VMware AirWatch Analytics Guide

Analyze your AirWatch deployment

AirWatch v9.3

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

Table of Contents

Chapter 1:
Overview

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 these event logs to your Security Information and Event Management tools or Business Intelligence systems. For more information, see Event Logs Overview on page 6.

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. AirWatch integrates with your SIEM tools by sending event logs using Syslog.

For more information, see Syslog Integration Overview on page 9.

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. For more information, see AirWatch DataMart Overview on page 13.

Chapter 2:
Event Logs

Event Logs Overview

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.

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.

To use a console event:

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

Use Device Events

Device events show 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.

To use the device event log.

1. Navigate to **Hub > Reports & Analytics > Events > Device Events**.
2. Filter the information to focus and narrow the list of devices. Filter by **Data Range**, **Severity**, **Category**, and **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.

Chapter 3:
Syslog

Syslog Integration Overview

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. AirWatch 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.

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.

To configure syslog:

1. Navigate to **Hub > 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** field.
Protocol	Select the required protocol from the available options to send data. Support for TLS 1.0, 1.1, and 1.2 is provided.
Port	Enter the port number to communicate with the SIEM tool in the **Port** field.

Setting	Description
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 AirWatch Console in the **Message Tag** field. For example, "AirWatch".
Message Content	Enter the data to include in the transmission in the **Message Content** field. This is how the message data gets formatted when sent using syslog to your SIEM tool. Use lookup values to set the content. In case of 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.
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.

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.

To configure the scheduler syslog task:

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.

Chapter 4:
AirWatch DataMart

AirWatch DataMart Overview

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 choose to export data in .csv format or as database tables. If data is exported in .csv format, you can choose 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.

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 recommended 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.

To run the AirWatch DataMart:

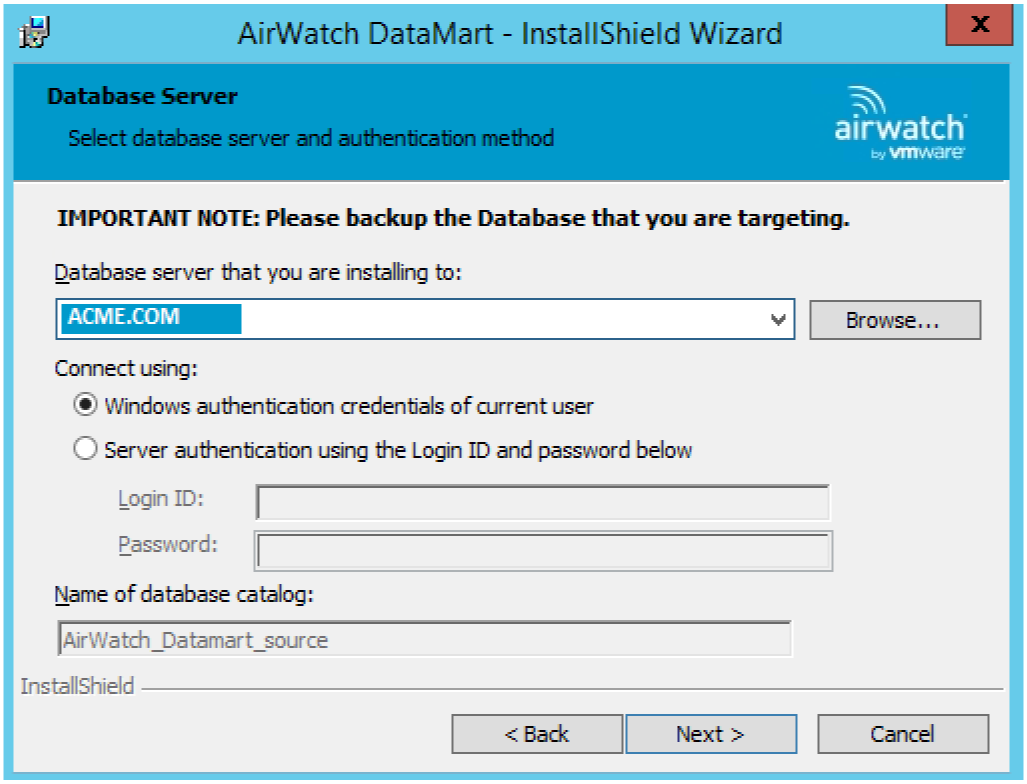
1. Run the DataMart installation executable file and select **Next**.
2. Read the End-User License Agreement, accept the terms to use the feature, and then select **Next**.
3. Select **Change** if desired, navigate to a destination folder where you want to place the installer log, and then choose **Next**.

   > **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**.



AirWatch DataMart - InstallShield Wizard

Database Server

Select database server and authentication method

IMPORTANT NOTE: Please backup the Database that you are targeting.

Database server that you are installing to: ACME.COM

Connect using:

● Windows authentication credentials of current user

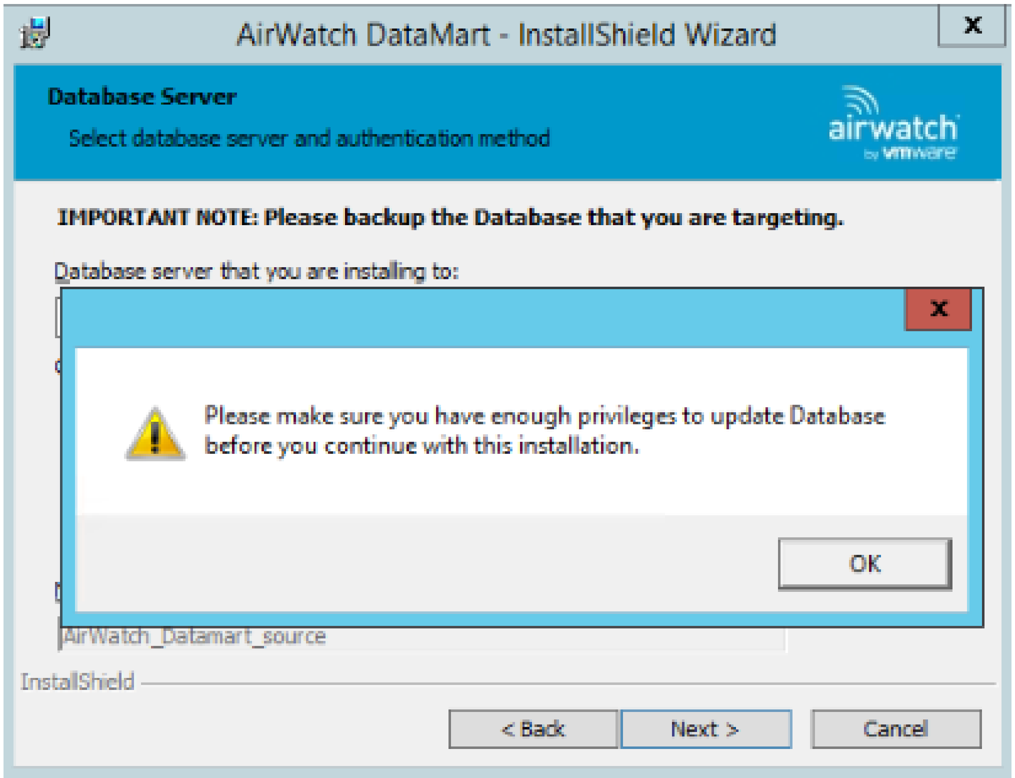
○ Server authentication using the Login ID and password below

Login ID:

Password:

Name of database catalog: AirWatch_Datamart_source

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



AirWatch DataMart - InstallShield Wizard

Database Server

Select database server and authentication method

IMPORTANT NOTE: Please backup the Database that you are targeting.

Database server that you are installing to:

Please make sure you have enough privileges to update Database before you continue with this installation.

AirWatch_Datamart_source

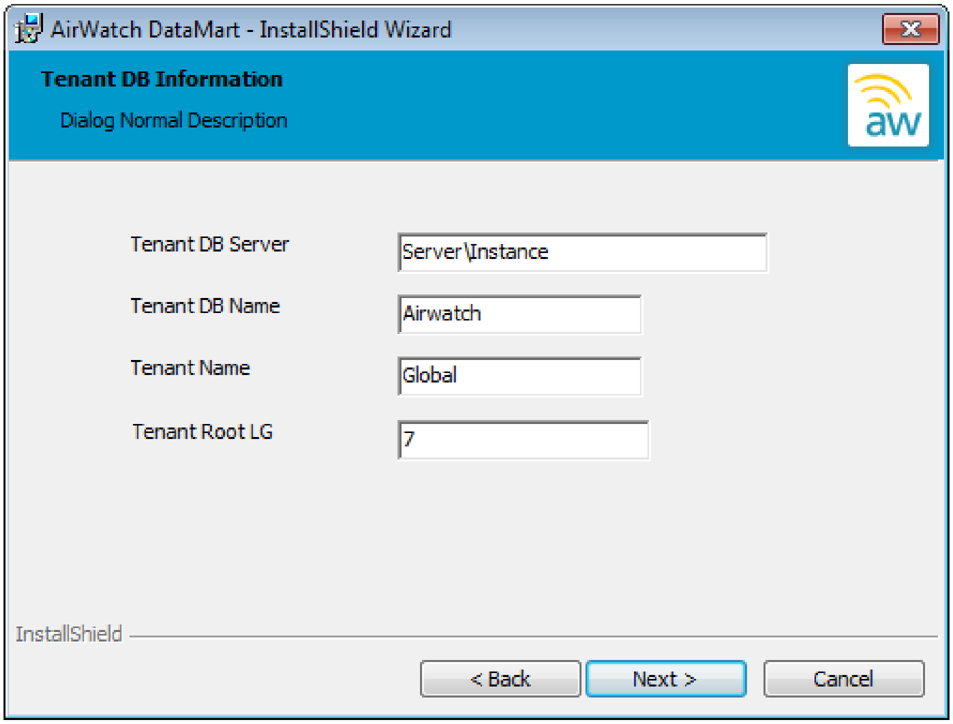
3. Select **OK**. You are directed to the **Tenant DB Information** screen.

4. Configure the source database for DataMart.

- **Tenant DB Server** – Enter the name of the SQL server hosting the AirWatch database.
- **Tenant DB Name** – Enter the name of the AirWatch database.
- **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.

    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).


AirWatch DataMart - InstallShield Wizard
Tenant DB Information
Dialog Normal Description
aw

Tenant DB Server: Server\Instance

Tenant DB Name: Airwatch

Tenant Name: Global

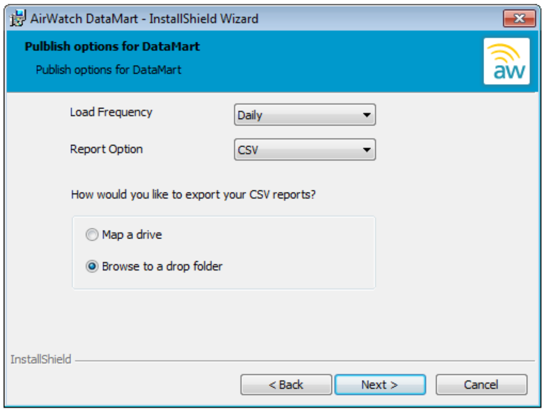
Tenant Root LG: 7

InstallShield
< Back
Next >
Cancel

5. Configure the following **Publish Options** for DataMart:

- **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.
- **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** – This option allows admins to specify a drive path and drop folder. Dedicated SaaS installations should use this option.
    - **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.s

Browse to drop folder option



Pulblish options for DataMart

Publish options for DataMart

Load Frequency: Daily

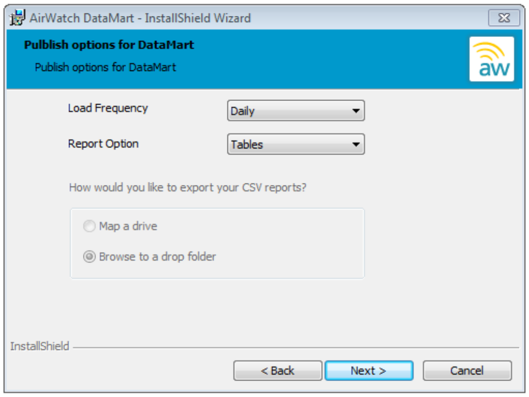
Report Option: CSV

How would you like to export your CSV reports?

○ Map a drive

● Browse to a drop folder

Database Table to Database Server option



Publish options for DataMart

Publish options for DataMart

Load Frequency: Daily

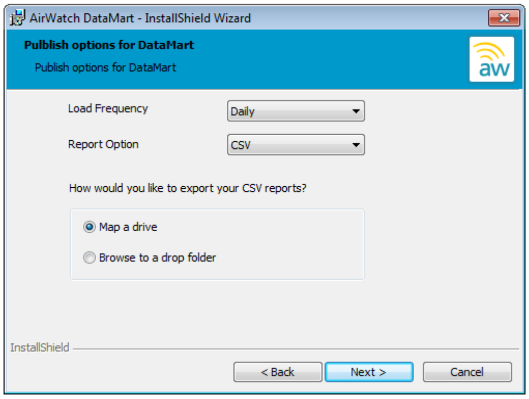
Report Option: Tables

How would you like to export your CSV reports?

○ Map a drive

● Browse to a drop folder

Map a drive options



Publish options for DataMart

Publish options for DataMart

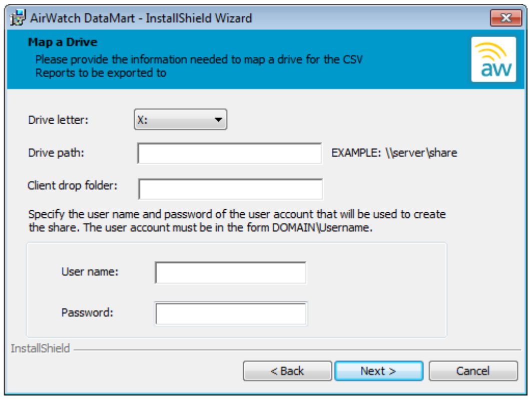
Load Frequency: Daily

Report Option: CSV

How would you like to export your CSV reports?

● Map a drive

○ Browse to a drop folder



Map a Drive

Please provide the information needed to map a drive for the CSV Reports to be exported to

Drive letter: X:

Drive path: EXAMPLE: \\server\share

Client drop folder:

Specify the user name and password of the user account that will be used to create the share. The user account must be in the form DOMAIN\Username.

User name:

Password:

6. Select **Install** to begin installation.

7. 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.	• ApplicationVersionKey • TenancyKey • LoadDate • LoadHour • DeviceID • FirstSeen
ApplicationDim	Provides application name and identifier.	• ApplicationKey • Identifier • Name
ApplicationFact	Provides details about device applications such as authorized applications to use and the number of applications installed and uninstalled.	• 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.	• ApplicationVersionKey • ApplicationKey • Version
ApplicationTypeDim	Provides application type and name.	• ApplicationTypeKey • ApplicationTypeName

DB Table/CSV File	Data	Columns
CarrierDim	Displays a list of carriers.	• TenancyKey • CarrierKey • Carrier
DeviceDetails	Displays device enrollment data and specifications of devices enrolled. Examples include the serial number, the model, and the MAC address.	• TenancyKey • LoadDate • LoadHour • DeviceID • Carrier • OSKey • CorpEmp • LocationGroupKey • Platform • DeviceName • EnrollmentUser • SerialNumber • DeviceIdentifier • DeviceModel • MACAddress • IMEI_ESN • PhoneNumber • LastSeen

DB Table/CSV File	Data	Columns
DeviceDetails (cont.)	Displays device enrollment data and specifications of devices enrolled. Examples include the serial number, model, and MAC address.	• DeployedProfileCount • IsMDMEnrolled • EnrollmentDate • AvailableSpace • TotalSpace • SpaceSampleTime • GPSLongitude • GPSLatitude • GPSSampleTime • WLANEnabled • VoiceRoamingEnabled • DataRoamingEnabled • IsRoaming • CellSampleTime • BatteryLifePercent • OnACPower • PowerSampleTIme • WLANSignalStrength • SignalStrengthSampleTime • TotalPhysicalMemory • AvailablePhysicalMemory • MemorySampleTime • BackupBatteryLifePercent • UserName • EnrollmentUserKey • AssetNumber

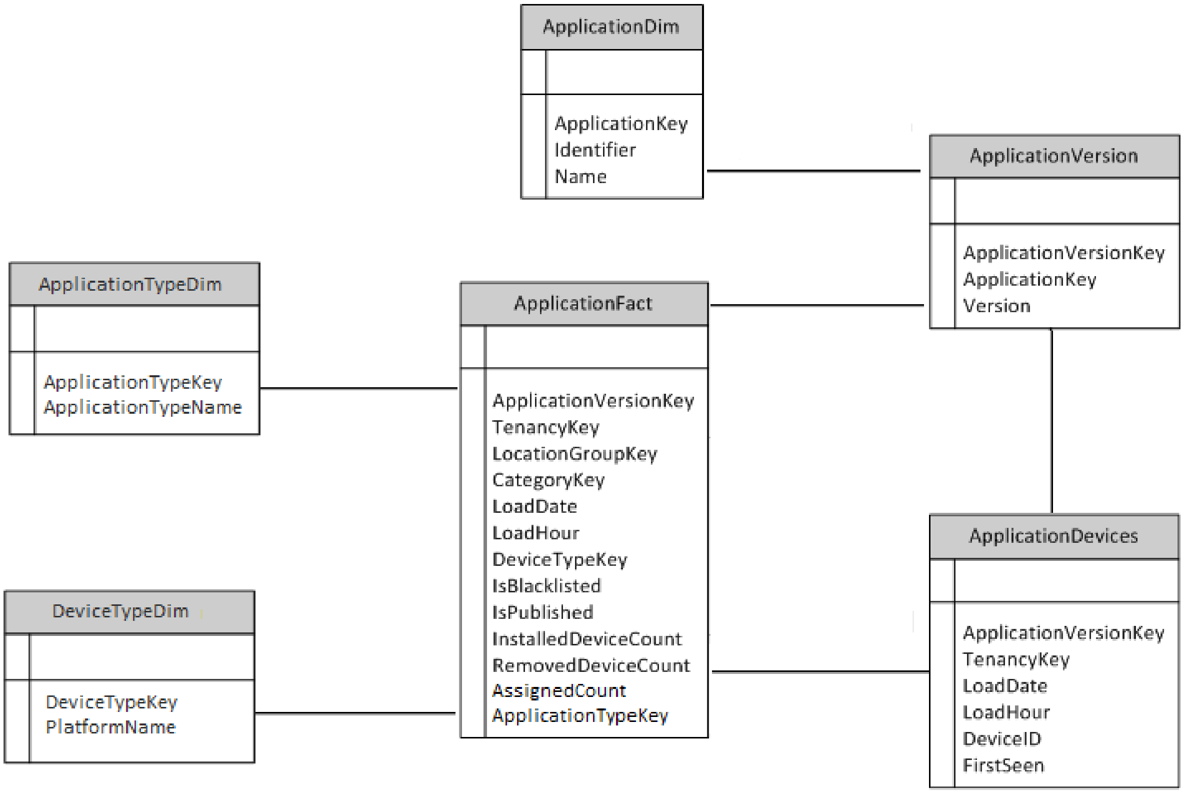
DB Table/CSV File	Data	Columns
DeviceFact	Provides device compliance status in addition to details about device activity.	• OSKey • OwnershipKey • LocationGroupKey • TenancyKey • LoadHour • LoadDate • IsCompliant • IsCompromised • Active24hrs • Active30days • DeviceCount
DeviceTypeDim	Provides device type and name.	• DeviceTypeKey • PlatformName
LocationGroupDim	Provides details about the location group.	• LocationGroupKey • TenancyKey • LocationGroupID • Name • TypeName • DefCountryCode • DefCountryName • RegionCode • RegionName • Status • CustomerCode CultureCode • CultureName • CultureNativeName • EffectiveStartDate • EffectiveEndDate

DB Table/CSV File	Data	Columns
LocationGroupFlat	Displays details about the hierarchy, culture, language, and organization groups.	• TenancyKey • ParentLocationGroupID • ChildLocationGroupID • ParentKey • ChildKey • LGlvl
OSDim	Provides details about the OS	• OSKey • OSMajorVersion • OSMinorVersion • OSBuildNumber • PlatformName • OSName
OwnershipDim	Provides details about the device ownership type	• PicklistItemID • Value • Text • SortOrder • LabelKey • Description
EnrollmentUserDim	Provides details about the enrollment user.	• TenancyKey • LocationGroupKey • EnrollmentUserKey • UserName • FirstName • MiddleName • LastName • EmailAddress • LastLoginDate • DeviceCount

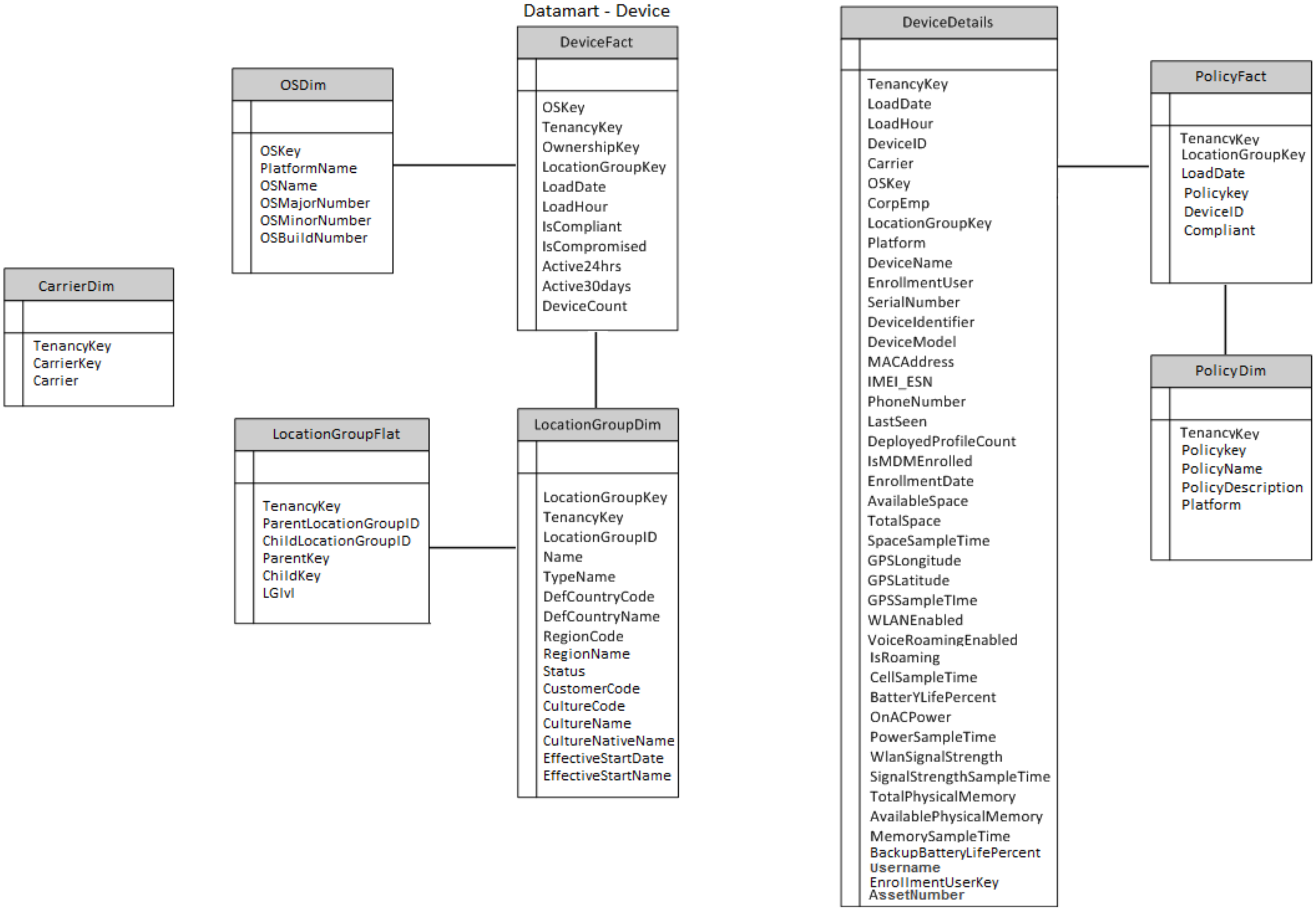
DB Table/CSV File	Data	Columns
AdministratorDim	Provides details about the Administrator.	• TenancyKey • LocationGroupKey • AdministratorKey • UserName • FirstName • MiddleName • LastName • EmailAddress • LastLoginDate
PolicyFact	Provides the identification number of the devices and compliant status of the devices.	• TenancyKey • LocationGroupKey • LoadDate • PolicyKey • DeviceID • Compliant
PolicyDim	Provides details about the Policy.	• TenancyKey • PolicyKey • PolicyName • PolicyDescription • Platform

DataMart Entity Relationship Diagram

Datamart - Application



Datamart - Device



DeviceFact

OSKey
TenancyKey
OwnershipKey
LocationGroupKey
LoadDate
LoadHour
IsCompliant
IsCompromised
Active24hrs
Active30days
DeviceCount

OSDim

OSKey
PlatformName
OSName
OSMajorNumber
OSMinorNumber
OSBuildNumber

CarrierDim

TenancyKey
CarrierKey
Carrier

LocationGroupFlat

TenancyKey
ParentLocationGroupID
ChildLocationGroupID
ParentKey
ChildKey
LGlvl

LocationGroupDim

LocationGroupKey
TenancyKey
LocationGroupID
Name
TypeName
DefCountryCode
DefCountryName
RegionCode
RegionName
Status
CustomerCode
CultureCode
CultureName
CultureNativeName
EffectiveStartDate
EffectiveStartName

DeviceDetails

TenancyKey
LoadDate
LoadHour
DeviceID
Carrier
OSKey
CorpEmp
LocationGroupKey
Platform
DeviceName
EnrollmentUser
SerialNumber
DeviceIdentifier
DeviceModel
MACAddress
IMEI_ESN
PhoneNumber
LastSeen
DeployedProfileCount
IsMDMEnrolled
EnrollmentDate
AvailableSpace
TotalSpace
SpaceSampleTime
GPSLongitude
GPSLatitude
GPSSampleTIme
WLANEnabled
VoiceRoamingEnabled
IsRoaming
CellSampleTime
BatterYLifePercent
OnACPower
PowerSampleTime
WlanSignalStrength
SignalStrengthSampleTime
TotalPhysicalMemory
AvailablePhysicalMemory
MemorySampleTime
BackupBatteryLifePercent
Username
EnrollmentUserKey
AssetNumber

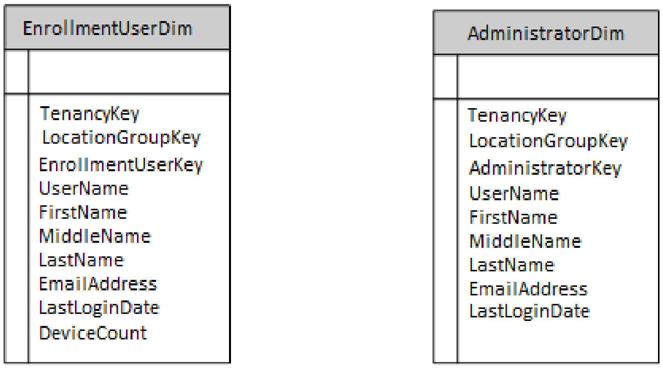
PolicyFact

TenancyKey
LocationGroupKey
LoadDate
Policykey
DeviceID
Compliant

PolicyDim

TenancyKey
Policykey
PolicyName
PolicyDescription
Platform

Datamart - Users



EnrollmentUserDim

TenancyKey
LocationGroupKey
EnrollmentUserKey
UserName
FirstName
MiddleName
LastName
EmailAddress
LastLoginDate
DeviceCount

AdministratorDim

TenancyKey
LocationGroupKey
AdministratorKey
UserName
FirstName
MiddleName
LastName
EmailAddress
LastLoginDate

Accessing Other Documents

While reading this documentation you may encounter references to documents that are not included here.

The quickest and easiest way to find a particular document is to navigate to https://my.air-watch.com/help/9.2/en/Content/Release_Notes/Doc_List_PDFs.htm and search for the document you need. Each release-specific document has a link to its PDF copy on AirWatch Resources.

Alternatively, you can navigate to AirWatch Resources on myAirWatch (resources.air-watch.com) and search. When searching for documentation on Resources, be sure to select your AirWatch version. You can use the filters to sort by PDF file type and AirWatch v9.3.