VMware Workspace ONE Intelligence Dashboards, Automation, and Reports

Integrated Insights, App Analytics, and Automation

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

Table of Contents

Chapter 1:
Workspace ONE Intelligence

VMware Workspace ONE Intelligence gives you insights into your digital workspace. It offers enterprise mobility management (EMM) planning and automation. All these components help to optimize resources, strengthen security and compliance, and increase user experience across your environment.

Product and Pricing Information

See the VMware Workspace™ ONE™ product page at https://www.vmware.com/products/workspace-one.html for information on features and pricing.

For information about opting in to Workspace ONE Intelligence Reports, see the knowledge base article **Opt-in today to take advantage of Workspace ONE Intelligence Reports!** at https://support.workspaceone.com/articles/360007232773.

Trial Versions

If you would like to try licensed features of Workspace ONE Intelligence, like Dashboards and Automation, you can activate a trial version and try them for free for 30 days.

After 30 days, access to the trail version ends unless you buy an enterprise license. However, data, connections, and automation configurations are stored. If you choose to buy the licensed features in the future, your data, connections, and automation configurations are not lost. You can pick up where your trial version ended.

To activate a trial version, enter the information associated with your Workspace ONE UEM admin credentials. The VMware Workspace ONE team contacts you to see if you want to purchase an enterprise license.

A trial version of Workspace ONE Intelligence displays TRIAL banners on the user interface. It also notifies you of how many days you have left on your trial.

Data Driven Community Forums

Find the Data Driven Community Forums on My Workspace ONE at https://support.workspaceone.com/forums and select Data Driven from the menu.

Storage and Sampling

Workspace ONE Intelligence uses deployment data to offer Dashboards, Automation, and Reports. All these features use the same data that streams from your Workspace ONE deployment.

Workspace ONE Intelligence stores data to offer historical analysis. The system stores raw data for three months and stores trend data for 12 months. Raw data examples are battery information and operating system versions. Some trend data examples are application installations and application adoption, device category data, and enrollment and OS versions over time.

VMware stores and manages the data in its cloud services infrastructure. The reports cloud service within the services infrastructure collects and imports data at regular intervals from Workspace ONE transactional databases.

Components

Workspace ONE Intelligence aggregates data from Workspace ONE UEM and Apteligent by VMware. It includes dashboards, reports, and automation to analyze data and perform actions for efficiency and remediation. It integrates with third-party connection services like Slack and ServiceNow for notifications.

Dashboards

- **My Dashboard** represents the latest data in the reports infrastructure. Workspace ONE Intelligence streams data from the database in the cloud so that the analytics you see are a current picture of the state of your Workspace ONE deployment. You can also view historical data by editing widgets displayed on My Dashboard. For information, see My Dashboard on page 13.
- Use the **Apps** dashboard to analyze application adoption and use for managed applications in your Workspace ONE environment. For information, see Apps Dashboard on page 19.
    - The applications dashboard displays data from your Apteligent by VMware environment. Register Apteligent with Workspace ONE Intelligence and add the Apteligent SDK to internal applications to display application statistics for internal applications managed in Workspace ONE UEM. For information, see Apteligent by VMware and Workspace ONE Intelligence on page 20.
- The **Security Risk** dashboard displays data concerning the security of managed devices in your Workspace ONE deployment. See data concerning compromised devices, passcode risk, encryption status, and top risks. For information about the Security Risk dashboard, see Security Risk Dashboard on page 16.
- The **OS Updates** dashboard displays data about versions of operating systems running in your environment. It also reports on application and operating system patches. For information, see OS Updates Dashboard on page 18.

Automation

Automation can increase efficiencies and reduce the burden of manual tasks by acting for you on problems triggered by parameters you configure. With rules that are based on a set of parameters. Create policies that take automated remediation actions based on context. Build contextual policies that fit your unique environment by automating workflows that extend to third-party services with REST APIs.

For information about automation, see Automation for Workspace ONE Intelligence on page 22.

Reports

You can create reports about your Workspace ONE deployment based on your business needs with the reports feature. The feature uses cloud-based report storage to gather data and create the reports. Reports powered by Workspace ONE Intelligence provide access to critical business intelligence data and is different from the reports created in the Workspace ONE UEM console.

For information about reports, see Reports for Workspace ONE Intelligence on page 33.

Chapter 2: 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.

  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

Requirement	Description
Software Requirements	
OS	Windows Server 2012 R2 or later
Java	Java 8
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
Application Authentication	Select one of the following authentication methods. • **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	Select the region for your cloud service. Whitelist the **api.ci.dpa0.org** , **discovery.awmdm.com**, and **artifactrepo.data.vmwservices.com** URLs for all regions. The installer calls these endpoints for a list of all supported regions. 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. 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. Whitelist the URLs depending on your region. • All Regions ◦ api.ci.dpa0.org ◦ artifactrepo.data.vmwservices.com ◦ discovery.awmdm.com • United States (UAT environment) ◦ api.sandbox.data.vmwservices.com ◦ auth.sandbox.data.vmwservices.com ◦ eventproxy.sandbox.data.vmwservices.com ◦ sandbox.data.vmwareservices.com • United States (Production) ◦ api.na1.data.vmwservices.com ◦ auth.na1.data.vmwservices.com ◦ eventproxy.na1.data.vmwservices.com ◦ na1.data.vmwservices.com • Frankfurt ◦ api.eu1.data.vmwservices.com ◦ auth.eu1.data.vmwservices.com ◦ eu1.data.vmwservices.com ◦ eventproxy.eu1.data.vmwservices.com • Ireland ◦ api.eu2.data.vmwservices.com ◦ auth.eu2.data.vmwservices.com ◦ eu2.data.vmwservices.com

Setting	Description
Installation Token	Enter your Workspace ONE UEM Installation Token. 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 documentation to you as part of the on-premises installation process).

Select **Next**.

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

Workspace ONE UEM SaaS Environment Location Mapped to a Workspace ONE Intelligence Region

Your Workspace ONE Intelligence region is assigned based on your Workspace ONE UEM SaaS deployment location. Find your shared and dedicated SaaS Workspace ONE UEM location and see its corresponding Workspace ONE Intelligence region.

For a list of Workspace ONE Intelligence regions, see Install the Workspace ONE Intelligence Connector Service for On-Premises on page 7.

Workspace ONE UEM SaaS Deployment Location	Workspace ONE Intelligence Location
United States	United States (Production)
Canada	United States (Production)
United Kingdom	Ireland
Germany	Frankfurt
Japan	Tokyo
India	Tokyo
Singapore	Tokyo
Australia	Sydney

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.

Chapter 3:
Requirements for Dashboards

To access the data in dashboards powered by Workspace ONE Intelligence, meet the requirements for your type of deployment.

Workspace ONE UEM Console

This feature works with the Workspace ONE UEM console v9.2 and newer.

Reports

Workspace ONE Intelligence uses the data in the reports data warehouse to display analytics from your Workspace ONE deployment. Reports are available in the Workspace ONE UEM console v9.2 and newer.

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 6 and Install the Workspace ONE Intelligence Connector Service for On-Premises on page 7.

SaaS Deployments

Shared SaaS have access to reports. No action is required.

Dedicated SaaS deployments contact their support representative or their SAM to set up Reports and Workspace ONE Intelligence.

On-Premises Deployments

On-premises deployments must install the Workspace ONE Intelligence Connector for communication between the Reports infrastructure and Dashboards.

Note: The Workspace ONE Intelligence Connector is also called the ETL Service.

Admin Roles

Existing admin roles that have permissions for reports, have access to Intelligence roles.

For new admin roles, include permissions for Intelligence so that admins can access settings.

My Dashboard

My Dashboard powered by Workspace ONE Intelligence displays data you customize with applied widgets. Display data as graphics and analyze the trends occurring in areas within your Workspace ONE platform by app, device, or operating system (OS) update. Data in this view are consolidated from other dashboards.

Navigation

Find the dashboard in the Workspace ONE Intelligence console at **Dashboards > My Dashboard**.

Latest Data Snapshot and Historical Data

My Dashboard can represent the latest data in the reports infrastructure. Workspace ONE Intelligence streams data from the database in the cloud so that the analytics you see are a current picture of the state of your Workspace ONE deployment.

It can also display historical data according to a customizable date range to help analyze trends over time.

Available Metrics

Use widgets to display various metrics for your deployment.

Metric	Widget
Asset tracking	iOS Device and OS Breakdown
Security	Compromised Status by OS Version
Application deployment	Most Popular Apps
Windows patches	Security Update Status

Customization

Define the layout of My Dashboard with widgets. Customize the data, as needed, to display the necessary data to solve problems, analyze deployment health, or view trends in use.

- Move widgets anywhere on the dashboard.
- Size widgets.
- Delete widgets.

Configure Widgets for My Dashboard

Configure the data widgets display with filters, charts and diagrams, and parameters. Change widget configurations at any time to view data differently.

For information about accessing the Workspace ONE Intelligence console, see Access Workspace ONE Intelligence on page 10.

Note: Historical data is not available for all widgets.

1. From **My Dashboard**, select **Add Widget**.
2. Select the template type.
3. Select the template and **Next**.
4. Select **Filters** to define the baseline data sets for the widget. Use **Add Filter** and other parameters to define the data you want to see on your dashboard.
5. Configure the **Data Visualization** area.

   To preview visualizations, scroll down the user interface.

Setting	Description
Chart Title	View or edit the titles of the widget.
Snapshot	Represents data in your deployment now.
Measure	• **Count** - Sets the number of rows in a particular data set. The count is the simplest function for verifying results. • **Max** - Returns the largest values in a particular data set. This setting only works with numerical columns. • **Min** - Returns the smallest values in a particular data set. This setting only works with numerical columns. • **Average** - Calculates the average of a selected group of values. This setting only works with numerical columns.
Of Key	Represents the data set you want aggregated by the **Measure** parameter. **Device GUID** is the default setting because it best represents data when the **Measure** is equal to the **Count**.
By Group	Separates data into groups. My Dashboard can display two groupings per data set.
Results per group	Reduces the results displayed. For example, use a value of 10 to show data for a top 10 list of the most installed applications.
Historical	Represents data over time.

Setting	Description
Chart Type	• **Vertical** bar charts compare the number of events that have occurred, such as the type of error that occurs the most in your system. • **Line** charts display data points connected with a line and help compare changes and trends over even time intervals. • **Tables** show multiple data values in rows and columns for a comparison of report data.
Measure	• **Count** - Sets the number of rows in a particular data set. The count is the simplest function for verifying results. • **Distinct Count** - Returns a count of unique or distinct values identified over the data range set. • **Max** - Returns the largest values in a particular data set. This setting only works with numerical columns. • **Min** - Returns the smallest values in a particular data set. This setting only works with numerical columns. • **Average** - Calculates the average of a selected group of values. This setting only works with numerical columns.
Of Key	Represents the data set you want aggregated by the **Measure** parameter. **Device GUID** is the default setting because it best represents data when the **Measure** is equal to the **Count**.
By Group	Separates data into groups. My Dashboard can display two groupings per data set.
Date Range	Sets a range in the past from which to pull and display data.
Results per group	Reduces the results displayed. For example, use a value of 10 to show data for a top 10 list of the most installed applications.

6. **Save** your widget.

   If My Dashboard does not have information to display, it notifies you. However, you can change configurations to see if a different parameter, like **Measure** or **Chart Type**, can display your widget.

Widgets Display Data in My Dashboard

Display your Workspace ONE deployment data with predefined widgets.

You can edit, copy, and add widgets with templates. Use the templates to display customized data for analyzing key performance indicators in your Workspace ONE deployment.

Widget Types

Widgets include but are not limited to the listed types.

Widget Type	Available Template	Description
Apps	Blank	This template is the base for creating a custom widget that displays the exact application data you want to analyze and track.
	Agent Install Status by Version	This template displays applications by name and version and how many times the Agent installed the application.
	Most Popular Apps	This template displays applications by name and listed by most to least installed.
Devices	Blank	This template is the base for creating a custom widget that displays the exact device data you want to analyze and track.
	Total Enrollments	This template displays the total number of enrolled devices at a given date.
	Compromised Status By OS Version	This template displays compromised devices grouped by operating system version.
	iOS Device and OS Breakdown	This template displays the number of iOS devices grouped by operating system version and model.
	Number of Enrollments Today	This template displays the number of newly enrolled devices on the current day.
OS Updates (Windows)	Blank	This template is the base for creating a custom widget that displays the Windows update data you want to analyze and track.
	Windows Devices by OS Version	This template displays the number of Windows devices grouped by operating system version.
	Security Updates Status	This template displays groups of Windows devices that have installed security updates, have not installed security updates (available), or removed security updates.
	Top Ten KB Installs	This template displays Windows Patch KB numbers grouped into the number of devices that installed the patch and ordered from the most installed to least installed.

Security Risk Dashboard

View device security in your Workspace ONE deployment with the Security Risk dashboard.

Navigation

Find the dashboard in the Workspace ONE Intelligence console at **Dashboards > Security Risk**.

Filters

Manipulate the analytics displayed on the dashboard with the filters on the default view.

The initial filter selected controls the available filters that follow. Depending on the risk you want to analyze, select between **Platform**, **OS Version**, and **Device Model** .

Time Filter Selected and Percentages

Select a time period for the data displayed. The time selected affects the percentages displayed beside the risk modules. For example, selecting 14 days sets the percentage to reflect a comparison between now and 14 days ago. A negative percentage indicates that a risk has decreased, and a positive percentage indicates that a risk has increased.

Risk Modules

Risks represented in the Security Risk dashboard include compromised devices, passcode risk, encryption status, and top risks.

- **Compromised Devices** - This module identifies that the Workspace ONE UEM compliance engine has detected a device as compromised. The compliance engine includes a Compromised Status policy for Android, iOS, and Windows Desktop (Windows 10) devices.
- **Passcode Risk** - This module identifies that the Workspace ONE UEM compliance engine has detected that the passcode is disabled on devices. The compliance engine includes a Passcode policy for Android, iOS, and Windows Desktop (Windows 10) devices.
- **Encryption Status** - This module identifies that the Workspace ONE UEM compliance engine has detected that the device is not encrypted. The compliance engine includes either an Encryption or a Laptop Encryption policy for Android, iOS, macOS, and Windows Desktop (Windows 10) devices.

Modules represent risk using a number, a percentage, and an arrow.

- **Number** - The number value corresponds to a risk over the selected time. The number 10 indicates that 10 risks were reported.
- **Percentage** - The percentage compares the risk now to the risk earlier, depending on the time selected. It is positive or negative number that coincides with the arrow. For example, if you selected to filter data by 14 days, and got a percentage of -64% with a downward pointing arrow, your deployment decreased risks by 64% over the last 14 days.
- **Arrow** - The arrow represents a comparison of the risk now to a time earlier, depending on the selected time. It can point up or down depending on the status and it coincides with the percentage. For example, if you selected to view data for the last 30 days and the arrow pointed up and had a positive percentage, your deployment increased risks over the last 30 days.

Top Risks

The top risks module shows a summation of risks that occurred during the time period selected. The number value for the top risks reflects the summation and does not directly correspond with the other modules.

The top risks are composed of the following data points collated from your Workspace ONE UEM environment.

Risk	Description
Non Compliant	Reports that an enrolled device is not compliant with policies.
Not on Latest Security Patch Date	Reports that an enrolled Windows Desktop device is not on the latest security patch.
Activation Lock Disabled	Reports that an enrolled iOS device does not have the activation lock enabled.
iCloud Backup Disabled	Reports that an enrolled iOS device does not have iCloud backup enabled.
BitLocker Disabled	Reports that an enrolled Windows Desktop device does not have BitLocker enabled.

Risk	Description
Code Integrity Disabled	Reports that an enrolled Windows Desktop device does not have code integrity enabled.
Boot Debugging Disabled	Reports that an enrolled Windows Desktop device does not have boot debugging enabled.
Firewall Status	Reports the status of the firewall for an enrolled Windows Desktop device.
Firewall Global Status	Reports the status of the firewall for an enrolled macOS device.
Firmware Password Status	Reports the status of the BIOS password configured in the BIOS payload for Windows Desktop devices.

OS Updates Dashboard

View version data for operating systems (OS) and view patch information for applications and operating systems in your Workspace ONE deployment with the OS Updates dashboard.

OS Updates data helps you know if your environment is fragmented and running older systems or applications. View a module to see how many different versions or patches are running in your deployment.

Navigation

Find the dashboard in the Workspace ONE Intelligence console at **Dashboards > OS Updates**.

OS Updates Modules

Select **ADD OS** to see a list of the systems the dashboard supports. The widgets display the number of operating system versions running on a reported number of devices.

OS-Specific Modules Information

Select **View** in an OS Updates module to get details for that operating system. A module displays current and historical information. You can edit the filters to display particular data for longer or shorter time periods.

Modules	Filters
OS Versions	Some available filters include the listed components. • Model • OS Version
Patches	Some available filters include the listed components. • Windows Patch KB Number • Windows Patch KB Title • Windows Patch Update Classification

Patches Information.

On the **Patches** tab, find data about patch updates for Windows operating systems and applications. You can use filters to find data on patches using a specific knowledge base (KB) number or title. The KB filters are useful when you want to know the status of a specific KB. The default view without edited filters, groups patches by the update status. Use the KB filters and the patch update status to determine the health of your Windows resources.

Status	Descriptions
Approved	The approved patch is successfully assigned to the device.
Assigned	The patch is approved and assigned to the device.
Available	The patch is available on the device for installation.
Failed	The patch failed to install.
Installed	The patch successfully installed.
Pending Installation	The patch installation is approved and available but not yet installed.
Pending Reboot	The patch installation is paused until the device reboots.
Removed	The patch is removed.

Apps Dashboard

Use the Apps dashboard to analyze application use for applications managed in your Workspace ONE UEM environment and accessed through the Workspace ONE catalog.

The dashboard displays data for applications from Workspace ONE UEM and Apteligent by VMware.

Note: Not all information available in Apteligent is available in the Apps dashboard.

Navigation

Find the dashboard in the Workspace ONE Intelligence console at **Dashboards > Apps**.

Adoption and Engagement

The Apps dashboard helps determine if users adopt applications and if they use them. Low adoption has several causes. Is the application unnecessary? Is the application hard to use or does it have bugs?

Whatever the analysis, use the data on the dashboard to prioritize your application resources. Troubleshooting can reveal that the application is not worth the resources required to install and maintain it. Or perhaps, the application needs updating to the next version due to bug fixes.

Supported Applications by System

The Apps dashboard displays data for the listed application types.

System	Supported Application Type
Workspace ONE UEM	Supports all managed applications.
Apteligent	Supports internal applications that include the Apteligent SDK and that are managed through Workspace ONE UEM.

Register Apteligent

Register Apteligent with Workspace ONE Intelligence. Registration authorizes the Apps dashboard to display data for supported applications from those systems.

For information, see Register Apteligent in Settings on page 21.

Available Metrics

View all applications installed, by platform, on the default view of the Apps dashboard.

You can also select a single application using the text box and drop-down menu at the top. Edit the version of the application for which you want data. You can select a time range to filter the amount of data for the application. The dashboard displays the listed deployment information.

Widget	Description
Total Installs	Displays the total number of installations of the application..
Devices Missing App	Displays the number of devices that do not have a specific application installed.
App Install Status Reason	Displays the installation status of the application. Some examples of app install status reasons are installing, failed, pending removal, and managed.
App Version Over Time	Displays the version of the application installed on devices during the selected time period.
Installs Over Time	Displays the number of times the application was installed during the selected time period.

Apteligent by VMware and Workspace ONE Intelligence

Integrate the application and user behavior analysis capabilities of Apteligent by VMware with Workspace ONE Intelligence.

Data from Apteligent displays on the Apps dashboard.

Apteligent by VMware

Apteligent by VMware captures event data from key user flows in applications, including data about screen load numbers, network events, and incidents reports. It tracks key metrics, helps to improve applications release-over-release, and focuses on problems that are relevant to users. Use numerous data points about the mobile infrastructure to benchmark applications and to make data-driven decisions.

Note: Not all information available in Apteligent is available in the Apps dashboard.

Apteligent Developer Resources

To connect Workspace ONE Intelligence and Apteligent data systems, add the App ID number created by Workspace ONE Intelligence to the internal application using the Apteligent software development kit (SDK).

Find the Apteligent SDK and applicable documentation in the **Developer Resources** section found at https://code.vmware.com/web/apteligent.

Supported Applications and Management Status

Workspace ONE Intelligence supports internal applications for the Android and iOS platforms for this connection. Workspace ONE UEM must manage these internal applications for this connection to work.

Register Apteligent in Settings

Register Apteligent with Workspace ONE Intelligence to include data concerning internal application engagement in the Apps dashboard.

Registration Procedure

To display Apteligent data in the Apps dashboard in the Workspace ONE Intelligence console, add applications and hook the Apteligent SDK into those applications.

1. In the Workspace ONE UEM console, upload and deploy, as managed, internal applications. This action makes the applications accessible in the Workspace ONE Intelligence console.
2. In the Workspace ONE Intelligence console, go to **Settings > Apteligent > Set Up > Get Started**.

   In a deployment with Apteligent already registered, select to **View** Apteligent and select **Add Application**.
3. In the **Select Mobile Applications** area, select or add the internal applications you want to analyze and display in the Apps dashboard.

   Workspace ONE Intelligence assigns an **App ID** to the application. Have the application developer add this App ID to the application.

   You can copy or email instructions for adding the App ID and the Apteligent SDK. Find Apteligent developer resources at https://code.vmware.com/web/apteligent.
4. If you do not want the system to send application data to data centers in the United States, select **Opt out of US data center**.
5. Add the Apteligent SDK with the App Id to applications.

   This process varies. For example, an admin creates a ticket requesting a developer to add the Apteligent SDK and the Workspace ONE Intelligence App ID to the application.
6. In the Workspace ONE UEM console, upload and deploy the internal application that now has the Apteligent SDK and Workspace ONE Intelligence App ID.

To capture application data, the application must be installed and used on devices. Workspace ONE Intelligence displays the data on the Apps Dashboard.

For information about the Apps Dashboard, see Apps Dashboard on page 19.

Chapter 4:
Automation for Workspace ONE Intelligence

The automation capabilities in Workspace ONE Intelligence use numerous parameters that trigger a workflow. You can customize the workflow to act on unique scenarios in your Workspace ONE environment. Automation is a robust feature but it is not intended to replace compliance policies.

Workflows

Automation uses workflows. A workflow consists of triggers caused by a state change or trend that cause the engine to use a set action through Workspace ONE or an integrated third-party service. You can create your own workflows or you can use preset workflow templates.

Workflows monitor immediate state changes. Configure triggers in workflows to recognize the state change that represents what you want remedied.

Note: Workflows monitor data from the time you configure them. They do not analyze historical data.

Automation and Compliance Policies

Automation offers many actions that help solve problems related to compliance, however, the compliance engine still serves an important purpose.

- **Automation** - Its decision engine acts on triggers from devices to automate actions across the digital workspace environment. You can extend the decision engine to third-party services.

  Use the automation feature in device-category scenarios that encompass various facets of your Workspace ONE deployment.

- **Compliance** - Its engine acts on closed-loop workflows where a user can have resources returned after becoming compliant again.

  Use compliance in scenarios focused on remediation and device state. Use it to force devices to comply with mandated security policies. Remove resources until devices comply with set compliance rules that return them to a working state.

Requirements for Automation

To use the automation features in your Workspace ONE Intelligence environment, install the reports service and connect to the VMware Workspace ONE UEM API server.

Workspace ONE UEM Console

This feature works with the Workspace ONE UEM console v9.2 and newer.

Reports

Workspace ONE Intelligence uses the data in the reports data warehouse to display analytics from your Workspace ONE deployment. Reports are available in the Workspace ONE UEM console v9.2 and newer.

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 6 and Install the Workspace ONE Intelligence Connector Service for On-Premises on page 7.

SaaS Deployments

Shared SaaS have access to reports. No action is required.

Dedicated SaaS deployments contact their support representative or their SAM to set up Reports and Workspace ONE Intelligence.

On-Premises Deployments

On-premises deployments must install the Workspace ONE Intelligence Connector for communication between the Reports infrastructure and Dashboards.

> **Note:** The Workspace ONE Intelligence Connector is also called the ETL Service.

Admin Roles

Existing admin roles that have permissions for reports, have access to Intelligence roles.

For new admin roles, include permissions for Intelligence so that admins can access settings.

Requirements to Connect to the API Server and to Use APIs for Communication

- Create an AirWatch Administrator account for the specific purpose of working with the automation feature. To use APIs, grant the admin account permissions.

- Configure the admin account to use the **Basic Authentication** for API communications because Directory accounts do not work. Find the API authentication items on the **API** tab in the **Add** or **Edit Admin** area.
- Configure Automation Connections. For details, see Automation Connections, API Communications, and Third-Party Connections on page 24.

Automation Connections, API Communications, and Third-Party Connections

The automation feature of Workspace ONE Intelligence uses APIs to communicate between your Workspace ONE environment, Workspace ONE Intelligence automation feature, and your third-party services.

To add connections to supported services, follow these general steps. If you do not follow all these steps, automation does not work.

1. Review the requirements for automation outlined in Requirements for Automation on page 23.
2. Create and use an AirWatch Administrator account specific for automation with API permissions.
3. Connect to the VMware Workspace ONE UEM API server. For details, see Configure API Communication for Automation on page 24.
4. Configure connections in the third-party services. For details, see Configure Connections in Supported Third-Party Services on page 25.
5. Enter the API authentication credentials to Workspace ONE Intelligence. For details, see Configure Automation Connections on page 26.

Configure API Communication for Automation

Workspace ONE Intelligence communicates with third-party services with APIs. To permit Workspace ONE to use APIs for automation, generate an API key in the Workspace ONE UEM console.

Procedural Tasks

For a list of all the steps available to configure automation, see Automation Connections, API Communications, and Third-Party Connections on page 24.

API Communication Task

1. Select the organization group where you want to connect to third-party services.
2. In the Workspace ONE UEM console, go to **Groups & Settings > All Settings > System > Advanced > API > REST API**.

3. Configure the settings on the **General** tab.

Setting	Description
Enable API Access	Permits you to generate an API key for the service.
Add	Select **Add** to generate an **API Key**. Record this value and enter it in the Intelligence environment as the **AirWatch Tenant Code**.
Service	Enter a descriptive name for the service, such as Automation.
Account Type	Select **Admin**.

4. Configure the settings on the **Authentication** tab.

Setting	Description
Basic	Select **Basic** authentication.
Certificates	Not applicable.
Directory	Not applicable.

Next Steps

Configure connections in the third-party services. For details, see Configure Connections in Supported Third-Party Services on page 25.

Configure Connections in Supported Third-Party Services

Connect supported services to the Workspace ONE Intelligence automation feature.

Disclaimer: These instructions intend to help configure services. However, find the most current documentation for services at their documentation sites.

Procedural Tasks

For a list of all the steps available to configure automation, see Automation Connections, API Communications, and Third-Party Connections on page 24.

Supported Services

Slack

In Slack Help, search for **Incoming WebHooks**.

Configure an Incoming Webhook Integration so that you can connect to the Slack API and send messages. Integration includes these general steps.

1. Define a default channel for messages.

   You can override this channel when you create a message.

2. Enter the WebHook URL into the connection settings.

ServiceNow

Follow the steps in the article **REST API roles**, at https://docs.servicenow.com/bundle/kingston-application-development/page/integrate/inbound-rest/reference/r_RESTAPIRoles.html as of March 5, 2018.

1. Add the **snc_platform_rest_api_access** role to the ServiceNow account. This API controls the Table API for Inbound REST operations.
2. Provide authentication credentials to Workspace ONE Intelligence. Enter `https://instance.service-now.com` for the **Base URL**.

Next Steps

Add credentials from third-party services to Workspace ONE Intelligence. See Configure Automation Connections on page 26.

Configure Automation Connections

Enter API Communication Credentials in Workspace ONE Intelligence so that it can communicate with third-party services for the automation feature.

Procedural Tasks

For a list of all the steps available to configure automation, see Automation Connections, API Communications, and Third-Party Connections on page 24.

Connections Procedure

1. Access the Workspace ONE Intelligence UI.
2. Navigate to **Settings > Automation Connections**.
3. Select **Authorize** for the **Workspace ONE UEM API** process.
4. Select **Provide Credentials** and configure the settings.

Setting	Description
Base URL	Enter the URL for your VMware Workspace ONE UEM server.
API User Name	Enter the user name for the specific admin you created for automation.
API User Password	Enter the password for the admin.
Workspace ONE UEM Tenant Code	Enter the API key that the Workspace ONE UEM console generated when you enabled REST API communications.

Related Topics

For information about configuring Workflows for automation, see Configure Workflows on page 27.

For information on setting up third party services, such as Slack and ServiceNow, see Configure Connections in Supported Third-Party Services on page 25.

For information on enabling API communications, see Configure API Communication for Automation on page 24.

For information about the prerequisites needed to set up automation, see Requirements for Automation on page 23.

Configure Workflows

Workflows monitor for state changes. Configure triggers in workflows to recognize the state change that represents what you want remedied.

Use an existing workflow or create a unique workflow. To add a customized workflow, follow the procedure.

For information about accessing the Workspace ONE Intelligence console, see Access Workspace ONE Intelligence on page 10.

For information on the available actions for Workspace ONE UEM, see Workspace ONE UEM Actions on page 28.

1. In the Workspace ONE Intelligence console, navigate to **Automation** > **Add Automation**.
2. Select Create a custom automation.
3. In the **Add Automation** procedure, configure the settings.

Setting	Description
Name	Enter a title for the automation.
Trigger	Create a **When** statement that the automation engine monitors for a state change. Add triggers depending on how complex or detailed the scenario.
Filter	Create an **If** statement to refine the trigger the engine monitors for a state change.
Action	Create a **Then** statement that the automation engine does when it identifies the If or trigger. For native actions, select Workspace ONE UEM API. If you use a third-party service, configure it to carry out the action.
Workspace ONE UEM API	
Workspace ONE UEM API	Select an action for Workspace ONE UEM to perform.
Slack API	
Send Channel Message	• **User Name** - Enter a user name that this message posts from. Messages post as "Workspace ONE Intelligence" by default. • **Icon Emoji** - (Optional) Change the icon the system uses for messages. • **Icon URL** - (Optional) Change the URL the system uses for messages. • **Channel** - Enter a name for the channel as it appears in the channel list. If you leave this blank, the system uses the default channel you configured in Slack. • **Text** - Enter the message. This text box supports dynamic values.
ServiceNow API	
Create Incident	Submits a new incident into the ServiceNow system. • **Short Description** - Enter a description of the incident. • **Comment** - Add relevant information that helps put the incident into context.
Delete Incident	**Sys ID** - Enter the unique identifier the ServiceNow system assigned to the incident.

4. If you use a third-party service for actions, authorize them to act.
   a. Select **Authorize** to permit Slack to perform actions.
   b. Select **Connection Permissions** and review them.
   c. Select **Provide Credentials**.

Connection	Setting
Slack	**Slack Webhook URL** - Enter the Webhook you configured in Slack.
ServiceNow	**Base URL** - Enter `https://instance.service-now.com` . **API User Name** - Enter the user name you configured in ServiceNow. **API User Password** - Enter the password for the user name.

5. Save the automation.

Workspace ONE UEM Actions

To configure a workflow for automation, you can select a supported Workspace ONE UEM action.

For information on connecting third-party services and Workspace ONE Intelligence, see Configure Connections in Supported Third-Party Services on page 25.

Important: The **Full Device Wipe** action returns a device to factory defaults and removes all corporate and personal data off the device.

Action	Description
Approve Patch	Approves an individual Windows patch for installation. Enter the title or the knowledge base number of the patch. You can enter the Revision ID of the patch.
Change Device Organization Group	Moves an enrolled device to another organization group. Consider the resource assignments the device loses and gains after it moves from its original group to the new group. For instructions on how to get the organization group ID number, see Find the ID Number of Organization Groups on page 31.
Clear Passcode	Removes a passcode requirement off a device so that a user can authenticate without it. Anyone can use this device after you automate this action.
Create Tag	Creates a tag in the selected organization group in the Workspace ONE UEM console. For instructions on how to get the tag ID number, see Find the ID Number of Tags on page 32.
Custom Apple MDM Command	Runs a custom command according to the entered command payload on iOS, tvOS, and macOS devices. Enter a valid PLIST for the MDM command.
Data Roaming	Admits or prevents the configuration of data roaming settings on iOS devices.

Action	Description
Delete ServiceNow Ticket	Deletes a ticket from the ServiceNow system. For this action to work, you must connect Workspace ONE Intelligence and ServiceNow.
Delete Tag	Deletes a tag from the selected organization group in the Workspace ONE UEM console. For instructions on how to get the tag ID number, see Find the ID Number of Tags on page 32.
Full Device Wipe	Performs a factory reset that removes everything from the device, which includes personal data.
Install Internal Application	Installs an internal application on a device that is uploaded and managed in Workspace ONE UEM. For instructions on how to get an application ID for internal and public applications, see Find the ID Number of Internal and Public Applications on page 30.
Install Profile	Installs a Workspace ONE UEM profile to a device. For instructions on how to get the profile ID, see Find the ID Number of Profiles on page 31.
Install Public Application	Installs a public application on a device that is uploaded and managed in Workspace ONE UEM. For instructions on how to get an application ID for internal and public applications, see Find the ID Number of Internal and Public Applications on page 30.
Install Purchased Application	Installs a purchased application on a device that is uploaded and managed in Workspace ONE UEM. For instructions on how to get an application ID for purchased applications, see Find the ID Number of Purchased Applications on page 31.
Lock Device	Forces a device to return to its lock screen.
Personal Hotspot	Admits or prevents the configuration of personal hotspot settings on iOS devices.
Query Device	Requests updated data from a device.
Remove Internal Application	Removes an internal application on a device that is uploaded and managed in Workspace ONE UEM. For instructions on how to get an application ID for internal and public applications, see Find the ID Number of Internal and Public Applications on page 30.
Remove Profile	Removes a Workspace ONE UEM profile off a device. For instructions on how to get the profile ID, see Find the ID Number of Profiles on page 31.
Remove Public Application	Removes a public application on a device that is uploaded and managed in Workspace ONE UEM. For instructions on how to get an application ID for internal and public applications, see Find the ID Number of Internal and Public Applications on page 30.
Remove Purchased Application	Removes a public application on a device that is uploaded and managed in Workspace ONE UEM. For instructions on how to get an application ID for purchased applications, see Find the ID Number of Purchased Applications on page 31.

Action	Description
Schedule OS Update	Schedules an OS update and forces an iOS device that is supervised and on 10.3+ (depending on configurations) to update to the latest OS version. • **DownloadOnly** - Configure the action to download only the update to make it available for installation. • **InstallASAP** - Installs the downloaded OS update. This action only works if the OS update is downloaded to the device.
Send Email	Sends an email to a user with the SMTP server configured in the Workspace ONE UEM environment.
Send Push Notification	Sends a push notification to a managed application, either the AirWatch Agent or VMware Content Locker.
Send SMS	Sends a notification to a device with the SMS gateway configured in the Workspace ONE UEM environment.
Stop AirPlay	Stops an AirPlay session on iOS devices.
Sync Device	Evaluates applications currently installed on a device and compares that state to the required applications configured in the Workspace ONE UEM console. The action prompts an installation command for any required applications that are missing from the device.
Voice Roaming	Admits or prevents the configuration of voice roaming settings on iOS devices.

Find the ID Number of Internal and Public Applications

You need the ID number of internal and public applications in the Workspace ONE UEM console to configure Workspace ONE UEM actions for workflows.

The ID number of the application is a number the Workspace ONE UEM system assigns to the application. It is different than the Application ID.

Note: This procedure uses Google Chrome as the browser. Steps vary depending on the browser used to access the Workspace ONE UEM console.

To get the application ID, go to the application record.

1. In the Workspace ONE UEM console, select the applicable organization group.
2. Go to **Apps & Books > Applications > Native**.
3. Select the **Internal** or **Public** tab depending on the type of application.
4. Select the application to see the **Details View**.
5. Find the ID number located in the middle of the string. An example of the string is:

`https://<Workspace_ONE_UEM>/AirWatch/#/AirWatch/Apps/Details/Internal/`**`246`**`/Summary?isDependencyFile=False`.

The **246** in the middle of the string is the ID number of the application.

Find the ID Number of Organization Groups

You need the ID number of the organization group to which you want to move the device in the Workspace ONE UEM console to configure the **Change Device Organization Group** action.

Note: This procedure uses Google Chrome as the browser. Steps vary depending on the browser used to access the Workspace ONE UEM console.

To get the ID number, follow these steps.

1. In the Workspace ONE UEM console, select the applicable organization group.
2. Go to **Groups & Settings > Groups > Organization Groups > Details**.
3. Find the ID number at the end of the URL string in the browser. An example of the string is:
   `https://<Workspace_ONE_UEM>/AirWatch/#/AirWatch/OrganizationGroup/Details/Index/`**`859`**.
   The **859** at the end of the string is the organization group ID.

Find the ID Number of Profiles

You need the ID number of the profile in the Workspace ONE UEM console to configure Workspace ONE UEM actions for workflows.

Note: This procedure uses Google Chrome as the browser. Steps vary depending on the browser used to access the Workspace ONE UEM console.

To get the ID number, follow these steps.

1. In the Workspace ONE UEM console, select the applicable organization group.
2. Go to **Devices > Profiles & Resources > Profiles**.
3. Point to the applicable profile in the **Profiles List View** to display the item's URL in the bottom left of the browser.
4. Find the ID number located in the middle of the string. An example of the string is:
   `https://<Workspace_ONE_UEM>/AirWatch/Profiles/DeviceProfileEdit/`**`85`**`?isReadOnlyProfileView=x`.
   The **85** in the middle of the string is the profile ID.

Find the ID Number of Purchased Applications

You need the ID of the purchased application in the Workspace ONE UEM console to configure Workspace ONE UEM actions for workflows.

The ID number of the application is a number the Workspace ONE UEM system assigns to the application. It is different than the Application ID.

Note: This procedure uses Google Chrome as the browser. Steps vary depending on the browser used to access the Workspace ONE UEM console.

To get the ID number, follow these steps.

1. In the Workspace ONE UEM console, select the applicable organization group.
2. Go to **Apps & Books > Applications > Native > Purchased**.
3. Point to the application in the **List View** to display the item's URL in the bottom left of the browser.
4. Find the ID number at the end of the string. An example of the string is:

   `https://<Workspace_ONE_UEM>/AirWatch/Orders/EditAssignment?AppLicensePollId=0&VppLicenseCountId=2448&ApplicationId=9193`.

   The **9193** at the end of the string is the ID of the application.

Find the ID Number of Tags

You need the ID number of the tag from the Workspace ONE UEM console to configure tag-related actions for workflows.

Note: This procedure uses Google Chrome as the browser. Steps vary depending on the browser used to access the Workspace ONE UEM console.

To get the ID number, follow these steps.

1. In the Workspace ONE UEM console, select the applicable organization group.
2. Go to **Groups & Settings > All Settings > Devices & Users > Advanced >Tags**.
3. Point to the applicable profile tag in the **Tags List View** to display the item's URL in the bottom left of the browser.
4. Find the ID number at the end of the string. An example of the string is:

   `https://<Workspace_ONE_UEM>/AirWatch/Tags/Actions/View/10028`.

   The **10028** at the end of the string is the tag ID.

Chapter 5:
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 6 and Install the Workspace ONE Intelligence Connector Service for On-Premises on page 7.

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 34.

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 56

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	
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 AirWatch Agent app details on your iOS and Android devices.
Device Templates	
Device Starter Template	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	
OS Updates Starter Template	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 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
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 name and a description for the report.
10. Select **Run 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.

Reports Filters for Apps

Reports use filters to create the report on specific areas of your Workspace ONE UEM deployment. These filters use a specific logic to determine what information to include in the report.

The available filters and their operators are outlined in the following table. The blank templates list filters in alphabetical order.

Filter	Operator
Active	Equals
App Created Date	Before, After, Between, Not Between
App First Seen	Before, After, Between, Not Between
App Install Status	Equals
App Last Seen	Before, After, Between, Not Between

Filter	Operator
App Name	Includes, Does Not Include, Equals, Starts With
App Version	Includes, Does Not Include, Equals, Starts With
Beta	Equals
Bundle Size	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Compliance Status	Includes, Does Not Include, Equals, Starts With
Compromised	Equals
Cost	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Cost Center	Includes, Does Not Include, Equals, Starts With
Created By User	Includes, Does Not Include, Equals, Starts With
Currency Description	Includes, Does Not Include, Equals, Starts With

Filter	Operator
Customer Organization Group ID	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Description	Includes, Does Not Include, Equals, Starts With
Developer	Includes, Does Not Include, Equals, Starts With
Developer Email	Includes, Does Not Include, Equals, Starts With
Developer Phone Number	Includes, Does Not Include, Equals, Starts With
Device GUID	Includes, Does Not Include, Equals, Starts With
Device ID	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Device Last Seen	Before, After, Between, Not Between
Device Name	Includes, Does Not Include, Equals, Starts With
Device Organization Group GUID	Includes, Does Not Include, Equals, Starts With
Device UDID	Includes, Does Not Include, Equals, Starts With

Filter	Operator
Dynamic Size	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Email	Includes, Does Not Include, Equals, Starts With
Enrollment Date	Before, After, Between, Not Between
Enrollment Status	Includes, Does Not Include, Equals, Starts With
First Name	Includes, Does Not Include, Equals, Starts With
Friendly Name	Includes, Does Not Include, Equals, Starts With
Identifier	Includes, Does Not Include, Equals, Starts With
Installation Date	Before, After, Between, Not Between
Installation Status Reason	Includes, Does Not Include, Equals, Starts With
Last Name	Includes, Does Not Include, Equals, Starts With
Launcher Active	Equals
Managed [Device]	Equals
Managed App	Equals
Managed App Status	Includes, Does Not Include, Equals, Starts With
Managed By	Includes, Does Not Include, Equals, Starts With
Middle Name	Includes, Does Not Include, Equals, Starts With
Model	Includes, Does Not Include, Equals, Starts With
Modification Date	Before, After, Between, Not Between
Modified By User	Includes, Does Not Include, Equals, Starts With

Filter	Operator
OS Version	Includes, Does Not Include, Equals, Starts With
OS Version Build	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
OS Version Major	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
OS Version Minor	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Organization Group GUID	Includes, Does Not Include, Equals, Starts With

Filter	Operator
Organization Group Hierarchy	• Contains All Of • Contains Any Of • Contains None Of • Contains
Ownership	Includes, Does Not Include, Equals, Starts With
Phone Number	Includes, Does Not Include, Equals, Starts With
Platform	Includes, Does Not Include, Equals, Starts With
Prevent Backup	Equals
Push Mode	Includes, Does Not Include, Equals, Starts With
Remove App On Unenrollment	Equals
Serial Number	Includes, Does Not Include, Equals, Starts With
Support Email	Includes, Does Not Include, Equals, Starts With
Support Number	Includes, Does Not Include, Equals, Starts With
Support URL	Includes, Does Not Include, Equals, Starts With
Type	Includes, Does Not Include, Equals, Starts With
Un-Enrollment Date	Before, After, Between, Not Between
User Domain	Includes, Does Not Include, Equals, Starts With
User GUID	Includes, Does Not Include, Equals, Starts With
Username	Includes, Does Not Include, Equals, Starts With

Filter	Operator
Version Code	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between

Reports Filters for Devices

The available devices filters and their operators are outlined in the following table. The blank templates list filters in alphabetical order.

Filter	Operator
AC Line Status	Includes, Does Not Include, Equals, Starts With
Activation Lock Enabled	Equals
Android Battery Health	Includes, Does Not Include, Equals, Starts With
Antivirus Status	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Asset Number	Includes, Does Not Include, Equals, Starts With

Filter	Operator
Autoupdate Status	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Available Capacity	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Available Physical Memory	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
BIOS Version	Includes, Does Not Include, Equals, Starts With

Filter	Operator
Battery Percent	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
BitLocker Status	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Boot App Security Version Update	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Boot Debugging Enabled	Equals

Filter	Operator
Boot Manager Rev List Version	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
CPU Virtualization	Equals
Capacity	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Cellular Technology	Includes, Does Not Include, Equals, Starts With
Cloud Backup Enabled	Equals
Code Integrity Enabled	Equals
Compliance Status	Includes, Does Not Include, Equals, Starts With
Compromised	Equals
Country	Includes, Does Not Include, Equals, Starts With
Current Carrier	Includes, Does Not Include, Equals, Starts With
Data Roaming Enabled	Equals

Filter	Operator
Dell Battery Health	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Description	Includes, Does Not Include, Equals, Starts With
Design Capacity	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Device GUID	Includes, Does Not Include, Equals, Starts With
Device ID	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Device Name	Includes, Does Not Include, Equals, Starts With
Device Organization Group GUID	Includes, Does Not Include, Equals, Starts With
Device UDID	Includes, Does Not Include, Equals, Starts With

Filter	Operator
Display Name	Includes, Does Not Include, Equals, Starts With
EAS Identifier	Includes, Does Not Include, Equals, Starts With
Email	Includes, Does Not Include, Equals, Starts With
Encryption Status	Equals
Enrollment Date	Before, After, Between, Not Between
Enrollment Status	Includes, Does Not Include, Equals, Starts With
Enterprise Version Description	Includes, Does Not Include, Equals, Starts With
Firewall Global State Status	Equals
Firewall Status	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Firmware Password Status	Equals
First Name	Includes, Does Not Include, Equals, Starts With
Friendly Name	Includes, Does Not Include, Equals, Starts With
Full Charge Capacity	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between

Filter	Operator
GPS Latitude	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
GPS Longitude	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Home Carrier	Includes, Does Not Include, Equals, Starts With
IMEI	Includes, Does Not Include, Equals, Starts With
IP Address	Includes, Does Not Include, Equals, Starts With
Interrogator Data	Equals
Last Cloud Backup	Before, After, Between, Not Between
Last Compliance Check	Before, After, Between, Not Between
Last Name	Includes, Does Not Include, Equals, Starts With
Last Seen	Before, After, Between, Not Between
Lost Mode Enabled	Equals

Filter	Operator
MAC Address	Includes, Does Not Include, Equals, Starts With
Managed	Equals
Managed By	Includes, Does Not Include, Equals, Starts With
Manufacturer Name	Includes, Does Not Include, Equals, Starts With
Middle Name	Includes, Does Not Include, Equals, Starts With
Model	Includes, Does Not Include, Equals, Starts With
Next Compliance Check	Before, After, Between, Not Between
OS Version	Includes, Does Not Include, Equals, Starts With
OS Version Build	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
OS Version Major	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between

Filter	Operator
OS Version Minor	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Organization Group GUID	Includes, Does Not Include, Equals, Starts With
Organization Group Hierarchy	• Contains All Of • Contains Any Of • Contains None Of • Contains
Organization Group ID	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Ownership	Includes, Does Not Include, Equals, Starts With
Passcode Compliant	Equals
Passcode Compliant with Profiles	Equals
Passcode Present	Equals
Personal Hotspot Enabled	Equals
Phone Number	Includes, Does Not Include, Equals, Starts With
Platform	Includes, Does Not Include, Equals, Starts With

Filter	Operator
Recovery Key Value	Includes, Does Not Include, Equals, Starts With
Reset Count	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Restart Count	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Roaming	Equals
SIM Card ID	Includes, Does Not Include, Equals, Starts With
SIM Sequence Number	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between

Filter	Operator
Safe Mode Enabled	Equals
Secure Boot Enabled	Equals
Security Patch Date	Before, After, Between, Not Between
Serial Number	Includes, Does Not Include, Equals, Starts With
Shared	Equals
Supervised	Equals
Supports Offline Geofencing	Equals
TPM Chip	Equals
Time Machine Backup	Before, After, Between, Not Between
Time Machine Backup Status	Equals
Total Physical Memory	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Trusted Execution	Equals
Unenrollment Date	Before, After, Between, Not Between
User GUID	Includes, Does Not Include, Equals, Starts With
Username	Includes, Does Not Include, Equals, Starts With
Virtual Secure Mode Status	Equals
Virtualization I/O	Equals
Voice Roaming Enabled	Equals

Filter	Operator
Zebra Battery Charge Cycle Count	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Zebra Battery Health	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Zebra Battery Manufacture Date	Includes, Does Not Include, Equals, Starts With
Zebra Battery Part Number	Includes, Does Not Include, Equals, Starts With
Zebra Battery Serial Number	Includes, Does Not Include, Equals, Starts With

Reports Filters for OS Updates

The available OS updates filters and their operators are outlined in the following table. The blank templates list filters in alphabetical order.

Filter	Operator
Device GUID	Includes, Does Not Include, Equals, Starts With

Filter	Operator
Device ID	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Device Name	Includes, Does Not Include, Equals, Starts With
Device UDID	Includes, Does Not Include, Equals, Starts With
Email	Includes, Does Not Include, Equals, Starts With
Enrollment Date	Before, After, Between, Not Between
Enrollment Status	Includes, Does Not Include, Equals, Starts With
Friendly Name	Includes, Does Not Include, Equals, Starts With
Last Seen	Before, After, Between, Not Between
Manufacturer Name	Includes, Does Not Include, Equals, Starts With
Model	Includes, Does Not Include, Equals, Starts With
OS Version	Includes, Does Not Include, Equals, Starts With
Organization Group GUID	Includes, Does Not Include, Equals, Starts With
Organization Group Hierarchy	• Contains All Of • Contains Any Of • Contains None Of • Contains

Filter	Operator
Organization Group ID	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Un-Enrollment Date	Before, After, Between, Not Between
User GUID	Includes, Does Not Include, Equals, Starts With
Username	Includes, Does Not Include, Equals, Starts With
Windows Patch Approval Status	Includes, Does Not Include, Equals, Starts With
Windows Patch Assignment Status	Includes, Does Not Include, Equals, Starts With
Windows Patch KB Description	Includes, Does Not Include, Equals, Starts With
Windows Patch KB Number	Includes, Does Not Include, Equals, Starts With
Windows Patch KB Title	Includes, Does Not Include, Equals, Starts With
Windows Patch Revision ID	• Equals • Not Equal To • Less Than • Less Than or Equal To • Greater Than • Greater Than or Equal To • Between • Not Between
Windows Patch Update Classification	Includes, Does Not Include, Equals, Starts With
Windows Patch Update ID	Includes, Does Not Include, Equals, Starts With
Windows Patch Update Status	Includes, Does Not Include, Equals, Starts With
Windows Patch Update Type	Includes, Does Not Include, Equals, Starts With

Reports Sync Status

See the current status of importing your data into the cloud service and the status on your Workspace ONE Intelligence Connector server (also known as ETL installer).

Data Import

The Data Import status chart displays the status on syncing and importing data from the Workspace ONE UEM console.

Status	Description
Percentage of devices imported	Displays the percent of your devices imported into the cloud service. If the percentage is less than 90%, a warning symbol displays. This warning indicates your reports do not cover all your devices.
Percentage of apps imported	Displays the percent of your applications imported into the cloud service.
Last device category sync	This status reports the last time the cloud service synced with the Workspace ONE UEM console to update device data.
Last app category sync	This status reports the last time the cloud service synced with the Workspace ONE UEM console to update app data.

Workspace ONE Intelligence Connector Service

The Workspace ONE Intelligence Connector Service (formerly the ETL Service) status chart displays status information on the service that collects information from your Workspace ONE UEM console and pushes it to the cloud service.

Status	Description
Last check-in time	Displays the last time the Workspace ONE Intelligence Connector Service checked in with the cloud service. If the service fails to check in for 3 consecutive check-in intervals, an alarm displays.
Current service version	Displays the current version of the Workspace ONE Intelligence Connector Service installed on the server. A warning displays if the current service is not the most recent version 24 hours after a new version releases.
Last service restart time	Reports the last time the Workspace ONE Intelligence Connector Service was restarted.
Last service upgrade time	Reports the last time the Workspace ONE Intelligence Connector Service was upgraded.

Workspace ONE Intelligence Connector Server

The Workspace ONE Intelligence Connector Server (formerly the ETS Server) status chart displays status information on the health of the server.

Status	Description
Total memory	Displays the total memory on the server.

Status	Description
Available memory	Displays the available memory on the server. If the available memory is less than 20% of the total, a warning displays.
Total disk	Displays the total disk space on the server.
Available disk	Displays the available disk space on the server. If the available space is less than 20% of the total, a warning displays.
JRE Version	Displays the Java Runtime Environment (JRE) version installed on the server. If the current version is not an approved version, a warning displays.

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.
- **Send**- Sends the report to another Workspace ONE UEM administrator. 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

- Send
- Schedule
- 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.

Setting	Description
Schedule Name	Enter a name for the schedule.
Recurrence	Select from the drop-down menu the frequency the report runs. • Hourly • Daily • Weekly • Monthly The **Recurrence** value affects the available time settings.
	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	Set the day of the month and the time of day you want the report to run. This setting displays when **Recurrence** is set to **Monthly**.
Starts At	Select the time of day the report runs.
	All Recurrence Settings
Ends	If you want to stop the recurrence of a report, set the end date.

Setting	Description
Send To	Enter each recipient email address.
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 **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