Integrate Microsoft ActiveSync with EventTracker
Abstract

Exchange ActiveSync enables mobile phone users to access their e-mail, calendar, contacts, and tasks allowing them to continue to have access to this information while they are working offline. This guide provides instructions to monitor mobile devices with ActiveSync using EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.X and later, and Exchange Server 2007/2010.

Audience

Exchange Server administrators who wish to monitor ActiveSync usage using EventTracker Manager.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>1</td>
</tr>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Integrate Microsoft ActiveSync to EventTracker</td>
<td>3</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>3</td>
</tr>
<tr>
<td>Verify IIS logging</td>
<td>3</td>
</tr>
<tr>
<td>Import Scheduled Task</td>
<td>5</td>
</tr>
<tr>
<td>EventTracker Agent LFM Configuration</td>
<td>8</td>
</tr>
<tr>
<td>Verify Logs on EventTracker Manager</td>
<td>11</td>
</tr>
<tr>
<td>EventTracker KP for Microsoft ActiveSync</td>
<td>14</td>
</tr>
<tr>
<td>Flex Reports</td>
<td>14</td>
</tr>
<tr>
<td>Import EventTracker KP for Microsoft ActiveSync</td>
<td>20</td>
</tr>
<tr>
<td>Parsing Rules</td>
<td>20</td>
</tr>
<tr>
<td>Flex Reports</td>
<td>21</td>
</tr>
<tr>
<td>Verify EventTracker KP for Microsoft ActiveSync</td>
<td>23</td>
</tr>
<tr>
<td>Parsing Rules</td>
<td>23</td>
</tr>
<tr>
<td>Flex Reports</td>
<td>23</td>
</tr>
<tr>
<td>Create Flex Dashboards in EventTracker</td>
<td>24</td>
</tr>
<tr>
<td>Schedule Reports</td>
<td>24</td>
</tr>
<tr>
<td>Create Dashlets</td>
<td>27</td>
</tr>
<tr>
<td>Sample Flex Dashboards</td>
<td>30</td>
</tr>
</tbody>
</table>
Introduction

Microsoft Exchange ActiveSync is a synchronization protocol that enables users of mobile devices to access email, calendar, contacts, and tasks from their organization's Microsoft Exchange server.

With EventTracker’s built-in knowledge packs, administrators can monitor all servers running Microsoft Exchange ActiveSync from a single view, and generate reports on the following:

- Exchange ActiveSync activity on a user-by-user basis.
- ActiveSync usage data based on user agent information.
- Mailbox server's usage data based on mobile device clients.
- Exchange ActiveSync clients that are currently in compliance with established ActiveSync policies.
- Spot network usage trends.

Integrate Microsoft ActiveSync to EventTracker

Prerequisites

- Exchange ActiveSync must be enabled.
- PowerShell script execution must be enabled and execution policy must be set to bypass or unrestricted.
- Administrator access to Microsoft Exchange.
- IIS 7.0 and later must be installed.
- IIS logging must be enabled.

Verify IIS logging

For generating Active Sync reports, ensure IIS logging is enabled on the Exchange server.

1. Start Internet Information Services (IIS) Manager.
2. Navigate to ServerName>Sites to view configured websites.
3. Select the Exchange’s Web Site for which logging is required to be enabled.
4. Click to select the **Logging** option.
5. Verify following settings in **Logging** pane:
   - Under **Log File** section, **W3C** is selected from the **Log File Format** drop down.
   - Under **Log File** section, take a note of IIS log file directory. By default, log file path is "C:\inetpub\logs\LogFiles\W3SVCwebsiteid".
   - Under **Log Event Destination** section, **Log file only** radio button is selected.
   - Under **Log File Rollover** section, **Daily schedule** is selected.

6. If any changes were made, click **Apply** under **Actions** pane.

![Image of log files]

Figure 3

7. Navigate to IIS log file directory mentioned above to view generated log files.

**Import Scheduled Task**

1. Request ActiveSync script pack from **EventTracker Support**.
2. Download and extract the files provided at a preferred path.
3. Open task scheduler by navigating to **Control Panel -> System and Security -> Administrative Tools -> Task Scheduler**.
4. In Task scheduler windows, click on **Import Task** in **Actions** pane.
5. Browse and select the xml file named **ActiveSync Reporting.xml** from earlier mentioned extraction location.

6. Double-click to edit the imported task named **ActiveSync Reporting**.
7. Click **General** tab and change the user account settings in **Security options** section. Please ensure concerned user has exchange admin privileges.
8. Click **Triggers** tab and select **Edit**. Please select an appropriate time for script execution.

![Edit Action](image.jpg)

**Figure 8**

9. Click **Actions** tab and select **Edit**. Alter expression provided in **Add parameters** as shown below.

```
-file "C:\Exchange ActiveSync\ActiveSync Report Exporter.ps1"
```

**Script Location**

10. Click **OK** to apply the changes.

11. When the script is executed, reports named **Hourly, PolicyCompliance, Servers, StatusCodes, UserAgents and Users** will be generated in CSV format at the script location in **ActiveSyncReports** folder.

**EventTracker Agent LFM Configuration**

1. Logon to Exchange server.

2. Navigate to `<%EventTracker install directory%>\Prism Microsystems\EventTracker\Agent`.
3. Right-click `etaconfig.exe` and select **run as administrator**.
4. Select **Logfile Monitor** tab and click **Add File Name**.

![Image](image11.png)

**Figure 11**

5. Select **Get All Existing Log Files** checkbox.

6. Select **CSV** from **Log File Type** drop-down.

![Image](image12.png)

**Figure 12**

7. Click **Browse** and browse to the earlier selected log file path. Select **Show all the files** checkbox.

![Image](image13.png)

**Figure 13**
8. Type \\.*.csv as file extension and click OK.

![Image of Enter File name dialog box]

**Figure 14**

9. Select 1 from Header Line Number drop-down and click OK.

![Image of Enter Search String dialog box]

**Figure 15**

10. Select Hour from Field Name drop-down.

11. Type * (asterisk) as Search String.

12. Click Ok and Save.

**Verify Logs on EventTracker Manager**

1. Logon to EventTracker manager with appropriate credentials.
2. Click **Search** from EventTracker homepage ribbon.

3. In log search window, initiate search with following criteria.
   - Select **File Transfer** checkbox and choose appropriate systems.
   - Select appropriate time duration.
   - In Custom Criteria, **Event Id** contains **3230**.
   - In Custom Criteria, **Source** contains **EventTracker**.
4. Consumed logs will be displayed as shown below.
EventTracker KP for Microsoft ActiveSync

Once ActiveSync logs are consumed in EventTracker, following Knowledge Packs are available to support ActiveSync monitoring:

Flex Reports

- **Microsoft ActiveSync-Policy Compliance Statistics**: This report supplies the number of Exchange ActiveSync clients that are currently in compliance with established ActiveSync policies. Although this report doesn't provide detailed data, it can help target deficiencies. For example, the report won't tell you why a client is not compliant with the ActiveSync policy, but it will tell you how many clients are compliant, how many are not compliant, how many are partially compliant and the number of clients in an unknown state.

Sample Report

![Sample Report](image)

Sample Log

![Sample Log](image)
• **Microsoft ActiveSync-Server Statistics:** This report essentially tells you which mailbox servers are used most frequently by mobile device clients. It provides total number of synchronization requests processed and total bytes sent and received by CAS server.

### Sample Report

![Sample Report](image)

### Sample Log

![Sample Log](image)

• **Microsoft ActiveSync-HTTP Status Statistics:** This report enlists HTTP response codes and their respective hit counts. An administrator can use this report to troubleshoot failed requests and monitor performance of ActiveSync. More information about status codes is available [here](#).
Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>HTTP Status</th>
<th>HTTP SubStatus</th>
<th>Hit Count</th>
<th>Hit Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/15/2017 05:33:16 PM</td>
<td>mail.contoso.com</td>
<td>403</td>
<td>3</td>
<td>45</td>
<td>2</td>
</tr>
<tr>
<td>02/15/2017 05:33:16 PM</td>
<td>mail.contoso.com</td>
<td>401</td>
<td>1</td>
<td>142</td>
<td>9</td>
</tr>
<tr>
<td>02/15/2017 05:33:16 PM</td>
<td>mail.contoso.com</td>
<td>101</td>
<td>0</td>
<td>1000</td>
<td>89</td>
</tr>
</tbody>
</table>

Figure 24

Sample Log

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/15/2017 05:33:16 PM</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 25

- **Microsoft ActiveSync-User Agent Statistics**: This report generates ActiveSync usage data based on user agent information. The term “user agent” refers to the operating system and builds number, the mobile device used. This report details which mobile device operating systems were in use, how many mobile devices using a particular user agent connected on a given day and how many hits each user agent generated.

Sample Report

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Agent Type</th>
<th>Hit Count</th>
<th>Unique Device Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/15/2017 05:33:16 PM</td>
<td>mail.contoso.com</td>
<td>Apple-iPhone5s/901.2 34</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>02/15/2017 05:33:16 PM</td>
<td>mail.contoso.com</td>
<td>Samsung-GT-45678/100 231</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>02/15/2017 05:33:16 PM</td>
<td>mail.contoso.com</td>
<td>Apple-MacBook/676/1412 765</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>02/15/2017 05:33:16 PM</td>
<td>mail.contoso.com</td>
<td>Samsung-GT/45675/100 236</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Integrate Microsoft ActiveSync with EventTracker

Sample Log

![Sample Log](image)

- **Microsoft ActiveSync-User Activity Statistics**: This report lets you analyze Exchange ActiveSync activity on a user-by-user basis. For example, you can see what type of mobile device individuals use to access Exchange Server. You can also see the number of items each user sends and receives.

Sample Report

![Sample Report](image)
Integrate Microsoft ActiveSync with EventTracker

Sample Log

![Sample Log](image)

- **Microsoft ActiveSync-Hourly Sync Statistics**: This report assists in spotting network usage trends. You can find out the number of unique mobile devices that synchronized with your Exchange server within a given hour. Because this report tracks activity throughout the day, it is easy to discover peak usage periods.

Sample Report

![Sample Report](image)
Sample Log

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/15/2017 5:38:16 PM</td>
<td>3220</td>
<td>PHP, I5-4570M</td>
<td>SYSTEM</td>
<td>NT AUTHORITY</td>
<td>EventTracker</td>
</tr>
</tbody>
</table>

Description:
ENTRY:
Day: Tuesday
Hour: 18
Unique Devices: 82
Sync Related Requests: 177
FILE:C:\Users\user\Desktop\logs\...Copy\Hourly.csv
TYPE:CSV
FIELD: 

Figure 31
Import EventTracker KP for Microsoft ActiveSync

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility.

3. Import knowledge pack items in the following sequence:
   - Parsing Rules
   - Flex Reports

Parsing Rules

1. Select Import tab, choose Token value from Options dialog box.
2. Click the browse button in Location section.
Integrate Microsoft ActiveSync with EventTracker

3. Locate the **ActiveSync Parsing Rules.istoken** file, and then click the **Open** button.
4. To import tokens, click the **Import** button.

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

**Flex Reports**

1. Select **Import** tab, choose **Reports** from **Options** dialog box.
2. Select Legacy (*.issch) from location dialog box, click the ‘browse’ button.
3. Locate ActiveSync Reports.issch file, and then click the Open button.
4. To import scheduled reports from selected file, click the Import button.
5. Click OK and Close.
Verify EventTracker KP for Microsoft ActiveSync

Parsing Rules

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Parsing rule.
3. Scroll down and select Microsoft ActiveSync from Groups. Imported Token-Values are shown in right pane.

Flex Reports

1. Logon to EventTracker Enterprise.
2. Navigate to Reports->Configuration.
3. Select **Defined** in report type.

4. In **Report Configuration** page, select **Microsoft ActiveSync** from **Report Groups**.

![Figure 39](image)

5. Imported reports are shown in the right pane.

**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.
Integrate Microsoft ActiveSync with EventTracker

Figure 40

2. Navigate to Reports>Configuration.
3. Select Microsoft ActiveSync in report groups. Check Defined dialog box.

![Image of REPORTS CONFIGURATION]

Figure 41

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

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.

![Dashboard](image)

2. Navigate to Dashboard>Flex.

![Flex Dashboard](image)

3. Fill suitable title and description and click Save button.
4. Click to configure a new flex dashlet. Widget configuration pane is shown.
5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.
14. If satisfied, click **Configure** button.

15. Click ‘customize’ to locate and choose created dashlet.

16. Click to add dashlet to earlier created dashboard.
Sample Flex Dashboards

1. **Widget Title:** HTTP response trend  
   **Data Source:** Microsoft ActiveSync-HTTP Status Statistics  
   **Chart Type:** Line  
   **Values [Y-AXIS]:** Hit Count  
   **Legend [SERIES]:** HTTP Code

![Figure 49](image1.png)

2. **Widget Title:** Policy compliance trend  
   **Data Source:** Microsoft ActiveSync-Policy Compliance Statistics  
   **Chart Type:** Line  
   **Values [Y-AXIS]:** Device Count  
   **Legend [SERIES]:** Compliance Type

![Figure 50](image2.png)
3. **Widget Title: Unique device detection trend**
   
   **Data Source:** Microsoft ActiveSync-Server Statistics
   
   **Chart Type:** Line
   
   **Values [Y-AXIS]:** Average Unique Device Count
   
   **Legend [SERIES]:** Server Name
   
   ![Figure 51]

4. **Widget Title: Cumulative user hit count variance**
   
   **Data Source:** Microsoft ActiveSync-User Activity Statistics
   
   **Chart Type:** Meter Guage
   
   **Values [Y-AXIS]:** Hit Count
   
   **Legend [SERIES]:** User Name
   
   ![Figure 52]
5. **Widget Title: User agent connection statistics**

**Data Source:** Microsoft ActiveSync-User Agent Statistics

**Chart Type:** Donut

**Axis Labels [X-AXIS]:** User Agent Type

**Values [Y-AXIS]:** Hit Count

Figure 53