EventTracker

Actionable Security Intelligence

Integrate IIS SMTP server

EventTracker v8.x and above

Publication Date: May 29, 2017

Abstract

This guide helps you in configuring IIS SMTP server and EventTracker to receive SMTP Server events. In this guide, you will find the detailed procedures required for monitoring IIS SMTP server.

Audience

Administrators, who are assigned the task to monitor and manage IIS SMTP server events using EventTracker.

Table of Contents

Overview

The Simple Mail Transfer Protocol (SMTP) service provided by IIS is a simple component for delivering outgoing e-mail messages. Delivery of a message is initiated by transferring the message to a designated SMTP server.

EventTracker helps you to monitor event activities in IIS SMTP server. It will trigger an alert whenever it detects an error or a blacklisted spam IP address. Its knowledge object will help you make the log search easier and informative. It generates flex reports, flex dashboards for IIS SMTP server.

Prerequisites

- EventTracker v8.x should be installed.
- IIS SMTP server 6.0 or later

Integration of IIS SMTP SERVER to EventTracker manager

In Internet Information Services 6 (IIS6) and earlier.

1. Right click the SMTP server and choose **Properties.**

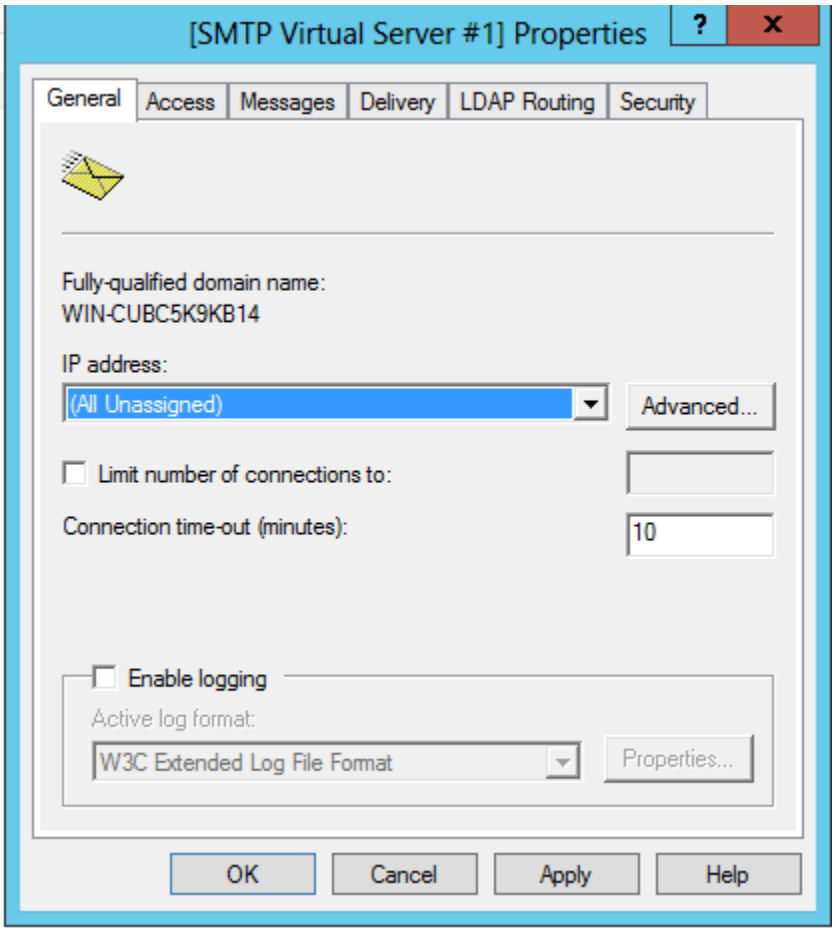

Figure 1

2. Check the **Enable logging** at the bottom.
3. Choose the log format **W3C Extended Log File Format** from the drop-down box.

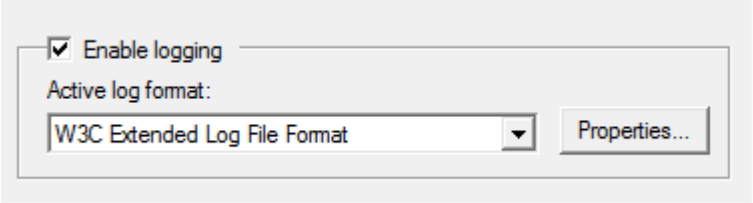

Figure 2

4. Click on the **Properties…** button and in the pop up the window, select the options as per your requirement. Under Directory, specify the path where the log file should be stored. The default is **%System Drive%\Windows\System32\LogFiles**

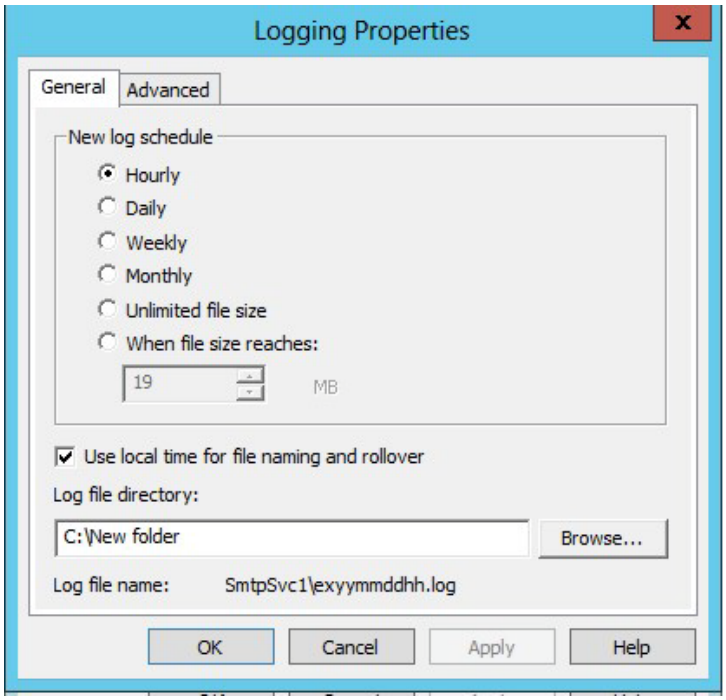

Figure 3

5. Move to the **Advanced** tab and set the configuration to collect all the available information in your SMTP logs to help you troubleshoot mail issues.

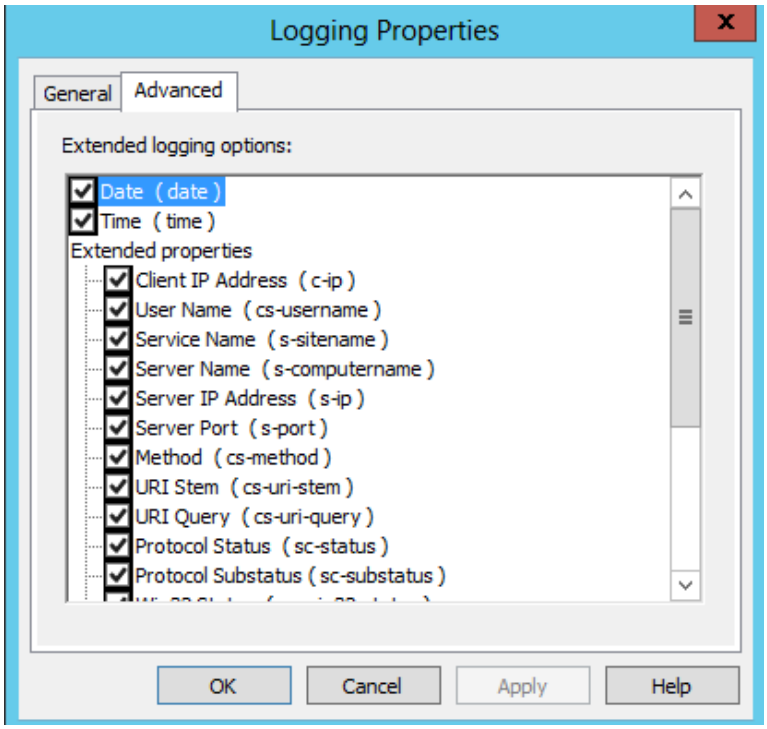

Figure 4

NOTE: We should monitor log file using EventTracker LFM Agent

LFM Configuration:

In **EventTracker Control Panel**,

1. Click **EventTracker Agent Configuration**.

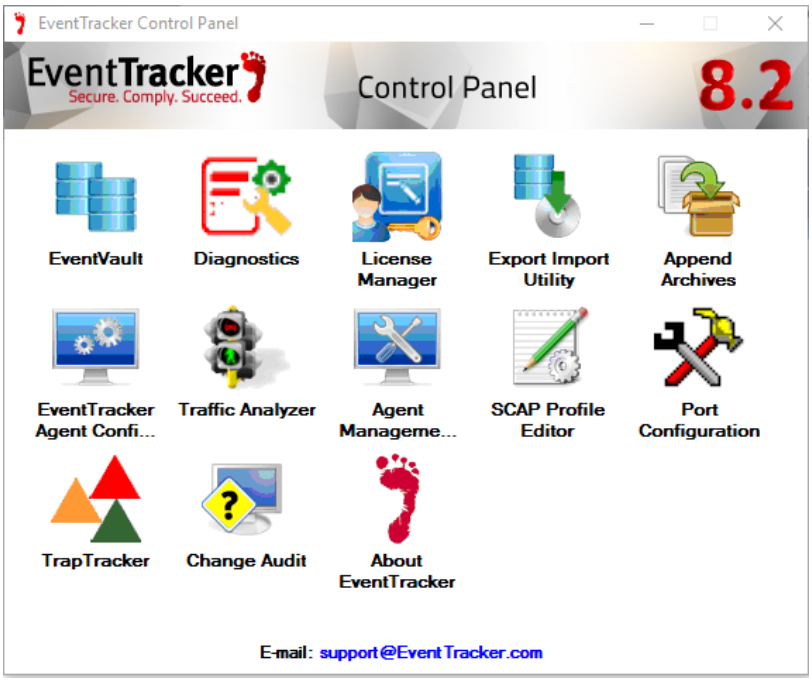

Figure 4

The **EventTracker Agent configuration** page displays.

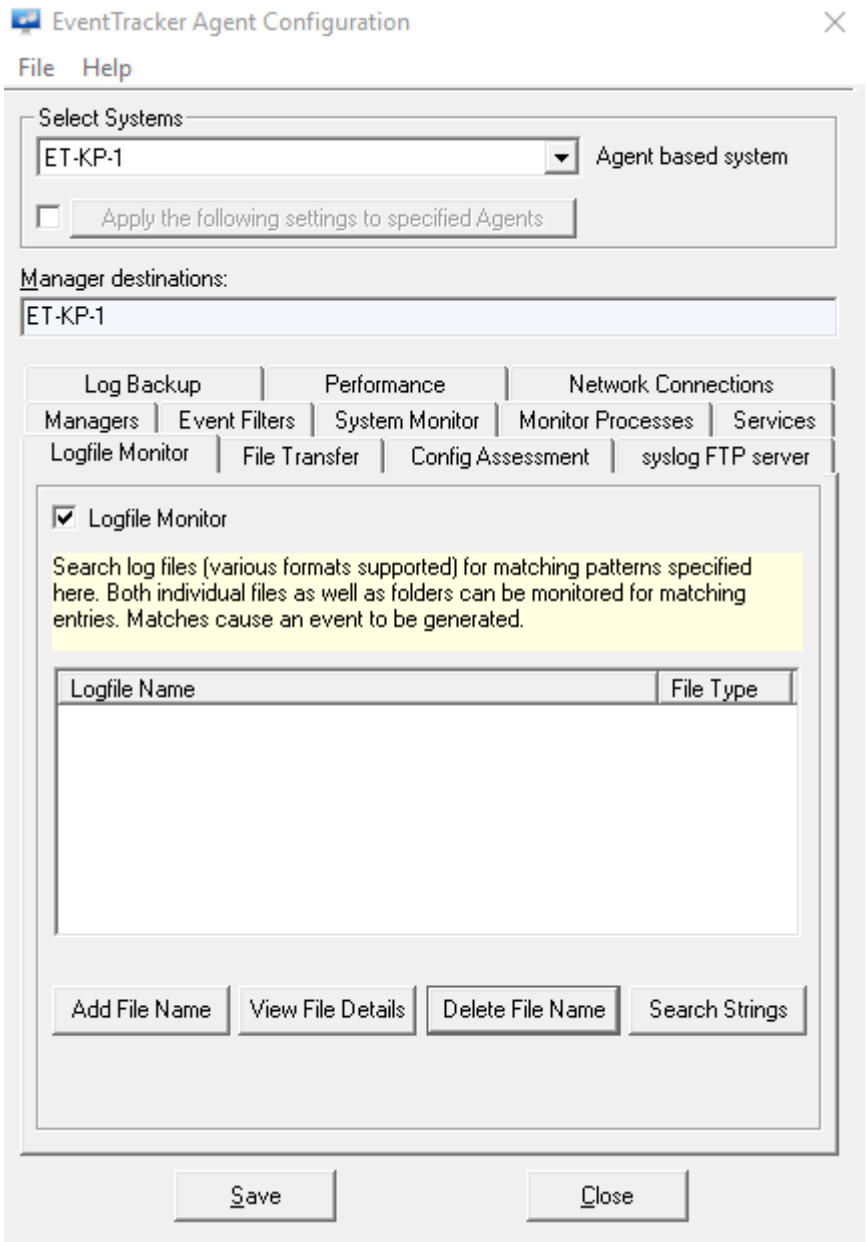

Figure 5

2. Select **Logfile Monitor** and click **Add File Name**. It will pop up a window.

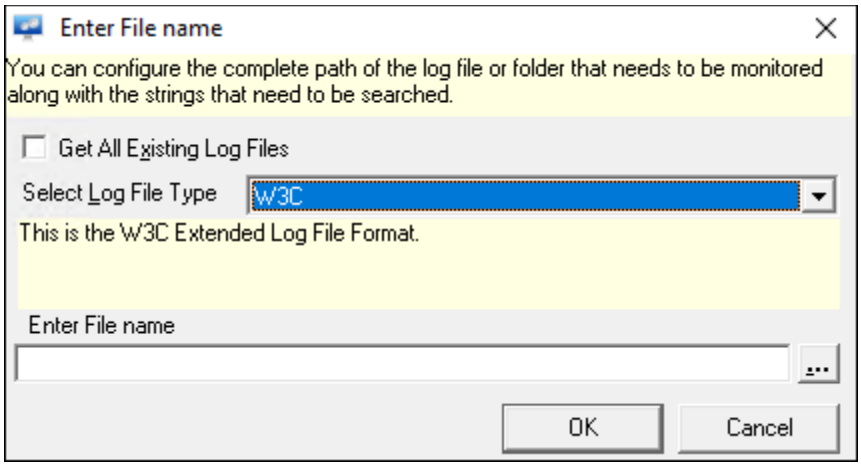

Figure 6

3. In the window check **Get All Existing Log Files** and Select Log File Type as **W3C**
4. Under **Enter File name** select brwose button to browse the location of the IIS SMTP log files.

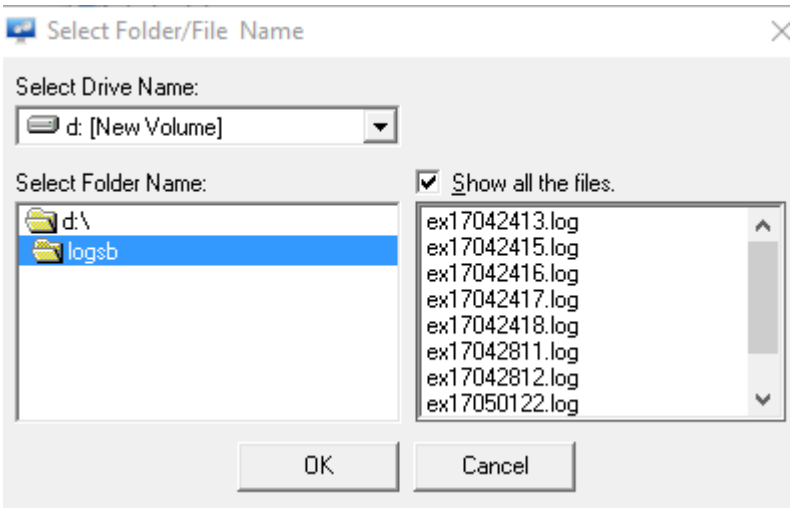

Figure 7

5. Select the drive, folder and check "**Show all the files**" to display all the files. Click **OK**
6. Select the log file extension as ***.log** and click **OK**

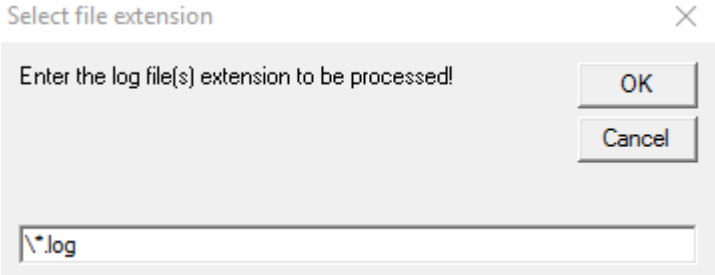

Figure 8

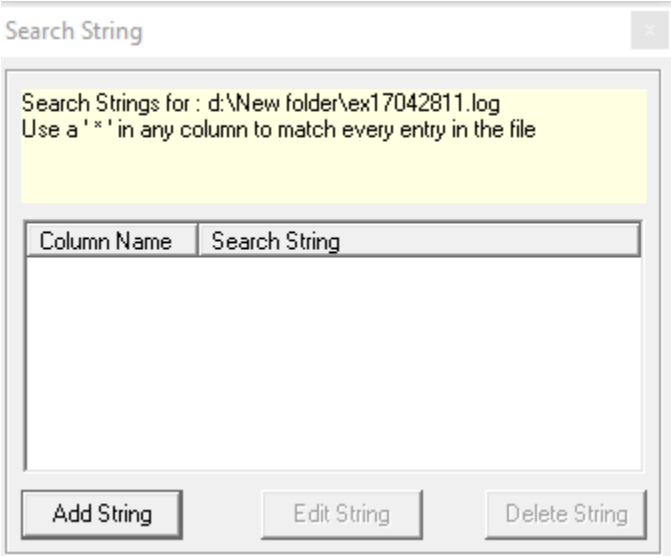

Figure 9

7. Click on **Add String** button
8. Select Field Name as **date** from dropdown menu.
9. Type ***** in Search String, check Current Date Time and click **OK** to exit.

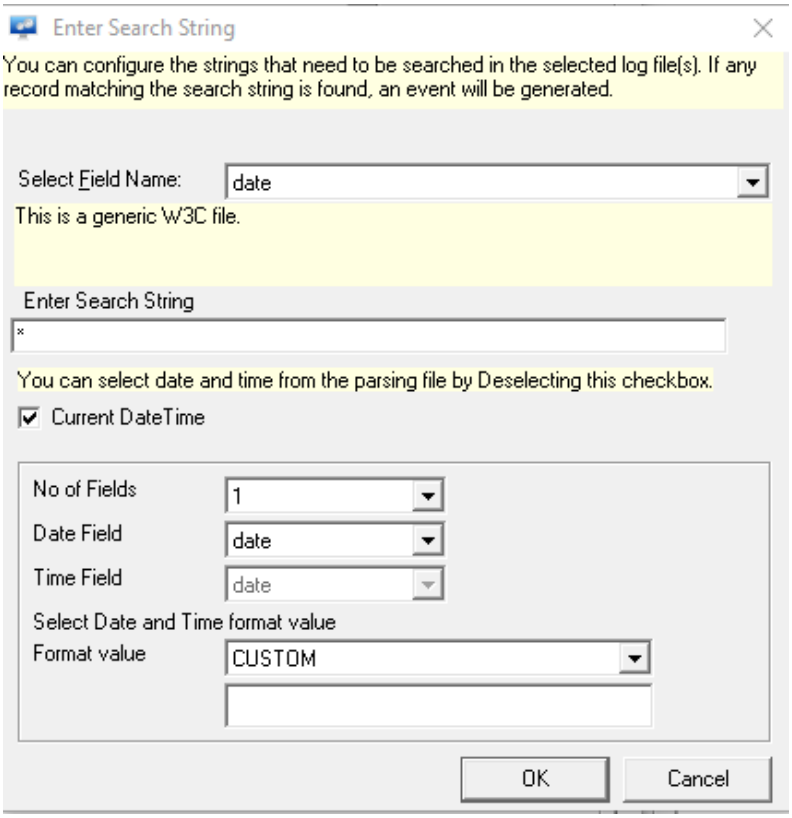

Figure 10

10. Search string will be added in the window. Click **OK** to exit.

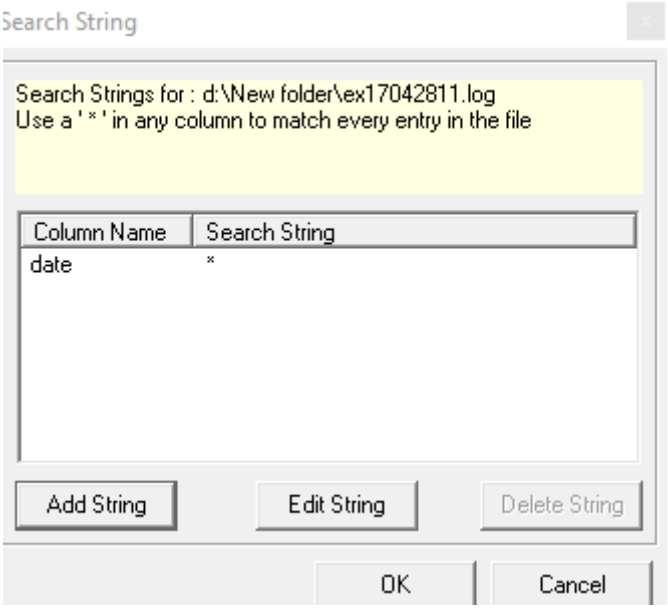

Figure 11

EventTracker Knowledge Pack

Once logs are received into EventTracker, alerts, reports and knowledge object can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support SMTP Server (IIS 6.0).

Alerts

- **IIS SMTP server: SPAM Blacklist IP detected –** This alert is generated when a Blacklisted IP accesses the server.
- **IIS SMTP server: AUTH error-** This alert is generated when an authentication failure happens.
- **IIS SMTP server: Slow mail flow-**This alert is generated when a process taken unlikely gets delayed.
- **IIS SMTP server: EHLO and HELO continuous request-** This alert is generated when there is a continuous request of EHLO or HELO from the client.

Flex Reports

- **IIS SMTP Server-Error reports–** This report provides information about the errors on SMTP methods like (MAIL, RCPT, DATA, AUTH, QUIT) in IIS SMTP server.

LogTime	Computer	Site Name	Client IP Address	CS Host	Client to server method	Status Code
05/08/2017 06:41:01 PM	ET-KP-1	SMTPSVC1	192.168.1.94	contoso.com	EHLO	501
05/08/2017 06:41:01 PM	ET-KP-1	SMTPSVC1	192.168.1.94	contoso.com	EHLO	501
05/08/2017 06:41:01 PM	ET-KP-1	SMTPSVC1	192.168.1.94	contoso.com	HELO	501
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	192.168.1.94	contoso.com	MAIL	501
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	192.168.1.94	contoso.com	AUTH	501
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	95.1.184.228	verizon.net	RCPT	500
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	109.234.238.114	verizon.net	EHLO	501

Sample Logs

5/3/2017 2:29:29 PM 3230 ET-KP-1 SYSTEM NT AUTHORITY EventTracker

Event Type: Information
Log Type: System
Category Id: 2

Description:
ENTRY:
date: 5/2/2017
time: 11:21:54 AM
c-ip: 192.168.1.94
cs-username: me
s-sitename: SMTPSVC1
s-computername: WIN-CUBC5K9KB14
s-ip: 192.168.1.185
s-port: 0
cs-method: MAIL
cs-uri-stem:

- **IIS SMTP Server-AUTH error details–** This report provides information about the client authentication failures and errors.

LogTime	Computer	Site Name	Client IP Address	Status Code
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	192.168.1.94	535
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	192.168.1.94	535
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	192.168.1.94	535
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	95.1.184.228	501
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	95.1.184.228	501
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	192.168.1.94	501
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	192.168.1.94	501
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	192.168.1.94	501
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	192.168.1.94	535
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	2.161.228.9	535
05/08/2017 06:41:02 PM	ET-KP-1	SMTPSVC1	2.161.228.9	535

Sample logs:

5/5/2017 12:03:28 PM 3230 contoso-et-svr N/A N/A EventTracker

Event Type: Information
Log Type: Application
Category Id: 0

Description:
ENTRY:
date: 3/4/2017
time: 22:56:20
c-ip: 1.179.166.243
cs-username: DOCUTRACK0253
s-sitename: SMTPSVC1
s-computername: contoso-svr-mail
s-ip:
s-port: 25
cs-method: AUTH
cs-uri-stem:
cs-uri-query:
sc-status: 211
sc-win32-status: 0
sc-bytes: 30
cs-bytes: 27

- **IIS SMTP Server-Mail sender and receiver details–** This report provides information about the Mail sender and recipient details.

LogTime	Computer	Site Name	Server Name	Address	Address	method	Sender	Recepitent	Status Code	Bytes sent	Received	Taken	URI Query	Versio
05/02/2017 11:40:03 AM	ET-KP-1	SMTPSVC1	DOCUTRACK0251	127.0.0.1	127.0.0.1	MAIL	zan@docutrack0251		250	42	29	0	+FROM:<zan@docutrack0251>	SMTP
05/02/2017 11:40:03 AM	ET-KP-1	SMTPSVC1	DOCUTRACK0251	127.0.0.1	127.0.0.1	MAIL	dt-zanmoye@docutrack.com		250	49	36	0	+FROM:<dt-zanmoye@docutrack.com>	SMTP
05/02/2017 11:40:03 AM	ET-KP-1	SMTPSVC1	DOCUTRACK0251	127.0.0.1	127.0.0.1	RCPT		zan@docutrack0251	250	30	27	0	+TO:<zan@docutrack0251>	SMTP
05/02/2017 11:40:03 AM	ET-KP-1	SMTPSVC1	DOCUTRACK0251	127.0.0.1	127.0.0.1	RCPT		zan@docutrack0251	250	30	27	0	+TO:<zan@docutrack0251>	SMTP
05/02/2017 11:40:03 AM	ET-KP-1	SMTPSVC1	DOCUTRACK0251	127.0.0.1	127.0.0.1	RCPT		dt-zanmoye@docutrack.com	250	37	34	0	+TO:<dt-zanmoye@docutrack.com>	SMTP
05/02/2017 11:40:03 AM	ET-KP-1	SMTPSVC1	DOCUTRACK0251	127.0.0.1	127.0.0.1	MAIL	dt-zanmoye@docutrack.com		250	49	36	0	+FROM:<dt-zanmoye@docutrack.com>	SMTP

Sample logs:

Event Type: Information
Log Type: Application
Category Id: 0

Description:
ENTRY:
date: 3/4/2017
time: 23:56:20
c-ip: 1.179.176.37
cs-username: DOCUTRACK0254
s-sitename: SMTPSVC1
s-computername: contoso-svr-mail
s-ip:
s-port: 25
cs-method: MAIL
cs-uri-stem:
cs-uri-query: +rand(O2:O16)
sc-status: 220
sc-win32-status: 16
sc-bytes: 140
cs-bytes: 18
time-taken: 0
cs-version: SMTP
cs-host:
cs(User-Agent):
cs(Cookie):
cs(Referer):

- **IIS SMTP Server-EHLO and HELO Request Details–** This report provides information about the client who requested EHLO and HELO to SMTP server. This report will provide the client IP address and query requested.

LogTime	Computer	Client to server method	Client IP Address	URI Query	Status Code	Bytes Received	Bytes sent	Time Taken
05/08/2017 06:41:01 PM	ET-KP-1	EHLO	207.46.163.10	WIN-CUBC5K9KB14	0	0	4	281
05/08/2017 06:41:01 PM	ET-KP-1	EHLO	192.168.1.94	+Administrator@contoso.com	501	30	27	0
05/08/2017 06:41:01 PM	ET-KP-1	HELO	192.168.1.94	+Administrator@contoso.com	501	30	27	0
05/08/2017 06:41:01 PM	ET-KP-1	EHLO	192.168.1.94	+test@contoso.com	501	21	27	0
05/08/2017 06:41:02 PM	ET-KP-1	HELO	109.234.238.114	+	501	18	193	0
05/08/2017 06:41:02 PM	ET-KP-1	EHLO	109.234.238.114	+	500	18	193	0
05/08/2017 06:41:02 PM	ET-KP-1	EHLO	109.234.238.114	+	500	18	193	0
05/08/2017 06:41:02 PM	ET-KP-1	EHLO	109.234.238.114	+	500	18	193	0
05/08/2017 06:41:02 PM	ET-KP-1	EHLO	109.234.238.114	+	501	18	193	0

Sample logs:

5/5/2017 12:08:47 PM | 2040 | CONTOSO-ET-SVR | N/A | N/A | EventTracker

Event Type: Information
Log Type: Application
Category id: 0

Description:
New activity found:
IP Address: 1.179.146.153
Rule Name: IP Address Activity
System: CONTOSO-ET-SVR
Time: 2017-05-05 12:03:25

Source Event:
Id: 3230
Source: EventTracker
Description: ENTRY:
date: 3/4/2017
time: 21:56:20
c-ip: 1.179.146.153
cs-username: DOCUTRACK0252
s-sitename: SMTPSVC1
s-computername: contoso-svr-mail
s-ip:
s-port: 25
cs-method: HELO
cs-uri-stem:
cs-uri-query: #NAME?
sc-status: 211
sc-win32-status: 0
sc-bytes: 76
cs-bytes: 27

- **IIS SMTP Server-All traffic reports–** This reports provides information about the mail traffic on the mail server.

LogTime	Computer	Site Name	Client IP Address	User Name	Sender	Recipitent	Client to server method	Status Code	URI Query
05/08/2017 03:18:24 PM	CONTOSO-ET-SVR	SMTPSVC1	1.179.185.249	contoso.com	hakim@sbcglobal.net		MAIL	452	From:<hakim@sbcglobal.net>
05/08/2017 03:18:31 PM	CONTOSO-ET-SVR	SMTPSVC1	192.168.0.3	contoso.com	hakim@sbcglobal.net		MAIL	502	From:<hakim@sbcglobal.net>
05/08/2017 03:19:47 PM	CONTOSO-ET-SVR	SMTPSVC1	192.168.0.3	contoso.com		bigmauler@gmail.com	RCPT	551	TO:<bigmauler@gmail.com>
05/08/2017 03:20:38 PM	CONTOSO-ET-SVR	SMTPSVC1	1.179.189.217	contoso.com			EHLO	554	bigmauler.contoso.com
05/08/2017 03:21:40 PM	CONTOSO-ET-SVR	SMTPSVC1	1.179.189.217	contoso.com		isorashi@icloud.com	RCPT	451	TO:<isorashi@icloud.com>
05/08/2017 03:21:43 PM	CONTOSO-ET-SVR	SMTPSVC1	1.179.185.253	contoso.com		isorashi@icloud.com	RCPT	450	TO:<isorashi@icloud.com>

Knowledge Object

- **IIS SMTP AUTH Error –** This knowledge object will help us to analyze the log related with IIS SMTP authentication errors.
- **IIS SMTP –** This knowledge object will help us to analyze the log related to IIS SMTP server.

Import IIS SMTP Server knowledge pack into EventTracker

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

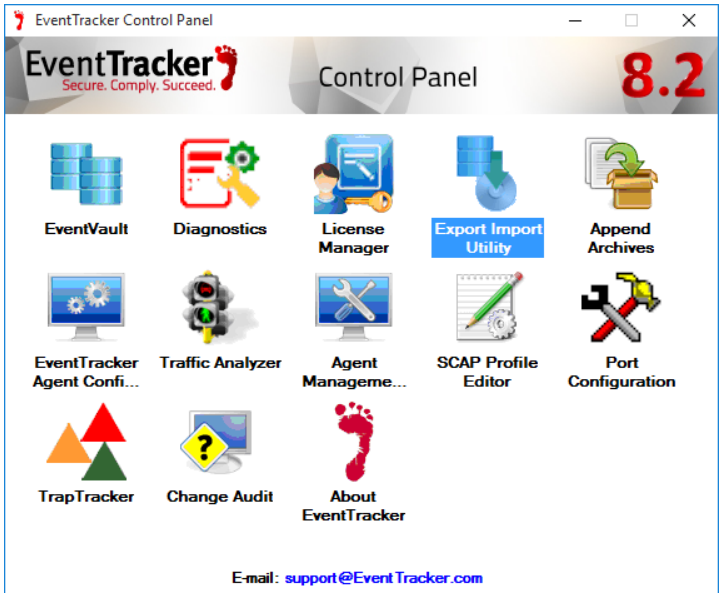

Figure 12

3. Click the **Import** tab.

Knowledge Objects

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
2. Locate the **IIS SMTP Server Knowledge Objected**, and then click **Import** button

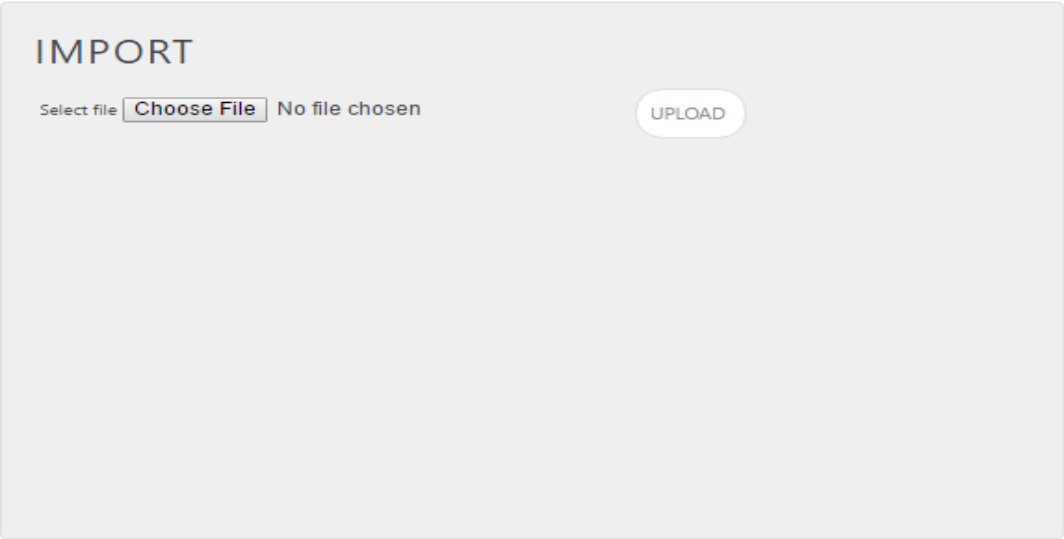

Figure 13

3. Choose the Knowledge objects that needs to be imported and click on **upload**.

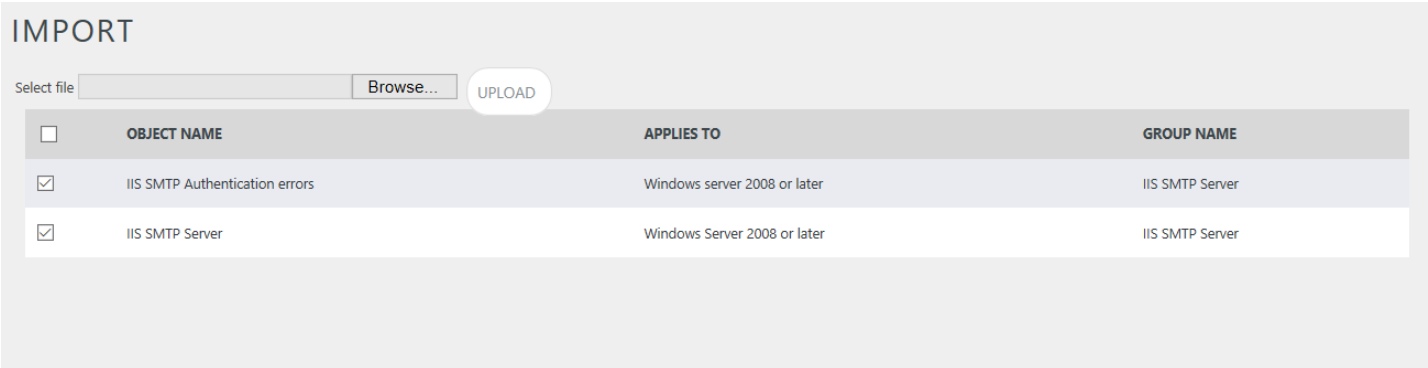

Figure 14

4. Knowledge objects are now imported successfully.

Figure 15

Alerts

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

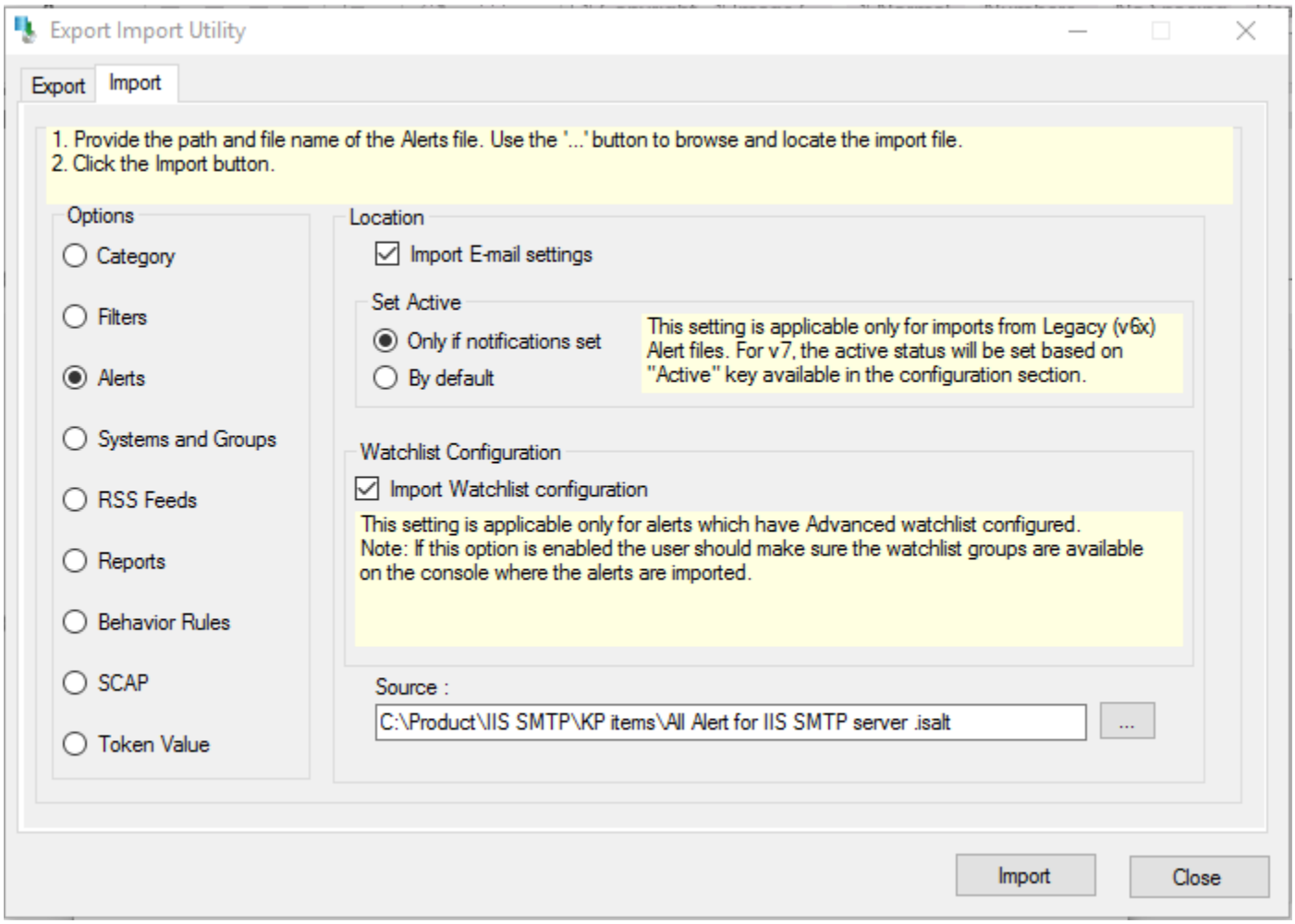

Figure 16

2. Locate **All alert for IIS SMTP Server.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

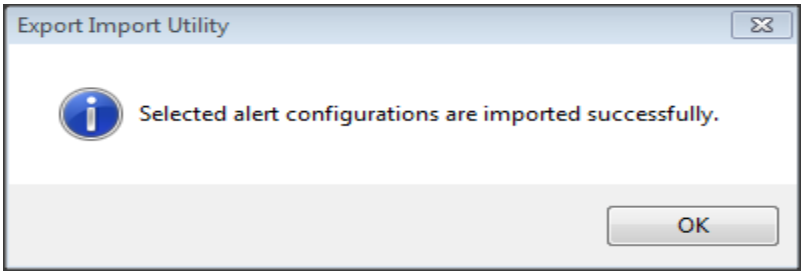

Figure 17

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

Flex Reports

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

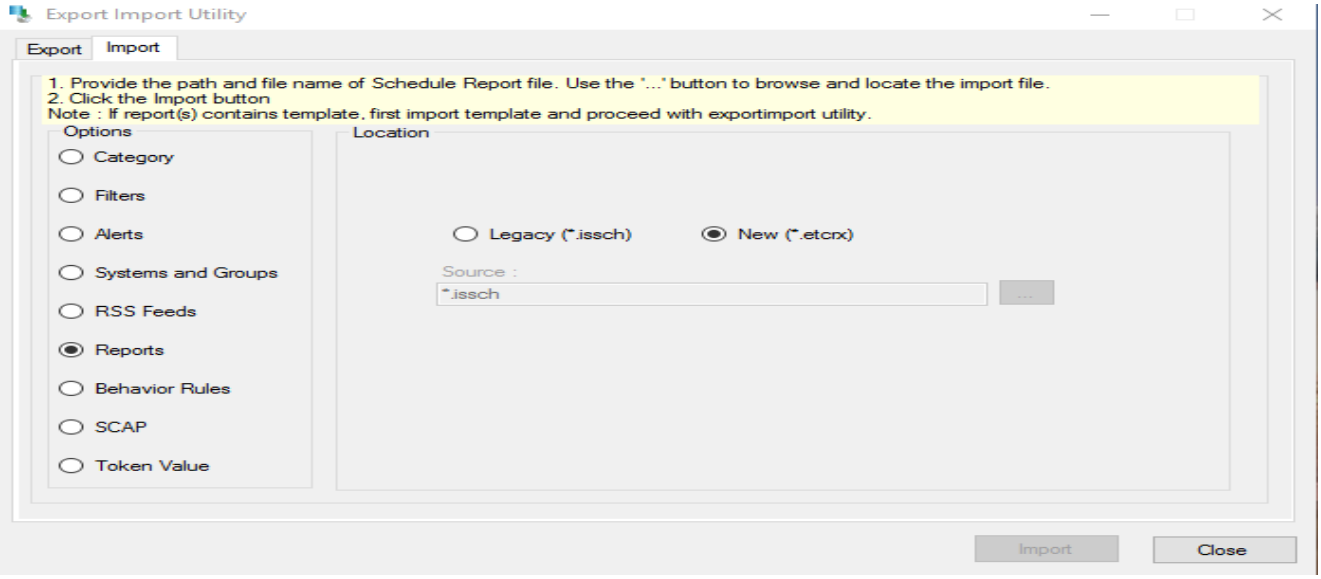

Figure 18

2. Locate the **IIS SMTP Server Reports.etcrx** file, and then click the **Open** button.

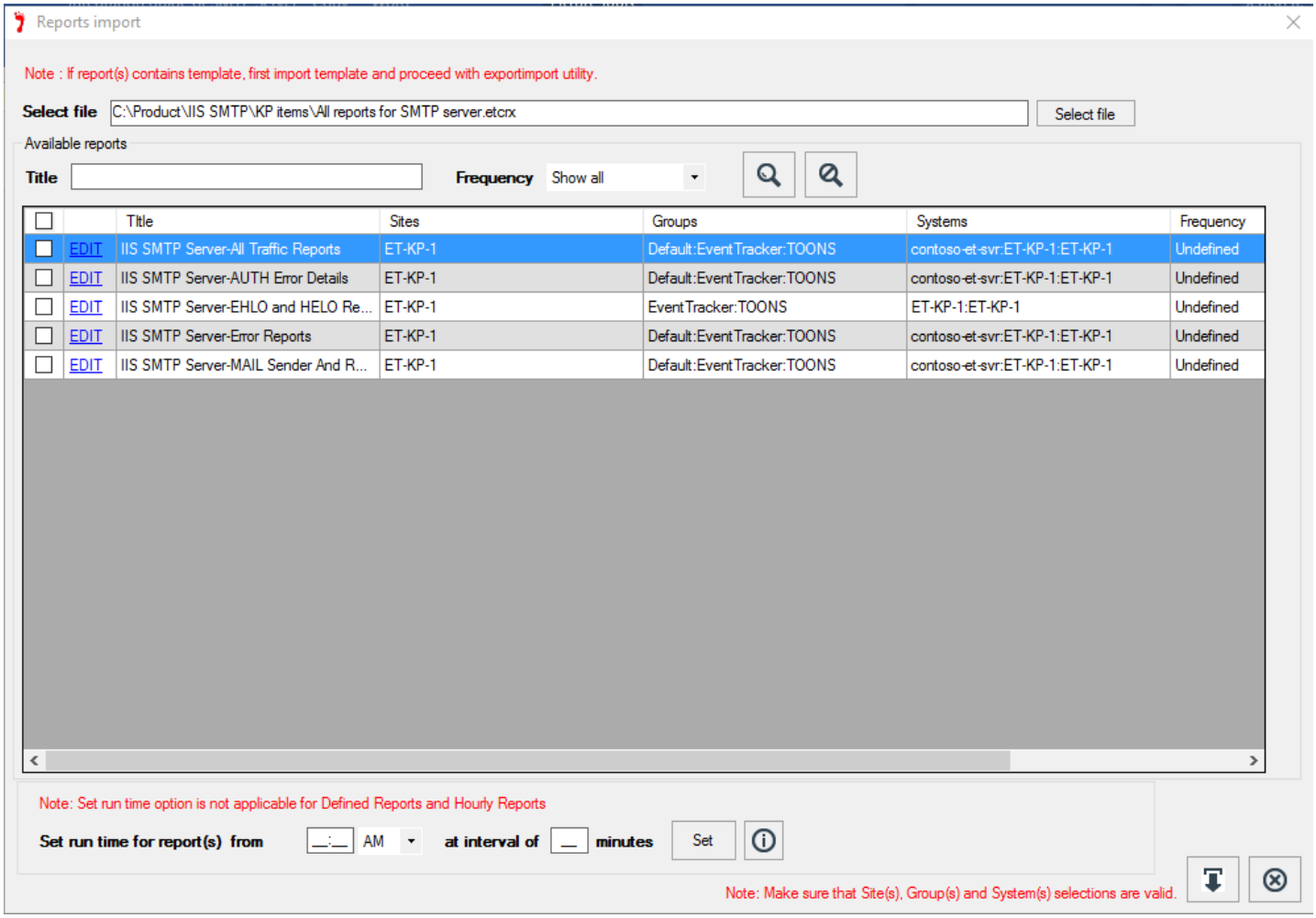

Figure 19

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

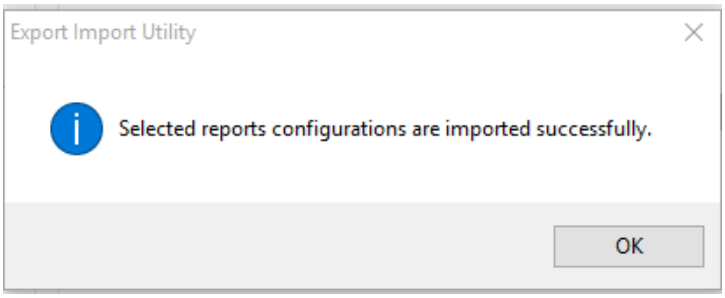

Figure 20

Verify IIS SMTP Server knowledge pack in EventTracker

Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects.**

In the **Knowledge Object tree**, expand **IIS SMTP group** folder to see the imported Knowledge objects.

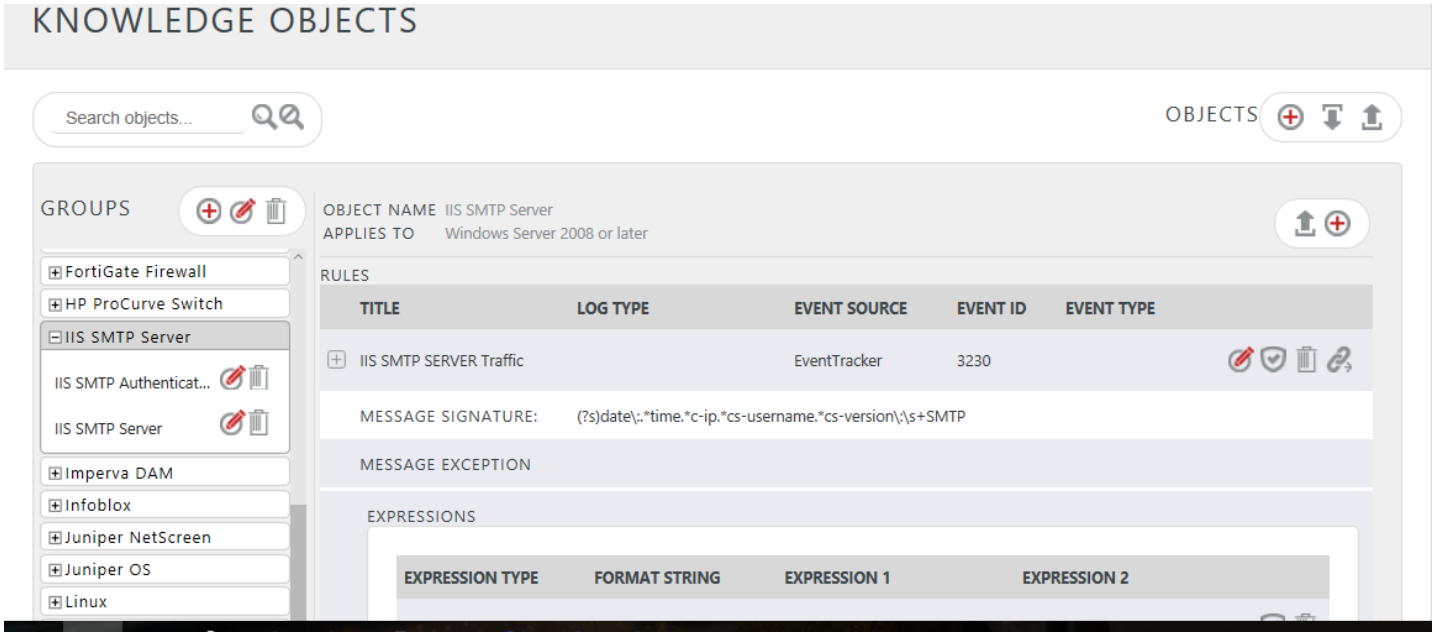

Figure 21

Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type '**IIS SMTP SERVER,** and then click the **Go** button.

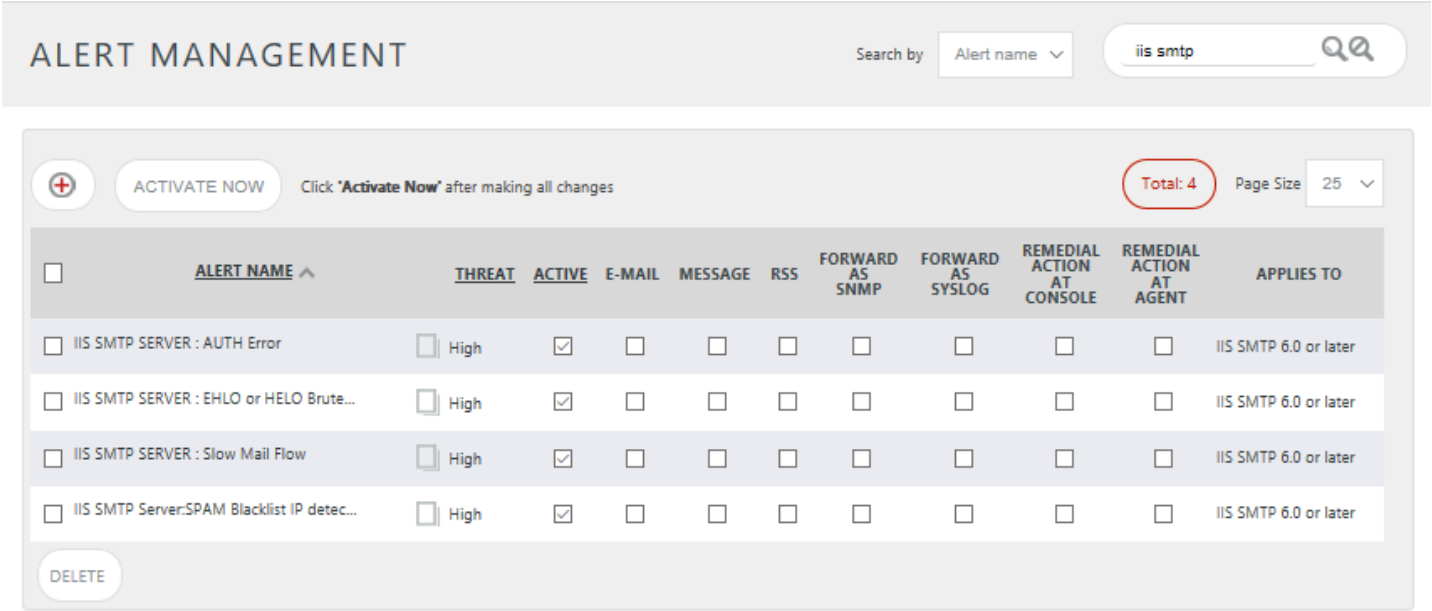

Figure 22

Alert Management page will display all the imported IIS SMTP alerts.

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.

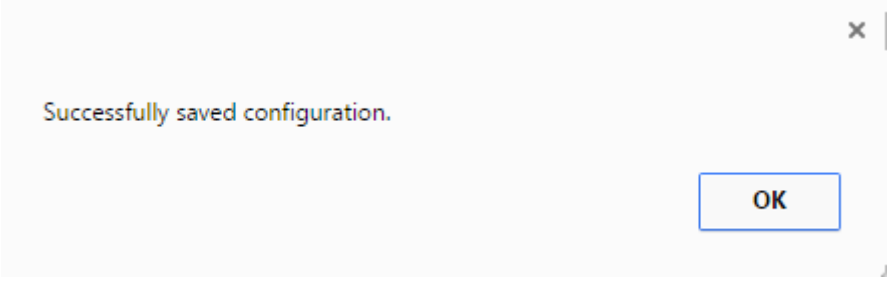

Figure 23

5. Click **OK**, and then click the **Activate Now** button.

NOTE: You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter '**IIS SMTP,** and then click the **Search** button.

EventTracker displays Flex reports of '**IIS SMTP Server**

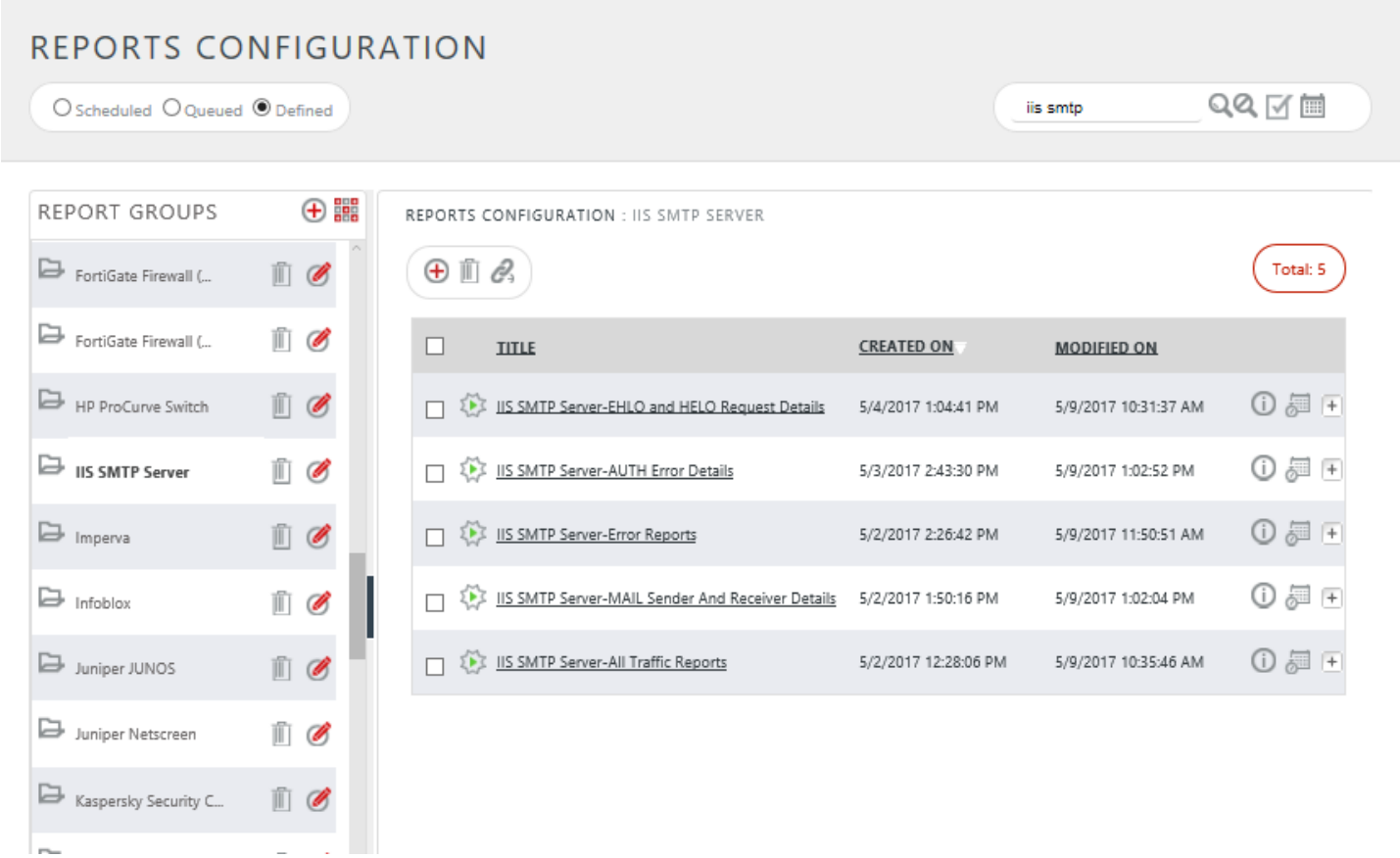

Figure 24

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.

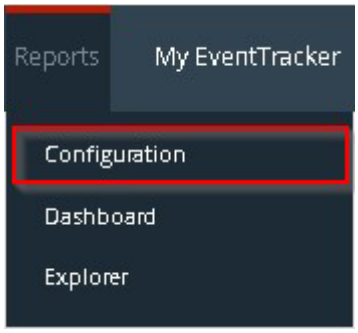

Figure 25

2. Navigate to **Reports>Configuration**.
3. Select **IIS SMTP Server** in report groups. Check **Defined** dialog box.

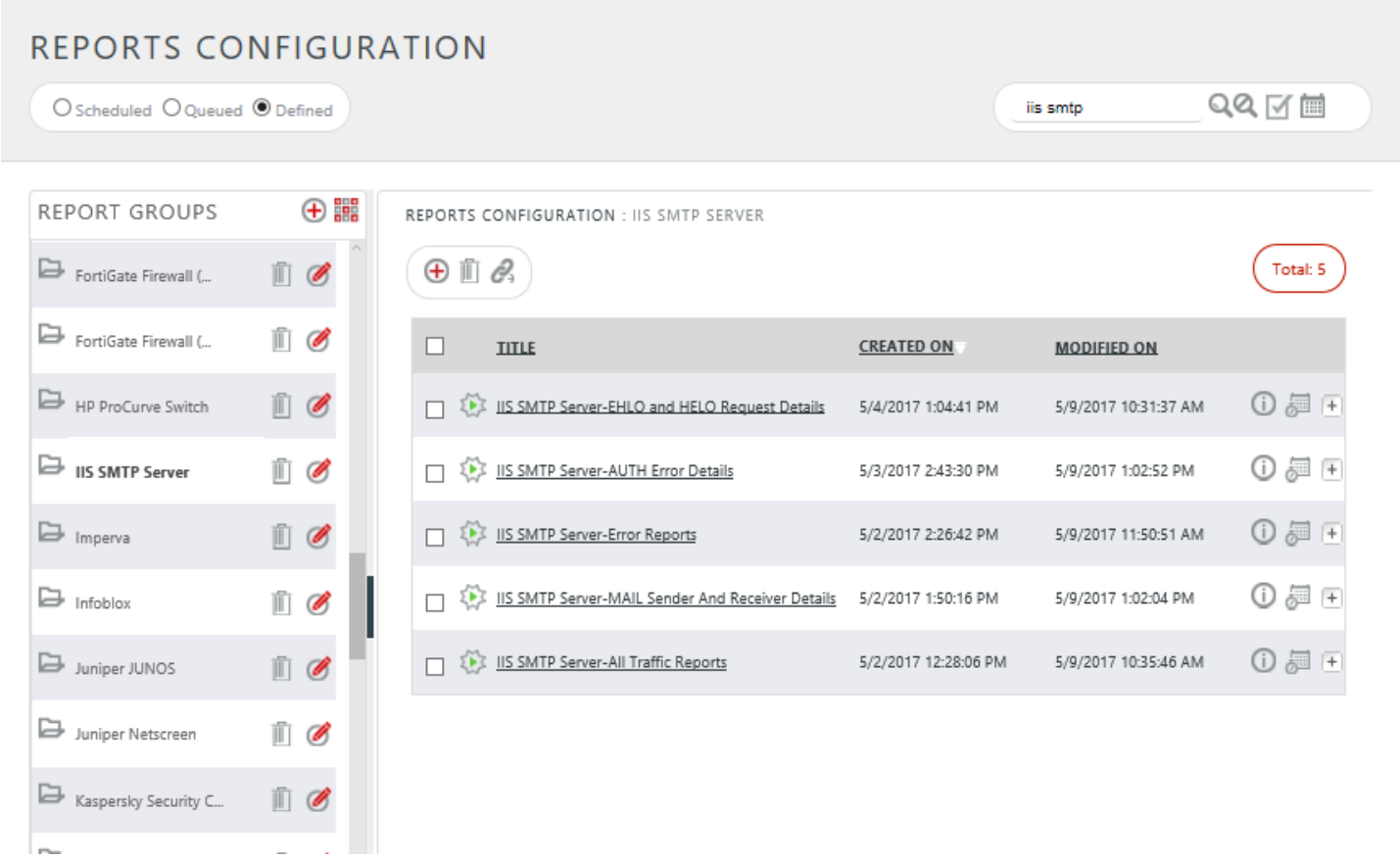

Figure 26

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.

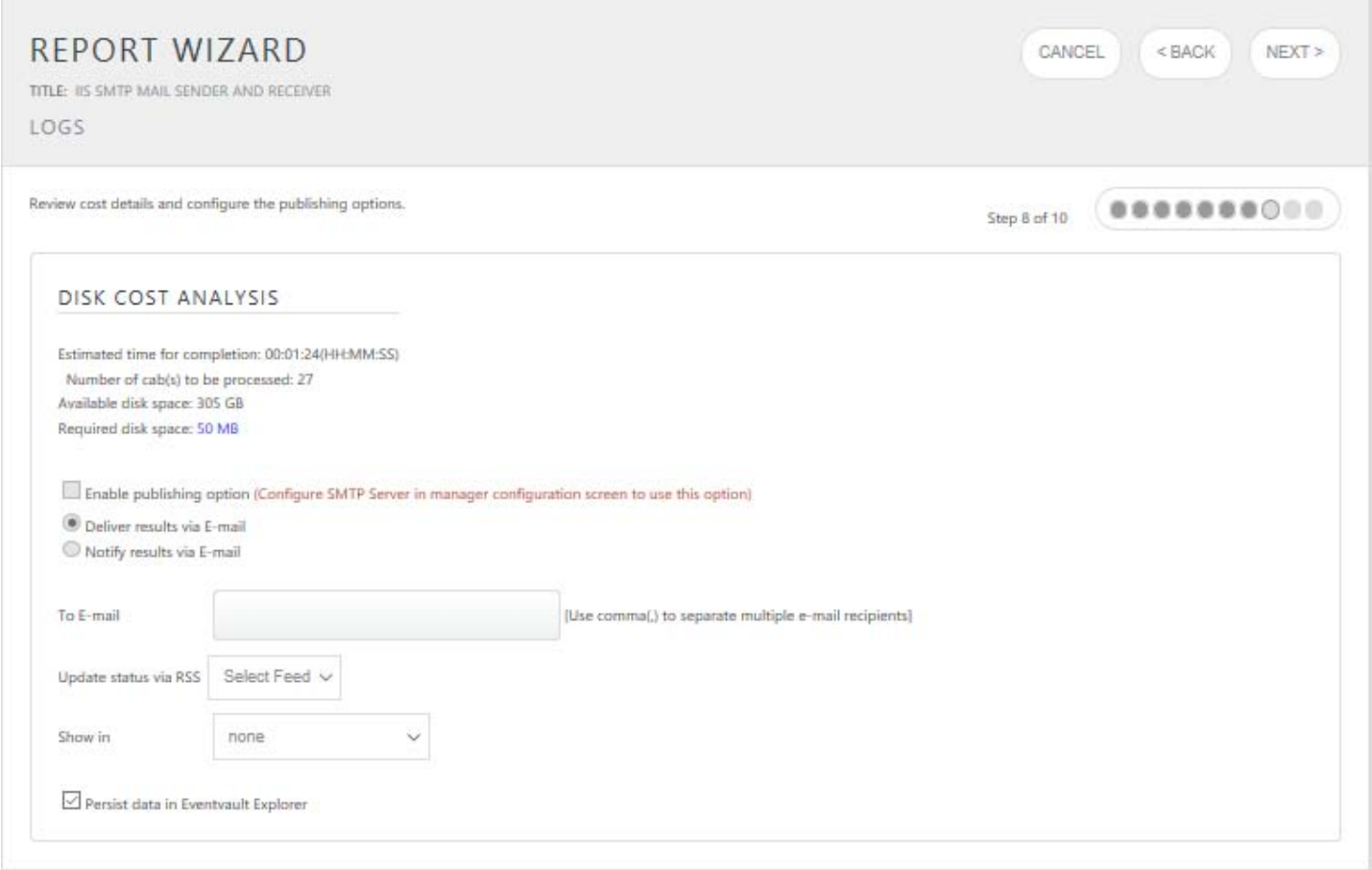

Figure 27

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

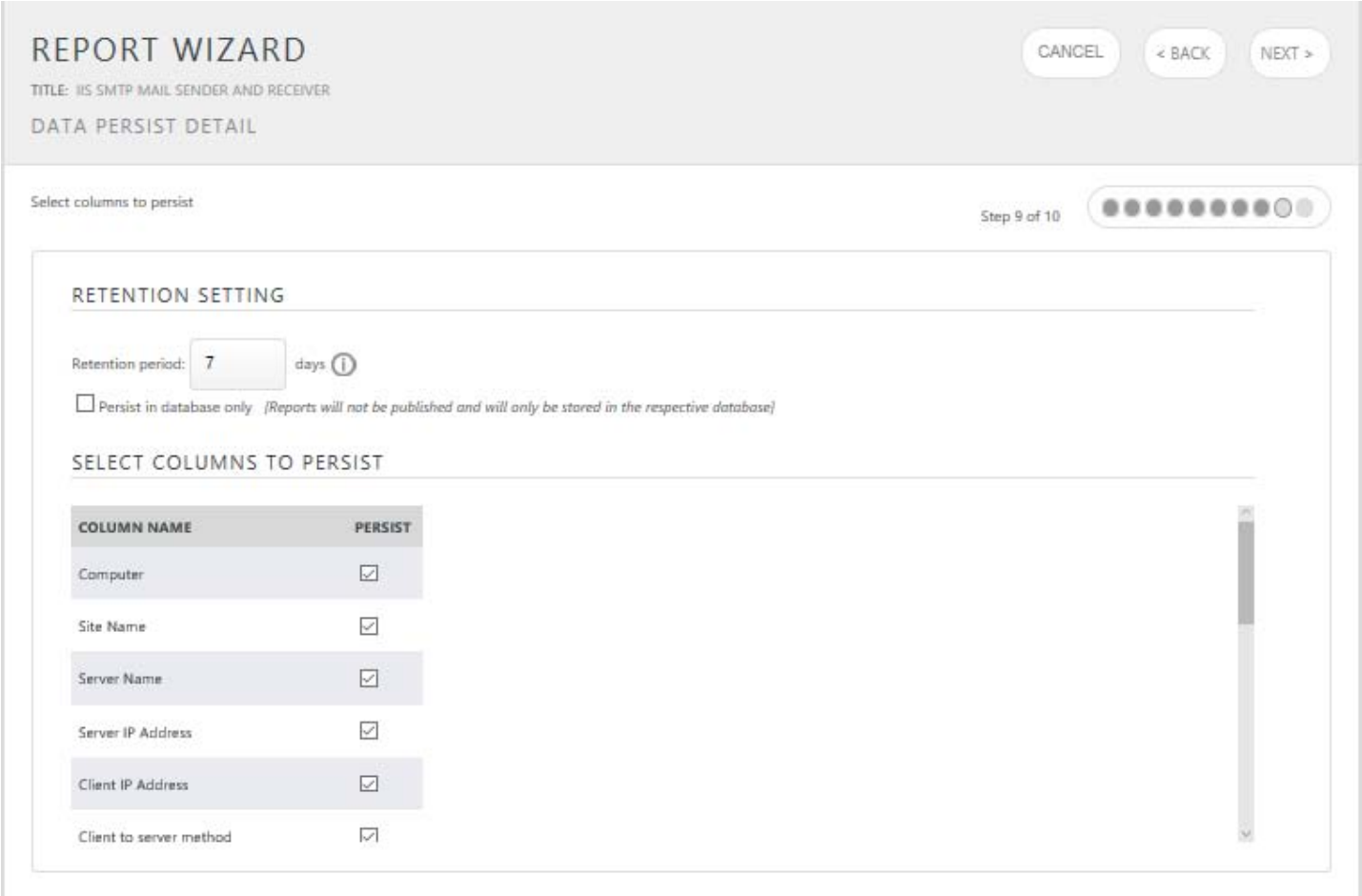

Figure 28

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.

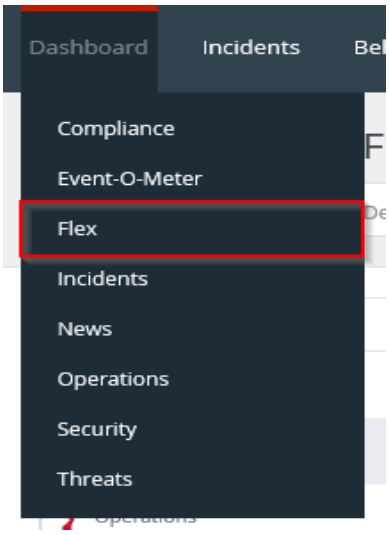

Figure 29

2. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

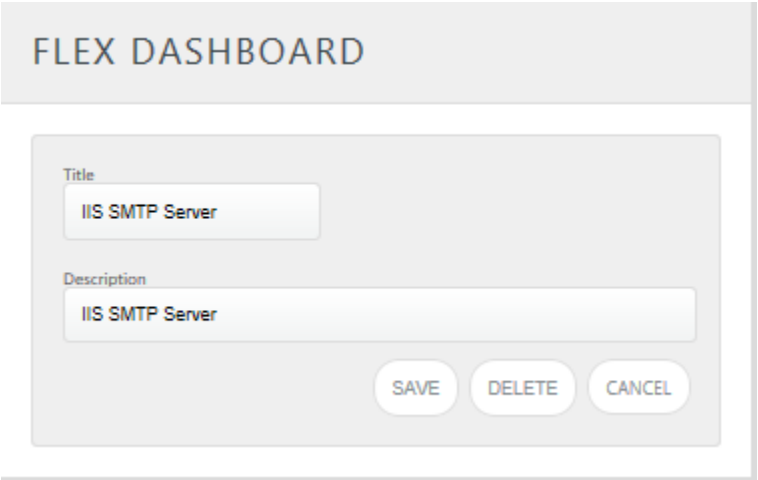

Figure 30

3. Fill suitable title and description and click **Save** button.
4. Click ⚙ to configure a new flex dashlet. Widget configuration pane is shown.

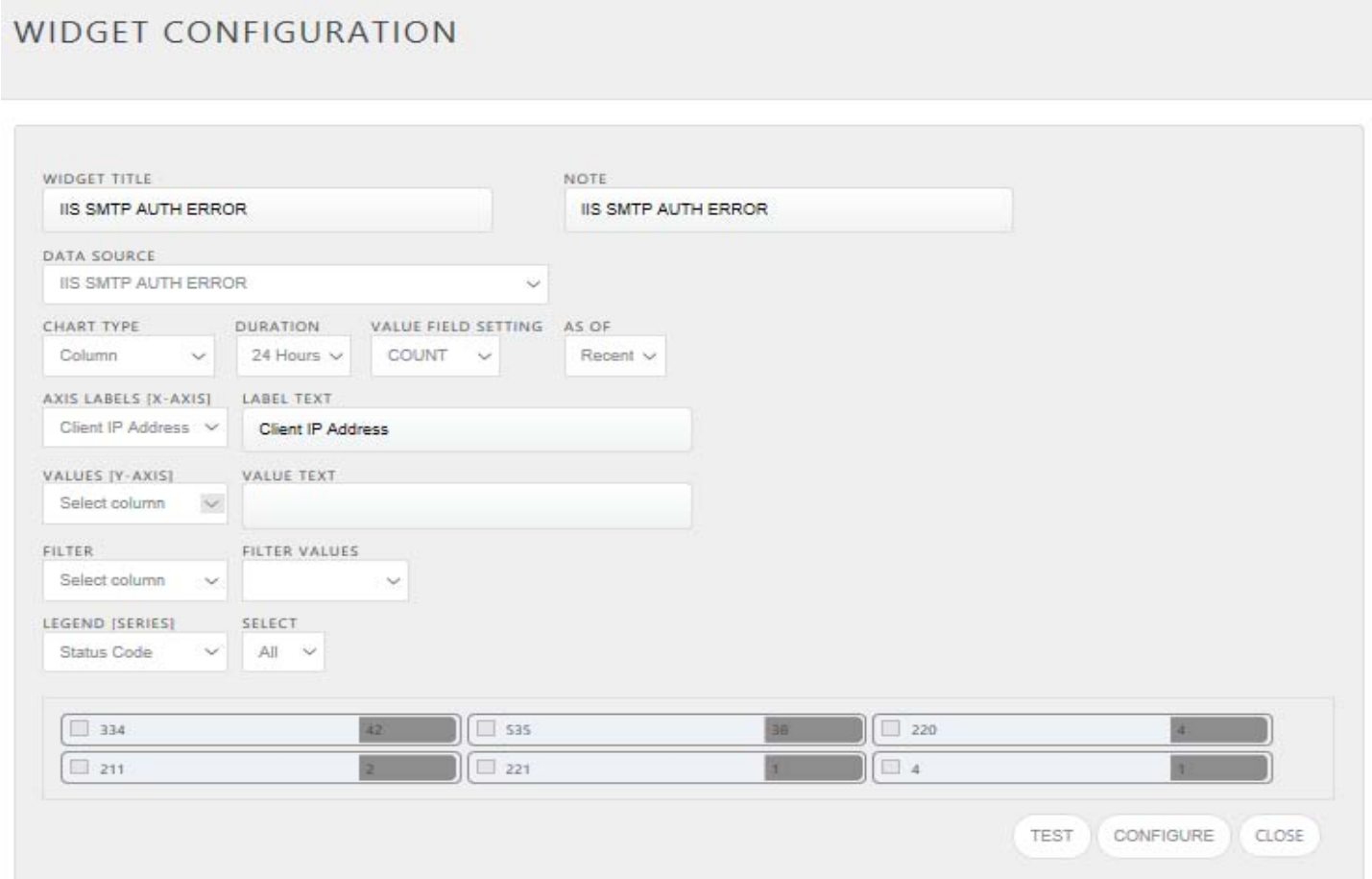

Figure 31

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.

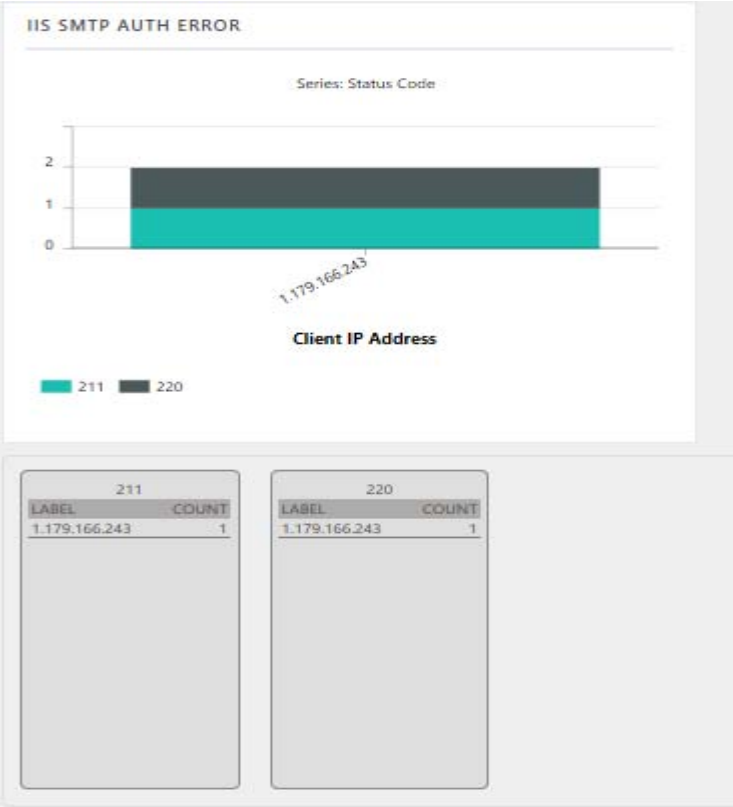

Figure 32

14. If satisfied, click **Configure** button.

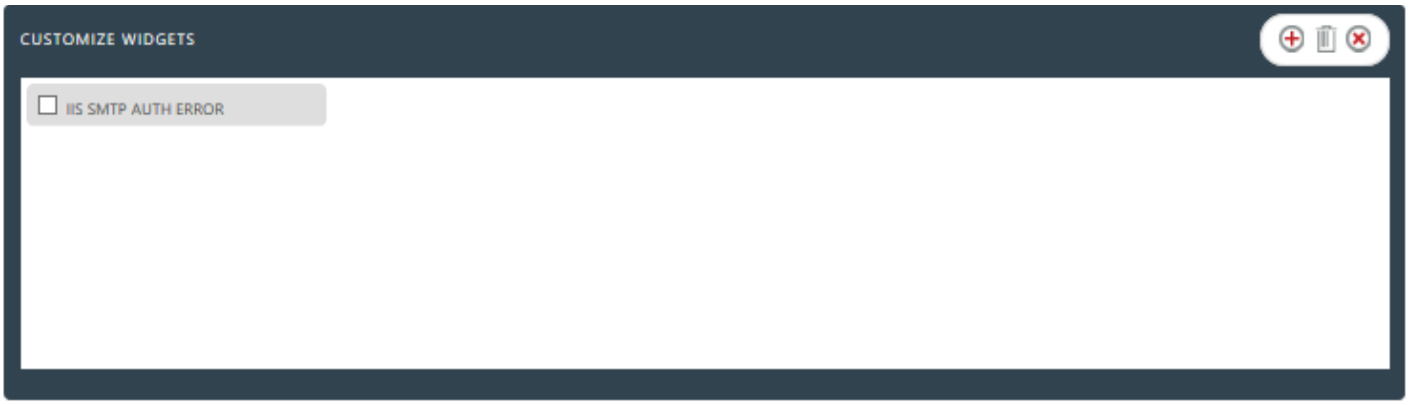

Figure 33

15. Click 'customize' to locate and choose created dashlet.
16. Click to add dashlet to earlier created dashboard.

Sample Flex Dashboards

For below dashboard-

WIDGET TITLE: IIS SMTP ERRORS
DATA SOURCE: IIS SMTP ERROR
CHART TYPE: Column
AXIS LABELS [X-AXIS]: Client IP Address
LEGEND [SERIES]: Client to server Method

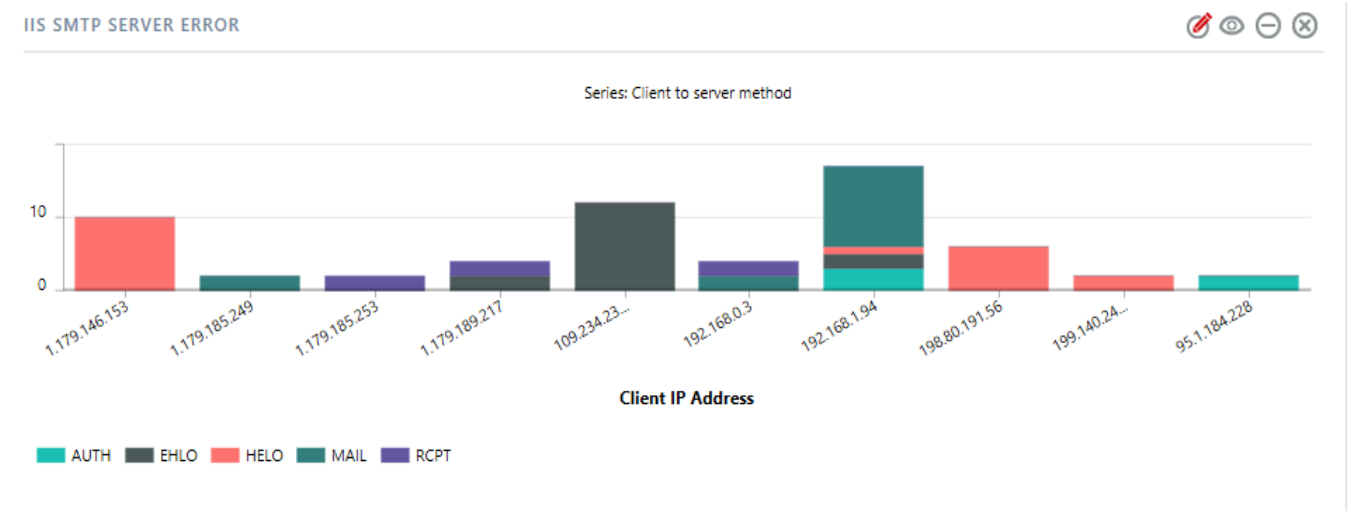

Figure 34

For below dashboard

WIDGET TITLE: IIS SMTP MAIL SENDER Details
DATA SOURCE: IIS SMTP MAIL SENDER and RECEIVER
CHART TYPE: Column
AXIS LABELS [X-AXIS]: sender

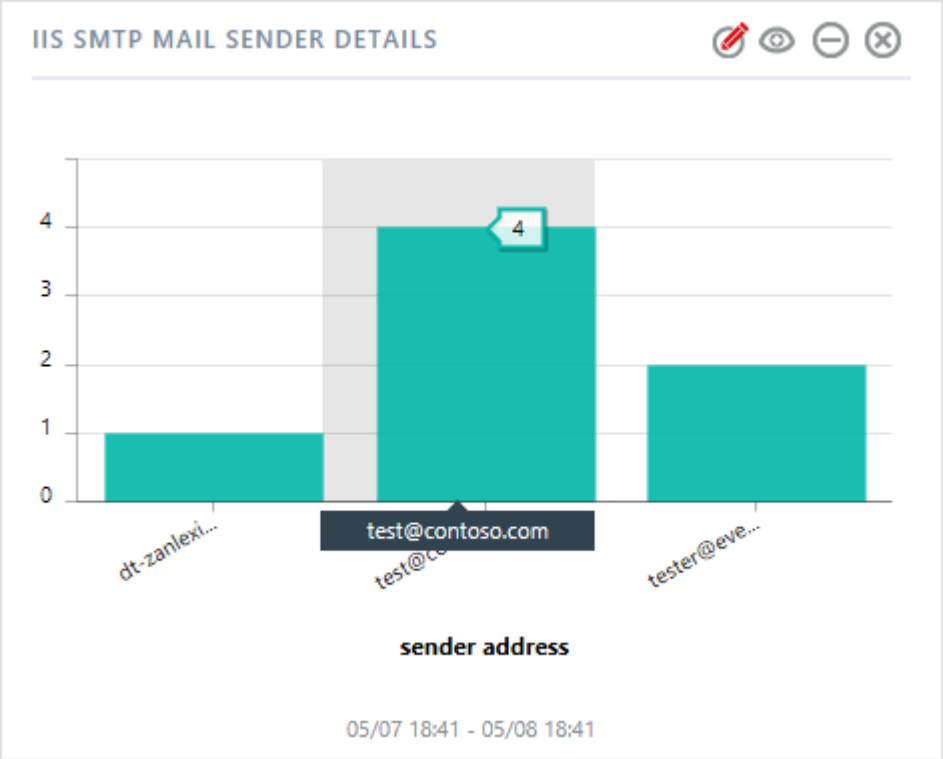

Figure 35

For below dashboard

WIDGET TITLE: IIS SMTP MAIL Recipient Details
DATA SOURCE: IIS SMTP MAIL SENDER and RECEIVER
CHART TYPE: Column
AXIS LABELS [X-AXIS]: Recipient

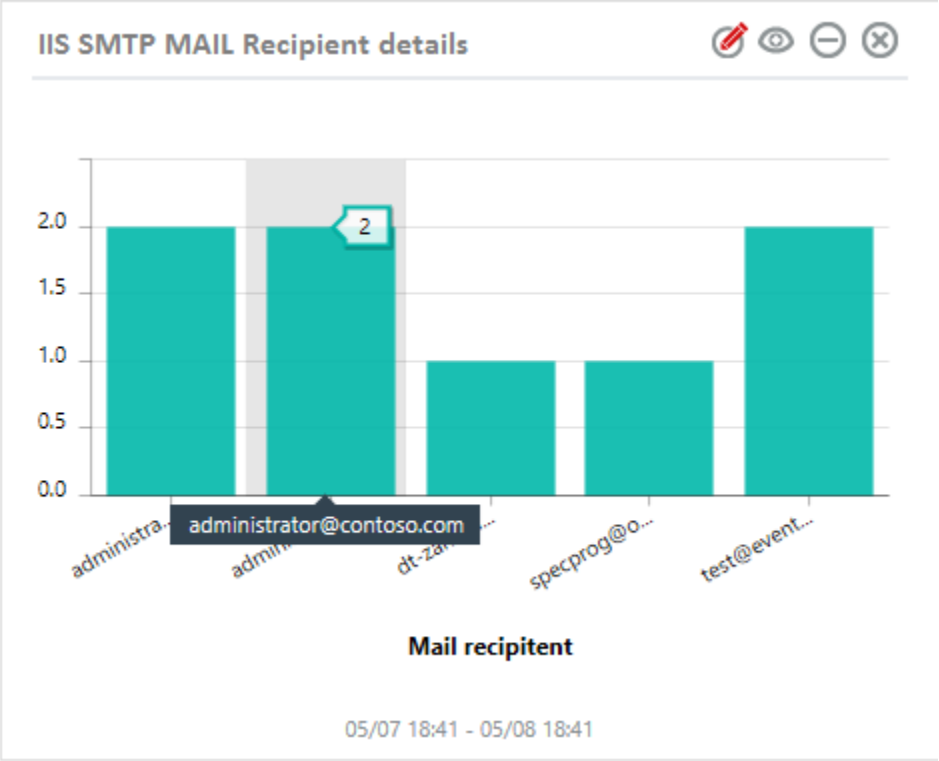

Figure 36

For below dashboard

WIDGET TITLE: IIS SMTP Server ERROR
DATA SOURCE: IIS SMTP ERROR
CHART TYPE: Column
AXIS LABELS [X-AXIS]: Client IP Address
LEGEND [SERIES]: Client to server method

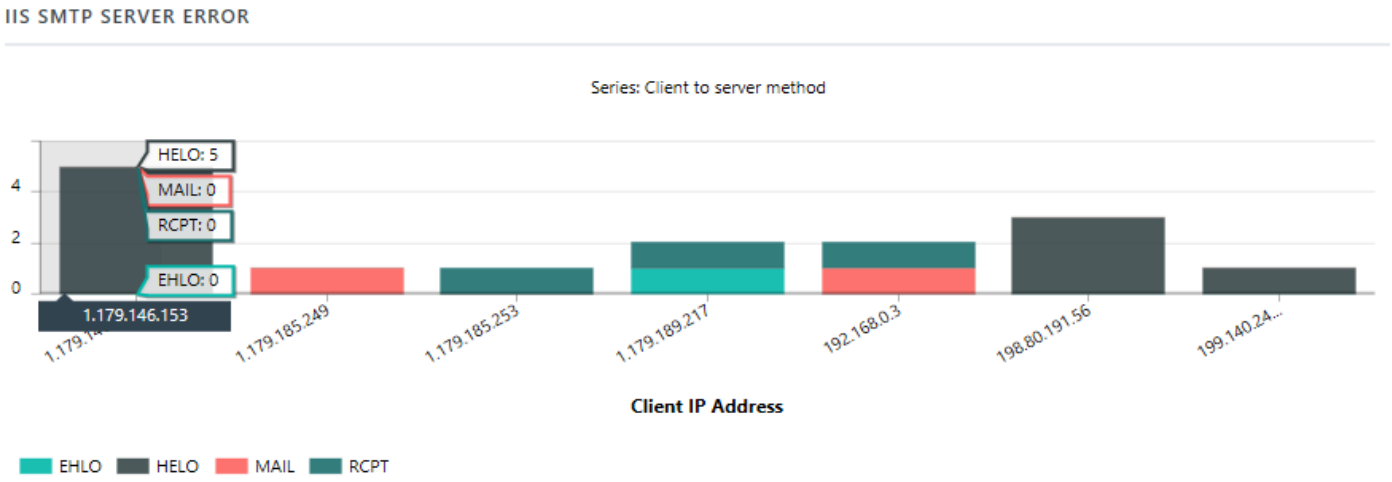

Figure 37

For below dashboard

WIDGET TITLE: Failed EHLO and HELO Request
DATA SOURCE: IIS SMTP EHLO and HELO Request
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Client IP Address
LEGEND[SERIES]: Status Code

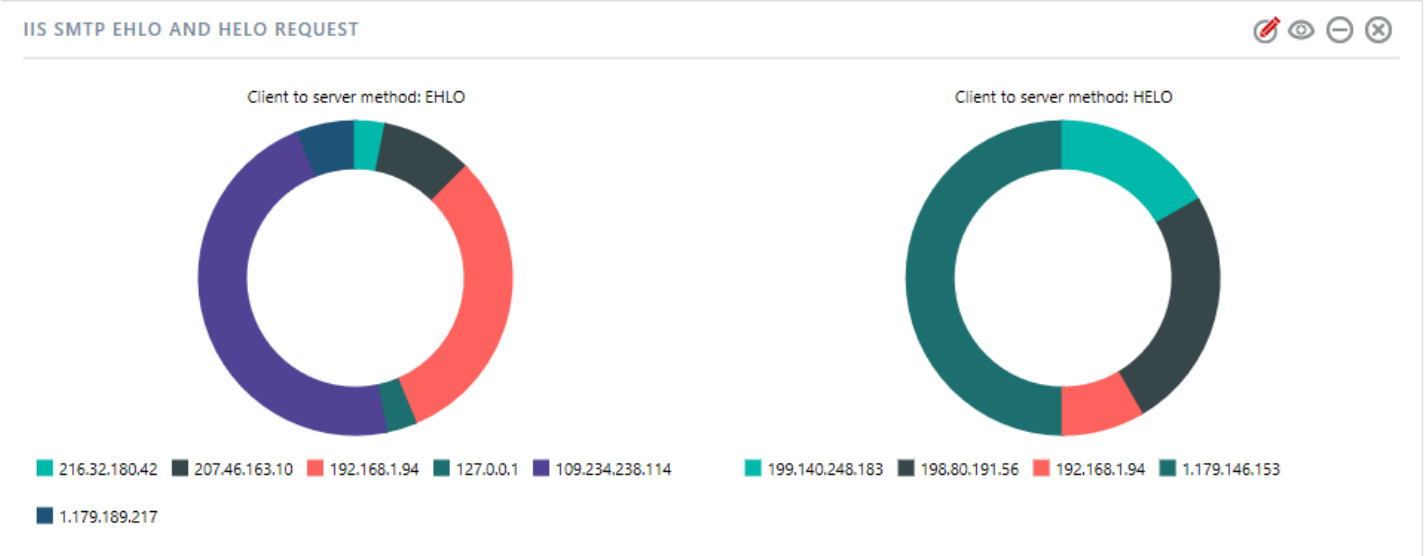

Figure 38

For below dashboard

WIDGET TITLE: IIS SMTP Server Methods
DATA SOURCE: IIS SMTP Server Traffic
CHART TYPE: Column
AXIS LABELS [X-AXIS]: Client to server method
LEGEND [SERIES]: Status Code

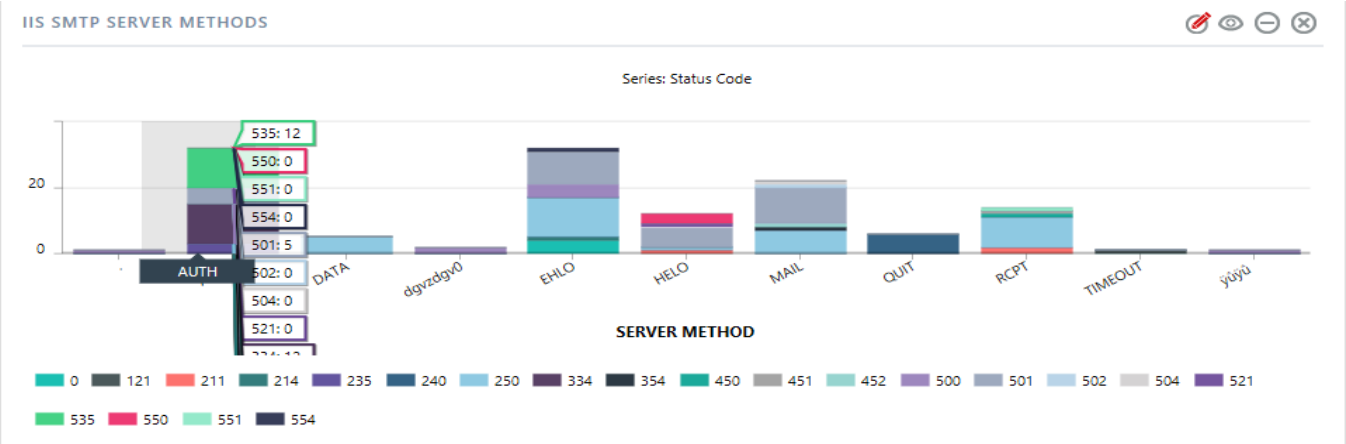

Figure 39

For below dashboard

WIDGET TITLE: Top client IP address
DATA SOURCE: IIS SMTP Server Traffic
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Client ip address

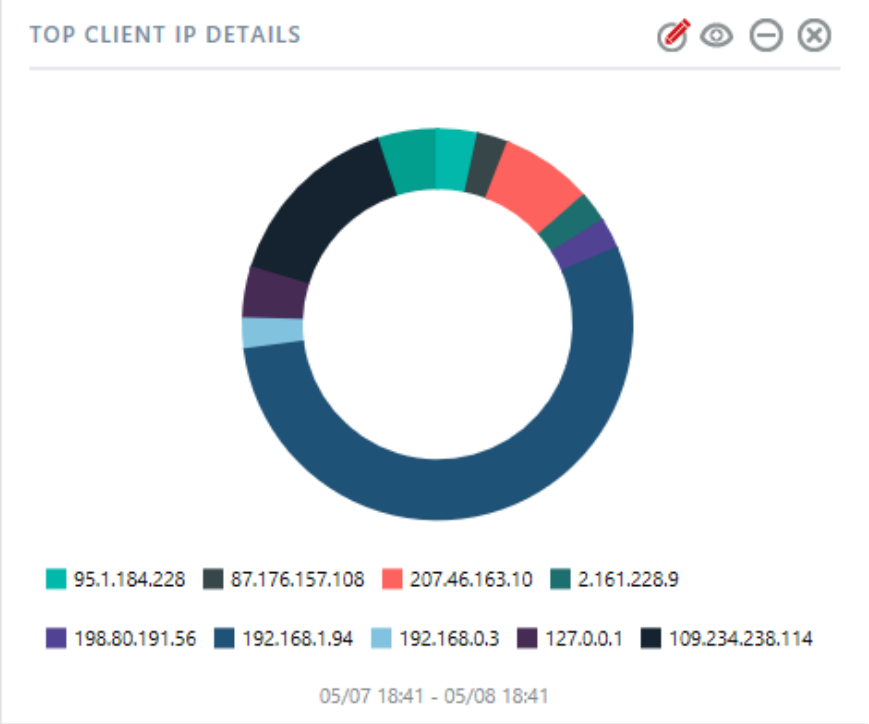

Figure 40