

Integrate Microsoft Exchange Server

EventTracker v9.x and above

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 configuration details in this guide are consistent with EventTracker version 9.x and later, and Microsoft Exchange Server 2010, 2013, 2016 and later.

Audience

EventTracker users, who want to monitor Microsoft Exchange Server.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

| | | |
|-----|--|----|
| 1. | Introduction | 3 |
| 2. | Prerequisites | 3 |
| 3. | Enabling Message Trace, Mailbox audit and admin audit Logging on Exchange Server | 3 |
| 4. | Integrating Exchange with EventTracker | 5 |
| 5. | EventTracker Knowledge Pack | 6 |
| 5.1 | Reports | 6 |
| 5.2 | Categories | 14 |
| 5.3 | Dashboards | 14 |
| 6. | Importing Exchange Server knowledge pack into EventTracker | 16 |
| 6.1 | Category | 17 |
| 6.2 | Parsing Rules | 18 |
| 6.3 | Knowledge Objects | 19 |
| 6.4 | Reports | 20 |
| 6.5 | Dashboards | 22 |
| 7. | Verifying Exchange Server knowledge pack in EventTracker | 24 |
| 7.1 | Categories | 24 |
| 7.2 | Knowledge Objects | 25 |
| 7.3 | Reports | 26 |
| 7.4 | Dashboards | 26 |

1. 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 reports for mailbox access, mailbox changes, message tracking, audit activity, user permission and database changes by admin.

2. Prerequisites

- EventTracker Agent should be installed on the Exchange server.
- PowerShell version 5.0 or later should be installed.
- User with admin permission on Exchange Server.
- Enabling Message Tracking, Admin and mailbox auditing using Exchange Server.
- Enable remote PowerShell on user which integrator can use to fetch logs.

3. Enabling Message Trace, Mailbox audit and admin audit Logging on Exchange Server

1. Please contact EventTracker Support for script which will help to enabling logging on Exchange Server
2. Login to Exchange Server.
3. Open "Exchange Management Shell" in exchange Server.
4. Click **Start > Microsoft Exchange Server > Exchange Management Shell**.
5. Run downloaded script using following command
& "<Downloaded path>\EnableLogging.ps1"
6. Once you run above script, it will ask for folder location where you want to store message tracking logs

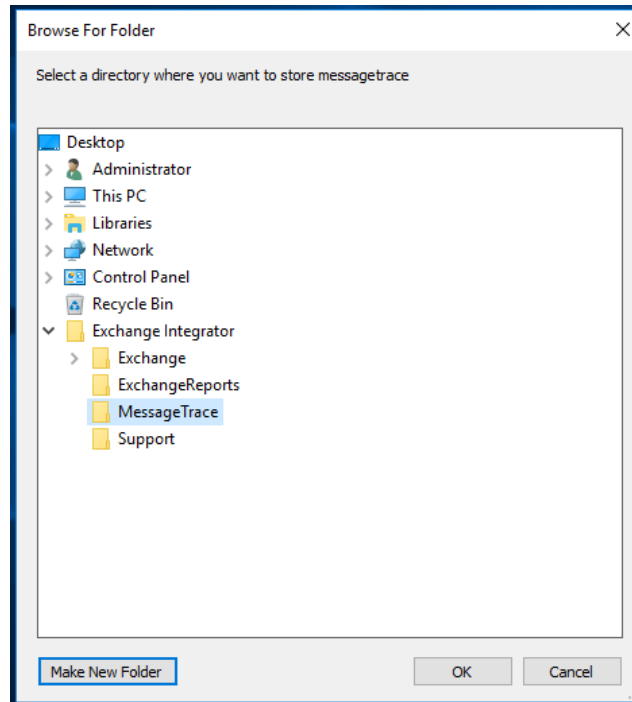


Figure 1

7. Select the folder or make new folder. Click **OK**.

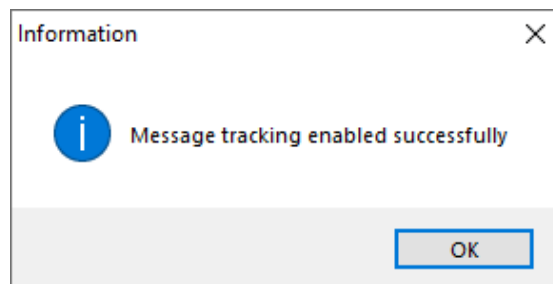


Figure 2

8. After message tracking is enabled, script will try to enable admin auditing on exchange sever. Once it's enabled, it will show following message

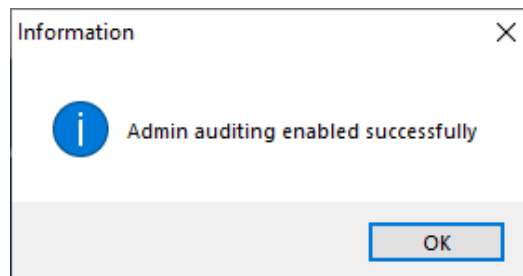


Figure 3

9. Now script will try to enable the mailbox auditing.
By default, script will enable the mailbox auditing for all the user.

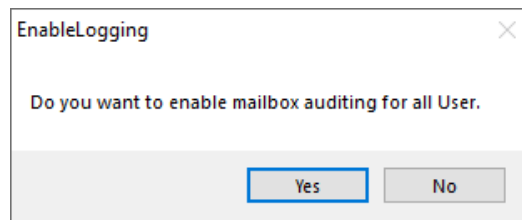


Figure 4

Once you click **Yes**, it will enable mailbox auditing for all the user.

If you don't want to enable mailbox auditing for all user. You can use following cmdlets in Exchange management shell for enabling mailbox auditing:

```
Set-Mailbox -Identity "Lahuara1" -AuditEnabled $true
```

You can also use CSV file of identity for enabling auditing logs. Following is the command set in Exchange management shell for enabling mailbox auditing using CSV

```
Import-Csv <path of CSV file> | %{  
Set-Mailbox -Identity $_ -AuditEnabled $true  
}
```

Above command will enable the auditing for users.

Now after doing above instruction, we are ready to integrate Exchange server to EventTracker

4. Integrating Exchange with EventTracker

Before running ExchangeIntegrator, we need to enable Remote PowerShell on one of the User which we can use to get logs from exchange sever. Following is the command used for enabling remote PowerShell in exchange server.

```
Set-user "Lahuara1" -RemotePowerShellEnabled $true
```

1. Run the integrator on any EventTracker agent machine.

Note: you can use Exchange Server also. Please install EventTracker agent on Exchange server.

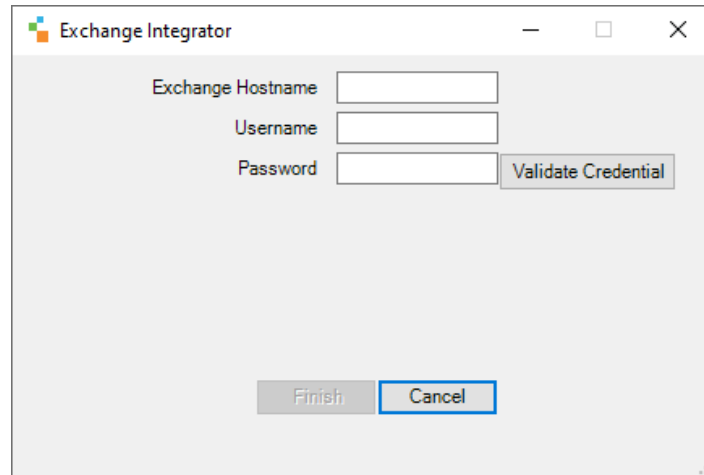


Figure 5

2. Provide the Exchange Server hostname, Username and password of identity on which remote PowerShell enabled.
3. Now, click on Validate credential to check the user.
4. If username/password is correct, it will enable the **Finish** button
5. Click **Finish** to complete the Integration.

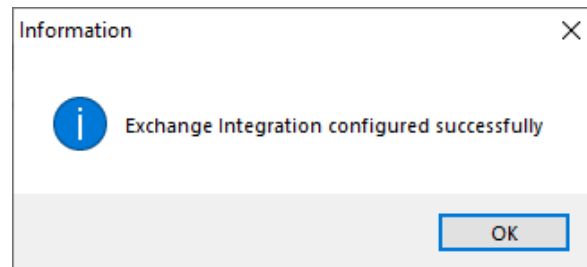


Figure 6

5. 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 to support Exchange Server.

5.1 Reports

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

| Event Time | Event SubType | Message Direction | Server Host Name | Server IP Address | Client Host Name | Client IP Address | Sender Address | Recipient Address | Message Subject | Message Size |
|--------------------------|---------------|-------------------|-------------------|-------------------|--------------------|-------------------|---------------------|-------------------------|--|--------------|
| 2018-06-21T14:09:31.569Z | RESOLVE | Incoming | contoso-server4dc | 10.12.23.56 | mpdc-r103.puto.com | 172.123.56.110 | postmaster@puto.com | IT.Alerts@puto.com | Symantec Messaging Gateway Alert - Service start after improper shutdown | 2281 |
| 2018-06-21T14:09:31.600Z | TRANSFER | Originating | contoso-server1dc | 12.13.23.152 | MPDC-EX01.puto.com | 182.35.36.56 | postmaster@puto.com | BP.Admin.AS.BP@puto.com | Meeting with CEO | 2708 |

Figure 7

Sample logs:

| Time | Description |
|--------------------|---|
| Jul 11 03:55:53 PM | ENTRY: #Fields: date-time : 2018-06-21T13:53:15.130Z client-ip : 172.123.56.110 client-hostname : mpdc-r103.puto.com server-ip : 10.12.23.56 server-hostname : contoso-server4dc |
| 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: #Fields: date-time : 2018-06-21T13:53:15.130Z client-ip : 172.123.56.110 client-hostname : mpdc-r103.puto.com server-ip : 10.12.23.56 server-hostname : MPDC-EX01 source-context : 08D5D47DB3611BBE;2018-06-21T13:53:14.428Z;0 connector-id : MPDC-EX01\Default MPDC-EX01 source : SMTP event-id : RECEIVE internal-message-id : 29924 message-id : <aac9313ba09f49c3a06c148cd5e0c42d@contoso-mail01.mcti.co.nz> recipient-address : access@puto.com recipient-status : total-bytes : 43598 recipient-count : 1 |

Figure 8

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

| Event Time | Server Name | Changed By | Object Changed | Command Executed | Command Parameters | Execution Status |
|---------------------|---------------------------------------|----------------------------|---|---------------------------|---|------------------|
| 7/4/2018 1:53:27 PM | contoso-server4dc (15.00.0516.025) | mtplkp.com/Users/ /gary | mtplkp.com/Users/gary | Set-Mailbox | Microsoft.Exchange.Data.MultiValuedProperty`1[Microsoft.Exchange.Data.AdminAuditLogCmdletParameter] | True |
| 7/4/2018 3:39:18 PM | contoso-server2dc (15.00.0516.025) | mtplkp.com/Users /gary | AuditLogSearch\73ef5eab-5856-47c1-96a1-bba8e291a0f7 | New-MailboxAuditLogSearch | Microsoft.Exchange.Data.MultiValuedProperty`1[Microsoft.Exchange.Data.AdminAuditLogCmdletParameter] | True |
| 7/4/2018 3:38:19 PM | contoso-server3dc (15.00.0516.025) | mtplkp.com/Users /gary | mtplkp.com/Users/John | Remove-Mailbox | Microsoft.Exchange.Data.MultiValuedProperty`1[Microsoft.Exchange.Data.AdminAuditLogCmdletParameter] | True |

Figure 9

Sample logs:

| Time | Description |
|--------------------|--|
| Jul 11 04:04:24 PM | ENTRY: RunDate: 7/2/2018 6:05:32 PM OriginatingServer: contoso-server4dc (15.00.0516.025) Caller: mtpkp.com/Users/mtplkp.com/... ObjectModified: mtpkp.com/... |
| 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: RunDate: 7/2/2018 6:05:32 PM OriginatingServer: contoso-server4dc (15.00.0516.025) Caller: mtpkp.com/Users/mtplkp.com/... ObjectModified: mtpkp.com/Users/mtplkp.com/... CmdletName: Set-Mailbox CmdletParameters: Microsoft.Exchange.Data.MultiValuedProperty`1[Microsoft.Exchange.Data.AdminAuditLogCmdletParameter] Succeeded: True FILE:e:\Official\Work Purpose\Report Logs\MS Exchange\ExchangeAdminAuditreport.csv TYPE:CSV FIELD: * |

Figure 10

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

| Event Time | Server Name | Changed By | Changed By Role | Operation Performed | Operation Status | User Changed | User Email Address | Folder Changed | User Workstation |
|---------------------|---------------------------------------|------------|-----------------|---------------------|------------------|-----------------|--------------------------|----------------|------------------|
| 7/9/2018 9:52:54 AM | contoso-server4dc (14.03.0227.000) | Carol | Delegate | SendAs | Succeeded | Tender HelpDesk | tender.helpdesk@puto.com | \Inbox | 11.12.23.125 |
| 7/9/2018 2:07:46 PM | contoso-server3dc (14.03.0227.000) | Nazia | Delegate | Update | Succeeded | Tender HelpDesk | nazia.C@puto.com | \Inbox | 11.23.23.241 |
| 7/9/2018 2:06:03 PM | contoso-server5dc (14.03.0227.000) | Nazia | Delegate | Create | Succeeded | Tender HelpDesk | nazia.C@puto.com | \Calendar | 11.23.25.12 |

Figure 11

Sample logs:

| Time | Description |
|--------------------|---|
| Jul 12 01:08:07 PM | ENTRY: LastAccessed : 7/9/2018 8:12:27 AM OriginatingServer : (14.03.0227.000) LogonUserDisplayName : LogonType : Deleg... |
| 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 : (14.03.0227.000) LogonUserDisplayName : LogonType : Delegate Operation : SoftDelete OperationResult : Succeeded MailboxResolvedOwnerName : Tender HelpDesk MailboxOwnerUPN : tender.helpdesk@pauto.com FolderPathName : \Inbox ClientIPAddress : FILE:C:\Scripts\KP-Microsoft Exchange Server(update_5)\ExchangeReports\ExchangeMailboxAuditreport.csv TYPE:CSV FIELD: * |

Figure 12

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

| Event Time | Server Name | Changed By | Changed By Role | Operation Performed | Operation Status | User Changed | User Email Address | User Workstation |
|---------------------|---------------------------------------|------------|-----------------|---------------------|------------------|-----------------|--------------------|------------------|
| 7/9/2018 2:07:47 PM | contoso-server4dc (14.03.0227.000) | Nazia | Owner | SendAs | Succeeded | Tender HelpDesk | nazia.C@pauto.com | 11.53.56.231 |
| 7/9/2018 2:07:47 PM | contoso-server5dc (14.03.0227.000) | Nazia | Owner | Create | Succeeded | Tender HelpDesk | nazia.C@pauto.com | 11.54.23.56 |

Figure 13

Sample logs:

| Time | Description |
|--------------------|--|
| Jul 12 01:08:07 PM | ENTRY: LastAccessed : 7/9/2018 2:07:47 PM OriginatingServer : contoso-server4dc (14.03.0227.000) LogonUserDisplayName : contoso\Tender HelpDesk LogonType : Owner... |
| 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 2:07:47 PM OriginatingServer : contoso-server4dc (14.03.0227.000) LogonUserDisplayName : contoso\Tender HelpDesk LogonType : Owner Operation : SendAs OperationResult : Succeeded MailboxResolvedOwnerName : Tender HelpDesk MailboxOwnerUPN : tender.helpdesk@puto.com FolderPathName : ClientIPAddress : 12.56.23.56 FILE:C:\Scripts\KP-Microsoft Exchange Server(update_5)\ExchangeReports\ExchangeMailboxAuditreport.csv TYPE:CSV FIELD: * |

Figure 14

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

| Event Time | Server Name | Changed By | Changed By Role | Operation Performed | Operation Status | User Changed | User Email Address | Folder Changed | User Workstation |
|---------------------|------------------------------------|------------|-----------------|---------------------|------------------|-----------------|--------------------------|----------------|------------------|
| 7/6/2018 5:49:32 PM | contoso-server4dc (14.03.0227.000) | Nazia | Delegate | SendAs | Succeeded | Tender HelpDesk | nazia.C@puto.com | | 12.56.23.56 |
| 7/9/2018 9:53:53 AM | contoso-server2dc (14.03.0227.000) | Nazia | Delegate | Update | Succeeded | Tender HelpDesk | tender.helpdesk@puto.com | \Inbox | 12.56.23.45 |

Figure 15

Sample logs:

| Time | Description |
|--------------------|--|
| Jul 12 01:08:07 PM | ENTRY: LastAccessed : 7/5/2018 3:38:04 PM OriginatingServer : 14.03.0227.000 LogonUserDisplayName : LogonType : Deleg... |
| 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 : 7/5/2018 3:38:04 PM OriginatingServer : 14.03.0227.000 LogonUserDisplayName : LogonType : Delegate Operation : SendAs OperationResult : Succeeded MailboxResolvedOwnerName : Tender HelpDesk MailboxOwnerUPN : FolderPathName : ClientIPAddress : FILE:C:\Scripts\KP-Microsoft Exchange Server(update_5)\ExchangeReports\ExchangeMailboxAuditreport.csv TYPE:CSV FIELD: * |

Figure 16

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

| Event Time | Server Name | Changed By | Object Changed | Command Executed | Command Parameters | Execution Status |
|---------------------|---------------------------------------|----------------------------|---|---------------------------|--|------------------|
| 7/4/2018 1:50:14 PM | contoso-server4dc (15.00.0516.025) | mtplkp.com/Users/ Kenny | mtplkp.com/Users/Kenny | Set-Mailbox | Microsoft.Exchange.Data.MultiValuedProperty' 1[Microsoft.Exchange.Data.AdminAuditLogCmdletParameter] | True |
| 7/4/2018 3:43:50 PM | contoso-server5dc (15.00.0516.025) | mtplkp.com/Users/ Kenny | mtplkp.com/John | New-Mailbox | Microsoft.Exchange.Data.MultiValuedProperty' 1[Microsoft.Exchange.Data.AdminAuditLogCmdletParameter] | True |
| 7/4/2018 3:39:18 PM | contoso-server6dc (15.00.0516.025) | mtplkp.com/Users/ Kenny | AuditLogSearch\73ef5eab-5856-47c1-96a1-bba8e291a0f7 | New-MailboxAuditLogSearch | Microsoft.Exchange.Data.MultiValuedProperty' 1[Microsoft.Exchange.Data.AdminAuditLogCmdletParameter] | True |

Figure 17

Sample logs:

| Time | Description |
|--------------------|---|
| Jul 11 04:04:24 PM | ENTRY: RunDate : 7/2/2018 6:05:32 PM OriginatingServer : 15.00.0516.025 Caller : mtlpkp.com/Users/mtplkp.com/ Joe Taylor ObjectModified : mtlpkp.com/Users/mtplkp.com/ Joe Taylor |
| 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: RunDate : 7/2/2018 6:05:32 PM OriginatingServer : 15.00.0516.025 Caller : mtlpkp.com/Users/mtplkp.com/ Joe Taylor ObjectModified : mtlpkp.com/Users/mtplkp.com/ Joe Taylor CmdletName : Set-Mailbox CmdletParameters : Microsoft.Exchange.Data.MultiValuedProperty`1[Microsoft.Exchange.Data.AdminAuditLogCmdletParameter] Succeeded : True FILE:e:\Official\Work Purpose\Report Logs\MS Exchange\ExchangeAdminAuditreport.csv TYPE:CSV FIELD: * |

Figure 18

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

| Event Time | Server Name | Changed By | Object Changed | Command Executed | Command Parameters | Execution Status |
|---------------------|------------------------------------|------------------------------|-----------------------------|-------------------|---|------------------|
| 7/4/2018 1:53:27 PM | contoso-server4dc (15.00.0516.025) | mtplkp.com/Users/ Joe Taylor | Mailbox Database 1365010500 | Mount-Database | CmdletParameters/Parameter/Name= [Identity]; CmdletParameters/Parameter/Value= [Mailbox Database 1365010500] | True |
| 7/4/2018 3:39:18 PM | contoso-server3dc (15.00.0516.025) | mtplkp.com/Users/ Joe Taylor | Mailbox Database 1365010565 | New-Database | CmdletParameters/Parameter/Name= [Identity]; CmdletParameters/Parameter/Value= [Mailbox Database 1365010565] | True |
| 7/4/2018 3:38:19 PM | contoso-server4dc (15.00.0516.025) | mtplkp.com/Users/ Joe Taylor | Mailbox Database 1365010500 | Dismount-Database | CmdletParameters/Parameter/Name= [Identity]; CmdletParameters/Parameter/Value= [Mailbox Database 1365010500] | True |

Figure 19

Sample logs:

| Time | Description |
|--------------------|--|
| Jul 11 04:04:24 PM | ENTRY: RunDate : 7/2/2018 6:05:32 PM OriginatingServer : contoso-server4dc (15.00.0516.025) Caller : mtlpkp.com/Users/Bill Smith ObjectModified : Mailbox Database 1365010565 |
| 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: RunDate : 7/2/2018 6:05:32 PM OriginatingServer : contoso-server4dc (15.00.0516.025) Caller : mtlpkp.com/Users/Bill Smith ObjectModified : Mailbox Database 1365010565 CmdletName : Mount-Database CmdletParameters : CmdletParameters/Parameter/Name= [Identity]; CmdletParameters/Parameter/Value= [Mailbox Database 1365010500] Succeeded : True FILE: \\Official\Work Purpose\Report Logs\MS Exchange\ExchangeAdminAuditreport.csv TYPE: CSV FIELD: * |

Figure 20

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

| Event Time | Server Name | Changed By | Object Changed | Command Executed | Command Parameters | Execution Status |
|---------------------|------------------------------------|------------------------------|-----------------------|-----------------------|--|------------------|
| 7/4/2018 1:53:27 PM | contoso-server4dc (15.00.0516.025) | mtlpkp.com/Users/ Bill Smith | mtlpkp.com/Users/John | Add-MailboxPermission | [Identity]; CmdletParameters/Parameter/Value= [Bill Smith]; CmdletParameters/Parameter/Name= [User]; CmdletParameters/Parameter/Value= [John]; CmdletParameters/Parameter/Name= [AccessRights]; CmdletParameters/Parameter/Value= [FullAccess] | True |
| 7/4/2018 3:39:18 PM | contoso-server4dc (15.00.0516.025) | mtlpkp.com/Users/ Bill Smith | mtlpkp.com/Users/Gary | Add-MailboxPermission | [Identity]; CmdletParameters/Parameter/Value= [Bill Smith]; CmdletParameters/Parameter/Name= [User]; CmdletParameters/Parameter/Value= [Gary]; CmdletParameters/Parameter/Name= [AccessRights]; CmdletParameters/Parameter/Value= [FullAccess] | True |

Figure 21

Sample logs:

| Time | Description |
|--------------------|--|
| Jul 11 04:04:24 PM | ENTRY: RunDate : 7/2/2018 6:05:32 PM OriginatingServer : 15.00.0516.025 Caller : 15.00.0516.025 ObjectModified : 15.00.0516.025 |
| 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: RunDate : 7/2/2018 6:05:32 PM OriginatingServer : 15.00.0516.025 Caller : 15.00.0516.025 ObjectModified : 15.00.0516.025 CmdletName : Add-MailboxPermission CmdletParameters : CmdletParameters/Parameter/Name= [Identity]; CmdletParameters/Parameter/Value= [Bill Smith]; CmdletParameters/Parameter/Name= [User]; CmdletParameters/Parameter/Value= [15.00.0516.025]; CmdletParameters/Parameter/Name= [AccessRights]; Succeeded : True FILE: e:\Official\Work Purpose\Report Logs\MS Exchange\ExchangeAdminAuditreport.csv TYPE: CSV FIELD: * |

Figure 22

5.2 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.

5.3 Dashboards

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

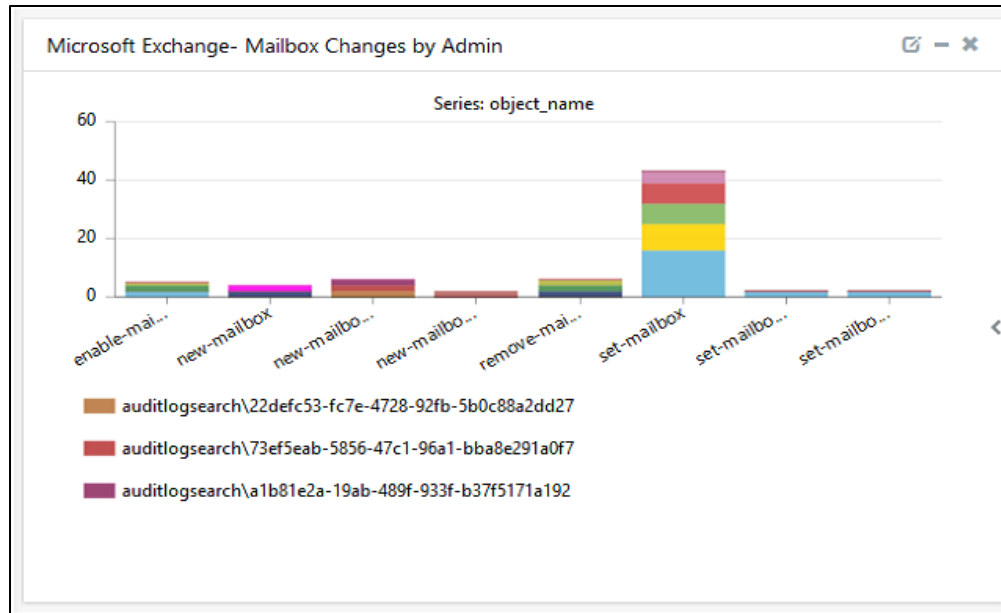


Figure 23

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

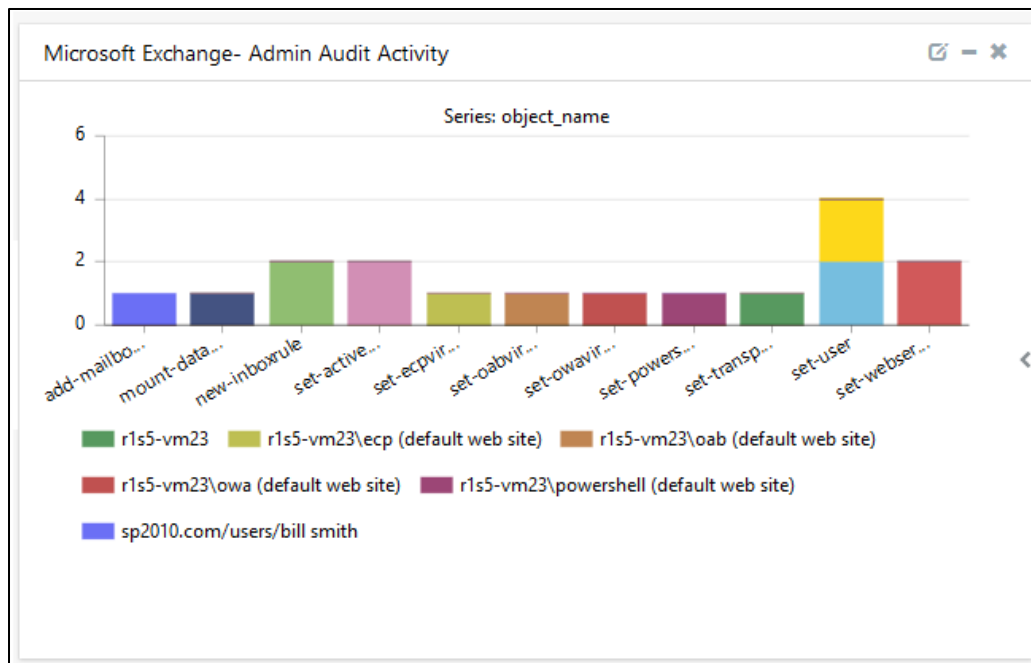


Figure 24

- **Microsoft Exchange- Mailbox Access by Non-Owner:** This dashboard provides information related to mailbox activities by non-owner.

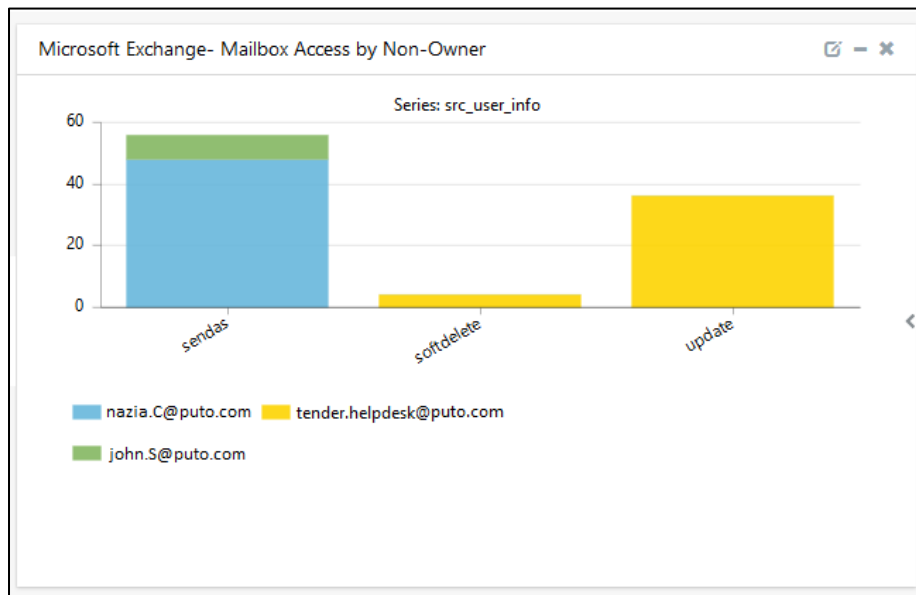


Figure 25

6. Importing 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**.

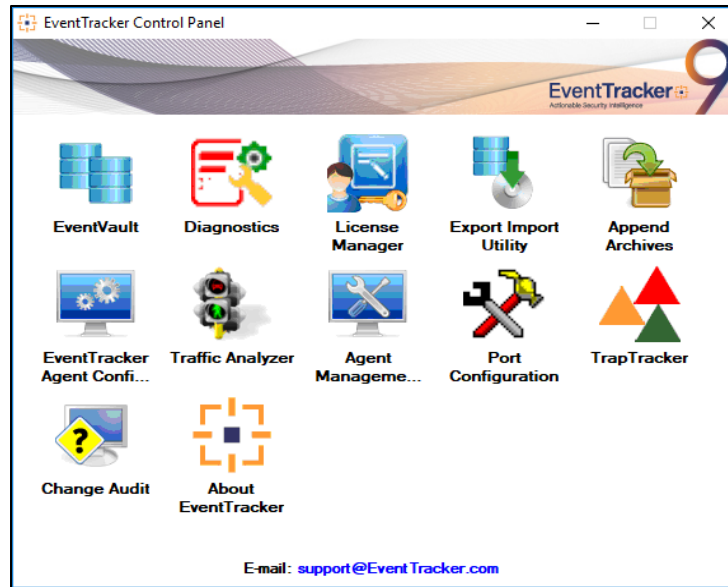



Figure 26

3. Click the **Import** tab.

6.1 Category

1. Click **Category** option, and then click **Browse** .

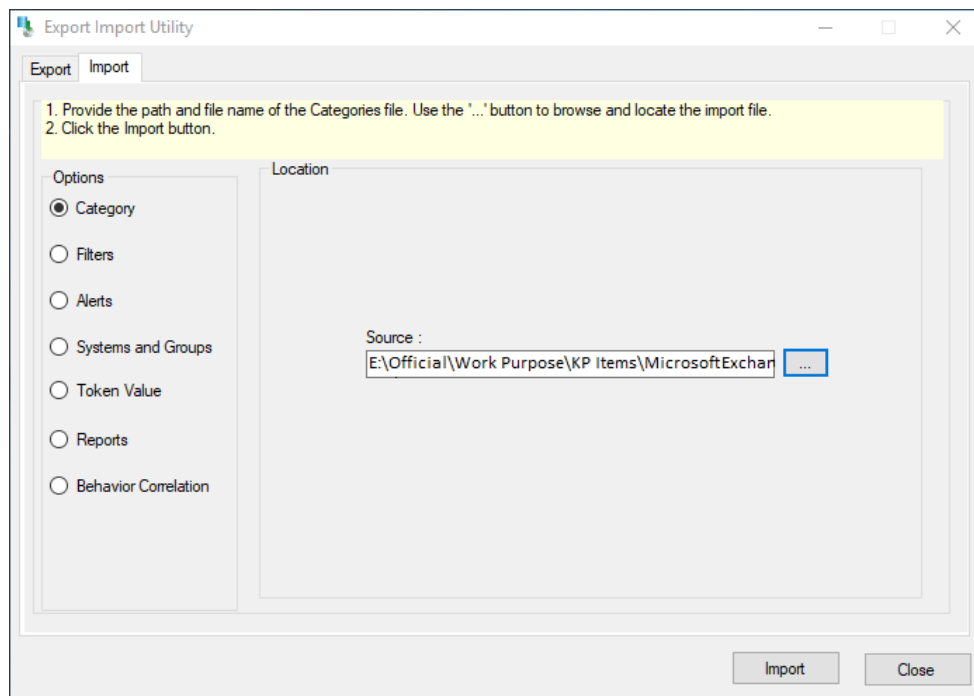


Figure 27

2. Locate **Category_Microsoft Exchange.iscat** file, and then click **Open**.
3. To import categories, click **Import**. EventTracker displays success message.

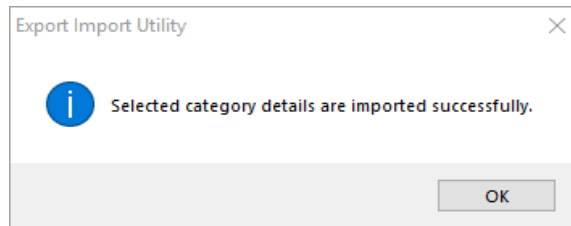


Figure 28

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

6.2 Parsing Rules

1. Click **Token Value** option, and then click Browse.

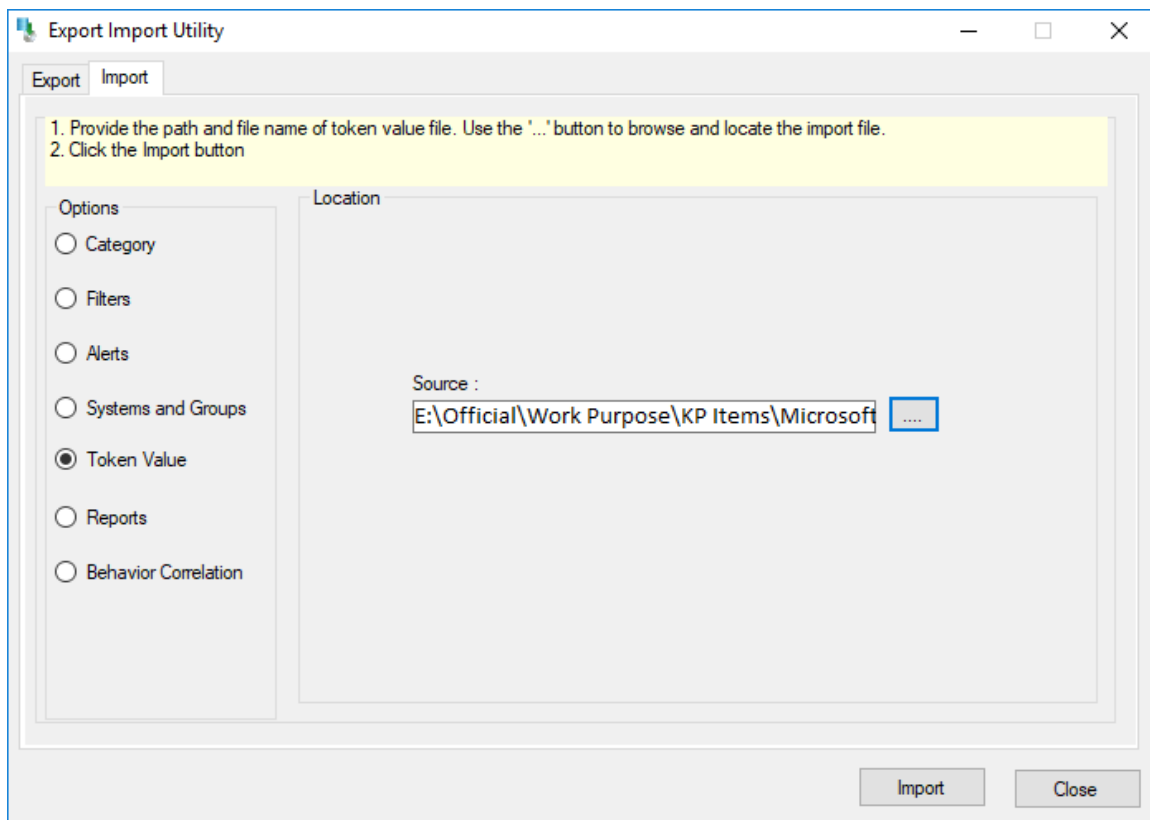


Figure 29

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

6.3 Knowledge Objects

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
2. Locate the **KO_Microsoft Exchange.etko** file.

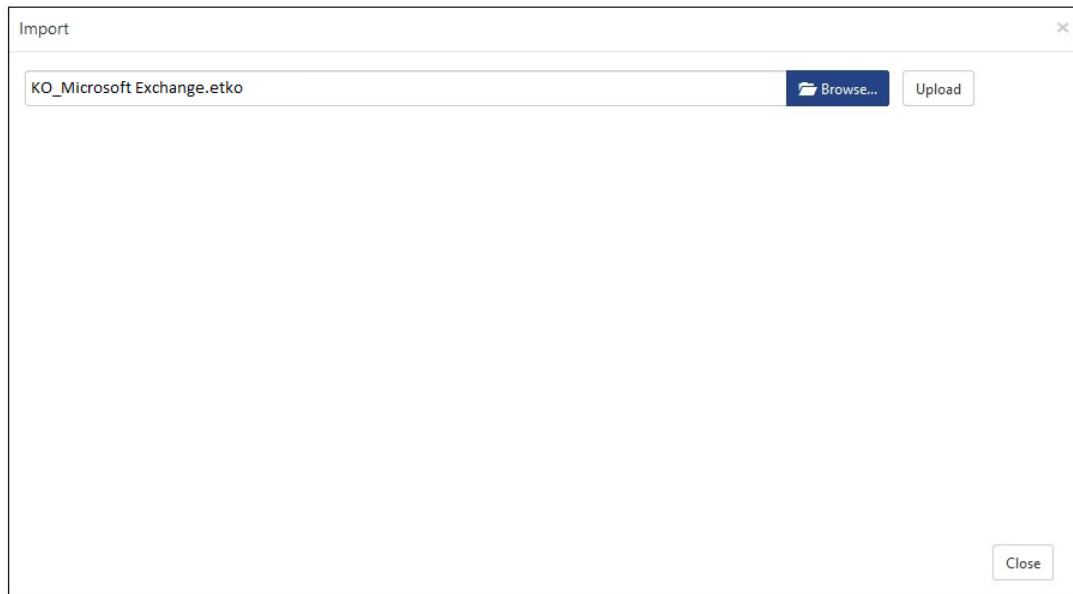


Figure 30

3. Click the **'Upload'** option.
4. Now select all the check box and then click on **'Import'** option.

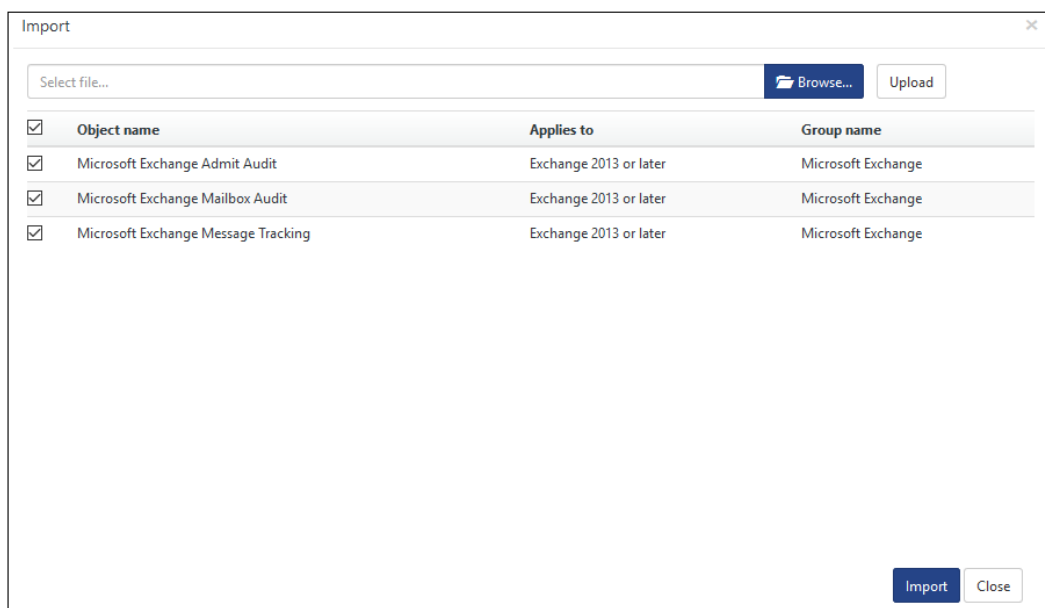


Figure 31

- Knowledge objects are now imported successfully.

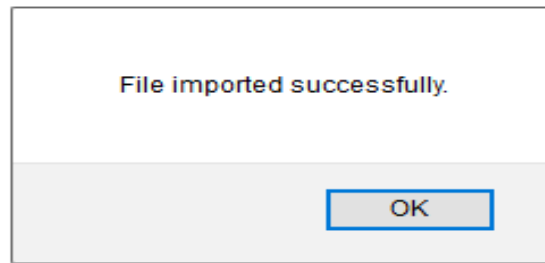


Figure 32

- Click **OK**, and then click **Close**.

6.4 Reports

On EventTracker Control Panel,

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

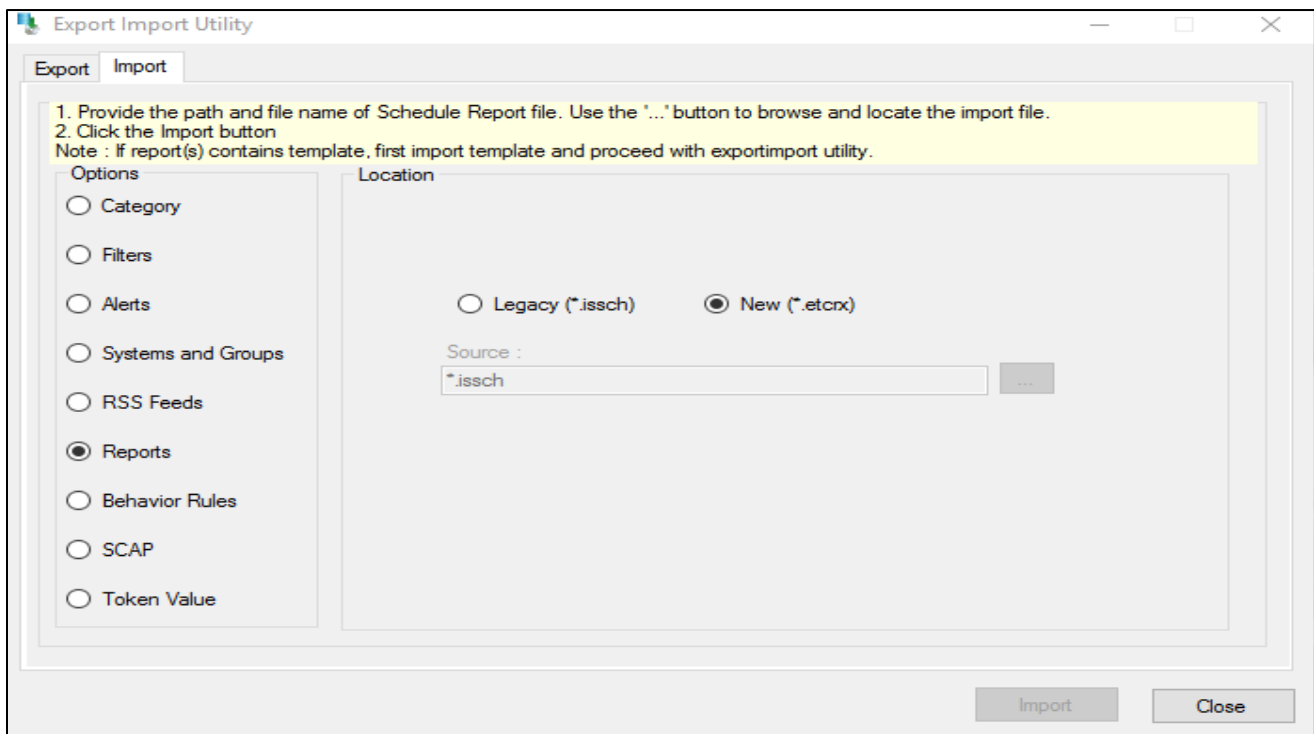


Figure 33

- Locate the **Reports_Microsoft Exchange.etcrx** file and select all the check box.

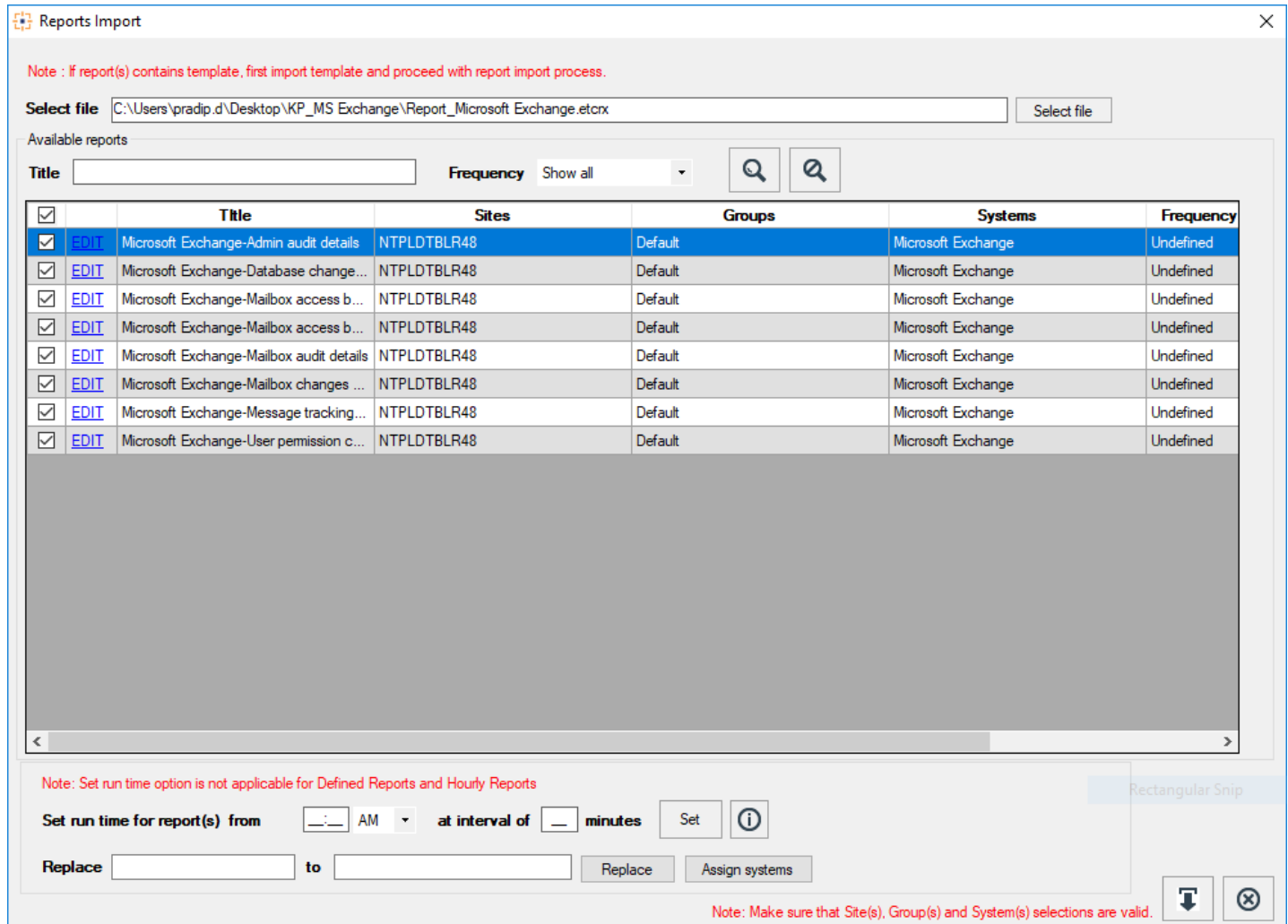


Figure 34

- Click **Import** to import the reports. EventTracker displays success message.

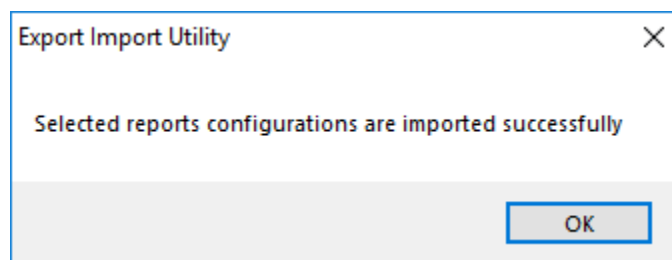


Figure 35

- Click **OK**, and then click **Close**.

6.5 Dashboards

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

1. Open **EventTracker**.

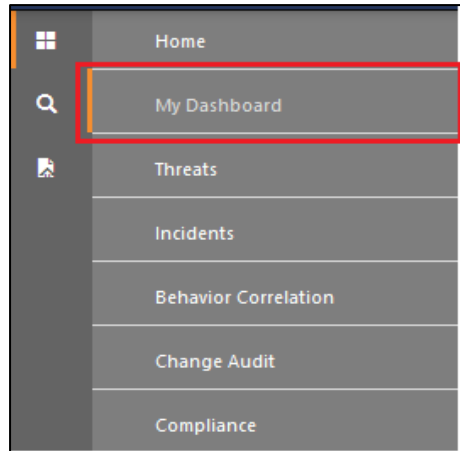



Figure 36

2. Navigate to **Dashboard>My Dashboard**.
3. Click the '**Import**'  to import the dashlets.

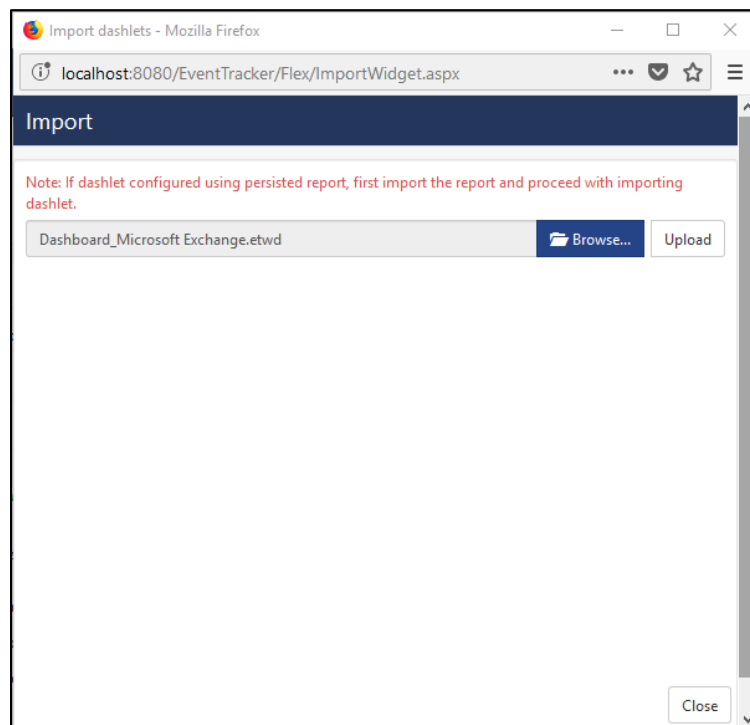


Figure 37

4. Locate the **Dashboard_Microsoft Exchange.etwd** file.
5. Click the **'Upload'** option.

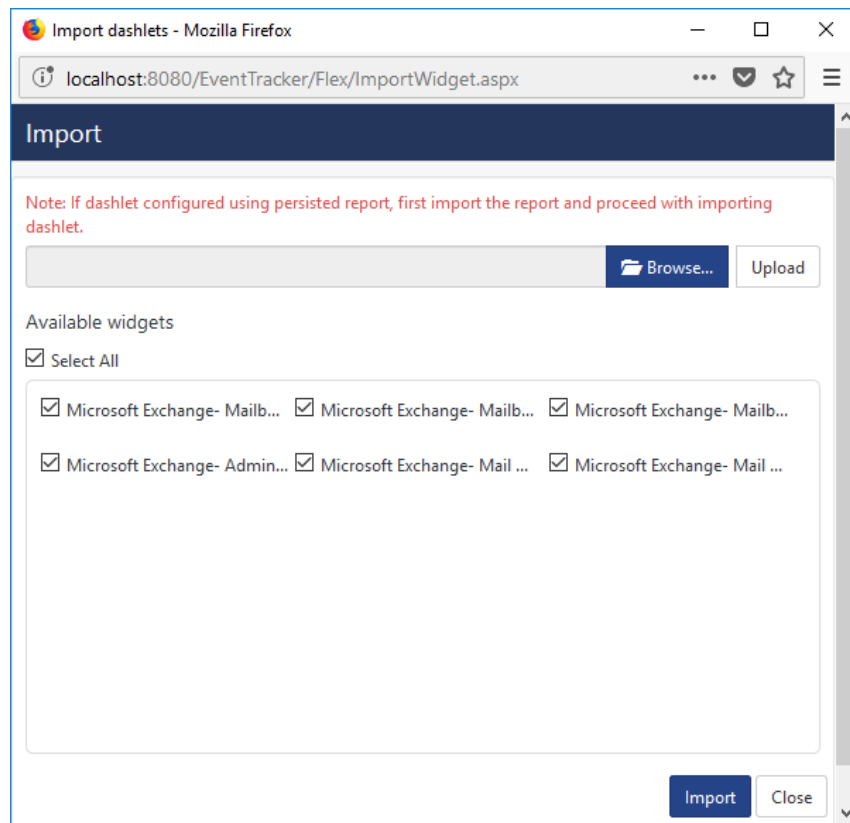



Figure 38

6. Now select all the check boxes and then click on **'Import'** option.
Dashlets are now imported successfully.
7. Click **'Add'**  to create a new dashboard.

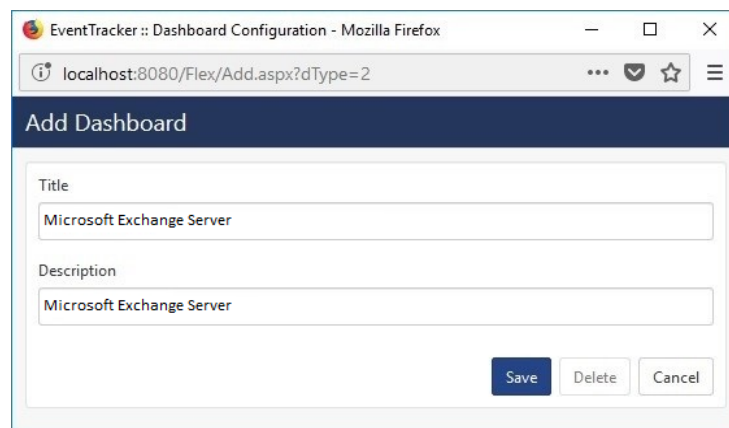



Figure 39

8. Fill suitable Title and Description and click **Save**.
9. Click '**Customize**'  to locate **Microsoft Exchange** dashlets and choose all imported dashlets for **Microsoft Exchange Server**.

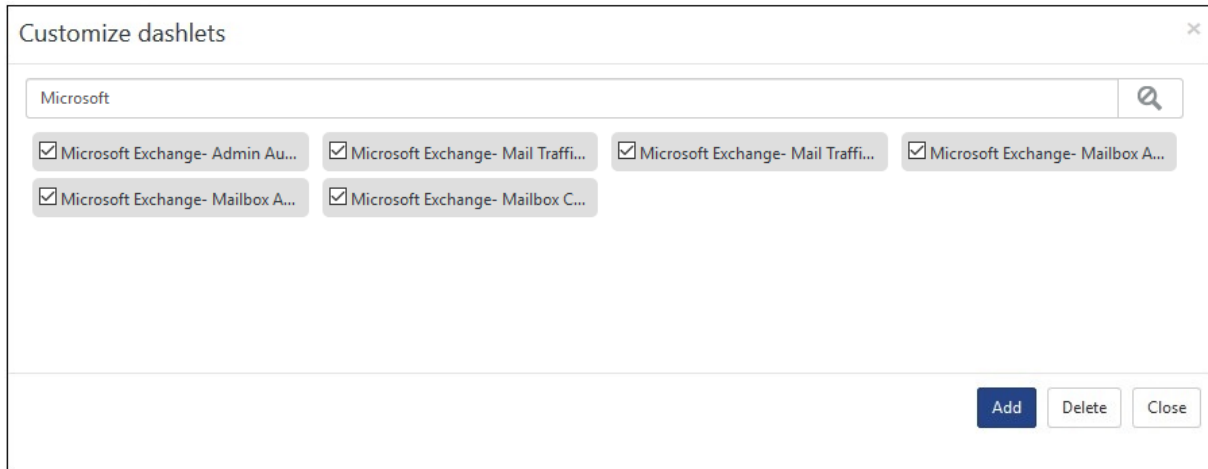


Figure 40

10. Click '**Add**' to include dashlets in dashboard.

7. Verifying Exchange Server knowledge pack in EventTracker

7.1 Categories

1. Logon to **EventTracker**.
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

Category Tree Search

- All Categories
 - *All error events
 - *All information events
 - *All warning events
 - *Security: All security events
 - AirWatch Mobile Device Management
 - Change Audit
 - Cisco IWAN
 - EventTracker
 - F-Secure Client Security
 - HP OfficeConnect Switch
 - Linux
 - Microsoft Exchange**
 - Microsoft Exchange: Admin Audit**
 - Microsoft Exchange: Mailbox Audit
 - Microsoft Exchange: Message Tracking
 - NIST 800-171
 - PCI DSS

Category Details

Parent Group: Microsoft Exchange

Event Category Name: Microsoft Exchange: Admin Audit

Description:

Applies to: Exchange 2013 or later Category version: 1.0

Show In: ☒ Operations ☐ Compliance ☐ Security

Event Rule

| Log Type | Event Type | Category | Event Id | Source | User | Match in Description | Description Exception | Lucene Query |
|----------|------------|----------|----------|--------------|------|--|-----------------------|---|
| 0 | 0 | 0 | 3230 | EventTracker | | (?s)Caller.*?ObjectModified.*?CmdletName.*?Succeeded | | log_source:'Microsoft Exchange Admin Audit' |

Save Cancel

Figure 41

7.2 Knowledge Objects

1. In the **EventTracker** 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.

Knowledge Objects

Search objects... Activate Now

Groups

- Cisco ASA Firewall
- Cisco IWAN
- Default
- EventTracker
- F-Secure Client Security
- HP OfficeConnect Switch
- Mac OS X
- Microsoft Exchange**
 - Microsoft Exchange Admin...
 - Microsoft Exchange Mail...
 - Microsoft Exchange Mes...

Object name Microsoft Exchange Admin Audit

Applies to Exchange 2013 or later

Rules

| Title | Log type | Event source | Event id | Event type |
|------------------------------------|----------|--------------|----------|------------|
| Microsoft Exchange Mailbox Changes | | EventTracker | 3230 | |

Message Signature: (?s)Caller.*?ObjectModified.*?CmdletName.*?Succeeded

Message Exception:

Expressions

| Expression type | Expression 1 | Expression 2 | Format string |
|--------------------|----------------------------------|--------------|---------------|
| Regular Expression | (?<key>[w+]+\s+:(?<Value>[^\n]+) | | |

Figure 42

7.3 Reports

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

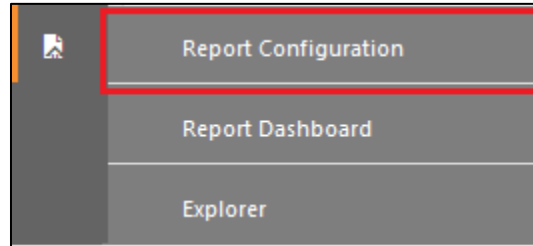


Figure 43

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

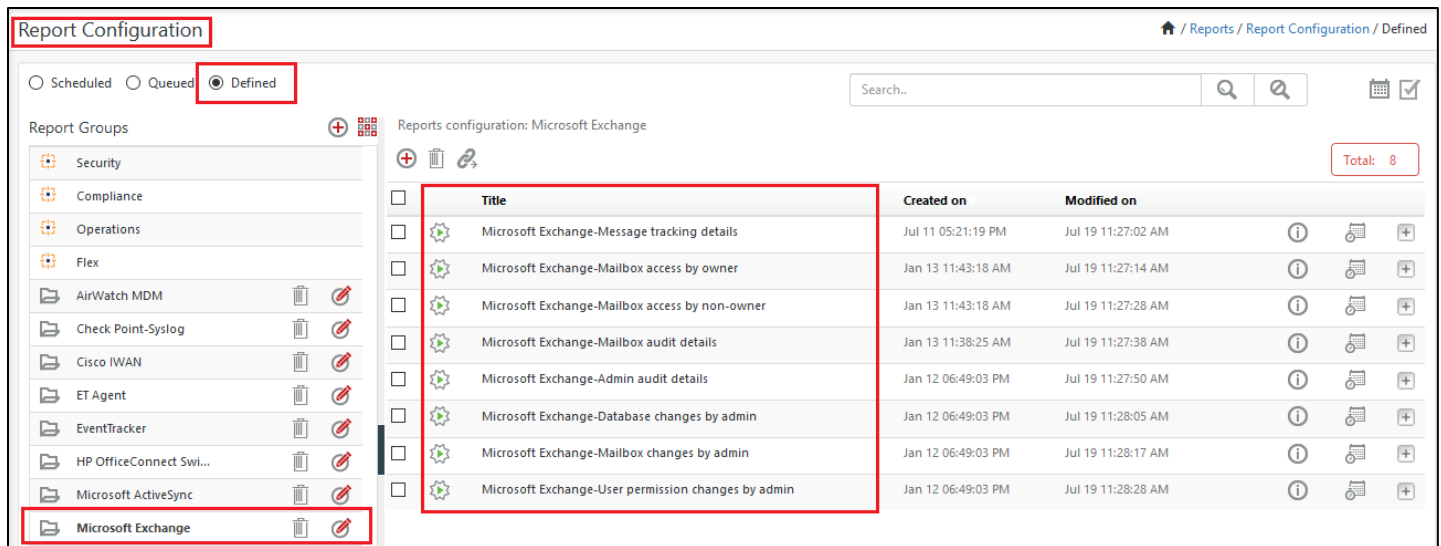


Figure 44

7.4 Dashboards

1. Open **EventTracker** in browser and logon.
2. Navigate to **Dashboard>My Dashboard**.
My Dashboard pane is shown.

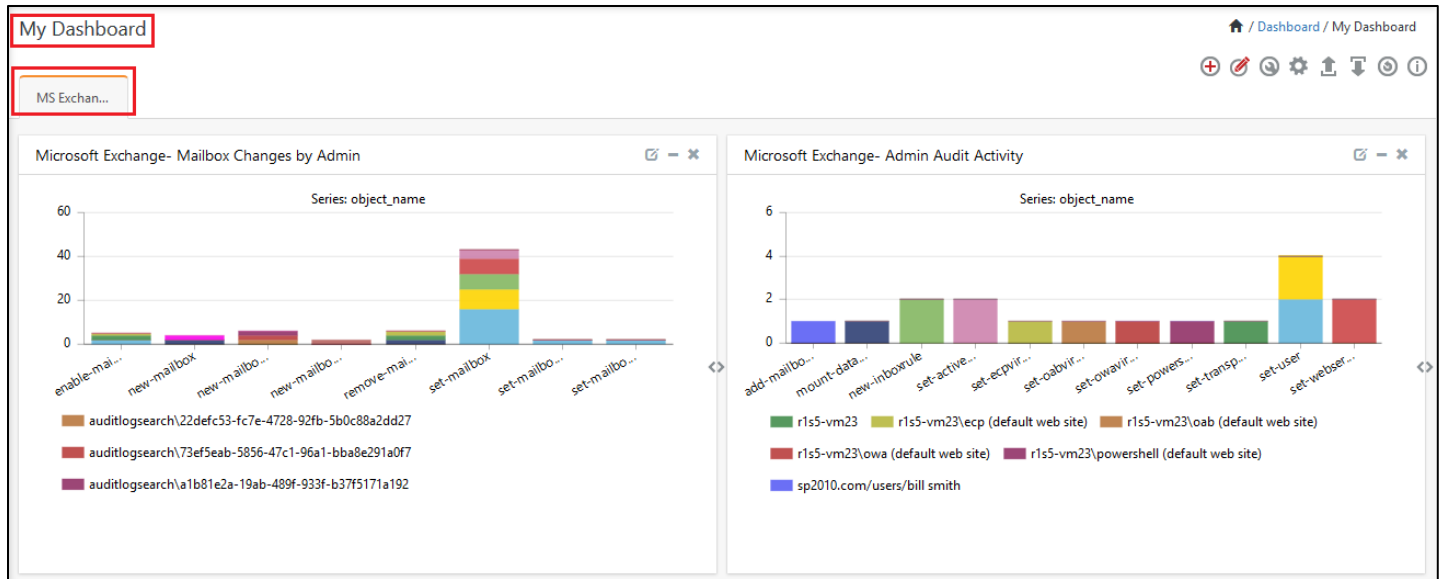


Figure 45