EventTracker
Secure. Comply. Succeed.

Monitor Mobile Devices via ActiveSync Using EventTracker

White Paper

Publication Date: March 1, 2013

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

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.

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:

- Install the EventTracker Agent on Exchange Server 2007/2010.
- 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

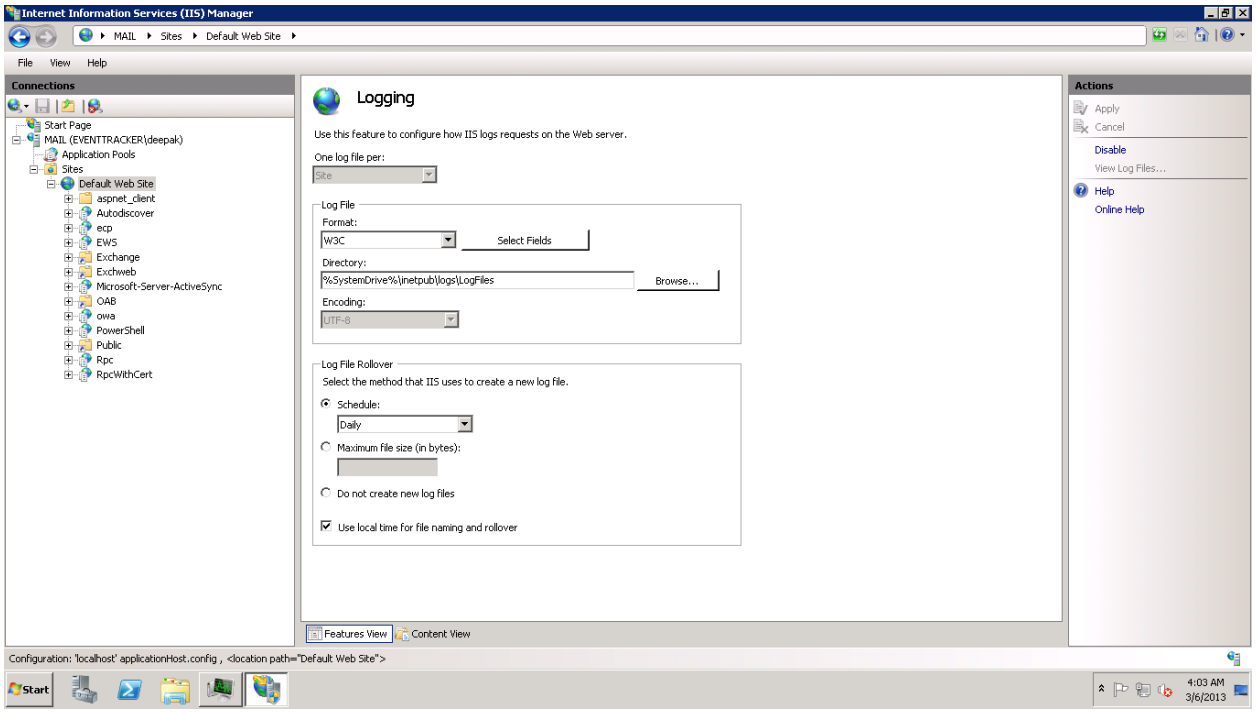
Internet Information Services (IIS) Manager
MAIL ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
MAIL (EVENTTRACKER\deepak)
Application Pools
Sites
Default Web Site
aspnet_client
Autodiscover
ecp
EWS
Exchange
Exchweb
Microsoft-Server-ActiveSync
OAB
owa
PowerShell
Public
Rpc
RpcWithCert
Logging
Use this feature to configure how IIS logs requests on the Web server.
One log file per:
Site
Log File
Format:
W3C
Select Fields
Directory:
%SystemDrive%\inetpub\logs\LogFiles
Browse...
Encoding:
UTF-8
Log File Rollover
Select the method that IIS uses to create a new log file.
Schedule:
Daily
Maximum file size (in bytes):
Do not create new log files
Use local time for file naming and rollover
Features View
Content View
Actions
Apply
Cancel
Disable
View Log Files...
Help
Online Help
Configuration: 'localhost' applicationHost.config , <location path="Default Web Site">
Start
4:03 AM
3/6/2013

Figure 1

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**.

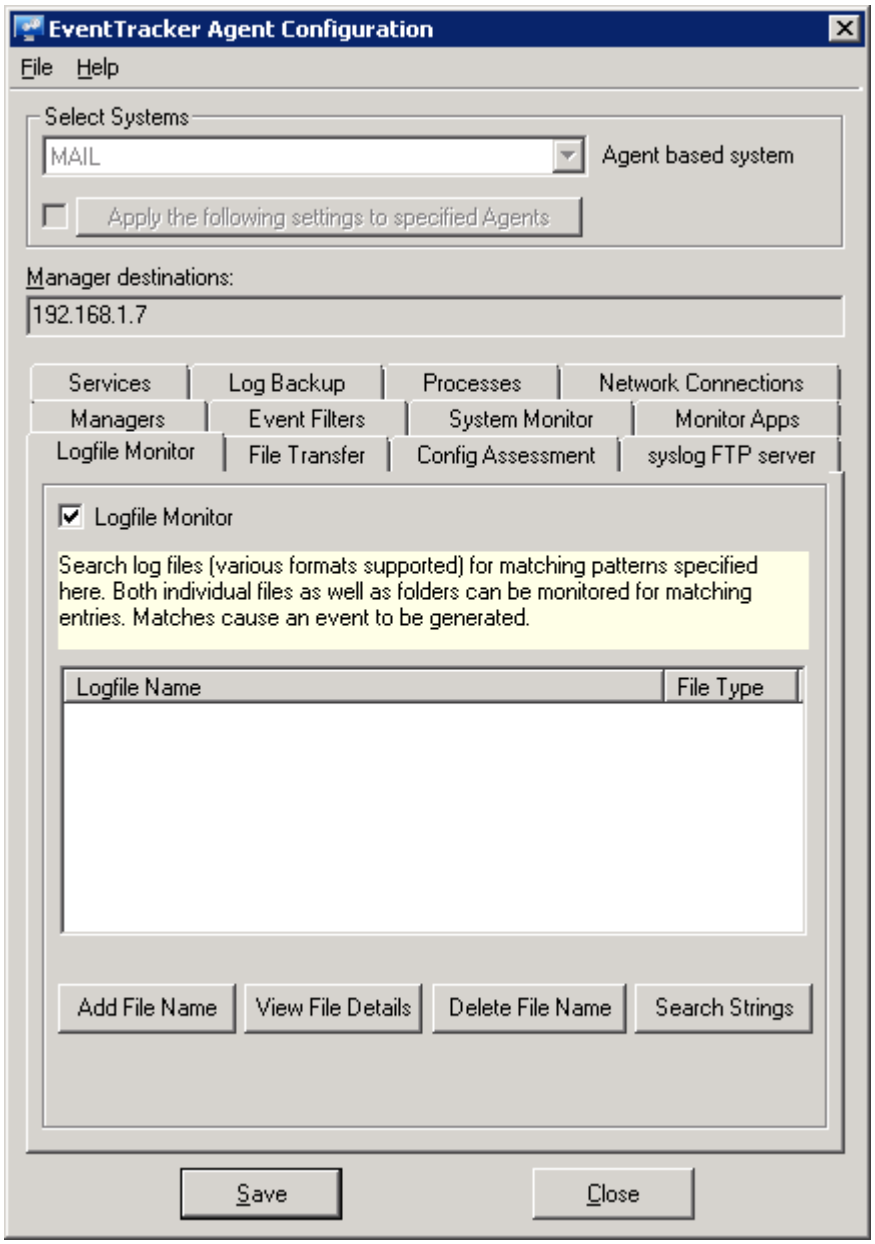

Figure 2

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

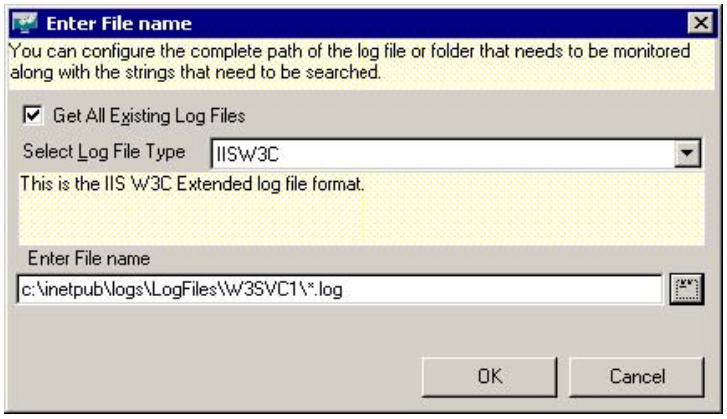

Figure 3

Log File Name displays in Logfile Monitor

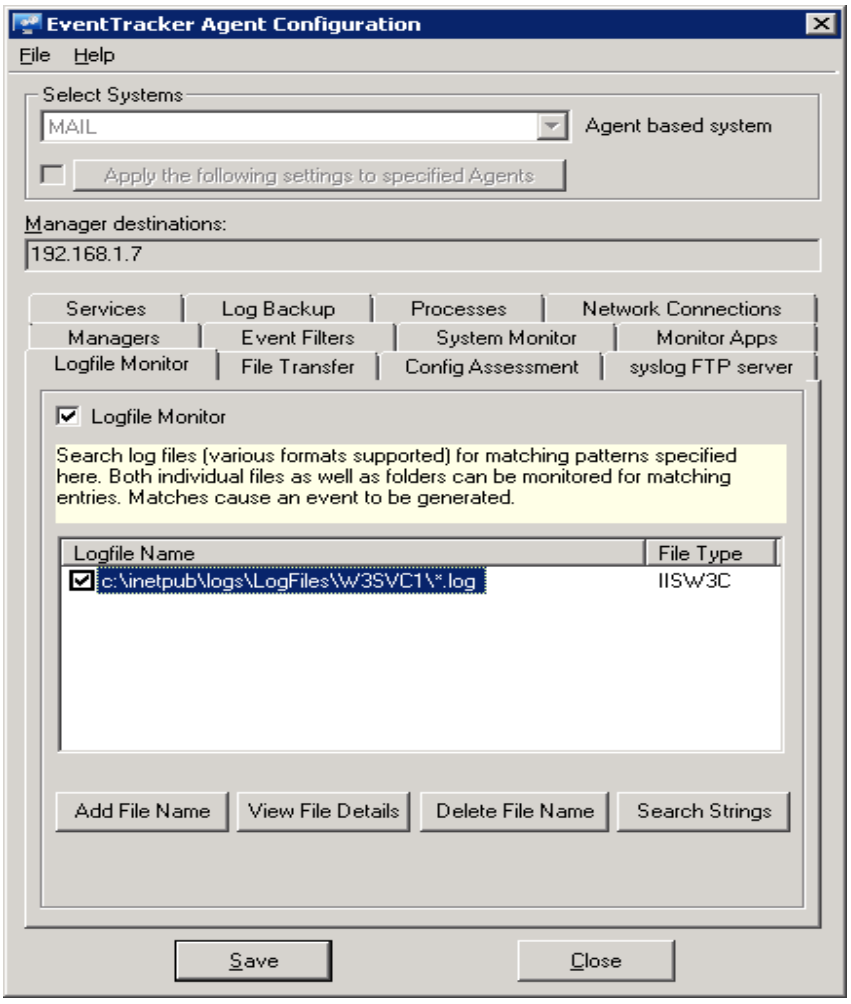
EventTracker Agent Configuration
File
Help
Select Systems
MAIL
Agent based system
Apply the following settings to specified Agents
Manager destinations:
192.168.1.7
Services
Log Backup
Processes
Network Connections
Managers
Event Filters
System Monitor
Monitor Apps
Logfile Monitor
File Transfer
Config Assessment
syslog FTP server
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
c:\inetpub\logs\LogFiles\W3SVC1*.log
IISW3C
Add File Name
View File Details
Delete File Name
Search Strings
Save
Close

Figure 4

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.

- 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.

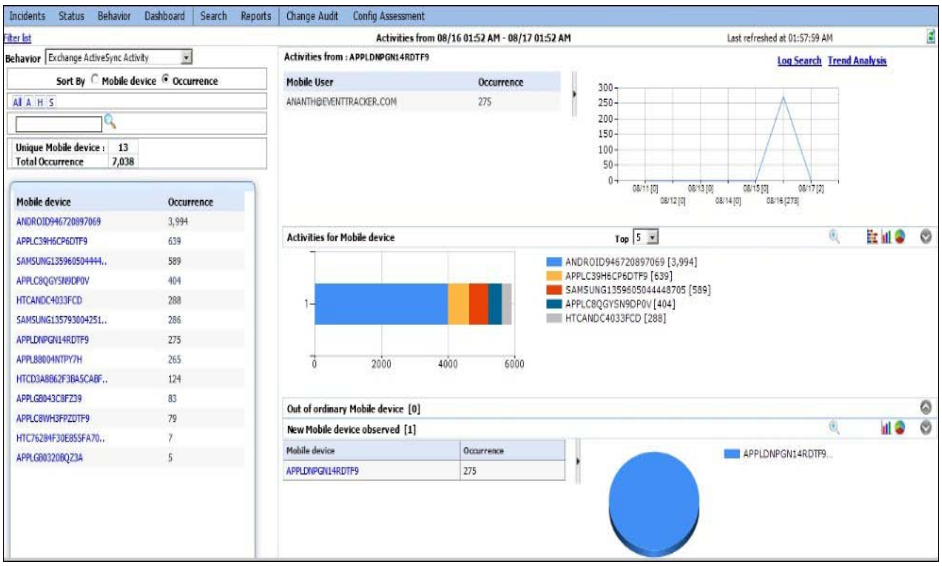

Figure 5

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

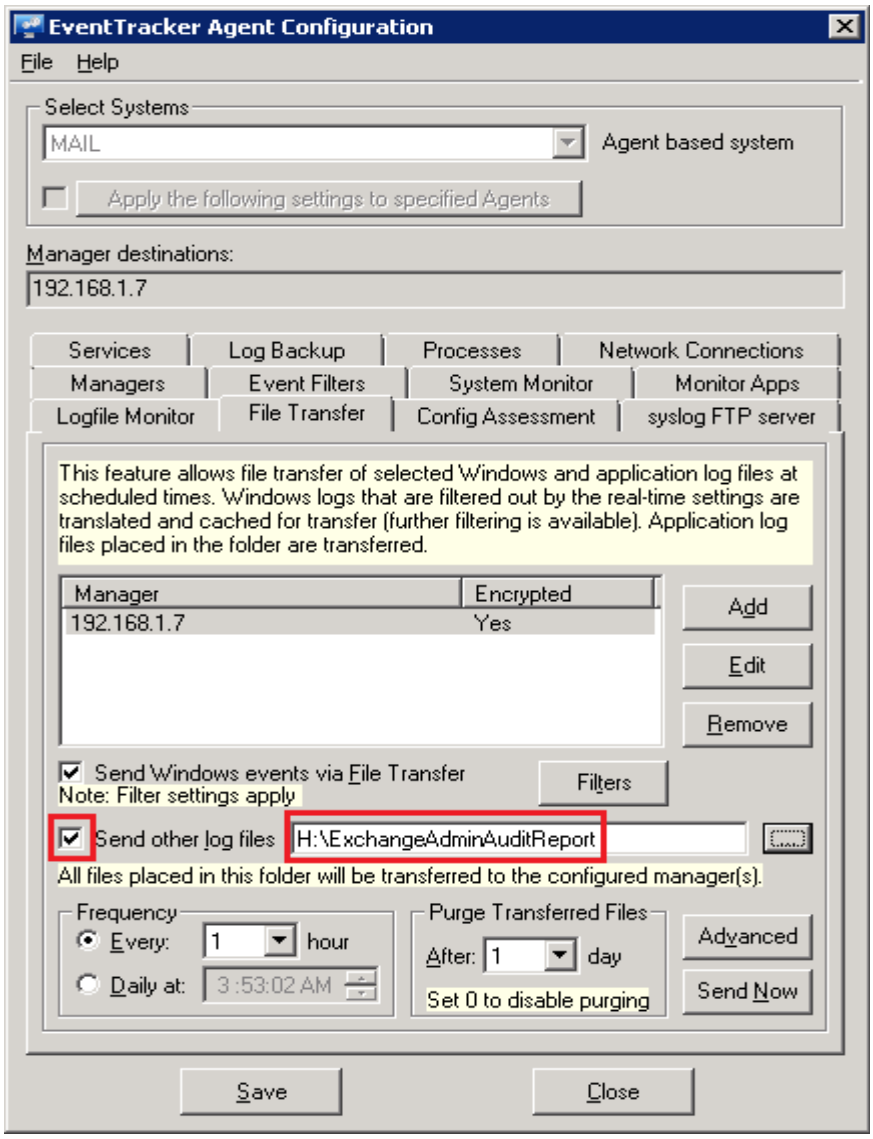

Figure 6

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.**

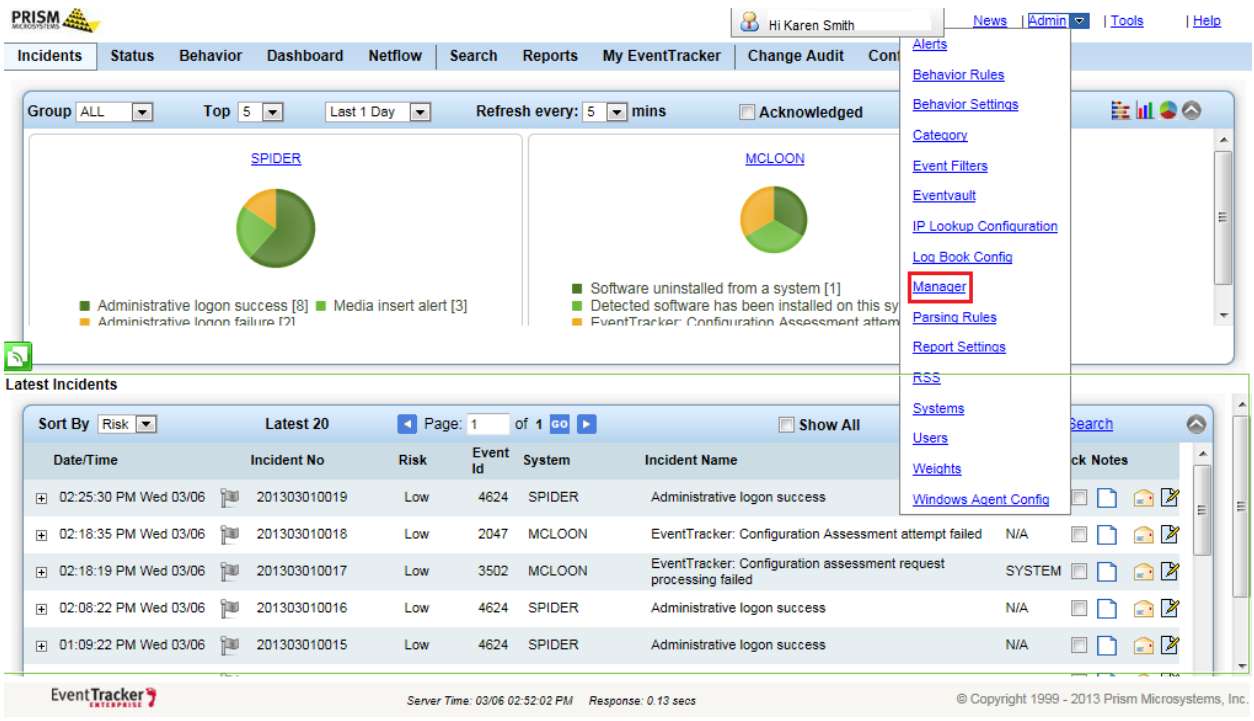

Figure 7

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.

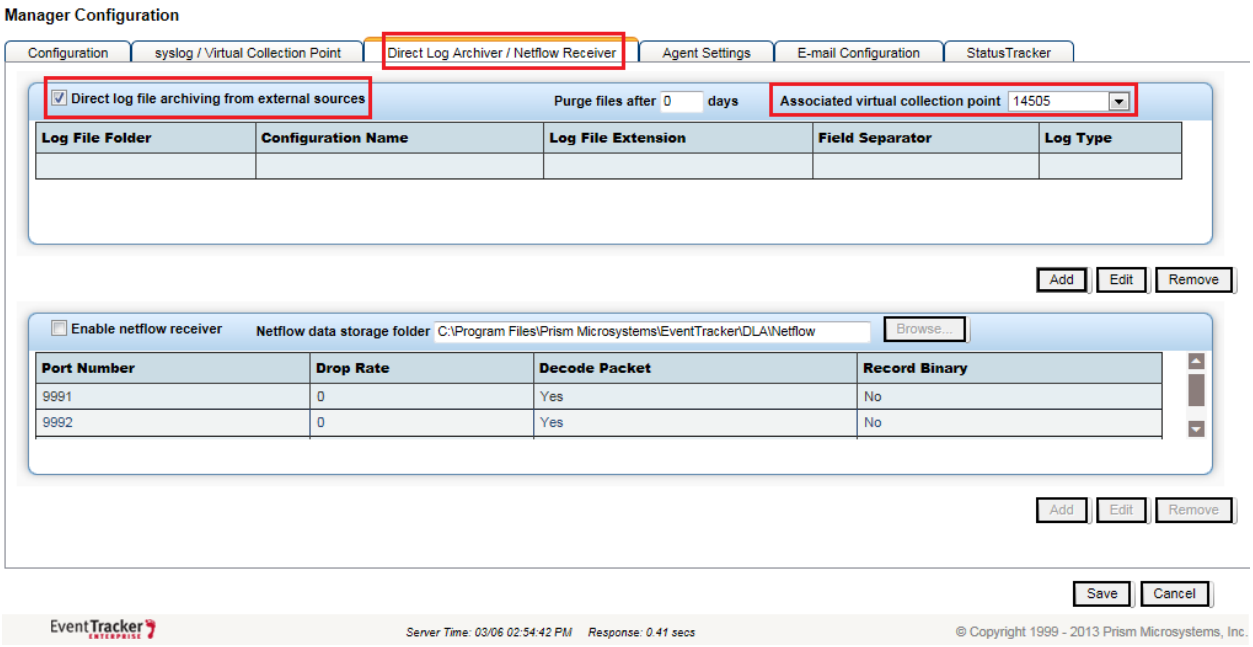

Figure 8

5. Select **Add**.
   Direct Archiver Configuration window displays.

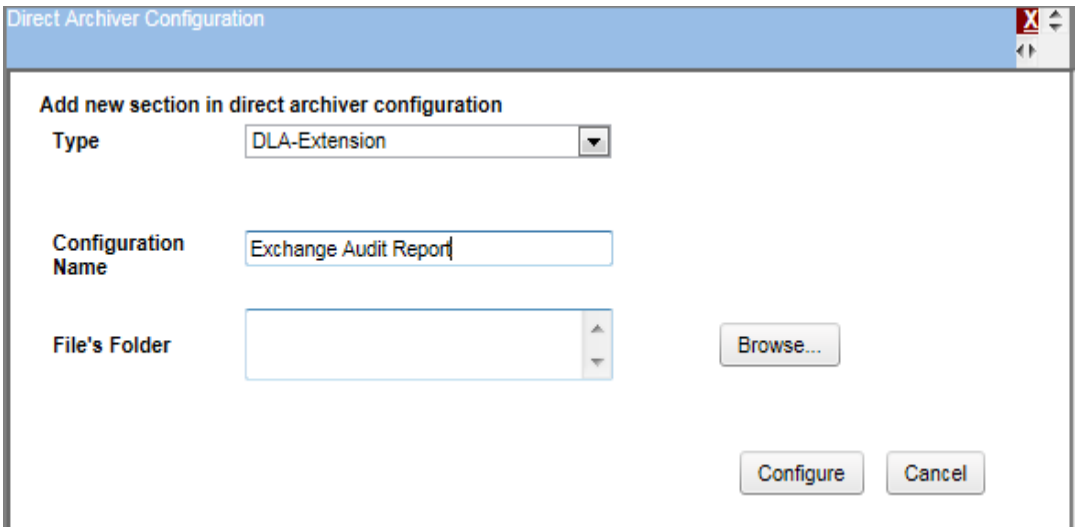

Figure 9

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.**

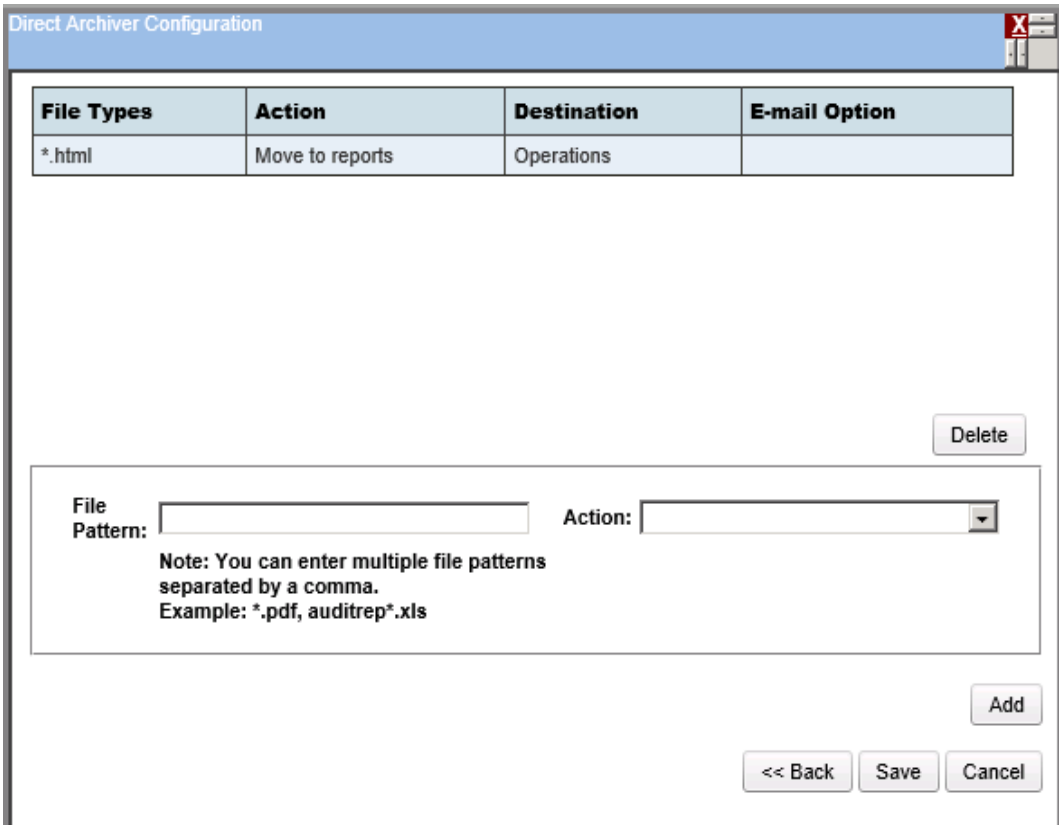

Figure 10

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.

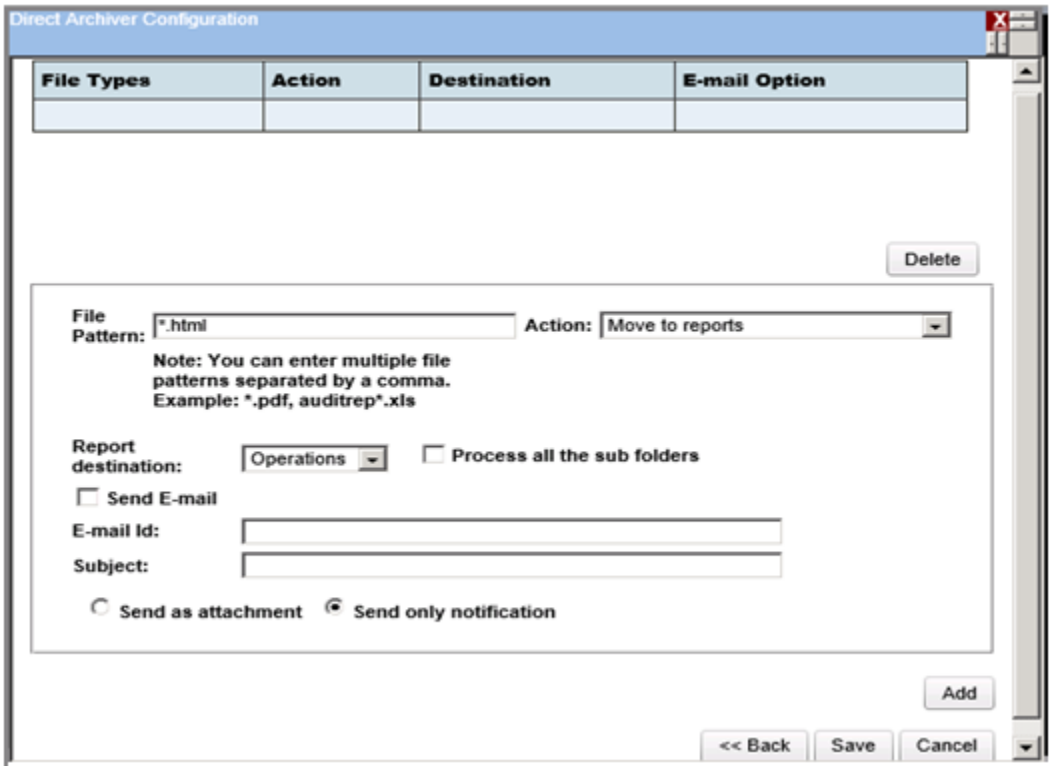

Figure 11

15. Click **Add**, and then click **Save**.

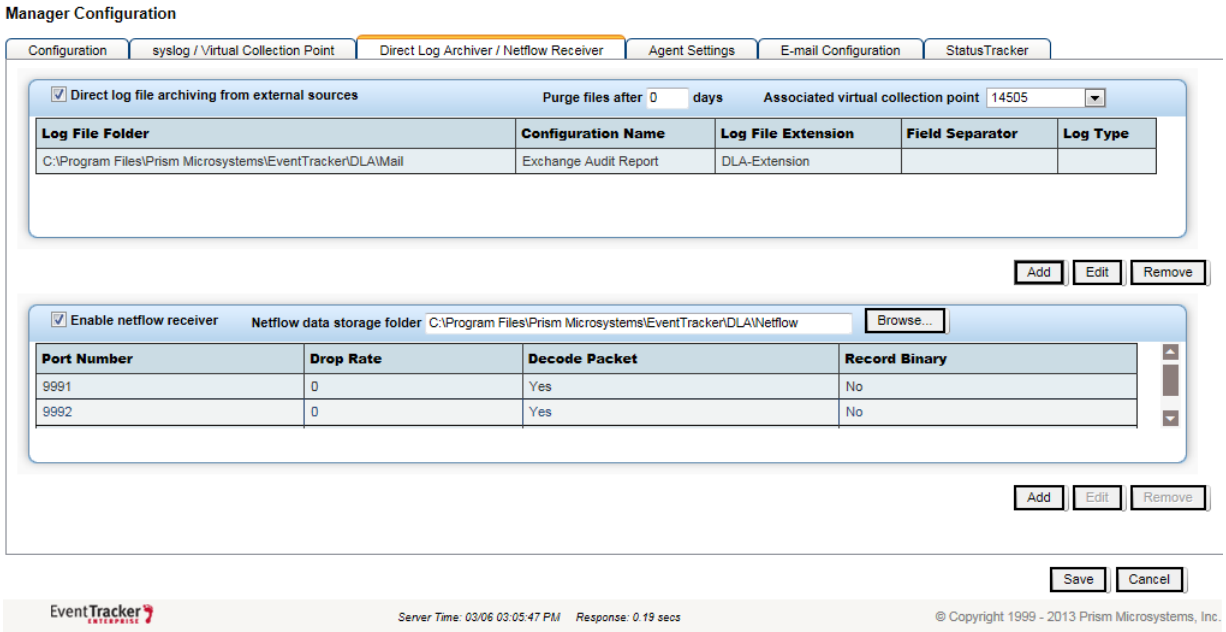

Figure 12

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.

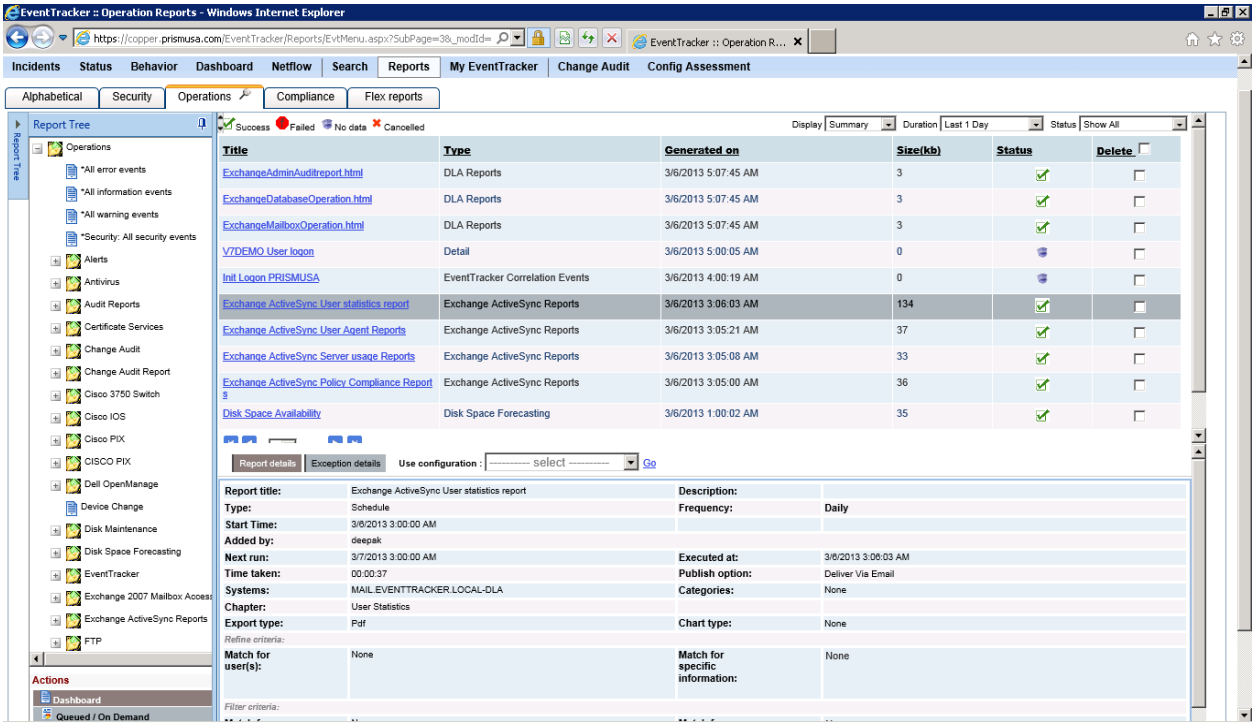

Figure 13

Sample report is shown below:

Exchange 2010 Administrator Audit Log Report					
Caller	**Run Date**	**Succeeded**	**Cmdlet**	**Parameters**	**Object Modified**
cmils	8/14/2012 12:35:55 PM	True	Set-CASMailbox	Identity : Pmilab.local/testusr1 ActiveSyncEnabled : False	Pmilab.local/testusr1
cmils	8/10/2012 5:12:27 AM	True	Disable-Mailbox	Identity : Pmilab.local/Jkaur	Pmilab.local/Jkaur
Matt	8/9/2012 11:55:46 PM	True	Remove-ActiveSyncDevice	Identity : 9d003e33-ebfa-4a22-99d6-a681e8797b93	Pmilab.local/Matt/ExchangeActiveSyncDevices/iPhone§Appl79051K7FA4S
Matt	8/9/2012 11:53:40 PM	True	Clear-ActiveSyncDevice	Cancel : False Identity : 9d003e33-ebfa-4a22-99d6-a681e8797b93	Pmilab.local/Matt/ExchangeActiveSyncDevices/iPhone§Appl79051K7FA4S
Sushan	8/6/2012 12:25:17 AM	True	Set-CASMailbox	Identity : 3f5e7e1d-18de-48a8-878c-ef37b0e1d78d ActiveSyncDebugLogging : True	Pmilab.local/Sushan

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