Integrate Microsoft Exchange Server

EventTracker v8.x and above

Publication Date: July 25, 2018
Abstract

EventTracker allows you to effectively manage your systems and provides operational efficiencies – reducing IT costs and freeing resources for other duties that increase the business value of your organization. EventTracker’s built-in knowledge base enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and Microsoft Exchange Server 2010, 2013 and 2016.

Audience

EventTracker users, who wish to monitor Microsoft Exchange Server.
# Table of Contents

Abstract .......................................................................................................................... 1  
Scope .............................................................................................................................. 1  
Audience ........................................................................................................................ 1  
Introduction ..................................................................................................................... 3  
Prerequisites .................................................................................................................... 3  
Enable Logging on Exchange Server ............................................................................. 3  
EventTracker Knowledge Pack ..................................................................................... 7  
  Flex Reports .................................................................................................................. 7  
  Categories ..................................................................................................................... 15  
  Knowledge Objects ....................................................................................................... 15  
Import Exchange Server knowledge pack into EventTracker ....................................... 16  
  Category ....................................................................................................................... 17  
  Parsing Rules ............................................................................................................... 18  
  Knowledge Objects ....................................................................................................... 18  
  Flex Reports .................................................................................................................. 20  
  Dashboards .................................................................................................................... 21  
Verify Exchange Server knowledge pack in EventTracker ........................................... 25  
  Categories ....................................................................................................................... 25  
  Knowledge Objects ....................................................................................................... 25  
  Flex Reports .................................................................................................................. 26  
  Dashboards .................................................................................................................... 27  
  Sample Flex Dashboards .............................................................................................. 28
Introduction

Microsoft Exchange Server is Microsoft's email, calendaring, contact, scheduling and collaboration platform deployed on the Windows Server operating system for use within a business or larger enterprise. Microsoft designed Exchange Server to give users access to the messaging platform on smartphones, tablets, desktops and web-based systems. Exchange users collaborate through calendar and document sharing. Storage and security features in the platform let organizations archive content, perform searches and execute compliance tasks.

With EventTracker you can monitor all your servers running Microsoft Exchange from a single view. EventTracker centrally consolidates all the event logs, SMTP logs and connectivity logs. Through consolidated logging you can monitor the performance, availability, and security of your Exchange servers. EventTracker can generate flex reports for mailbox access, mailbox changes, message tracking, audit activity, user permission and database changes by admin.

Prerequisites

- Exchange Server should be installed on Microsoft Windows Server 2010 R2 and later.
- EventTracker Agent should be installed on the respective server.
- PowerShell version 4.0 or later should be installed.
- PS session module should be installed.
- User Permissions needed.

Enable Logging on Exchange Server

1. Copy the MSExchange folder from <Installation Path>\Prism Microsystems\EventTracker\Knowledge Packs\Microsoft Exchange.
2. Save MSExchange folder to a desired location in exchange server, run executable file “MSExchange Integrator.exe” as Exchange Admin.
3. After launching integrator, a prerequisite check for Exchange server, EventTracker Agent and PowerShell 5.0 is done. If all the perquisites are available, then integrator will allow you to continue with the configuration.
4. Select the logs you want to monitor.
5. Under **Message Trace Logs**, you have an option of writing logs to either Default or Custom Location.

6. **Monitor Mailbox Operation** section gives you options to enable mailbox monitoring either for all users or selected users.
7. **Administrator Audit Logging** enables logging for admin activities.

8. Once all the required logging are selected, click **Next**.
9. On clicking **Next**, the configuration will be applied and relevant information about successful configuration or any errors that occur are written in the console.
10. Enter the **Exchange admin credentials**, this will create a task in task scheduler.

11. Once all the configuration are done, a **Configuration successful!** message is displayed.
Integrate Microsoft Exchange Server

Figure 7

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Exchange Server.

Flex Reports

- **Microsoft Exchange- Message tracking details** - This report gives the information about all mails sent or received through the exchange server.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Event SubType</th>
<th>Message Direction</th>
<th>Server Host Name</th>
<th>Server IP Address</th>
<th>Client Host Name</th>
<th>Client IP Address</th>
<th>Sender Address</th>
<th>Recipient Address</th>
<th>Message Subject</th>
<th>Message Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-08-21T14:09:31.568Z</td>
<td>RESOLVE</td>
<td>Incoming</td>
<td>centos-exchange1dc</td>
<td>10.12.23.56</td>
<td>mgeo-k01.puto.com</td>
<td>172.123.56.110</td>
<td><a href="mailto:pealmaster@puto.com">pealmaster@puto.com</a></td>
<td><a href="mailto:IT.Alers@puto.com">IT.Alers@puto.com</a></td>
<td>Systemic Messaging Gateway Alert - Service start after improper shutdown</td>
<td>2281</td>
</tr>
<tr>
<td>2018-08-21T14:09:31.568Z</td>
<td>TRANSFER</td>
<td>Originating</td>
<td>centos-exchange1dc</td>
<td>12.13.35.162</td>
<td>MDC-EX01.puto.com</td>
<td>193.36.16.68</td>
<td><a href="mailto:pealmaster@puto.com">pealmaster@puto.com</a></td>
<td>BP:Admin <a href="mailto:AS.BB@auto.com">AS.BB@auto.com</a> Meeting with CEO</td>
<td></td>
<td>2768</td>
</tr>
</tbody>
</table>

Figure 8
Sample logs:

### Figure 9

- **Microsoft Exchange - Mailbox changes by admin** - This report gives the information about mailbox changes by admin.
Sample logs:

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Role</th>
<th>Operation</th>
<th>Operation Status</th>
<th>User Changed</th>
<th>User Email Address</th>
<th>Folder Changed</th>
<th>User Workstation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 11 04:04:24 PM</td>
<td>contoso-server4dc</td>
<td>Carol</td>
<td>Delegate</td>
<td>SendAs</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td><a href="mailto:tender.helpdesk@poto.com">tender.helpdesk@poto.com</a></td>
<td>\Inbox</td>
<td>11.12.23.125</td>
</tr>
<tr>
<td>Jul 11 07:06:00 AM</td>
<td>contoso-server5dc</td>
<td>Nazir</td>
<td>Delegate</td>
<td>Create</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td><a href="mailto:nazir.C@poto.com">nazir.C@poto.com</a></td>
<td>\Calendar</td>
<td>11.23.25.125</td>
</tr>
</tbody>
</table>

- **Microsoft Exchange- Mailbox audit details** - This report gives the information about all mailbox audit activities.

**Figure 11**

**Figure 12**
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 12 01:08:07 PM</td>
<td>ENTRY: LastAccessed : 7/9/2018 8:12:27 AM OriginatingServer : \b0\b1\b2\b3\b4\b5 (14.03.0227.000) LogonUserName : \b0\b1\b2\b3\b4\b5\b6\b7\b8 LogonType : Delegate</td>
</tr>
</tbody>
</table>

- event_log_type: Application
- event_type: Information
- event_id: 3230
- event_source: EventTracker
- event_user_domain: N/A
- event_computer: Microsoft Exchange
- event_user_name: N/A
- event_description: ENTRY:

LastAccessed : 7/9/2018 8:12:27 AM
OriginatingServer : \b0\b1\b2\b3\b4\b5 (14.03.0227.000)
LogonUserName : \b0\b1\b2\b3\b4\b5\b6\b7\b8
LogonType : Delegate
Operation : SoftDelete
OperationResult : Succeeded
MailboxResolvedOwnerName : Tender HelpDesk
MailboxOwnerUPN : tender.helpdesk@wessoauto.com
FolderPathName : \\b0\b1\b2\b3\b4\b5\b6\b7\b8
ClientIpAddress : \\b0\b1\b2\b3\b4\b5

FILE:C:\Scripts\XP-Microsoft Exchange Server(update_S)\ExchangeReports\ExchangeMailboxAuditReport.csv
TYPE:CSV
FIELD:*

- **Microsoft Exchange- Mailbox access by owner** - This report gives the information about mailbox activities by owner.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Changed By Role</th>
<th>Operation Performed</th>
<th>Operation Status</th>
<th>User Changed</th>
<th>User Email Address</th>
<th>User Workstation</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/6/2018 2:07:47 PM</td>
<td>contoso-server4dc</td>
<td>Nazia</td>
<td>Owner</td>
<td>Create</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td>nazia <a href="mailto:C@puto.com">C@puto.com</a></td>
<td>11:53:56.231</td>
</tr>
<tr>
<td>7/6/2018 2:07:47 PM</td>
<td>contoso-server5dc</td>
<td>Nazia</td>
<td>Owner</td>
<td>SendAs</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td>nazia <a href="mailto:C@puto.com">C@puto.com</a></td>
<td>11:54:23.66</td>
</tr>
</tbody>
</table>
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
</table>
| Jul 12 01:08:07 PM | ENTRY: LastAccessed: 7/9/2018 2:07:47 PM OriginatingServer: \\local\admin (14:03:02:27.000) LogonUserName: \\local\admin LogonType: Owner event_log_type + Application event_type + Information event_id + 3280 event_source + EventTracker event_user_domain + N/A event_computer + Microsoft Exchange event_user_name + N/A event_description ENTRY: LastAccessed: 7/9/2018 2:07:47 PM OriginatingServer: \\local\admin (14:03:02:27.000) LogonUserName: \\local\admin LogonType: Owner Operation : SendAs OperationResult : Succeeded MailboxResolvedOwnerName : Tender HelpDesk MailboxOwnerUPN : tenderkhelals@gmail.com FolderPathName : C:\\MailboxAuditReport.csv TYPE: CSV FIELD: ^

- **Microsoft Exchange- Mailbox access by non-owner** - This report gives the information about mailbox activities by non-owner.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Changed By Role</th>
<th>Operation Performed</th>
<th>Operation Status</th>
<th>User Changed</th>
<th>User Email Address</th>
<th>Folder Changed</th>
<th>User Workstation</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/8/2018 5:49:32 PM</td>
<td>contoso-server4dc (14:03:02:27.000)</td>
<td>Nazila</td>
<td>Delegate</td>
<td>SendAs</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td><a href="mailto:nazilaC@pauto.com">nazilaC@pauto.com</a></td>
<td></td>
<td>12.56.23.56</td>
</tr>
<tr>
<td>7/8/2018 9:55:53 AM</td>
<td>contoso-server2dc (14:03:02:27.000)</td>
<td>Nazila</td>
<td>Delegate</td>
<td>Update</td>
<td>Succeeded</td>
<td>Tender HelpDesk</td>
<td><a href="mailto:tender.helpdesk@gmail.com">tender.helpdesk@gmail.com</a></td>
<td></td>
<td>12.56.23.45</td>
</tr>
</tbody>
</table>
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 12 01:08:07 PM</td>
<td>ENTRY: LastAccessed: 7/5/2018 3:38:04 PM OriginatingServer: mspm20097a (14.03.0227.000) LogonUserName: <a href="mailto:f@exchange.com">f@exchange.com</a> LogonType: Delegate</td>
</tr>
</tbody>
</table>

- **Microsoft Exchange - Admin audit details** - This report gives the information about admin audit activities.
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 11 04:04:24 PM</td>
<td>ENTRY: RunDate: 7/2/2018 6:03:22 PM OriginatingServer: \15.00.0516.025\ Caller: \15.00.0516.025\ ObjectModified: \15.00.0516.025\</td>
</tr>
</tbody>
</table>

- **Microsoft Exchange - Database changes by admin** - This report gives the information about database changes by admin.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Object Changed</th>
<th>Command Executed</th>
<th>Command Parameters</th>
<th>Execution Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/4/2018 1:53:27 PM</td>
<td>contoso-server4dc</td>
<td>mtpkp.com/Users/Joe Taylor</td>
<td>Mailbox Database 1365010500</td>
<td>Mount-Database</td>
<td>CmdletParameters/Parameter/Name True e=[Identity]; CmdletParameters/Parameter/Value e=[Mailbox Database 1365010500]</td>
<td></td>
</tr>
<tr>
<td>7/4/2018 3:39:16 PM</td>
<td>contoso-server3dc</td>
<td>mtpkp.com/Users/Joe Taylor</td>
<td>Mailbox Database 1365010565</td>
<td>New-Database</td>
<td>CmdletParameters/Parameter/Name True e=[Identity]; CmdletParameters/Parameter/Value e=[Mailbox Database 1365010565]</td>
<td></td>
</tr>
<tr>
<td>7/4/2018 3:38:19 PM</td>
<td>contoso-server4dc</td>
<td>mtpkp.com/Users/Joe Taylor</td>
<td>Mailbox Database 1365010500</td>
<td>Dismount-Database</td>
<td>CmdletParameters/Parameter/Name True e=[Identity]; CmdletParameters/Parameter/Value e=[Mailbox Database 1365010500]</td>
<td></td>
</tr>
</tbody>
</table>
Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 11 04:04:24 PM</td>
<td>ENTRY: RunDate: 7/2/2018 6:05:32 PM OriginatingServer: (15.00.0516.025) Caller: .\SystemTray\ServerName\\Users\User\User\Run\Executable</td>
</tr>
<tr>
<td></td>
<td>event_log_type: Application</td>
</tr>
<tr>
<td></td>
<td>event_type: Information</td>
</tr>
<tr>
<td></td>
<td>event_id: 3230</td>
</tr>
<tr>
<td></td>
<td>event_source: EventTracker</td>
</tr>
<tr>
<td></td>
<td>event_user_domain: N/A</td>
</tr>
<tr>
<td></td>
<td>event_computer: Microsoft Exchange</td>
</tr>
<tr>
<td></td>
<td>event_user_name: N/A</td>
</tr>
<tr>
<td></td>
<td>event_description: ENTR</td>
</tr>
</tbody>
</table>

- **Microsoft Exchange - User permission changes by admin** - This report gives the information about user permission changes by admin.

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Server Name</th>
<th>Changed By</th>
<th>Object Changed</th>
<th>Command Executed</th>
<th>Command Parameters</th>
<th>Execution Status</th>
</tr>
</thead>
</table>
Integrate Microsoft Exchange Server

Sample logs:

<table>
<thead>
<tr>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
</table>
| Jul 11 04:04 PM | ENTRY: RunDate: 7/2/2018 6:05:32 PM OriginatingServer: (15.00.0516.025) Caller: \paul\paul@\paul\ObjectModification|...

- **event_log_type**: Application
- **event_type**: Information
- **event_id**: 3230
- **event_source**: EventTracker
- **event_user_domain**: N/A
- **event_computer**: Microsoft Exchange
- **event_user_name**: N/A
- **event_description**: ENTRV:

RunDate: 7/2/2018 6:05:32 PM
OriginatingServer: (15.00.0516.025)
Caller: \paul\paul@\paul\ObjectModification
ObjectModified: \paul\paul\paul\Users\Bill Smith
CmdletName: Add-MailboxPermission
CmdletParameters: Parameter/Name: Identity, Parameter/Value: \paul\paul@\paul\User
Succeeded: True
FILE: e:\Official\Work Purpose\Report Logs\MS Exchange\ExchangeAdminAuditReport.csv
TYPE: CSV
FIELD: *

Figure 23

Categories

- **Microsoft Exchange: Admin Audit** - This category provides information related to admin audit activities.
- **Microsoft Exchange: Mailbox Audit** - This category provides information related to mailbox audit activities.
- **Microsoft Exchange: Message Tracking** - This category provides information related to all mails traversing the exchange server.

Knowledge Objects

- **Microsoft Exchange: Admin Audit** - This knowledge object helps to analyze logs related to admin audit activities.
- **Microsoft Exchange: Mailbox Audit** - This knowledge object helps to analyze logs related to mailbox audit activities.
- **Microsoft Exchange: Message Tracking** - This knowledge object helps to analyze logs related to all mails traversing the exchange server.

EventTracker
Actionable Security Intelligence
Import Exchange Server knowledge pack into EventTracker

**NOTE**: Import knowledge pack items in the following sequence:

- Categories
- Parsing Rules
- Knowledge Objects
- Flex Reports
- Dashboards

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.

![Export Import Utility](image)

*Figure 25*

2. Locate **Category_Microsoft Exchange.iscat** file, and then click the **Open** button.

3. To import categories, click the **Import** button. EventTracker displays success message.

![Export Import Utility](image)

*Figure 26*
4. Click OK, and then click the Close button.

Parsing Rules

1. Click **Token Value** option, and then click the browse button.

2. Locate **Token Value_Microsoft Exchange.istoken** file, and then click the Open button.
3. To import alerts, click the Import button.

Knowledge Objects

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.
2. Locate the **KO_Microsoft Exchange.etko** file.
3. Click the ‘Upload’ option.
4. Now select all the check box and then click on ‘Import’ option.
5. Knowledge objects are now imported successfully.

![File imported successfully.](image)

Figure 30

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

**Flex Reports**

On EventTracker Control Panel,

1. Click **Reports** option, and select new (*.etcrx) from the option.

![Export Import Utility](image)

Figure 31

2. Locate the **Reports_Microsoft Exchange.etcrx** file, and select all the check box.
3. Click the **Import** button to import the reports. EventTracker displays success message.

![Import reports success message](image)

Figure 32

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

![Dashboard configuration success message](image)

Figure 33

Dashboards

**Note:** If you have EventTracker Enterprise version **v9.0**, you can import dashboards.
1. Open EventTracker Enterprise.

![Figure 34](image)

2. Navigate to Dashboard>My Dashboard.

3. Click the ‘Import’ button to import the dashlets.

![Figure 35](image)
4. Locate the **Dashboard_Microsoft Exchange.etwd** file.
5. Click the ‘**Upload**’ option.

![Image of Import dashlets - Mozilla Firefox](image)

6. Now select all the check boxes and then click on ‘**Import**’ option.
   Dashlets are now imported successfully.
7. Click the ‘**Add**’ button to create a new dashboard.
8. Fill suitable Title and Description and click Save button.

9. Click ‘Customize’ to locate Microsoft Exchange dashlets and choose all imported dashlets for Microsoft Exchange Server.

10. Click ‘Add’ to include dashlets in dashboard.
Verify Exchange Server knowledge pack in EventTracker

Categories

1. Logon to EventTracker Enterprise.
2. Click Admin dropdown, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand Microsoft Exchange group folder to view the imported categories.

![Category Tree](category_tree.png)

Figure 39

Knowledge Objects

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Knowledge Objects.
2. In the Knowledge Object tree, expand Microsoft Exchange group folder to view the imported Knowledge objects.
Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select Report Configuration.

2. In Reports Configuration pane, select Defined option.
3. Click on the Microsoft Exchange group folder to view the imported Exchange Server reports.
Integrate Microsoft Exchange Server

Dashboards

1. Open EventTracker Enterprise in browser and logon.
2. Navigate to Dashboard>My Dashboard.
   My Dashboard pane is shown.
Sample Flex Dashboards

1. **Microsoft Exchange- Mailbox Changes by Admin**: This dashboard provides information related to mailbox changes by admin.

![Figure 44](image-url)

2. **Microsoft Exchange- Admin Audit Activity**: This dashboard provides information related to admin audit activates.

![Figure 45](image-url)
3. **Microsoft Exchange- Mailbox Access by Non-Owner**: This dashboard provides information related to mailbox activities by non-owner.

![Microsoft Exchange- Mailbox Access by Non-Owner]

*Figure 46*