Monitor Mobile Devices via ActiveSync Using EventTracker
About This Guide

Exchange ActiveSync is a Microsoft Exchange synchronization protocol that is optimized to work in conjunction with high-latency/low-bandwidth networks. The protocol, based on HTTP and XML, lets mobile phones access an organization's information on Microsoft Exchange servers. 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 Enterprise version 7.X and later, and Exchange Server 2007/2010.

Audience

Exchange Server administrators who wish to monitor ActiveSync usage.

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

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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 Prism Microsystems, 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.

© 2012 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective
# Table of Contents

Overview ....................................................................................................................................................... 3  
Monitor Mobiles device with ActiveSync .................................................................................................. 4  
Event Log Consolidation ............................................................................................................................. 5  
  - Enable Logfile Monitor in EventTracker Agent ..................................................................................... 7  
  - Monitor Exchange ActiveSync Server Uptime Status ........................................................................ 10  
  - Generate Exchange ActiveSync Reports ............................................................................................. 10  
Generate Exchange ActiveSync Administrative Reports ........................................................................ 12  
  - Configure DLA-Extension in EventTracker Manager to process report files transferred from file ................................................................................................................................................................ 14  
About Prism Microsystems ...................................................................................................................... 19
Overview

EventTracker is a fully-featured SIEM and log management solution that allows organizations to maintain continuous compliance, reduce actual audit times from weeks to days, and increase operational uptime... thereby reducing the stress on the IT team, as well as management. EventTracker’s built-in knowledge base enables users to gather business intelligence providing increased security, performance, availability, and reliability of the systems within the IT infrastructure.

When administrators install the Client Access Server (CAS) role on a computer running Microsoft Exchange Server, Microsoft Exchange ActiveSync is enabled. This feature lets users synchronize their mobile phones with their Exchange mailboxes allowing them to access email, calendar, contacts, and tasks making this information accessible while working offline.

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

- ActiveSync usage by mobile users
- Server Utilization
- Devices used by mobile users
- Policy compliant details of mobile devices used by users to access their Mailbox
Monitor Mobiles device with ActiveSync

- ActiveSync server uptime status
- ActiveSync server usage
- ActiveSync usage statistics
- ActiveSync policy configuration changes
- ActiveSync policy compliance
- Remote wipe performed by Administrator/Users
- Mobile user’s behavior (New mobile users, unauthorized users connecting to MSExchange ActiveSync)
- ActiveSync administrative tasks performed by Administrators/Delegates
Event Log Consolidation

Based on audit settings, MS Exchange logs the necessary audit, availability, and performance events, which EventTracker collects to a centralized secure storage. Administrators can either collect all events or can choose to filter any events that are not necessary. Event definitions can be found at the EventTracker Knowledge Base at http://kb.prismmicrosys.com to decide which events should be kept and which events can be filtered. All these events may be received in real-time and can configured to generate an alert. Administrators can write intensive, complex pattern matching rules using industry standard regular expressions that parse the information within the event description, or alerts can be created when a sequence of events occurs within a predefined time frame. Once EventTracker consolidates the event logs, hundreds of reports can be generated based on various conditions.

To monitor Exchange ActiveSync server following things need to be checked:

- Enable IIS logging on Exchange Server.
- IIS logging should be configured properly for Exchange web access and Exchange ActiveSync usage monitoring:
  1. Open IIS Manager
  2. Navigate to Default website
  3. Click Logging
  4. Select W3C Log Format
  5. Select Fields
  6. Check all fields checkbox
  7. Click OK and then click Apply
Enable Logfile Monitor in EventTracker Agent

EventTracker Agent has to be enabled in order to start retrieving events from the IIS Logfile Monitoring.

1. To do this, select the **Start** button, and then select **All Programs**.
2. Select **EventTracker**, select **Agent Config**, and then select **Logfile Monitor**.

![EventTracker Agent Configuration](image)

Figure 2
3. To add SMTP logs that require monitoring, select **Add File Name**, **Select Log File Type** drop-down.
4. Select IISW3C. Enter the filename `<systemroot>\inetpub\logs\LogFiles\W3SVC1\*.log`
Monitor Mobile Devices via ActiveSync Using EventTracker

Figure 4

EventTracker Agent Configuration

Select Systems:
MAIL
Agent based system

Manager destinations:
192.168.1.7

Logfile Monitor
Search log files (various formats supported) for matching patterns specified here. Both individual files as well as folders can be monitored for matching entries. Matches cause an event to be generated.

Logfile Name
File Type

Add File Name
View File Details
Delete File Name
Search Strings

Save
Close
Monitor Exchange ActiveSync Server Uptime Status

Exchange ActiveSync server Uptime status can be monitored using the StatusTracker component available in EventTracker. Following are the components, which should be configured in the Status Tracker module to monitor:

- **System availability**: Status Tracker alerts when Exchange ActiveSync server is not reachable or down
- **Ports monitoring**: Status Tracker alerts when Exchange ActiveSync ports are not available or down
- **EventTracker**: **StatusTracker resource down**: This predefined alert, and category enables you to get alerted and reports generated for resource downtime status when Exchange ActiveSync server system or exchange services ports are down

Generate Exchange ActiveSync Reports

Once IIS logging has been enabled on the Exchange server running the Client Access role and the EventTracker agent is configured to read IIS logs, Exchange ActiveSync reports can be generated in EventTracker.

The following Knowledge Packs are available in EventTracker v7 to support ActiveSync monitoring:

- **Exchange ActiveSync User Statistics Report**: This report includes the total bytes that were sent and received and a count of each type of item sent and received. Item types include email messages, calendar items, contact items, and task items.

- **Exchange ActiveSync User Agent Report**: This report includes the total number of unique users, organized by a mobile phone Device ID

- **Exchange ActiveSync Server Usage Reports**: This report tells you the total number of synchronization requests processed and Total bytes sent and received by CAS server

- **Exchange ActiveSync Policy Compliance Reports**: This report provides information about the number of fully compliant, partially compliant, and noncompliant devices.
  - Fully compliant device is one that has accepted the Exchange ActiveSync policy and can implement all aspects of the policy.
  - Partially compliant device is one that has accepted the policy but has a mobile device operating system that is unable to enforce all aspects of the policy.

EventTracker
Monitor Mobile Devices via ActiveSync Using EventTracker

- Noncompliant device is either unable to accept the policy or has rejected the policy.

- **Monitoring Real-time Exchange ActiveSync User’s Behavior**: EventTracker has built in behavior rule for monitoring ActiveSync mobile users. This keeps track of mobile device syncing mailboxes with Exchange ActiveSync and displays respective users.

  This rule allows administrators to receive alerts when any new mobile device has initiated synchronization with ActiveSync server. It performs correlation for the synchronization of events and alerts if behavior changes are detected as out of ordinary activity.
Generate Exchange ActiveSync Administrative Reports

When administrators have enabled Exchange ActiveSync role on client access server, it is important to monitor any configuration changes or policy changes done by administrators or users have initiated a remote wipe to clear all data from a lost or stolen mobile phone.

Using the Search-AdminAuditLog cmdlet Exchange, organization configuration Change Audit log can be exported to CSV or HTML. It can be transferred via FTP to EventTracker for offline processing and Report generation.

1. Create a powershell script using Search-AdminAuditLog cmdlet for generating daily exchange server configuration change report:
   a. Create a folder (for example `<systemroot>\scripts`)
   b. Save attached .ps1 and .bat files in the Attachment section of this document to `<systemroot>\scripts`
2. Schedule ExchangeAdminAuditReports.bat in windows task scheduler to run once daily
3. Configure EventTracker Agent File Transfer to transfer HTML report to EventTracker Manager
4. Launch **EventTracker Agent** configuration console on Exchange server. Select **File Transfer** tab.
5. Select **Send other log files** to enable file transfer, and then select HTML report file path.
6. Click **Save** and then click **Close** Agent Configuration console.

Once report file is transferred it will be available in ...

...Prism Microsystems\EventTracker\DLA\ SystemName folder on EventTracker Manager System
Configure DLA-Extension in EventTracker Manager to process report files transferred from file

1. Log on to EventTracker. Type valid user credentials and then click Login.
2. Click the Admin drop-down, and then click Manager.

3. Click Direct Log Archive/Netflow Receiver tab.

4. Select Direct log file archiving from external sources option, and then select VCP port from Associated virtual collection point drop-down.
Monitor Mobile Devices via ActiveSync Using EventTracker

Figure 8

5. Select Add.
   Direct Archiver Configuration window displays.

Figure 9

6. Select Type drop-down, and then select DLA-Extension.
7. Type Configuration Name as ExchangeAuditReport.
8. Click Browse and select path of audit report file and click Configure.
9. Type *.html in File Pattern text box
10. In Action dropdown, select Move to Reports. (This can be customized accordingly)
11. In Report Destination dropdown, select Operation. (This can be customized accordingly)
12. Select Send E-mail to receive the report in respective mailbox.
13. Type a valid sender e-mail address in the E-mail Id field, and a brief description in subject field
14. Select Send as attachment option to receive reports in attached format or select Send only notification option to receive notification.
15. Click **Add**, and then click **Save**.
16. Click **Save**.

Once Reports are imported to EventTracker, it will be displayed in Operation dashboard. In addition, an E-mail will be send to the configured email address.

![Sample report](image13.png)

**Figure 13**

Sample report is shown below:

![Sample report](image14.png)

**Figure 14**
About Prism Microsystems

Prism Microsystems delivers business-critical solutions to consolidate, correlate and detect changes that impact the performance, availability and security of your IT infrastructure. With a proven history of innovation and leadership, Prism provides easy-to-deploy products and solutions for integrated Security Management, Change Management and Intrusion Detection. EventTracker, Prism’s market leading Security Information and Event Log Management solution, enables commercial enterprises, educational institutions and government organizations to increase the security of their environments and reduce risk to their enterprise. Customers span multiple sectors including financial, communications, scientific, healthcare, banking and consulting.

Prism Microsystems was formed in 1999 and is a privately held corporation with corporate headquarters in the Baltimore-Washington high tech corridor. Research and development facilities are located in both Maryland and India. For additional information, please visit http://www.eventtracker.com