

Legacy Analytics

VMware Workspace ONE UEM 1903



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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

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

Contents

- 1** Introduction to Analytics 4
- 2** Event Logs 5
 - Use Console Events 5
 - Use Device Event Log 6
- 3** Syslog Integration 8
 - Configure Syslog 9
 - Admin Scheduler Tasks 10
 - Configure the Scheduler Syslog Task 13
- 4** AirWatch DataMart 14
 - DataMart Requirements 14
 - Install DataMart 15
 - DataMart Tables 19
 - DataMart Entity Relationship Diagram 23

Introduction to Analytics

AirWatch Analytics provides detailed feedback on your AirWatch deployment. Use the analytics tools to review how you use AirWatch to manage your devices and applications.

Analytics Basics

Two components provide the information necessary to access the health of your AirWatch solution. The event logs list each admin and device action taken in the AirWatch Console. AirWatch DataMart provides scheduled exports of data for analysis.

You can also integrate and Security Information and Event Management (SIEM) tools into your AirWatch solution using the AirWatch Syslog settings.

Event Logs

The event logs provide records of administrative and device actions that the AirWatch Console stores in logs. Export event logs as CSV files or configure the AirWatch Console to send event logs to your Security Information and Event Management tools or Business Intelligence systems.

Syslog Integration

Security Information and Event Management (SIEM) technology gathers information about security alerts generated by network hardware and software components. It centralizes this data and generates reports to help you monitor activity, perform log audits, and respond to incidents. Workspace ONE UEM integrates with your SIEM tools by sending event logs using Syslog.

AirWatch DataMart

AirWatch DataMart that enables scheduled automatic data exports from the AirWatch database for statistical analysis and reporting. To use the tool, load DataMart on the server hosting the AirWatch database or in a separate network location. Successful installation creates two SQL Server Agent jobs on the server.

Event Logs

Events are records of administrative and device actions that the AirWatch Console stores in logs. Export event logs as CSV files. You can also configure the AirWatch Console to send the event logs to your Security Information and Event Management tools or Business Intelligence systems.

The event logs show both device events and AirWatch Console events. Device events show the commands sent from the AirWatch Console to devices, device responses, and device user actions. The AirWatch Console events show actions taken from the AirWatch Console including login sessions, failed login attempts, admin actions, system settings changes, and user preferences.

You can filter the severity level, category, or module. Severity levels include:

- **Critical** – Indicates a failure in a primary AirWatch Console system.
- **Error** – Indicates a failure in a non-primary AirWatch Console system.
- **Warning** – Indicates a possible issue in the future.
- **Notice** – Indicates unusual conditions.
- **Information** – Indicates normal operational data.
- **Debug** – Indicates useful information for troubleshooting.

This chapter includes the following topics:

- [Use Console Events](#)
- [Use Device Event Log](#)

Use Console Events

Console events show MDM actions from the AirWatch Console that include the following examples. Login sessions, Failed login attempts, Admin actions, System settings changes, and User preferences.

Severity levels include the following descriptions.

- **Critical** – Indicates a failure in a primary AirWatch Console system.
- **Error** – Indicates a failure in a non-primary AirWatch Console system.
- **Warning** – Indicates an issue in the future if action is not taken.
- **Notice** – Indicates unusual conditions.

- **Information** – Indicates normal operational data.
- **Debug** – Indicates useful information for troubleshooting.

Procedure

- 1 Navigate to **Monitor > Reports and Analytics > Events > Console Events**.
- 2 Filter the information to focus and narrow the list of devices.
 - Data Range
 - Severity
 - Category
 - Module
- 3 Click the **Event Data** option to view information for a specific console event.

Use Device Event Log

Device events is a listing of several different kinds of events logged by the system. It lists Mobile Device Management (MDM) commands to devices, device responses, and device user actions. You can filter the log by date range, the severity level, category, or module.

Severity levels include the following descriptions.

- **Emergency** – Indicates a catastrophic MDM failure requiring immediate attention.
- **Alert** – Indicates a failure of a foundational MDM system requiring attention.
- **Critical** – Indicates a failure in a primary MDM system.
- **Error** – Indicates a failure in a non-primary MDM system.
- **Warning** – Indicates an issue in the future if action is not taken.
- **Notice** – Indicates unusual conditions.
- **Information** – Indicates normal operational data.
- **Debug** – Indicates useful information for troubleshooting.

Procedure

- 1 Navigate to **Monitor > Reports and Analytics > Events > Device Events**.
- 2 Filter the information to focus and narrow the list of devices.
 - **Data Range**
 - **Severity**
 - **Category**
 - **Module**
- 3 Select the **Friendly Name** option to view data about a specific device.

- 4 Select the **User** option to perform various functions, including **Add Device**, **Edit** options, and **Change Organization Group**.

You can also view device information from this option.

What to do next

If you wish to make logging setting changes, navigate to the settings page at **Groups & Settings > All Settings > System > Enterprise Integration > Syslog**.

Alternatively, you can select the **Syslog** menu item located below the **Device Events** menu item at **Monitor > Reports and Analytics > Events > Syslog**.

Syslog Integration

Security Information and Event Management (SIEM) technology gathers information about security alerts generated by network hardware and software components. It centralizes this data and generates reports to help you monitor activity, perform log audits, and respond to incidents. Workspace ONE UEM integrates with your SIEM tools by sending event logs using Syslog.

The event messages sent are the same that display from the Event Logs page in the AirWatch Console with the same Event Categories. During syslog configuration, you can opt to send Console events, Device events, or both. Any events generated by the AirWatch Console are sent to your SIEM tool according to the scheduler settings. The only way for you to control which events send messages is to customize the logging levels at the Events Settings system settings page.

On the Events Settings page, you can select a logging level for both the Console and Devices. Any logging level you select applies to what is shown in AirWatch, stored in the AirWatch database, and sent to your SIEM tool. Currently, you cannot opt to generate and store all events in AirWatch while sending a separate batch of select messages to your SIEM tool, or conversely.

Integrating Advantages

Event logs are sent to a SIEM tool for security and convenience:

- Security – Keep logs off site in a secure location in your SIEM systems.
- Convenience – Store logs in a central location for easy access.

The data transmitted through the syslog server is tied to event data. For example, a device event categorized with the Debug severity by the AirWatch Console, the syslog server uses the same severity. You can filter these settings but you cannot change the severity categorization of the events in the AirWatch Console.

This chapter includes the following topics:

- [Configure Syslog](#)
- [Admin Scheduler Tasks](#)
- [Configure the Scheduler Syslog Task](#)

Configure Syslog

During syslog configuration, you can opt to send Console events, Device events, or both. Any events generated by the AirWatch Console are sent to your SIEM tool according to the scheduler settings. Syslog can be configured for both on-premises and SaaS deployments.

Procedure

- 1 Navigate to **Monitor > Reports & Analytics > Events > Syslog**.
- 2 On the **General** tab, configure the following syslog settings,

Setting	Description
Syslog Integration	Enable or disable syslog integration.
Host Name	Enter the URL for the SIEM tool in the Host Name text box.
Protocol	Select the required protocol from available options to send the data. It is to be noted that support for TLS v1.1 is provided.
Port	Enter the port number to communicate with the SIEM tool in the Port text box.
Syslog Facility	Select the facility level for the feature from the Syslog Facility menu. The syslog protocol defines the syslog facility. The widespread use and manipulation of the syslog protocol can clutter the meaning of the syslog facility. However, it can roughly suggest from what part of a system a message originated and it can help distinguish different classes of messages. Some administrators use the syslog facility in rules to route parts of messages to different log files.
Message Tag	Enter a descriptive tag to identify events from the Workspace ONE UEM console in the Message Tag text box. For example, "AirWatch".
Message Content	Enter the data to include in the transmission in the Message Content text box. This is how the message data gets formatted when sent using syslog to your SIEM tool. Use lookup values to set the content. For secure TCP, New line (CRLF) formatting using Enter, \n, \r does not work and gets automatically converted to tab, \t for secure TCP.

- 3 On the **Advanced** tab, configure the following settings.

Setting	Description
Console Events	Select whether to enable or disable the reporting of Console events.
Select Console Events to Send to Syslog	Visible if you enable Console Events. For each sub-heading, select the specific events that you want to trigger a message to syslog. Use Select All or Clear All to select or unselect all the events all at once. To select or unselect specific events, enable or disable the checkboxes. Note On enabling the Console Events , by default, all events under all categories of console events are selected.

Setting	Description
Device Events	Select whether to enable or disable the reporting of Device events.
Select Device Events to Send to Syslog	Visible if you enable Device Events. For each sub-heading, select the specific events that you want to trigger a message to syslog. Use Select All or Clear All to select or unselect all the events all at once. To select or unselect specific events, enable or disable the checkboxes. Note On enabling the Device Events , by default, all events under all categories of device events are selected.

- 4 Select **Save** and use the **Test Connection** button to ensure successful communication between the AirWatch Console and the SIEM tool.

Admin Scheduler Tasks

You can configure scheduler tasks by editing the frequency of individual tasks or by disabling tasks. Use the following table to get an understanding of what each task is for.

Scheduler Task	Description
Hub Package Process Repository	Watches the package repository directory for WinMo Hub packages and pulls them in to the database.
Android Work Google Device Id Validation Job	Upon enrollment into Android, the server waits for a Google generated deviceId, so that it can initiate the application assignment and push. There are a few minutes delay in getting this ID and this scheduler checks whether any new enrolled device has the ID updated and if yes, start the application sync process.
App EULA Update Notification	Accounts for all devices for which App EULA acceptance is pending and sends notifications. Once final notification is sent, app is removed from the device.
Auto Renew Expiring Profile	Checks for certificates that expired within a renewal grace period configured on Certificate Authority and renews them.
Auto-rotate Google Password	Handles password provisioning and purging for integration with Google Sync.
BitLocker Recovery Key Rotation Job	Rotates the BitLocker admin recovery key based on the values configured in the profile.
Command Publish Batch Job	
Console Notifications	Checks to see if any new notifications must be added to an admin's notification list (for example, APNs expiration notification). These notifications appear in the admin console and are emailed to the admins.
Device Based VPP Apps to Track Update	Checks which VPP applications at an organization group have device-based licensing and auto update enabled. This adds or removes apps from the list used by the VPP auto update scheduler job.
Device Enrollment Program Update	Initiates sync command from Apple to send the added and removed devices for a DEP token at a given OG to update our records.
Email Password Removal	Removes Google password generated for email from Workspace ONE UEM database.
File Encryption Migration	Encrypts or decrypts the content stored in the file storage based on the settings in All Settings > Admin > Storage.

Scheduler Task	Description
Install Application On Demand.	Triggers install of Apple VPP applications upon VPP invite acceptance and triggers install of failed-eligible Apple VPP applications.
List View Export	Checks if an export is requested by an admin for the device or user list view. If it has, it schedules a background job to run asynchronously. Once that background job is completed, the list view export is available for download.
MDM Application List Sample	Collects the status of applications that are marked as 'MDM apps' from all the devices. Applicable only for iOS apps and devices. Scheduler is turned off by default and is enabled only for customers who request the functionality.
MDM License Count Update	Checks device enrollment counts and updates the customer's license counts. Used to track product usage.
P2P license true-up with vendor	Identifies all the peer distribution server licenses that are about to expire, renews the licenses by communicating with the Adaptiva cloud licensing service and distributes the renewed license key to the peer distribution server.
Peer Distribution Software Notification Job	Identifies all the Peer Distribution servers that do not have the latest version installed and notifies the administrator to update.
Profile Publish Batch Job	Profile publishes for CA and Tunnel profile queues the install profile command in held status is by Profile Publish Batch Job in batches. Selects a batch and batch size, based on the settings configured in the UEM Console (under Settings > Installation > Performance Tuning for on-premise environments).
Purge Marked For Delete.	This job deletes repo(s)/folder(s)/file(s) under a repository that is marked for deletion.
Query Feedback Service	Checks Apple's Feedback Service for statuses and causes of failed APNs commands.
Re-queue Device Commands	Applicable only for Windows devices. Identifies devices with failed application installs and re-tries installation. The number of re-try attempts and the interval for the next attempt are identified from the performance tuning settings 'Max re-try attempts for failed app install' and 'Failed Application Install Retry Interval' respectively.
Run Compliance Engine.	The scheduler job evaluates compliance in scenarios where: <ul style="list-style-type: none"> ■ Compliance policy is created Post-enrollment. ■ Any subsequent changes are made to the compliance policy. ■ Any changes made to smart group ■ Device moves organization groups ■ Changes made to app groups ■ Certain Telecom based compliance policies are enabled ■ Apple Templates are used
S/MIME Certificate Cleanup	Checks for all SMIME certificates that have completed their retention period and purges them.
Scheduled Application Batch Release	Used to release internal application install commands created and held by 'Scheduled Application Publish' job. Selects queued application batch (roundrobin). Calculates device list using configured 'Batch Size' text box of performance tuning section. Releases install commands for batch.
Scheduled Application Publish	Used to trigger the installation and removal of internal applications based on newly effective assignments. Creates held batch of install commands. Creates remove commands for the immediate release.

Scheduler Task	Description
Send Apps to App Scan Vendor.	Send a unique list of applications installed across entire device fleet to the configured app scan vendor.
Send VPP Invites and Apps	Checks for users assigned user-based VPP apps and either sends email or device notifications inviting users or devices to participate in user-based licenses of the Volume Purchase Program.
Server Action Task	Handles Time Schedule profiles. The job runs at configured intervals and takes action of Install or Remove profile as per the time span configured for Time schedule profiles.
Staged Command Data Processing Job	Used to schedule the processing of bulk commands from the Device List View page.
Sync Chrome OS Devices	Retrieves new Chrome OS enrollments from Google and creates a corresponding device record in Workspace ONE UEM.
Sync Directory Groups.	Queries the directory to grab all members of synchronized directory groups. Stores users who are part of the group in the UserGroupEnrollmentUserMapSync table. Compares those users by Distinguished Name (DN) or other unique attribute in the UserGroupEnrollmentUserMapSync table to the Mobilemanagement.EnrollmentUser table. If group is configured with add missing users enabled and User does not exist with that DN, user details are pulled from the AD using user ExternalID and stored in the Mobilemanagement.EnrollmentUser table.
Sync Directory User and Admin Attributes	Queries the directory to sync user attributes based on eternalID.
Sync External Content.	Syncs admin repo metadata for all the repositories where admin user credentials are set in the MCM console.
Sync MEM Device Resource ID Job	Syncs Google device records with Workspace ONE UEM for approving new enrollments / mobile mail configurations
Telecom Assign Plans/Roll-up Usage	Calculate usage limits for devices whose Admin has enabled Telecom tracking. Necessary to run reports, populate dashboard, and have the accurate list-view for Telecom.
Temporary Session Key Clean Up	Clears temporary encryption keys used to encrypt the admin provided passphrase in a downloaded configuration file. The key is removed from the database so that it is impossible to retrieve the passphrase from the configuration file after the 48-hour key rotation window has passed.
VPP Auto Update	Checks iTunes for latest version of VPP applications from the list created by Device Based VPP Apps to Track Update job. Each app is checked once every 24 hours. If an update is available, the job kicks off the update command to assigned devices.
VPP Revoke Licenses	Checks for users with associated licenses but no corresponding assigned application. It then issues a revoke command of the license from the user to disassociate it from the license so it can be reused.
Workflow Service	Used with the App store restriction, if the restriction is enabled then only one app workflow is active at a time. If there is any issue with the application installation, it deletes in 15 minutes and next one starts.
Purge Job	Removes orphan application blobs from the file storage, and CDN origin server if CDN is configured. Removes expired SDK application log files from the database. By default, the application log files expire every 14 days. Moves any application binary blobs to the file storage from the database if the file storage is configured. Moves non-expired SDK application log files from the database to file storage, if the file storage is configured. Global OG data does not get impacted with respect to the changes made to the blob purge. By default, the scheduler triggers every 24 hours and can either handle 2 GB of data from the database or actively perform tasks for 2 hours.

Configure the Scheduler Syslog Task

You can configure the Scheduler Syslog Task for on-premises deployments. This task sets the intervals at which the AirWatch Console sends request to the SIEM tool for data.

Procedure

- 1 Navigate to **Groups & Settings > All Settings > Admin > Scheduler**.
- 2 Select the **Edit** icon from the actions area for the **Syslog** task.
- 3 Define the interval at which the AirWatch Console sends data to the options configured in the **Syslog** feature in the **Recurrence Type** setting.
- 4 Define a limited time range for the AirWatch Console to send data in the **Range** setting.

This setting is optional.

AirWatch DataMart

AirWatch DataMart that enables scheduled automatic data exports from the AirWatch database for statistical analysis and reporting. To use the tool, load DataMart on the server hosting the AirWatch database or in a separate network location.

Successful installation creates two SQL Server Agent jobs on the server.

There are multiple options for exporting data. You can select to export data in .csv format or as database tables. If data is exported in .csv format, you can select to save exported data on the AirWatch database server or in a separate network location.

If you select a separate network location, use a network folder in the .csv path accessible by the Windows account the SQL Server Agent uses. You use these account credentials to access the destination folder for CSV file output. If data is exported in a database table format, you can access the DataMart exports by following the information in relevant pages. DataMart export is available for both on-premises and SaaS (dedicated) AirWatch deployments.

This chapter includes the following topics:

- [DataMart Requirements](#)
- [Install DataMart](#)
- [DataMart Tables](#)
- [DataMart Entity Relationship Diagram](#)

DataMart Requirements

Before using DataMart, ensure that your system meets the requirements.

General Requirements

- Login credentials with both public and sysadmin server roles enabled in SQL Server.
- Database server requirements for the AirWatch DataMart are identical to the host server requirements for the AirWatch Console. No additional hardware or upgrades are necessary.

Software Requirements

- Windows Server 2008 R2, 2012 (64-bit), and 2014 (64-bit) with the latest service packs and updates from Microsoft (<http://www.update.microsoft.com>).
- .NET Framework 3.5 & 4. A Windows post-installation update is required to update additional software components for .NET Framework 4.
- Microsoft SQL Server 2012, 2014, or 2016 with Client Tools (SQL Management Studio, Reporting Services, Integration Services, SQL Server Agent, latest server packs).

Important For dedicated SaaS installations, only install DataMart once. Subsequent clients are added to the DataMart database manually.

Install DataMart

You need the AirWatch DataMart Installer to receive this feature. You can configure the AirWatch DataMart Installer to run an Extract, Transform, and Load (ETL) job daily to export data as a CSV file or as a cube (CUB) for your SQL Server Analysis Services (SSAS).

For on-premises deployments, the DataMart is installed on your AirWatch database server according to settings you configure when you install the application. You can install AirWatch DataMart on the AirWatch database server or any server from which the AirWatch database is accessible.

Note Dedicated SaaS deployments receive a data mart in only .csv format and can access it in their specified folder from the AirWatch secure FTP location. If your company is interested in this feature, contact your AirWatch Account Services Manager.

Procedure

- 1 Run the DataMart installation executable file and select **Next**.
- 2 Read the End-User License Agreement, accept the terms to use the feature, and then select **Next**.
- 3 Select **Change** if desired, navigate to a destination folder where you want to place the installer log, and then choose **Next**.

Note If you export to a separate network location, the destination folder must be accessible to the SQL Agent service.

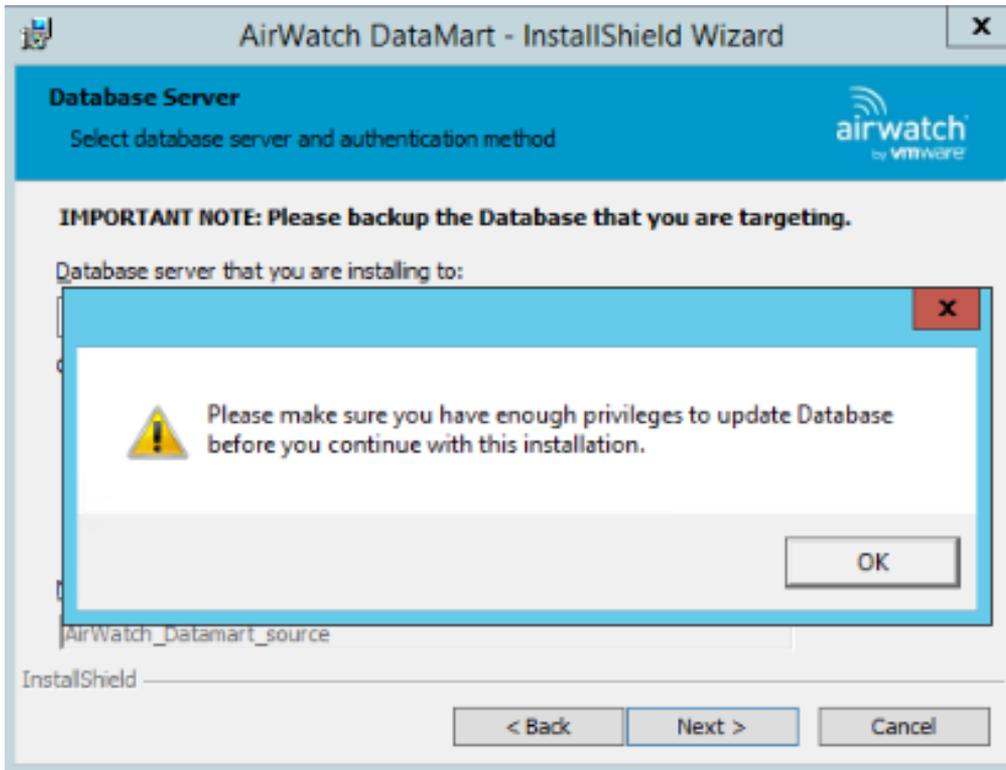
- 4 Ensure the database server to which you are installing DataMart is correct.

Note This is the AirWatch database and not the reporting database.

- 5 Select **Browse** and navigate to the AirWatch Console SQL instance if needed.

6 Select **Windows authentication credentials of current user**.

If you have enough rights to update the database before you continue with the installation, a warning message appears.



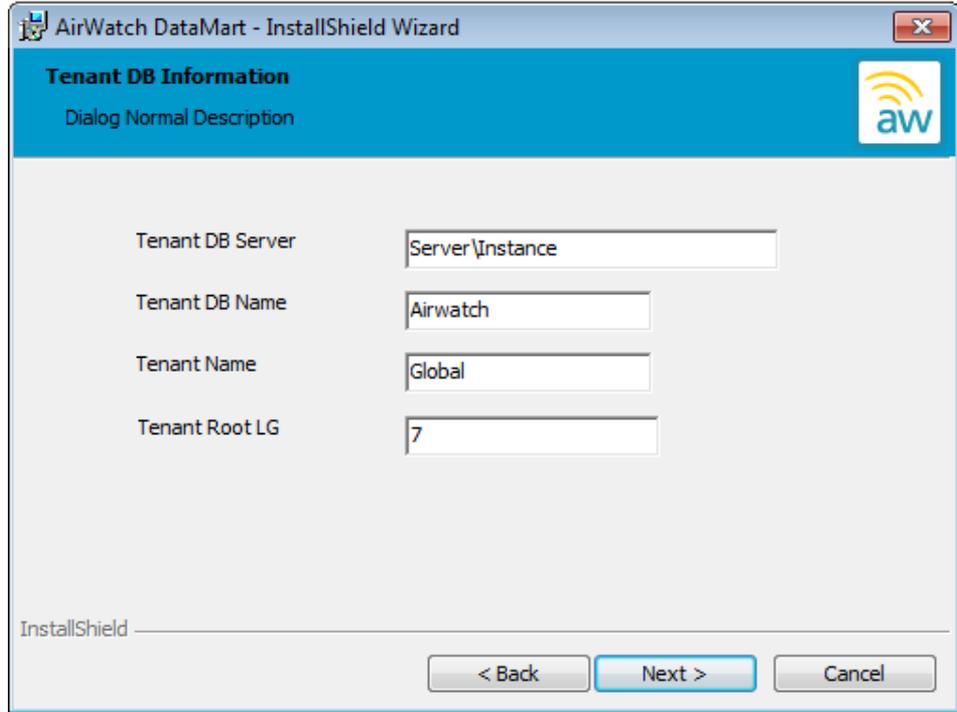
7 Select **OK**.

You are directed to the **Tenant DB Information** screen.

8 Configure the source database for DataMart.

Setting	Description
Tenant DB Server	Enter the name of the SQL server hosting the AirWatch database.
Tenant DB Name	Enter the name of the AirWatch database.

Setting	Description
Tenant Name	Enter the name of the tenant (used for reference in the DataMart database).
Tenant Root LG	Enter the root organization group ID of the tenant for which you are installing. <ul style="list-style-type: none"> a On-premises installations normally enter 7 (Global). b SaaS installations enter the root organization group ID (normally the ID of the organization group with the group type of customer).

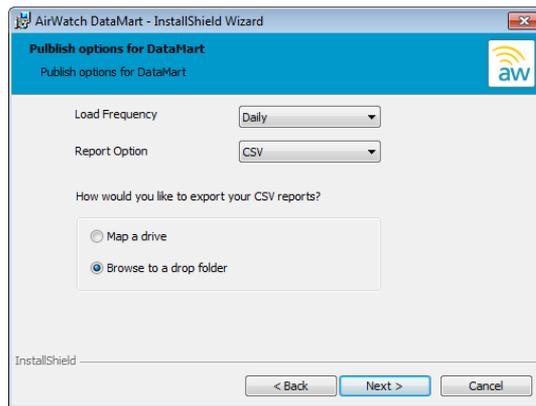


9 Configure the following **Publish Options** for DataMart

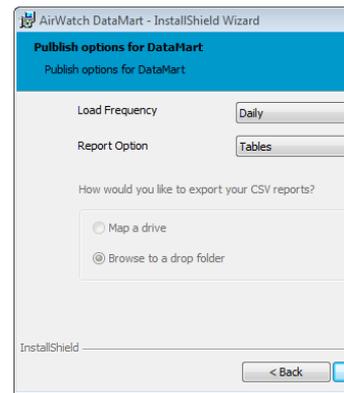
Setting	Description
Load Frequency	Select Daily or Hourly as the frequency for publishing data.
Report Option	Select CSV or Tables as the format for the exported data.

Setting	Description
Browse to drop folder	This option allows admins to browse to the folder that has the CSV files. On-premises installations should use this option.
Map a drive	<p>This option allows admins to specify a drive path and drop folder. Dedicated SaaS installations should use this option.</p> <ul style="list-style-type: none"> ▪ Drive Letter – Specify the letter of the drive to be mapped. ▪ Drive Path – Specify the drive path. Do not specify the client folder in this path. ▪ Client Drop folder – Specify the client drop folder. The folder name must not contain spaces.

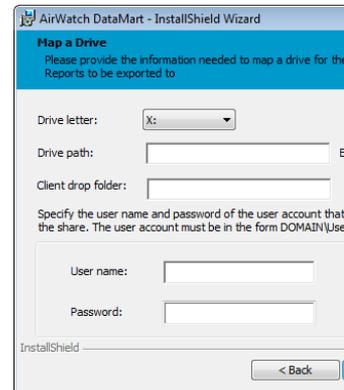
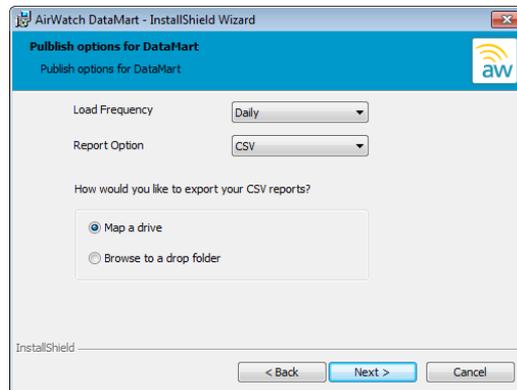
Browse to drop folder option



Database Table to Database Serv



Map a drive options



10 Select **Install** to begin installation.

11 Select **Finish** to exit the installation wizard.

After the installation finishes, the process creates two SQL Server Agent Jobs that run daily at midnight or hourly. DataMart creates applicable exports in the specified folder.

DataMart Tables

Access DataMart exports as database tables in the AirWatch Database or in the CSV files in a network location. The AirWatch_DataMart_source database table contains the exports.

The following table highlights key table/.csv export results and associated columns within.

DB Table/CSV File	Data	Columns
ApplicationDevices	Provides the identification number of devices, date, and time of any first-time enrollment.	<ul style="list-style-type: none"> ■ ApplicationVersionKey ■ TenancyKey ■ LoadDate ■ LoadHour ■ DeviceID ■ FirstSeen
ApplicationDim	Provides application name and identifier.	<ul style="list-style-type: none"> ■ ApplicationKey ■ Identifier ■ Name
ApplicationFact	Provides details about device applications such as authorized applications to use and the number of applications installed and uninstalled.	<ul style="list-style-type: none"> ■ ApplicationVersionKey ■ TenancyKey ■ LocationGroupKey ■ CategoryKey ■ LoadDate ■ LoadHour ■ DeviceTypeKey ■ IsBlacklisted ■ IsPublished ■ InstalledDeviceCount ■ RemovedDeviceCount ■ AssignedCount ■ ApplicationTypeKey
ApplicationVersion	Displays the version of applications listed in the database and available to the device end users.	<ul style="list-style-type: none"> ■ ApplicationVersionKey ■ ApplicationKey ■ Version
ApplicationTypeDim	Provides application type and name.	<ul style="list-style-type: none"> ■ ApplicationTypeKey ■ ApplicationTypeName
CarrierDim	Displays a list of carriers.	<ul style="list-style-type: none"> ■ TenancyKey ■ CarrierKey ■ Carrier

DB Table/CSV File	Data	Columns
DeviceDetails	Displays device enrollment data and specifications of devices enrolled. Examples include the serial number, the model, and the MAC address.	<ul style="list-style-type: none"> ■ TenancyKey ■ LoadDate ■ LoadHour ■ DeviceID ■ Carrier ■ OSKey ■ CorpEmp ■ LocationGroupKey ■ Platform ■ DeviceName ■ EnrollmentUser ■ SerialNumber ■ DeviceIdentifier ■ DeviceModel ■ MACAddress ■ IMEI_ESN ■ PhoneNumber ■ LastSeen
DeviceDetails (cont.)	Displays device enrollment data and specifications of devices enrolled. Examples include the serial number, model, and MAC address.	<ul style="list-style-type: none"> ■ DeployedProfileCount ■ IsMDMEnrolled ■ EnrollmentDate ■ AvailableSpace ■ TotalSpace ■ SpaceSampleTime ■ GPSLongitude ■ GPSLatitude ■ GPSSampleTime ■ WLANEnabled ■ VoiceRoamingEnabled ■ DataRoamingEnabled ■ IsRoaming ■ CellSampleTime ■ BatteryLifePercent ■ OnACPower ■ PowerSampleTime ■ WLANSignalStrength ■ SignalStrengthSampleTime ■ TotalPhysicalMemory ■ AvailablePhysicalMemory ■ MemorySampleTime ■ BackupBatteryLifePercent ■ User Name ■ EnrollmentUserKey ■ AssetNumber

DB Table/CSV File	Data	Columns
DeviceFact	Provides device compliance status in addition to details about device activity.	<ul style="list-style-type: none"> ■ OSKey ■ OwnershipKey ■ LocationGroupKey ■ TenancyKey ■ LoadHour ■ LoadDate ■ IsCompliant ■ IsCompromised ■ Active24hrs ■ Active30days ■ DeviceCount
DeviceTypeDim	Provides device type and name.	<ul style="list-style-type: none"> ■ DeviceTypeKey ■ PlatformName
LocationGroupDim	Provides details about the location group.	<ul style="list-style-type: none"> ■ LocationGroupKey ■ TenancyKey ■ LocationGroupID ■ Name ■ TypeName ■ DefCountryCode ■ DefCountryName ■ RegionCode ■ RegionName ■ Status ■ CustomerCode ■ CultureCode ■ CultureName ■ CultureNativeName ■ EffectiveStartDate ■ EffectiveEndDate
LocationGroupFlat	Displays details about the hierarchy, culture, language, and organization groups.	<ul style="list-style-type: none"> ■ TenancyKey ■ ParentLocationGroupID ■ ChildLocationGroupID ■ ParentKey ■ ChildKey ■ LGLvl
OSDim	Provides details about the OS	<ul style="list-style-type: none"> ■ OSKey ■ OSMajorVersion ■ OSMinorVersion ■ OSBuildNumber ■ PlatformName ■ OSName

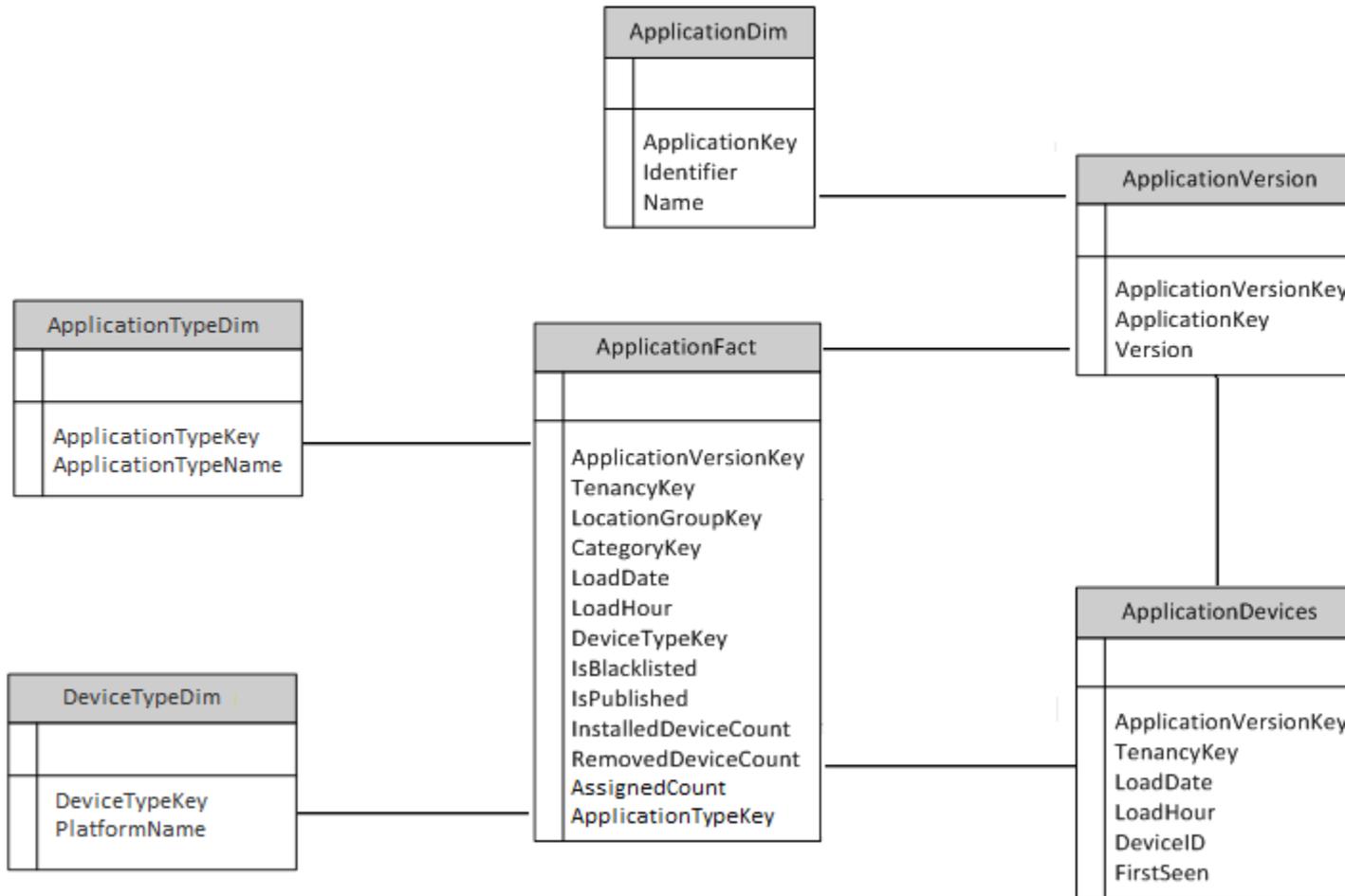
DB Table/CSV File	Data	Columns
OwnershipDim	Provides details about the device ownership type	<ul style="list-style-type: none"> ■ PicklistItemID ■ Value ■ Text ■ SortOrder ■ LabelKey ■ Description
EnrollmentUserDim	Provides details about the enrollment user.	<ul style="list-style-type: none"> ■ TenancyKey ■ LocationGroupKey ■ EnrollmentUserKey ■ User Name ■ FirstName ■ MiddleName ■ LastName ■ EmailAddress ■ LastLoginDate ■ DeviceCount
EnrollmentUserFact		<ul style="list-style-type: none"> ■ TenancyKey ■ LocationGroupKey ■ EnrollmentUserKey ■ DeviceCount
AdministratorDim	Provides details about the administrator.	<ul style="list-style-type: none"> ■ TenancyKey ■ LocationGroupKey ■ AdministratorKey ■ User Name ■ FirstName ■ MiddleName ■ LastName ■ EmailAddress ■ LastLoginDate
AdministratorFact		<ul style="list-style-type: none"> ■ TenancyKey ■ LocationGroupKey ■ AdministratorKey ■ LastLoginDate
PolicyFact	Provides the identification number of the devices and compliant status of the devices.	<ul style="list-style-type: none"> ■ TenancyKey ■ LocationGroupKey ■ LoadDate ■ PolicyKey ■ DeviceID ■ Compliant
PolicyDim	Provides details about the Policy.	<ul style="list-style-type: none"> ■ TenancyKey ■ PolicyKey ■ PolicyName ■ PolicyDescription ■ Platform

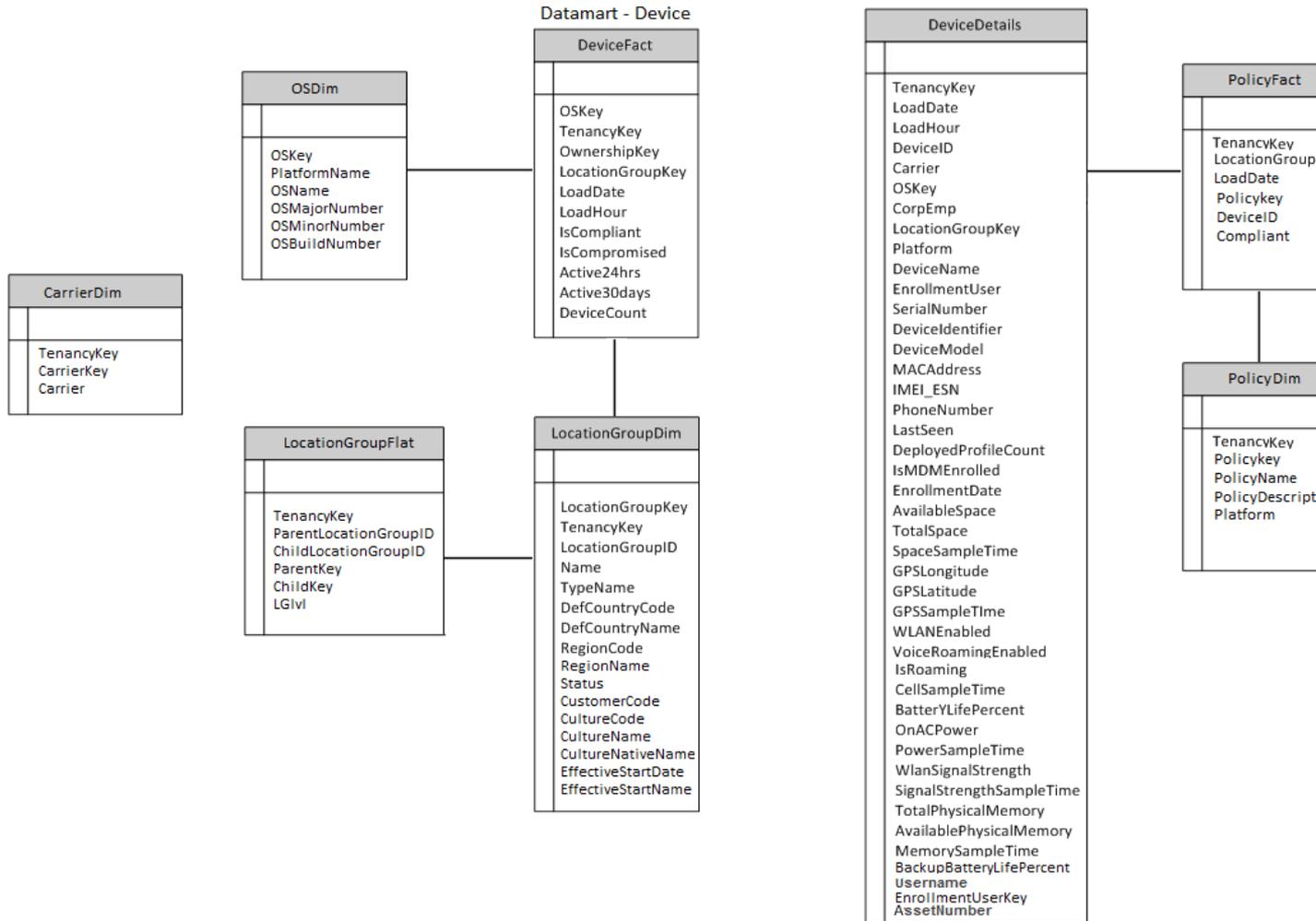
DB Table/CSV File	Data	Columns
ProfileDim		<ul style="list-style-type: none">■ TenancyKey■ ProfileKey■ ProfileName■ AssignmentType■ Platform
ProfileFact		<ul style="list-style-type: none">■ TenancyKey■ LocationGroupKey■ LoadDate■ LoadHour■ DeviceTypeKey■ ProfileKey
ProfileDevices		<ul style="list-style-type: none">■ TenancyKey■ LoadDate■ LoadHour■ ProfileKey■ DeviceID■ Installed

DataMart Entity Relationship Diagram

Knowing how the various DataMarts relate to one another can help you understand how they function.

Datamart - Application





Datamart - Users

