Integrate AirWatch Mobile Device Management

Publication Date: November 10, 2016
Abstract

This guide provides instructions to configure AirWatch Mobile Device Management to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.x and later, and AirWatch Mobile Device Management.

Audience

Administrators, who are responsible for monitoring AirWatch Mobile Device Management Version 8 using EventTracker.

The information contained in this document represents the current view of EventTracker on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

Abstract .............................................................................................................................................. 1  
Overview ........................................................................................................................................... 3  
Pre-requisites .................................................................................................................................... 3  
Integration Method for AirWatch MDM ......................................................................................... 3  
EventTracker Knowledge Pack (KP) ............................................................................................... 3  
   Categories ...................................................................................................................................... 3  
   Flex Reports ................................................................................................................................. 4  
Import AirWatch MDM knowledge pack into EventTracker ............................................................ 7  
   Category ....................................................................................................................................... 8  
   Templates ...................................................................................................................................... 9  
   Flex Reports ............................................................................................................................... 11  
   Knowledge Object ...................................................................................................................... 12  
Verify AirWatch MDM knowledge pack in EventTracker ............................................................... 14  
   Category ..................................................................................................................................... 14  
   Template .................................................................................................................................... 15  
   Flex Reports ............................................................................................................................. 16  
   Knowledge Object ..................................................................................................................... 17  
Create Flex Dashboards in EventTracker ..................................................................................... 18  
   Schedule Reports ....................................................................................................................... 18  
   Create Dashlets .......................................................................................................................... 20  
Sample Flex Dashboards .............................................................................................................. 23
Overview

Mobile Device Management (MDM) is the foundation of a comprehensive Enterprise Mobility Management (EMM) platform. VMware AirWatch® Mobile Device Management™ provides a simplified, efficient way to view and manage a diverse fleet of devices from a central admin console.

EventTracker collects the logs, helps administrator to analyze the events and generate the reports.

Pre-requisites

- EventTracker v7.x or later should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.
- AirWatch Mobile Device Management must be installed and configured.

Integration Method for AirWatch MDM

1. Login to Admin Console and navigate to Groups & Settings > All Settings > System > Enterprise Integration > Syslog.
2. Enter the Hostname or IP Address of the EventTracker into the Host Name.
4. Enter 514 into Port.
5. Select UserLevelMessages for Syslog Facility.
6. Check the boxes for Console and Device for Event Types Logged.
7. Enter AirWatch into Message Tag.
8. Ensure the Message Content field follows the default format.

EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and Reports can be configured into EventTracker. The following Knowledge Packs are applicable in EventTracker v7.x and later to support AirWatch MDM.

Categories

- **AirWatch MDM: All events**
  This category provides information related to all the events that occur in AirWatch MDM.
- **AirWatch MDM: Profile management**
  This category provides information related to Profile management like profile install, remove, confirm, etc. that occurs in device of AirWatch MDM.
- **AirWatch MDM: Application management**
  This category provides information related to Application management like request and confirm that occurs in device of AirWatch MDM.

- **AirWatch MDM: Status change**
  This category provides information related to status change that occurs in device of AirWatch MDM.

- **AirWatch MDM: Enrollment activity**
  This category provides information related to enrollment activity that occurs in device of AirWatch MDM.

- **AirWatch MDM: Security information management**
  This category provides information related to security information management that occurs in device of AirWatch MDM.

**Flex Reports**

- **AirWatch MDM-Enrollment activity**
  This report provides the information related Events like enrollment complete, MDM enrollment complete that occurs in device etc of AirWatch MDM.

  **Sample Report:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>User Name</th>
<th>Event</th>
<th>Event Type</th>
<th>Event Category</th>
<th>Event Module</th>
<th>Event Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/07/2018 02:54:32 PM</td>
<td>ARWATCH</td>
<td>sysadmin</td>
<td>MDMEnrollmentComplete</td>
<td>Device</td>
<td>Enrollment</td>
<td>Enrollment</td>
<td></td>
</tr>
<tr>
<td>11/07/2018 02:54:32 PM</td>
<td>ARWATCH</td>
<td>sysadmin</td>
<td>MDMEnrollmentAuthentication</td>
<td>Device</td>
<td>Enrollment</td>
<td>Enrollment</td>
<td></td>
</tr>
<tr>
<td>11/07/2018 02:54:32 PM</td>
<td>ARWATCH</td>
<td>sysadmin</td>
<td>EnrollmentComplete</td>
<td>Device</td>
<td>Enrollment</td>
<td>Enrollment</td>
<td></td>
</tr>
</tbody>
</table>

  ![Figure 1](image1.png)

- **Logs Considered:**

  ![Figure 2](image2.png)

- **AirWatch MDM-Security information management**
  This report provides the information related to security information like whether it is refused or confirmed in device of AirWatch MDM.
Sample Report:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Name</th>
<th>Event</th>
<th>Event Category</th>
<th>Event Module</th>
<th>Event Type</th>
<th>Event Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/07/2016 02:54:32 PM</td>
<td>AIRWATCH</td>
<td>sysadmin</td>
<td>SecurityInformation Confirmed</td>
<td>Command</td>
<td>Devices</td>
<td>Device</td>
<td>ReasonCode= BytesReceived=4</td>
</tr>
<tr>
<td>11/07/2016 02:54:32 PM</td>
<td>AIRWATCH</td>
<td>sysadmin</td>
<td>SecurityInformation Refused</td>
<td>Command</td>
<td>Devices</td>
<td>Device</td>
<td>ReasonCode= BytesReceived=747</td>
</tr>
<tr>
<td>11/07/2016 02:54:32 PM</td>
<td>AIRWATCH</td>
<td>sysadmin</td>
<td>SecurityInformation Delivery</td>
<td>Delivery</td>
<td>Devices</td>
<td>Device</td>
<td>BytesReceived=747</td>
</tr>
</tbody>
</table>

Logs Considered:

- **AirWatch MDM: Status change**
  This report provides the information related to Status change that occurs in device of AirWatch MDM.

Sample Report:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>User Name</th>
<th>Computer</th>
<th>Event</th>
<th>Event Category</th>
<th>Event Module</th>
<th>Event Type</th>
<th>Event Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/07/2016 02:54:32 PM</td>
<td>sysadmin</td>
<td>AIRWATCH</td>
<td>CompromisedStatusChanged</td>
<td>Device</td>
<td>CompromisedStatus</td>
<td>Devices</td>
<td>CompromisedStatus=NotCompromised</td>
</tr>
</tbody>
</table>

Logs Considered:

- **AirWatch MDM: Application management**
  This report provides the information related to application management like request for the application to be removed, to confirm etc that occurs in device of AirWatch MDM.
Sample Report:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Name</th>
<th>Event</th>
<th>Event Type</th>
<th>Event Category</th>
<th>Event Module</th>
<th>Event Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/7/2016 02:54:32 PM</td>
<td>AIRWATCH</td>
<td>sysadmin</td>
<td>RemoveApplicationRequested</td>
<td>Device</td>
<td>Command</td>
<td>Dashboard</td>
<td>Application=ApplicationVersion=ApplicationType=ApplicationEngageMedia</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>S:ApplicationVersion=ApplicationTtype=External</td>
</tr>
</tbody>
</table>

Logs Considered:

![Figure 7]

- **AirWatch MDM: Profile management**
  This report provides the information related to Profile management like whether the profile request to install is confirmed or failed, that occurs in device of AirWatch MDM.

Sample Report:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Name</th>
<th>Event</th>
<th>Event Type</th>
<th>Event Category</th>
<th>Event Module</th>
<th>Event Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/7/2016 02:54:32 PM</td>
<td>AIRWATCH</td>
<td>sysadmin</td>
<td>InstallProfileRequested</td>
<td>Device</td>
<td>Command</td>
<td>Dashboard</td>
<td>Profile=Android Default Settings</td>
</tr>
</tbody>
</table>

Logs Considered:

![Figure 8]

![Figure 9]

![Figure 10]
• **AirWatch MDM: All events**
  This report provides the information related to all events that occurred in AirWatch MDM.

**Sample Report:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Event Type</th>
<th>Event Name</th>
<th>User Name</th>
<th>Event Category</th>
<th>Event Module</th>
<th>Event Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/07/2016 02:54:32 PM</td>
<td>AIRWATCH</td>
<td>Device</td>
<td>InstallApplicationRequested</td>
<td>sysadmin</td>
<td>Command</td>
<td>Devices</td>
<td>Applications/Engage Mobile 5/ApplicationVersion/ApplicationType/External</td>
</tr>
<tr>
<td>11/07/2016 02:54:32 PM</td>
<td>AIRWATCH</td>
<td>Device</td>
<td>InstallProfileConfirmed</td>
<td>sysadmin</td>
<td>Command</td>
<td>Devices</td>
<td>Profiles/SharedDeviceSettings</td>
</tr>
<tr>
<td>11/07/2016 02:54:32 PM</td>
<td>AIRWATCH</td>
<td>Device</td>
<td>InstallProfileFailed</td>
<td>sysadmin</td>
<td>Command</td>
<td>Devices</td>
<td>Error Code=4091 Profile Installation Failed, Error Code=4091 Profile Failed to Install, Error Code=1009, The profile 7OS-Email_V_3P could not be installed, Error Code=21006, An identical Exchange account already exists, Profile=7OS-Email</td>
</tr>
<tr>
<td>11/07/2016 02:54:32 PM</td>
<td>AIRWATCH</td>
<td>Device</td>
<td>RemoveProfileFailed</td>
<td>sysadmin</td>
<td>Command</td>
<td>Devices</td>
<td>Error Code=1207E, The profile 7E701C6F-7E70-4EFC-A217-ABR1C46FBEECF is not installed, Profile=7OS-Email</td>
</tr>
</tbody>
</table>

**Logs Considered:**

1. **Import AirWatch MDM knowledge pack into EventTracker**
   
   **NOTE:** Import knowledge pack items in the following sequence:
   - Categories
   - Alerts
   - Parsing Rule
   - Knowledge Objects
   - Flex Reports

   1. Launch EventTracker Control Panel.
   2. Double click Export Import Utility.
3. Click the **Import** tab.

### Category

1. Click **Category** option, and then click the browse button.
2. Locate the **All AirWatch MDM group of categories.iscat** file, and then click **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

![Export Import Utility](image1.png)

**Figure 15**

4. Click the **OK**, and then click the **Close** button.

### Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on ![Import](image2.png) ‘Import’ option.

![Parsing Rule](image3.png)

**Figure 16**

3. Click on **Browse** button.
4. Locate All AirWatch MDM Template.ettdd file, and then click the Open button.

5. Now select the check box and then click on Import option. EventTracker displays success message.

6. Click on OK button.
Flex Reports

1. Click **Reports** option, and then click the browse button.
2. Locate the **All AirWatch MDM group of flex reports.issch** file, and then click the **Open** button.

![Figure 20](image)

3. Click the **Import** button to import the scheduled reports. EventTracker displays success message.

![Figure 21](image)
Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on the ‘**Import**’ option.

![Figure 22](image)

3. In the **IMPORT** pane, click on the *Browse* button.

![Figure 23](image)

4. Locate the **All AirWatch MDM KO.eto** file, and then click the **UPLOAD** button.
5. Now select the check box and then click on ‘OVERWRITE’ option. EventTracker displays success message.

6. Click on OK button
Verify AirWatch MDM knowledge pack in EventTracker

Category

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Categories.
2. In the Category Tree, expand AirWatch MDM group folder to see the imported categories.

![Category Management](image-url)

Figure 26
1. Logon to EventTracker Enterprise web interface and click the Admin menu, and then click Parsing Rules and click Template.

![Parsing Rule](image)

Figure 27
Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select Configuration.
2. In Reports Configuration pane, select Defined option.
3. In search box enter ‘AirWatch’, and then click the Search button.

EventTracker displays Flex reports of AirWatch.

Figure 28
Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**
2. Scroll down and select **AirWatch MDM** in **Objects** pane. Imported **AirWatch MDM** object details are shown.

![Knowledge Object Diagram](image)

**Figure 29**
Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

1. Open EventTracker in browser and logon.

   ![Figure 30](image)

2. Navigate to Reports>Configuration.

3. Select AirWatch in report groups. Check Defined dialog box.

   ![Figure 31](image)
4. Click on ‘schedule’ 🕒 to plan a report for later execution.
5. Click Next button to proceed.
6. In review page, check Persist data in EventVault Explorer option.

![Figure 32](image1)

7. In next page, check column names to persist using PERSIST checkboxes beside them. Choose suitable Retention period.

![Figure 33](image2)
8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

**Create Dashlets**

1. Open **EventTracker Enterprise** in browser and logon.

2. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

---

![Figure 34](image1.png)

![Figure 35](image2.png)
4. Fill suitable title and description and click **Save** button.
5. Click ✎ to configure a new flex dashlet. Widget configuration pane is shown.

![Figure 36](image)

6. Locate earlier scheduled report in **Data Source** dropdown.
7. Select **Chart Type** from dropdown.
8. Select extent of data to be displayed in **Duration** dropdown.
9. Select computation type in **Value Field Setting** dropdown.
10. Select evaluation duration in **As Of** dropdown.
11. Select comparable values in **X Axis** with suitable label.
12. Select numeric values in **Y Axis** with suitable label.
13. Select comparable sequence in **Legend**.
14. Click **Test** button to evaluate. Evaluated chart is shown.
15. If satisfied, click **Configure** button.

16. Click ‘customize’ to locate and choose created dashlet.
17. Click **+** to add dashlet to earlier created dashboard.
Sample Flex Dashboards

For below dashboard **DATA SOURCE: AirWatch MDM-Profile management**

- **AirWatch MDM-Profile management**
  - **WIDGET TITLE:** AirWatch MDM-Profile management
  - **CHART TYPE:** Donut
  - **AXIS LABELS [X-AXIS]:** Event
  - **FILTER:** Eventstamp
  - **LEGEND [SERIES]:** Event Module

![Sample Flex Dashboard](image)

*Figure 39*