 **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.

Hub > Reports & Analytics > Reports >

### List View

Home Star

All Reports | My Reports | Recent Reports

Filters >

Name	Category	Description
<input type="radio"/> <b>New</b> Application Details By Device	Applications	Displays devices with application details
<input type="radio"/> <b>New</b> Device Inventory	Device Inventory	Displays device inventory details
<input checked="" type="radio"/> <b>New</b> 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](#).

## 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

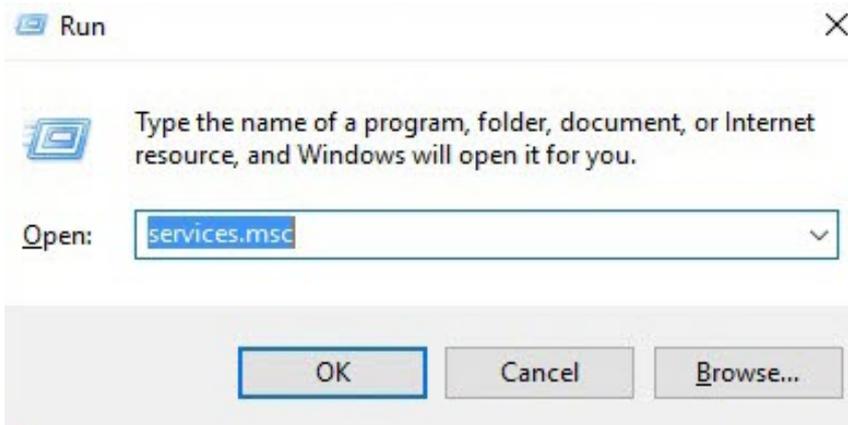
Workspace ONE UEM Reports require the background processing service running on the UEM console server. The installation process enables this process but if it is not running, you must enable it to use Workspace ONE UEM Reports.

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.

### Procedure

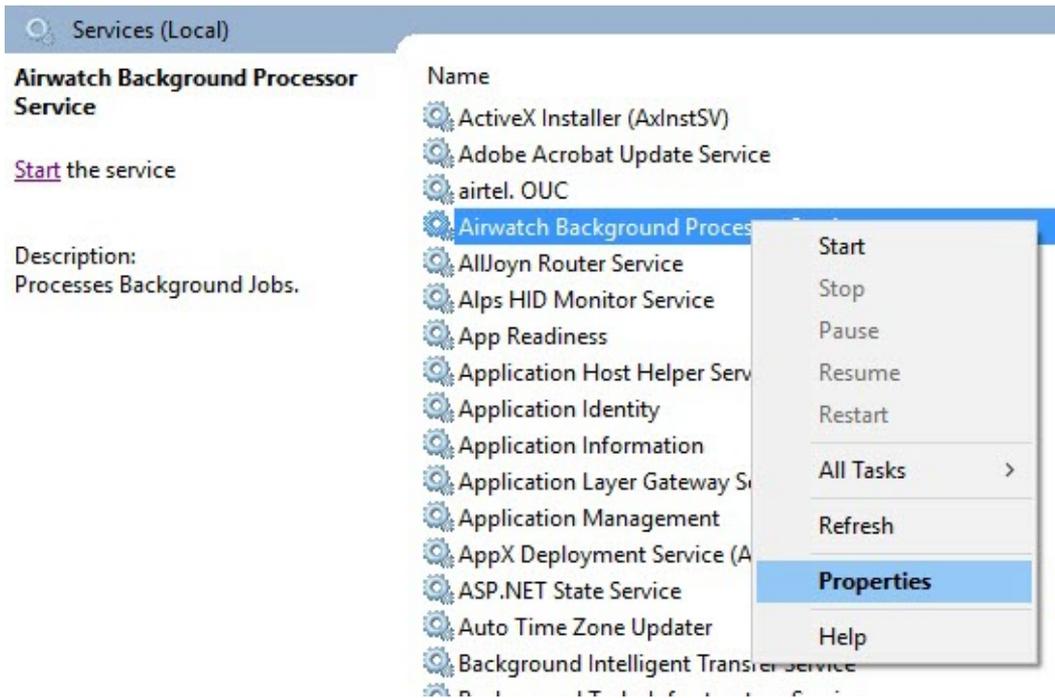
- 1 Press **Windows key + R** on the console server box.

- 2 Run the command "services.msc".



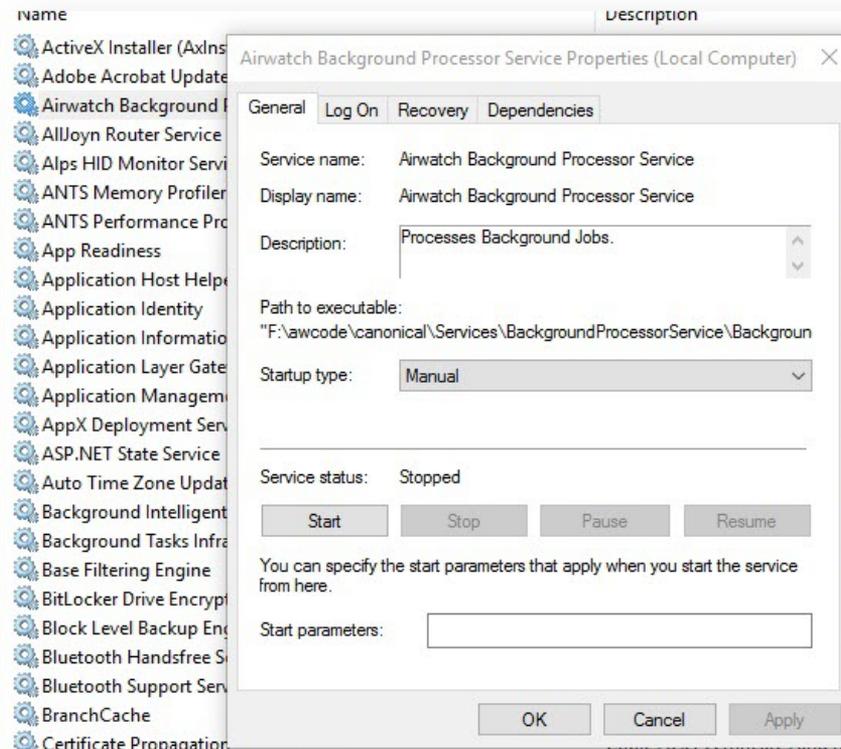
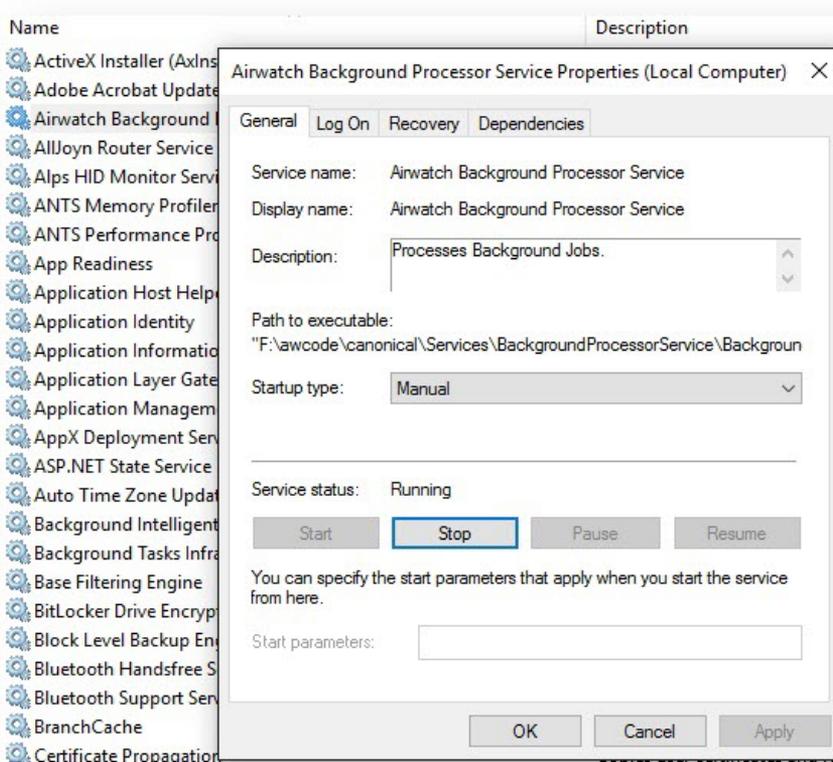
A screen appears listing all services running on the Console Server box.

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



A screen appears showing if the service status.

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



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

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.

## 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.

## 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.

This chapter includes the following topics:

- [File Storage Requirements](#)

- [Enable File Storage for Reports](#)

## File Storage Requirements

Separate the managed content from the Workspace ONE UEM database by storing it in a dedicated File Storage. To set up a file storage, you must determine the location and storage capacity for your file storage, configure the network requirements, and create an impersonation account.

---

**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.

## Enable File Storage for Reports

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

### 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
<b>File Storage Path</b>	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.
<b>File Storage Caching Enabled</b>	If you enable caching, consider accommodating for the amount of space needed on the server.
<b>File Storage Impersonation Enabled</b>	Select to add a service account with the correct permissions.
<b>File Storage Impersonation Username</b>	Provide a valid service account user name to obtain both read and write permissions to the shared storage directory.
<b>Password</b>	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

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.

This chapter includes the following topics:

- [Reports Storage Requirements](#)
- [Enable Reports Storage](#)

## 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.

### Procedure

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

3 Configure the report storage settings.

Settings	Description
<b>Report Storage File Path</b>	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.
<b>Report Storage Caching Enabled</b>	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 <a href="#">Reports Storage Requirements</a> .
<b>Report Storage Impersonation Enabled</b>	Enabling this option adds a service account with the correct permissions.
<b>Report Storage Impersonation user name</b>	Enter the user name of a valid service account with both read, write, and modify permissions to the shared storage directory.  Displays when <b>Report Storage Impersonation Enabled</b> is enabled.
<b>Report Storage Impersonation Password</b>	Enter the password of a valid service account with both read, write, and modify permissions to the shared storage directory.  Displays when <b>Report Storage Impersonation Enabled</b> is enabled.

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