



Actionable Security Intelligence

Integrate IIS SMTP server

EventTracker v8.x and above

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.

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

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

EventTracker 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 EventTracker, 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.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Abstract	1
Audience	1
Overview	3
Prerequisites	3
Integration of IIS SMTP SERVER to EventTracker manager	3
EventTracker Knowledge Pack.....	10
Alerts	10
Flex Reports	10
Knowledge Object	13
Import IIS SMTP Server knowledge pack into EventTracker	14
Knowledge Objects	14
Alerts	16
Flex Reports	17
Verify IIS SMTP Server knowledge pack in EventTracker.....	19
Knowledge Objects	19
Alerts	19
Flex Reports	20
Create Flex Dashboards in EventTracker	21
Schedule Reports	21
Create Dashlets.....	24
Sample Flex Dashboards	28

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**.

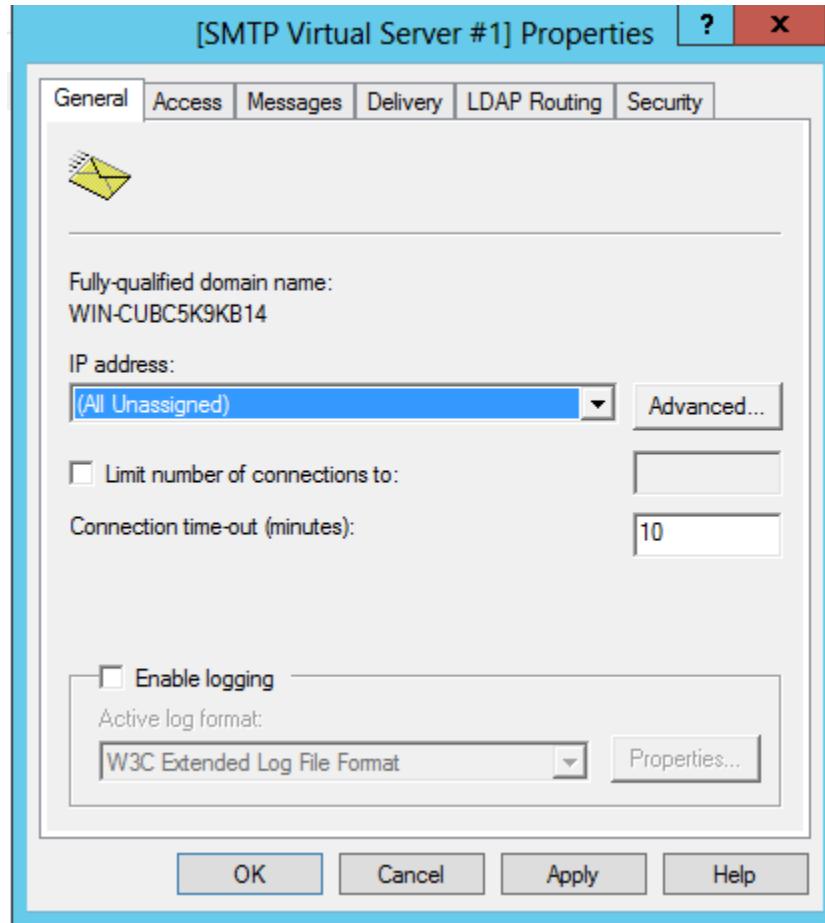


Figure 1

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

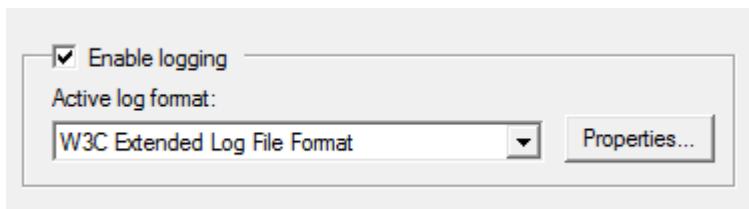


Figure 2

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**

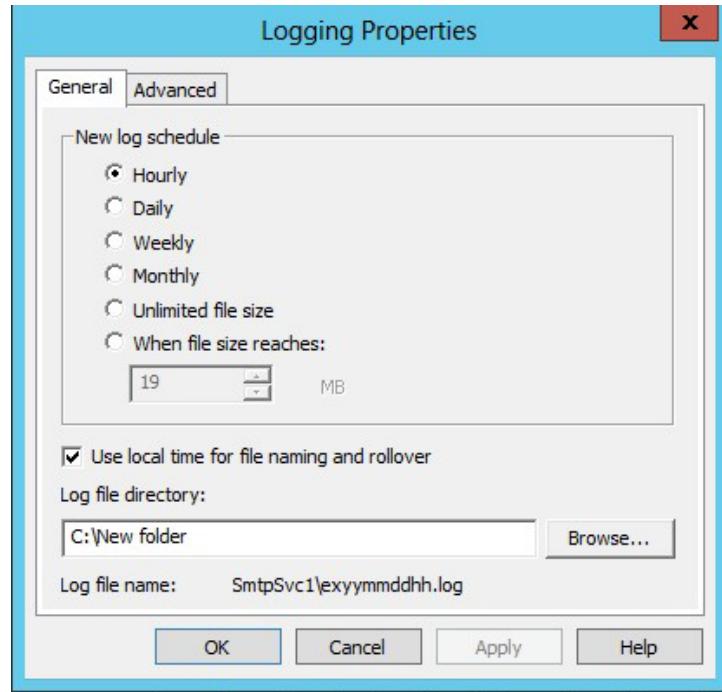


Figure 3

- 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.

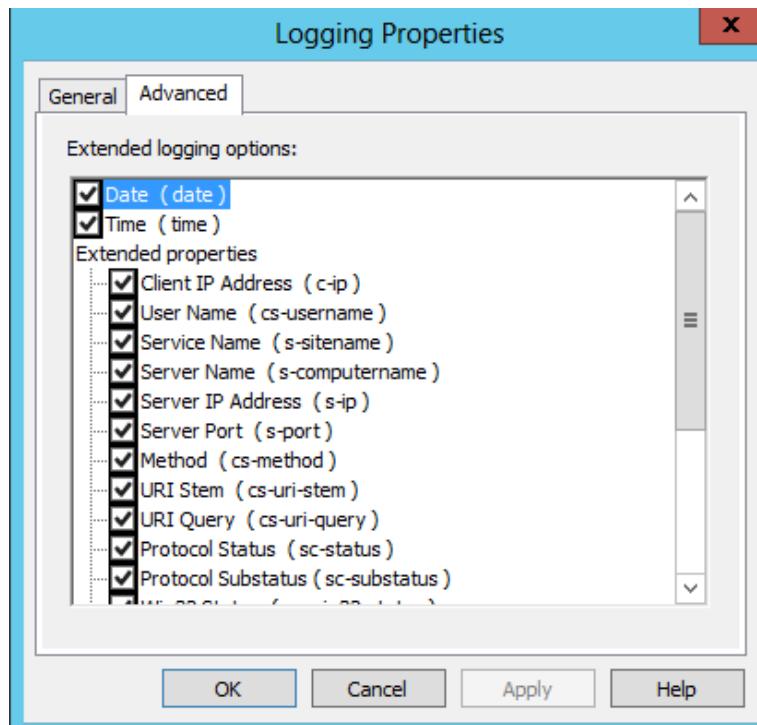


Figure 4

NOTE: We should monitor log file using EventTracker LFM Agent

LFM Configuration:

In EventTracker Control Panel,

1. Click EventTracker Agent Configuration.

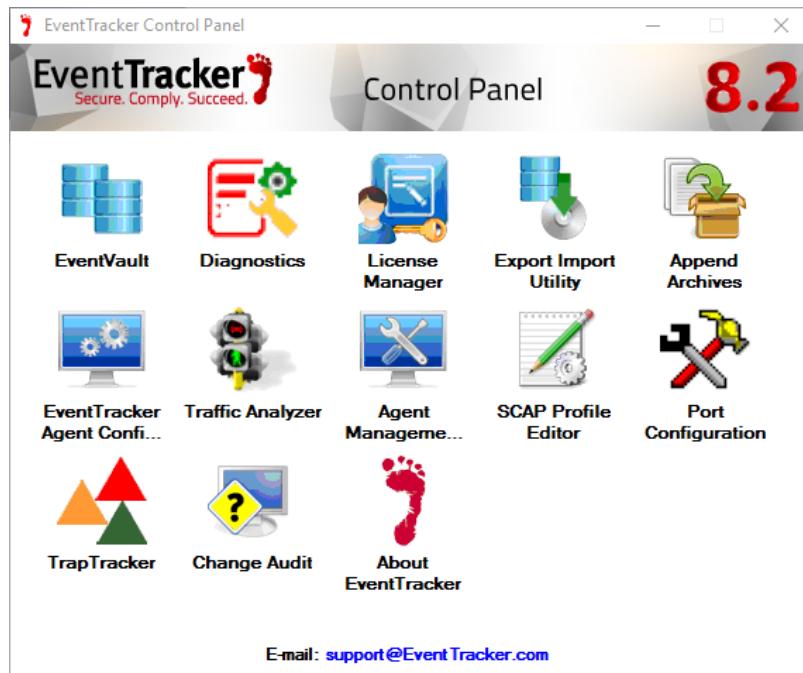


Figure 4

The **EventTracker Agent configuration** page displays.

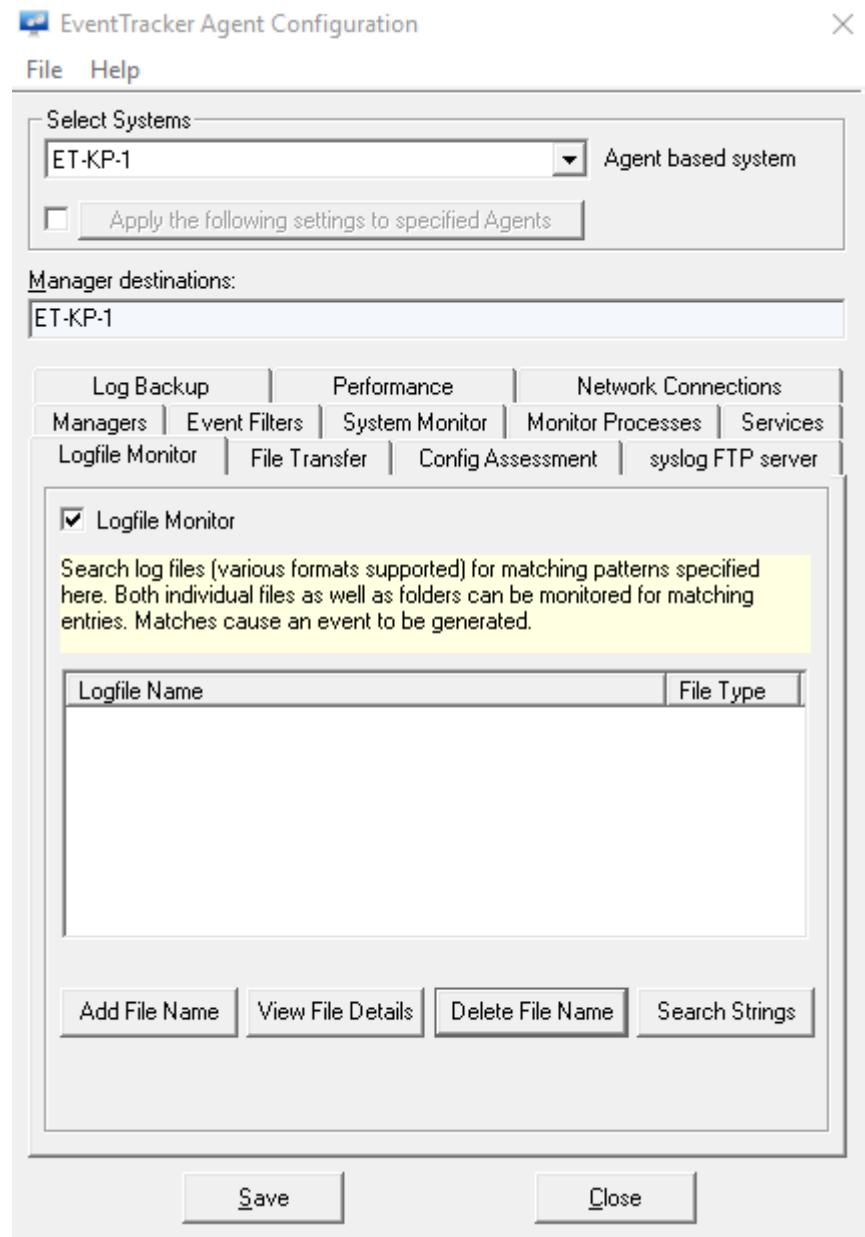


Figure 5

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

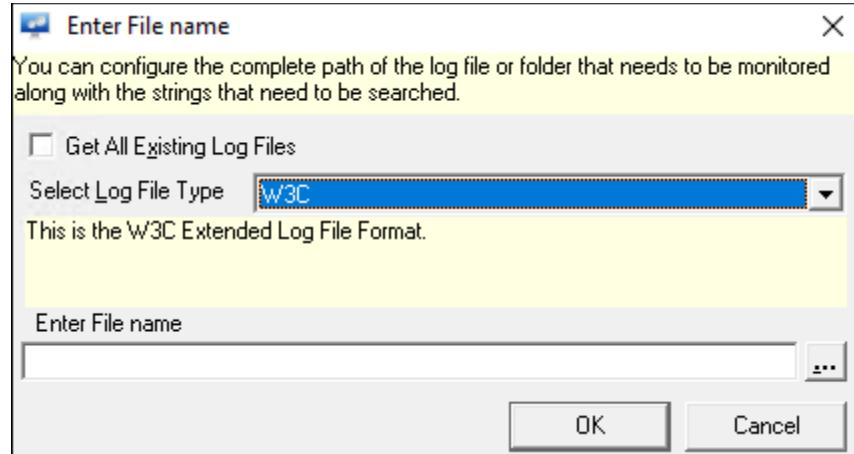


Figure 6

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.

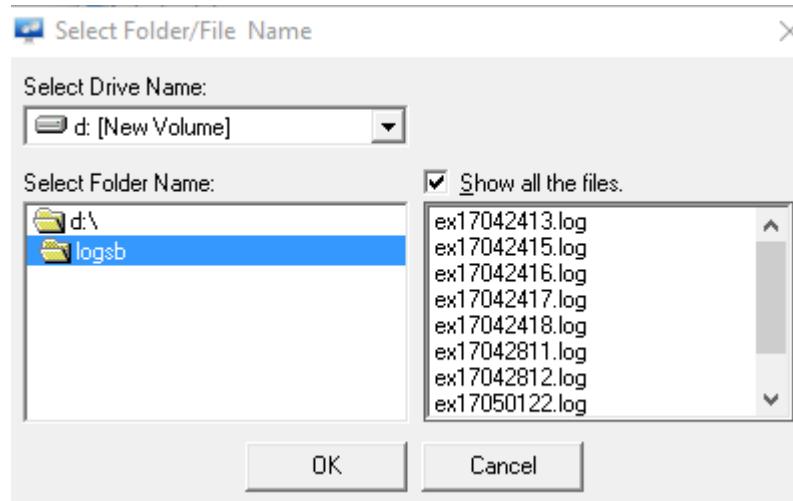


Figure 7

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**

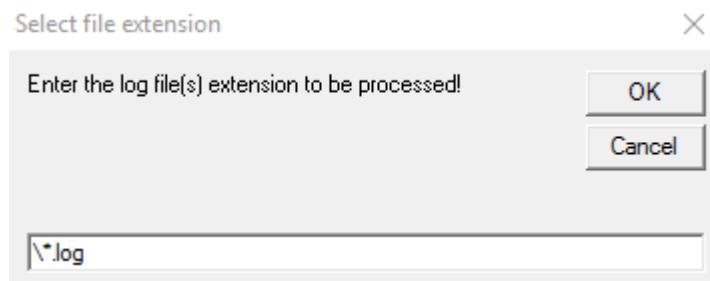


Figure 8

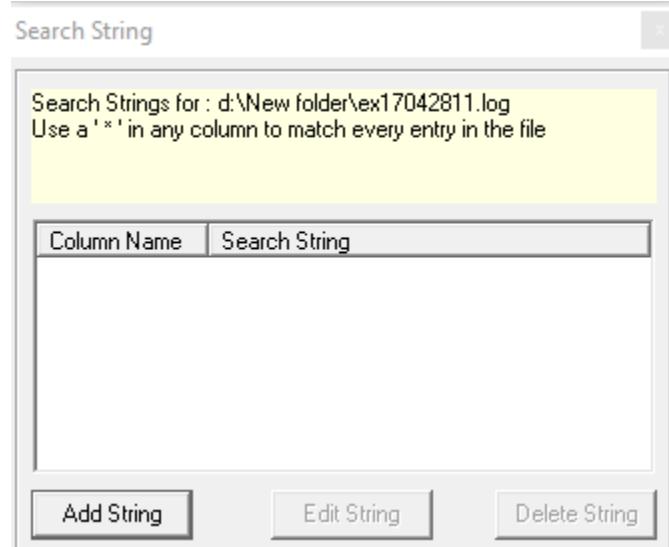


Figure 9

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.

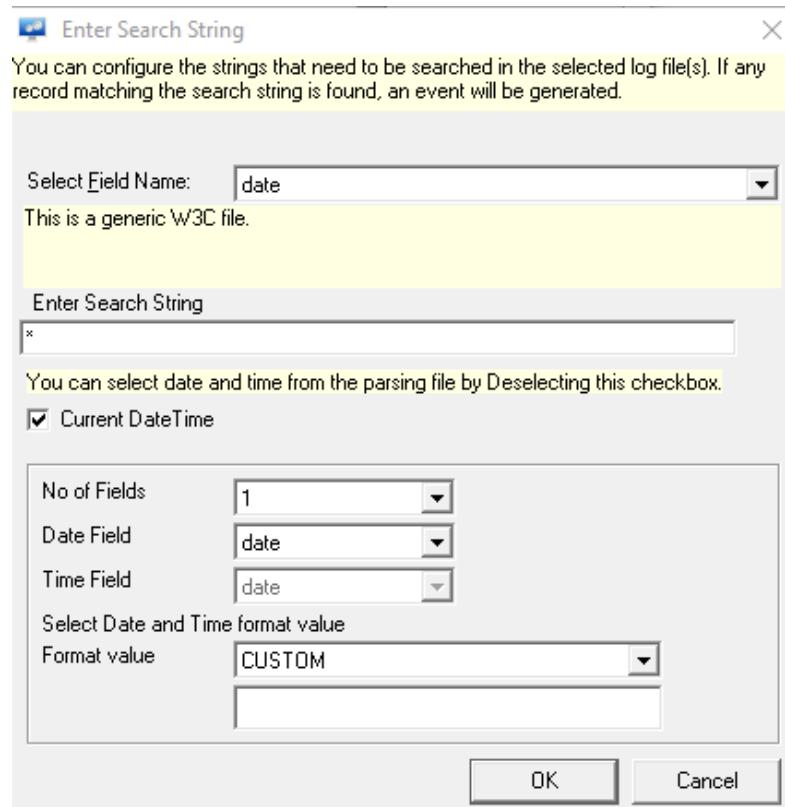


Figure 10

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

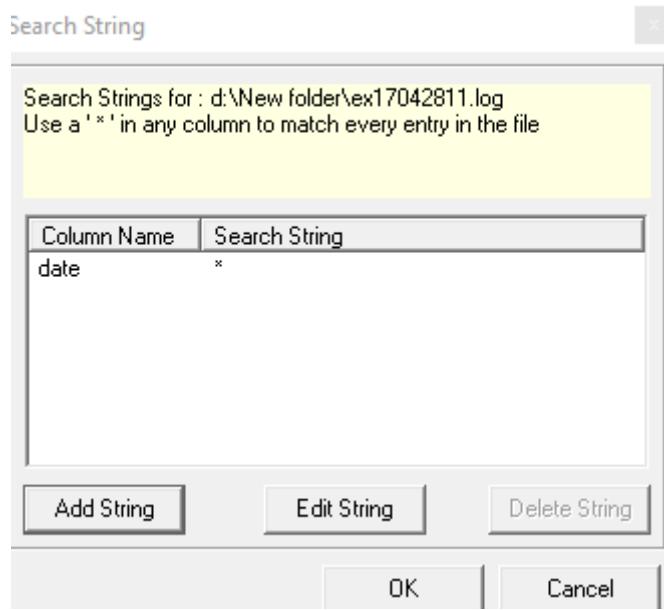


Figure 11

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	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	Recipient	Status Code	Bytes sent	Received	Taken	URI Quer	Version
05/02/2017 11:40:03 AM	ET-KP-1	SMTPSVCI	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	SMTPSVCI	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	SMTPSVCI	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	SMTPSVCI	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	SMTPSVCI	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	SMTPSVCI	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	Description:
Log Type: Application	ENTRY:
Category Id: 0	date: 3/4/2017
	time: 23:56:20
	c-ip: 1.179.176.37
	cs-username: DOCUTRACK0254
	s-sitename: SMTPSVCI
	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 Quer	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	192.168.194	+Administrator@contoso.com	501	30	27	0
05/08/2017 06:41:01 PM	ET-KP-1	HELO	192.168.194	+Administrator@contoso.com	501	30	27	0
05/08/2017 06:41:01 PM	ET-KP-1	EHLO	192.168.194	+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	Recipient	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 Object**, and then click **Import** button

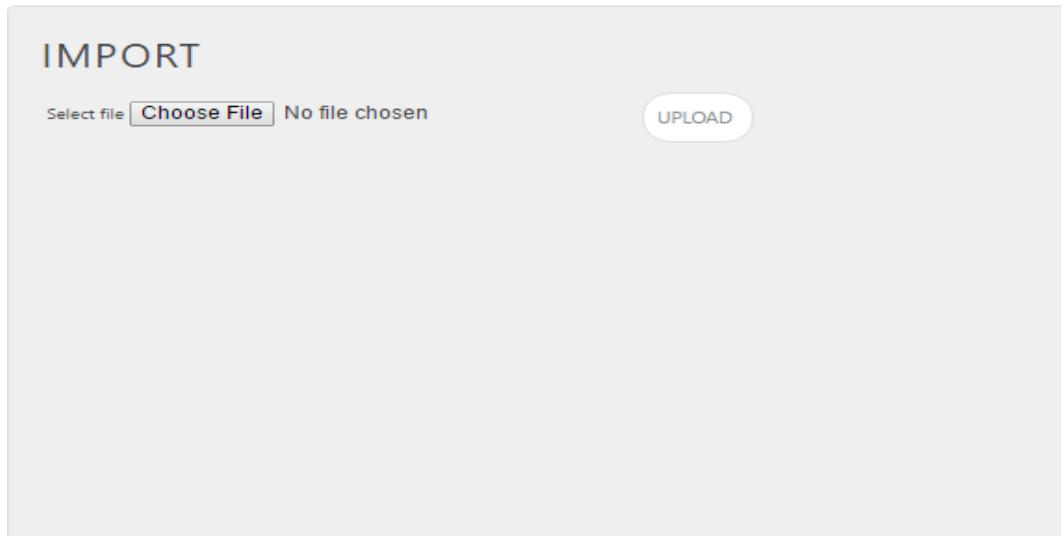


Figure 13

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

IMPORT			
Select file	Browse...	UPLOAD	
<input type="checkbox"/>	OBJECT NAME	APPLIES TO	GROUP NAME
<input checked="" type="checkbox"/>	IIS SMTP Authentication errors	Windows server 2008 or later	IIS SMTP Server
<input checked="" type="checkbox"/>	IIS SMTP Server	Windows Server 2008 or later	IIS SMTP Server

Figure 14

4. Knowledge objects are now imported successfully.

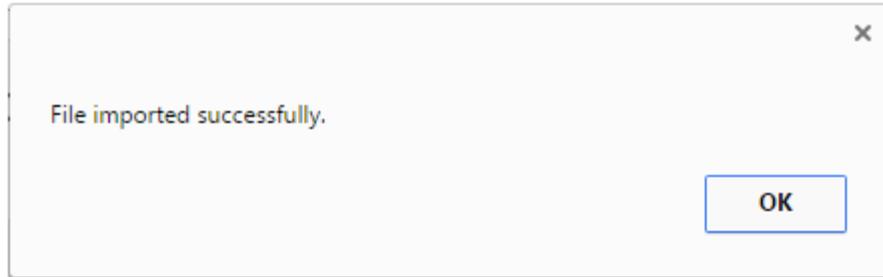


Figure 15

Alerts

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

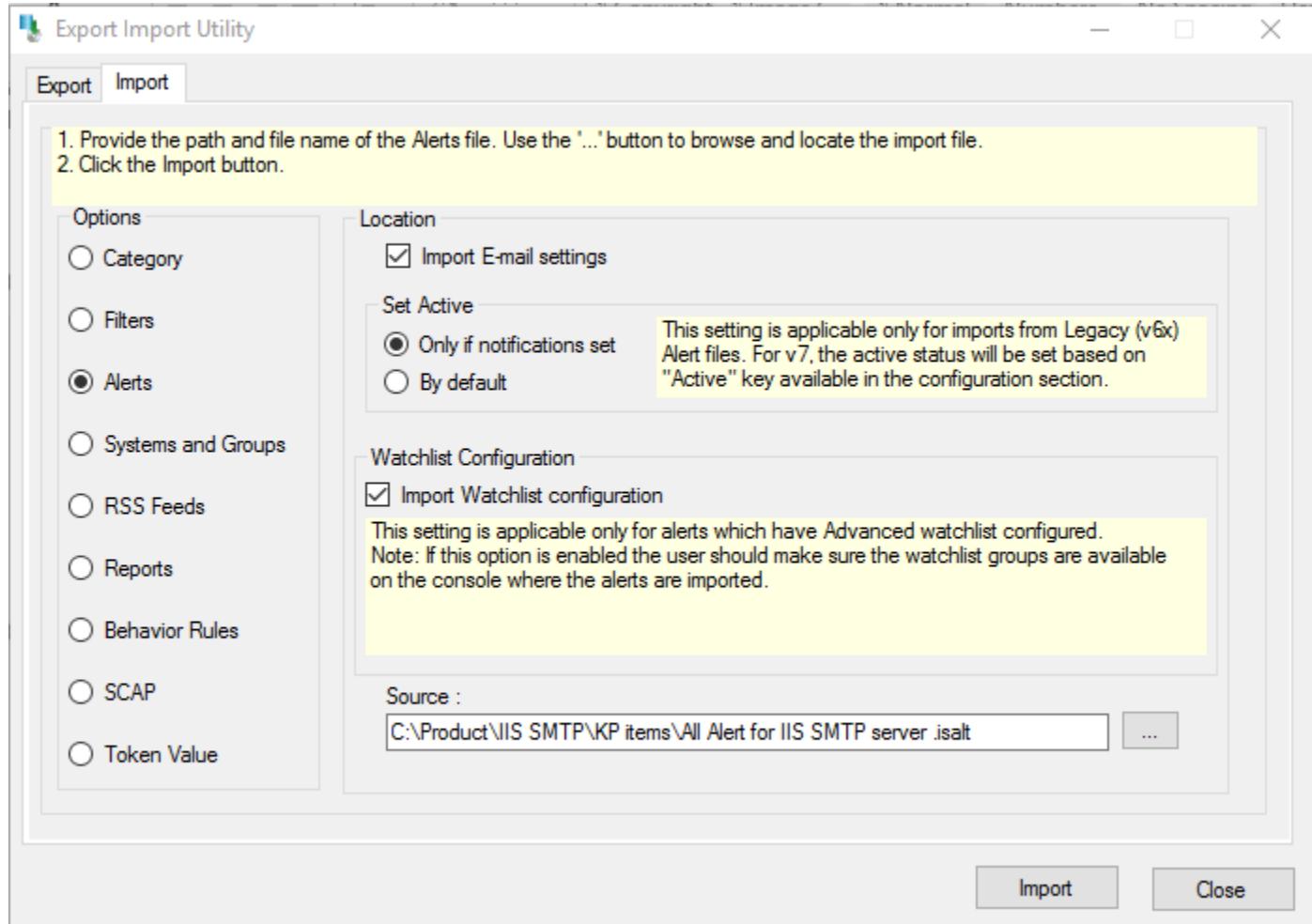


Figure 16

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

EventTracker displays success message.

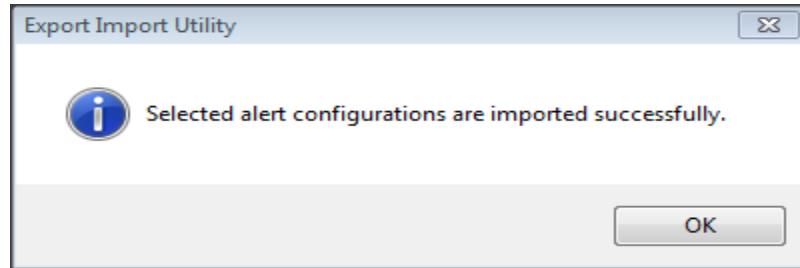


Figure 17

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

Flex Reports

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

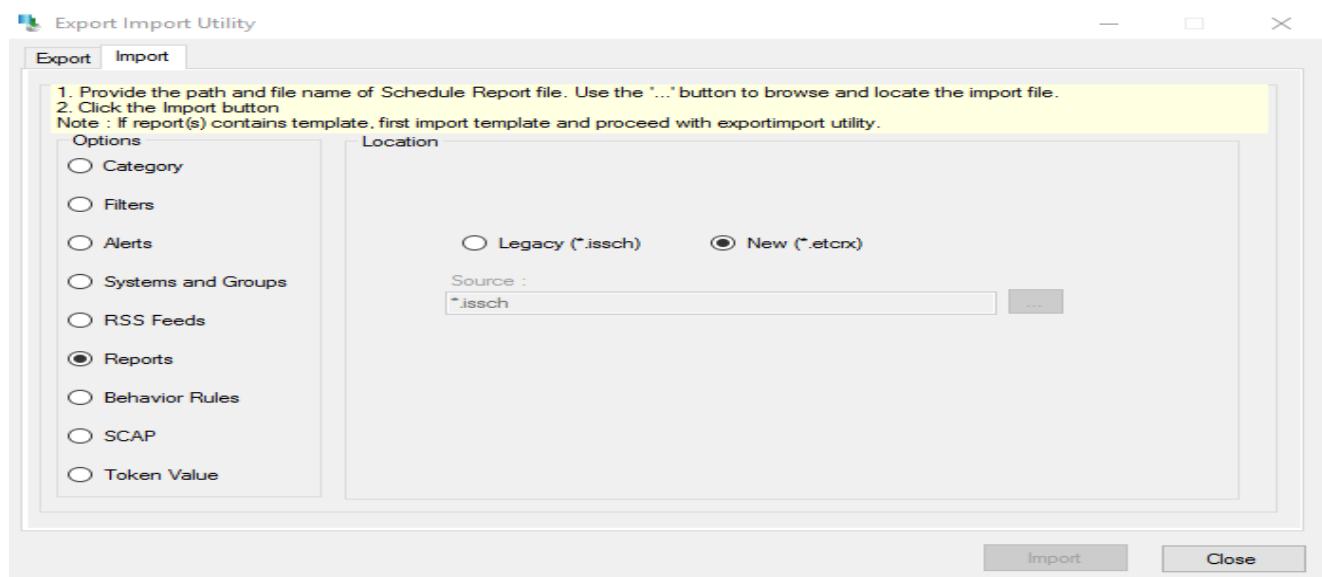


Figure 18

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

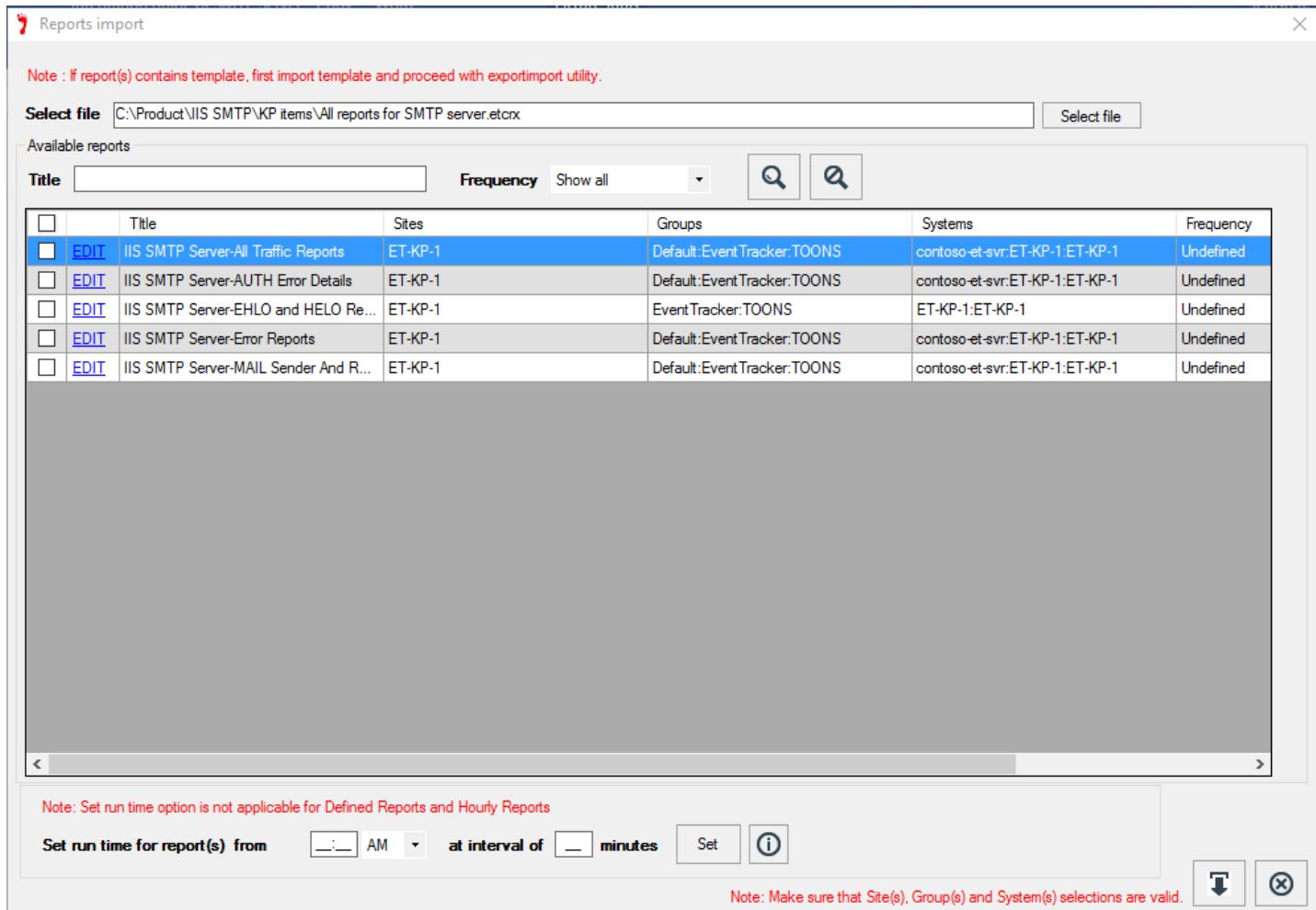


Figure 19

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

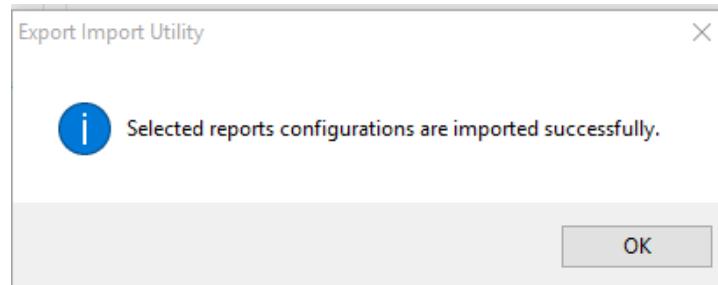


Figure 20

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.

The screenshot shows the 'KNOWLEDGE OBJECTS' page in the EventTracker web interface. On the left, there's a sidebar titled 'GROUPS' with various network device and system categories like FortiGate Firewall, HP ProCurve Switch, and IIS SMTP Server. The 'IIS SMTP Server' category is expanded, showing two sub-items: 'IIS SMTP Authenticat...' and 'IIS SMTP Server'. The main panel displays a rule for 'IIS SMTP SERVER Traffic'. The rule details are as follows:

OBJECT NAME	IIS SMTP Server		
APPLIES TO	Windows Server 2008 or later		
RULES			
TITLE	IIS SMTP SERVER Traffic		
LOG TYPE	EventTracker		
EVENT SOURCE	3230		
EVENT ID			
EVENT TYPE			
MESSAGE SIGNATURE:		(?s:date\ ;*time.*c-ip.*cs-username.*cs-version\\s+SMTP	
MESSAGE EXCEPTION			
EXPRESSIONS			
EXPRESSION TYPE	FORMAT STRING	EXPRESSION 1	EXPRESSION 2

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.

The screenshot shows the 'ALERT MANAGEMENT' section of the EventTracker interface. At the top, there is a search bar with the text 'iis smtp' and a magnifying glass icon. Below the search bar, a message says 'Click 'Activate Now' after making all changes.' To the right, there are buttons for 'Total: 4' and 'Page Size 25'. The main area is a table with the following columns: ALERT NAME, THREAT, ACTIVE, E-MAIL, MESSAGE, RSS, FORWARD AS SNMP, FORWARD AS SYSLOG, REMEDIAL ACTION AT CONSOLE, REMEDIAL ACTION AT AGENT, and APPLIES TO. The table contains four rows of data:

	<u>ALERT NAME</u>	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
<input type="checkbox"/>	IIS SMTP SERVER : AUTH Error	<input type="checkbox"/> High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IIS SMTP 6.0 or later					
<input type="checkbox"/>	IIS SMTP SERVER : EHLO or HELO Brute...	<input type="checkbox"/> High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IIS SMTP 6.0 or later					
<input type="checkbox"/>	IIS SMTP SERVER : Slow Mail Flow	<input type="checkbox"/> High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IIS SMTP 6.0 or later					
<input type="checkbox"/>	IIS SMTP Server:SPAM Blacklist IP detect...	<input type="checkbox"/> High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IIS SMTP 6.0 or later					

At the bottom left of the table area is a 'DELETE' button.

Figure 22

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

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

EventTracker displays message box.

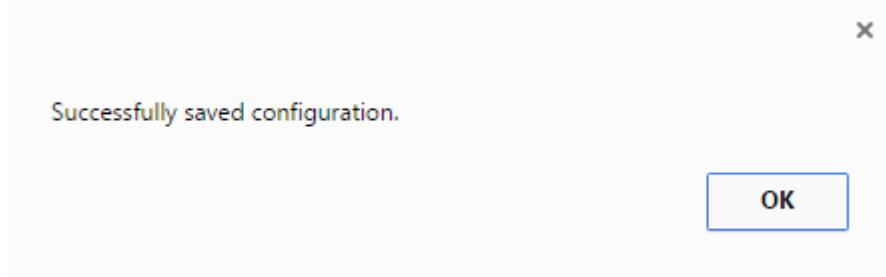


Figure 23

- 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

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

EventTracker displays Flex reports of 'IIS SMTP Server'

The screenshot shows the 'REPORTS CONFIGURATION' page in EventTracker. On the left, there's a sidebar titled 'REPORT GROUPS' listing various network devices with edit icons. The main area is titled 'REPORTS CONFIGURATION : IIS SMTP SERVER' and contains a table of five reports. The table has columns for 'TITLE', 'CREATED ON', and 'MODIFIED ON'. Each report row includes a checkbox, a preview icon, and a detailed link. A search bar at the top right shows 'iis smtp' and a total count of 5.

	TITLE	CREATED ON	MODIFIED ON
<input type="checkbox"/>	IIS SMTP Server-EHLO and HELO Request Details	5/4/2017 1:04:41 PM	5/9/2017 10:31:37 AM
<input type="checkbox"/>	IIS SMTP Server-AUTH Error Details	5/3/2017 2:43:30 PM	5/9/2017 1:02:52 PM
<input type="checkbox"/>	IIS SMTP Server-Error Reports	5/2/2017 2:26:42 PM	5/9/2017 11:50:51 AM
<input type="checkbox"/>	IIS SMTP Server-MAIL Sender And Receiver Details	5/2/2017 1:50:16 PM	5/9/2017 1:02:04 PM
<input type="checkbox"/>	IIS SMTP Server-All Traffic Reports	5/2/2017 12:28:06 PM	5/9/2017 10:35:46 AM

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.

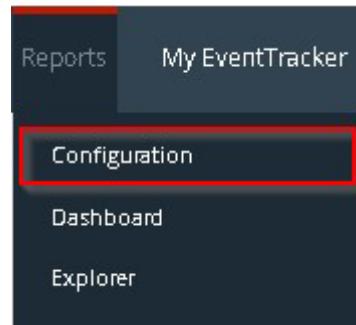


Figure 25

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

The screenshot shows the 'REPORTS CONFIGURATION' page. On the left, there's a sidebar titled 'REPORT GROUPS' with a '+' icon and a delete icon. It lists several report groups: FortiGate Firewall, HP ProCurve Switch, IIS SMTP Server, Imperva, Infoblox, Juniper JUNOS, Juniper Netscreen, and Kaspersky Security C... Each group has edit and delete icons. The main area is titled 'REPORTS CONFIGURATION : IIS SMTP SERVER' and shows a table of reports. The table has columns: 'TITLE', 'CREATED ON', and 'MODIFIED ON'. There are five entries, each with a checkbox, a gear icon, and a plus sign icon. The last entry is 'IIS SMTP Server-All Traffic Reports'. A 'Total: 5' button is at the top right of the table. At the bottom right of the main area, there are three icons: a magnifying glass, a checkmark, and a calendar.

	TITLE	CREATED ON	MODIFIED ON
<input type="checkbox"/>	IIS SMTP Server-EHLO and HELO Request Details	5/4/2017 1:04:41 PM	5/9/2017 10:31:37 AM
<input type="checkbox"/>	IIS SMTP Server-AUTH Error Details	5/3/2017 2:43:30 PM	5/9/2017 1:02:52 PM
<input type="checkbox"/>	IIS SMTP Server-Error Reports	5/2/2017 2:26:42 PM	5/9/2017 11:50:51 AM
<input type="checkbox"/>	IIS SMTP Server-MAIL Sender And Receiver Details	5/2/2017 1:50:16 PM	5/9/2017 1:02:04 PM
<input type="checkbox"/>	IIS SMTP Server-All Traffic Reports	5/2/2017 12:28:06 PM	5/9/2017 10:35:46 AM

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.

REPORT WIZARD

TITLE: IIS SMTP MAIL SENDER AND RECEIVER

LOGS

Review cost details and configure the publishing options.

Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:01:24(HH:MM:SS)

Number of log(s) to be processed: 27

Available disk space: 305 GB

Required disk space: 50 MB

Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)

Deliver results via E-mail

Notify results via E-mail

To E-mail: [Text input field] (Use comma(,) to separate multiple e-mail recipients)

Update status via RSS: Select Feed ▾

Show in: none ▾

Persist data in EventVault Explorer

Figure 27

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

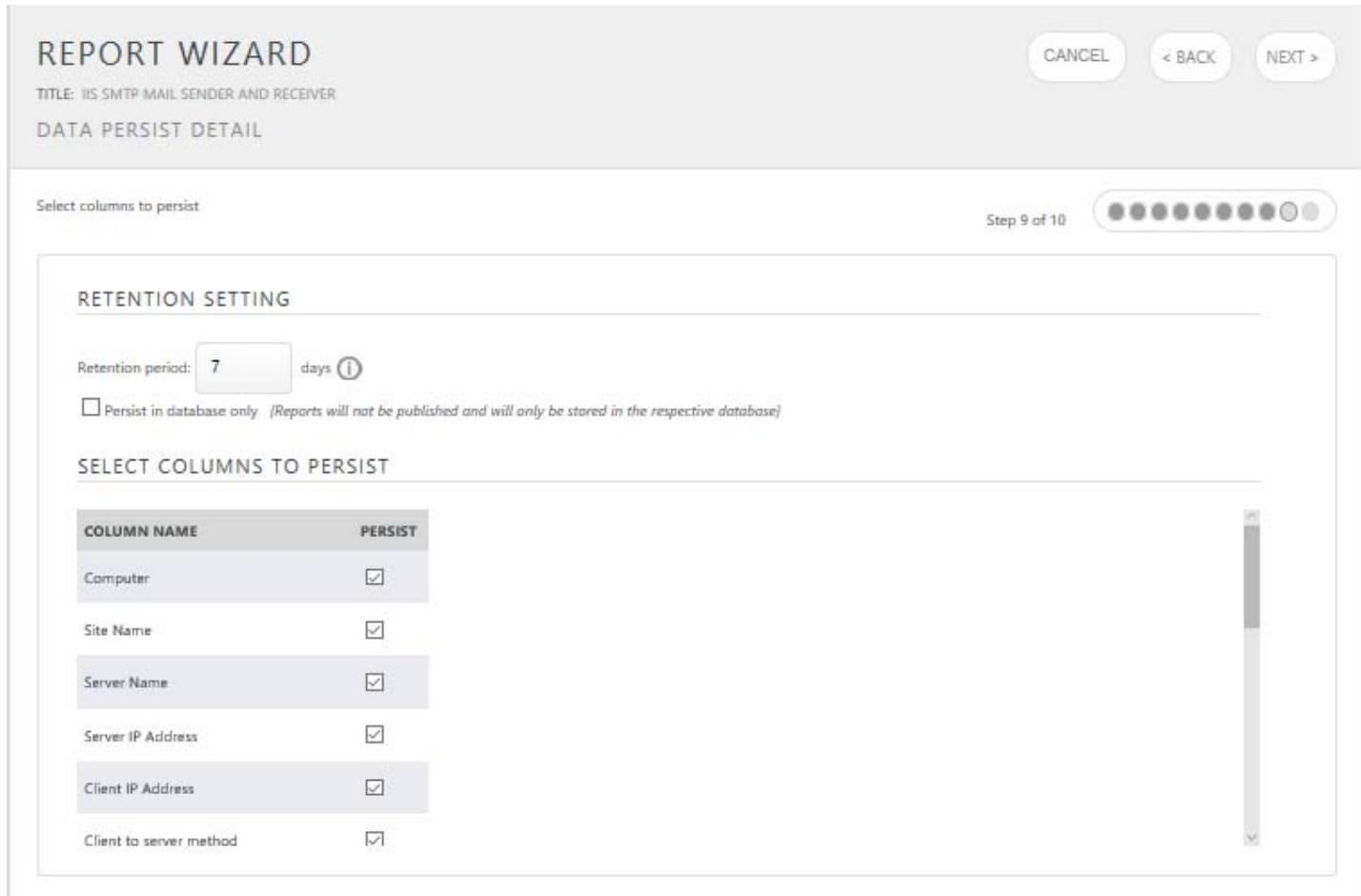


Figure 28

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.

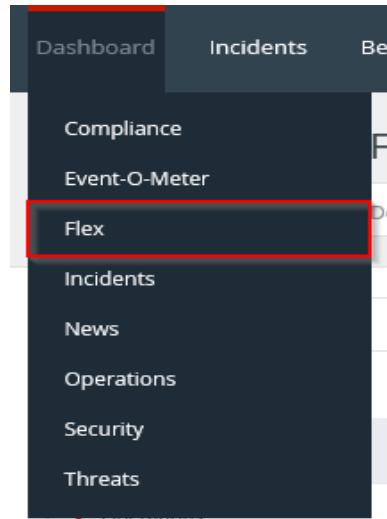


Figure 29

2. Navigate to **Dashboard>Flex**.

Flex Dashboard pane is shown.

A screenshot of the Flex Dashboard configuration pane. It has two input fields: 'Title' containing 'IIS SMTP Server' and 'Description' also containing 'IIS SMTP Server'. Below the fields are three buttons: 'SAVE', 'DELETE', and 'CANCEL'.

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.

WIDGET CONFIGURATION

The screenshot shows the 'Widget Configuration' interface. At the top left is the 'WIDGET TITLE' field containing 'IIS SMTP AUTH ERROR'. To its right is the 'NOTE' field also containing 'IIS SMTP AUTH ERROR'. Below these are sections for 'DATA SOURCE' (set to 'IIS SMTP AUTH ERROR'), 'CHART TYPE' (set to 'Column'), 'DURATION' (set to '24 Hours'), 'VALUE FIELD SETTING' (set to 'COUNT'), and 'AS OF' (set to 'Recent'). Under 'AXIS LABELS [X-AXIS]', 'Client IP Address' is selected as the label. In the 'VALUES [Y-AXIS]' section, 'Select column' is chosen. A 'FILTER' section allows selecting a column and filtering values, with 'Status Code' selected and 'All' chosen. Below this is a legend table:

	334	42	535	38	220	4
	334	42	535	38	220	4
	211	2	221	1	4	3

At the bottom right are three buttons: 'TEST', 'CONFIGURE', and 'CLOSE'.

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.

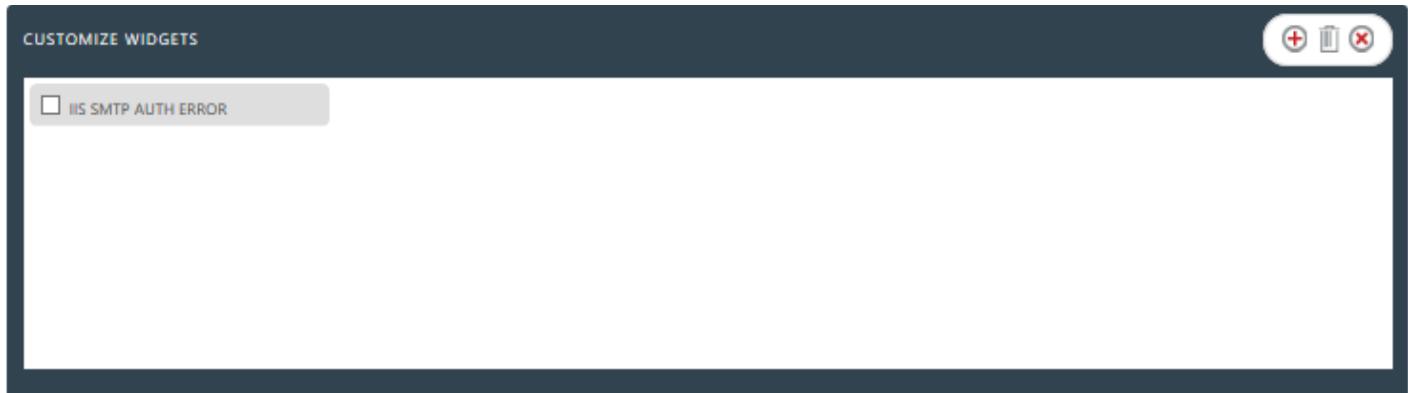


Figure 33

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

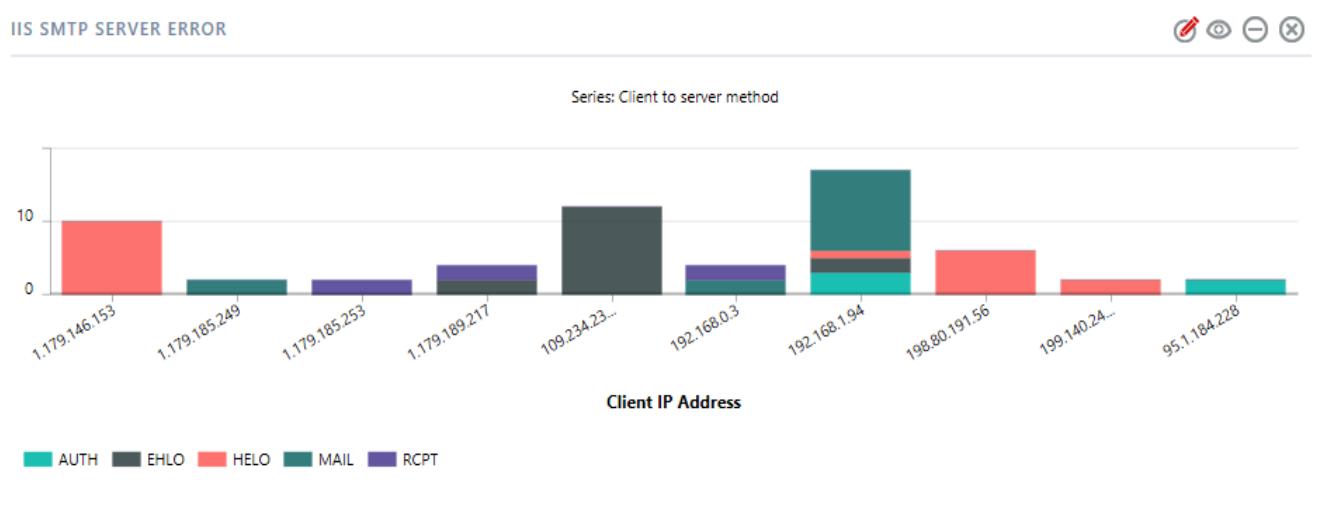


Figure 34

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

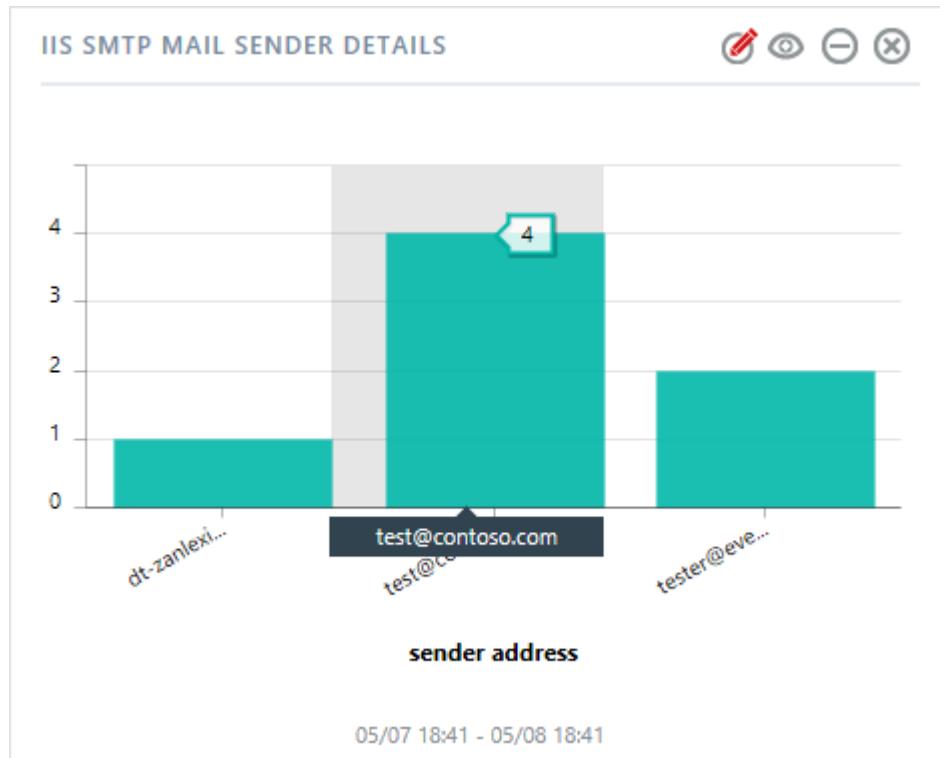


Figure 35

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

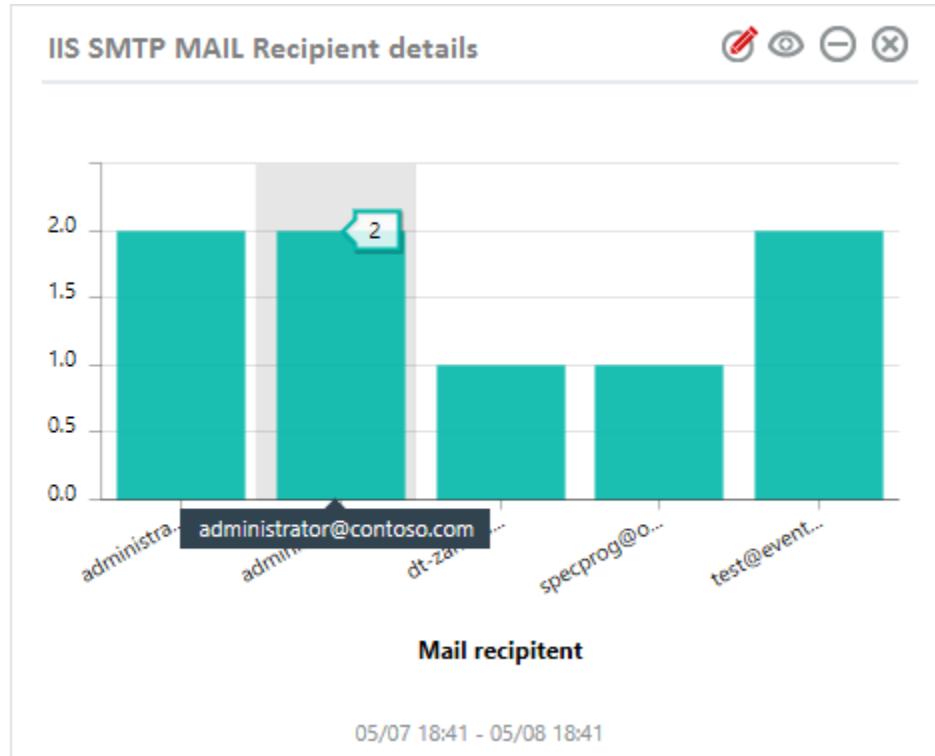


Figure 36

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

IIS SMTP SERVER ERROR

Series: Client to server method

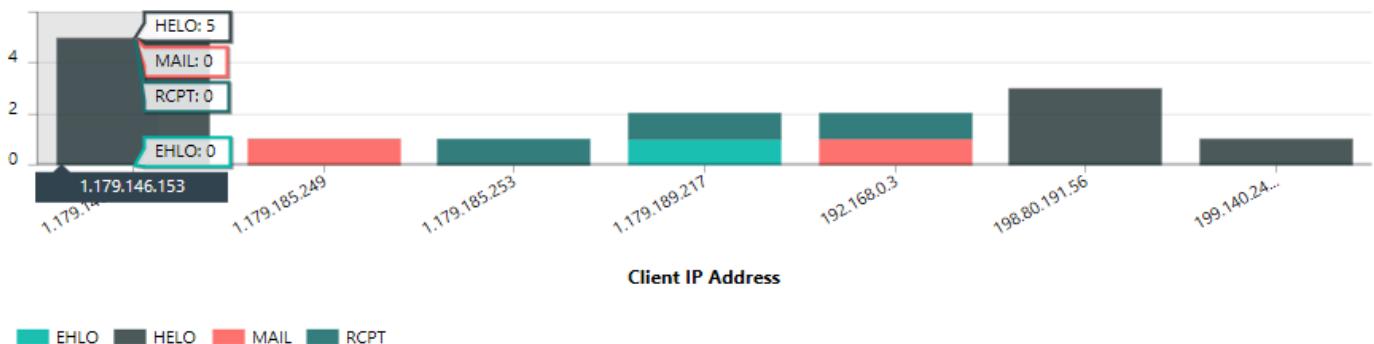


Figure 37

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

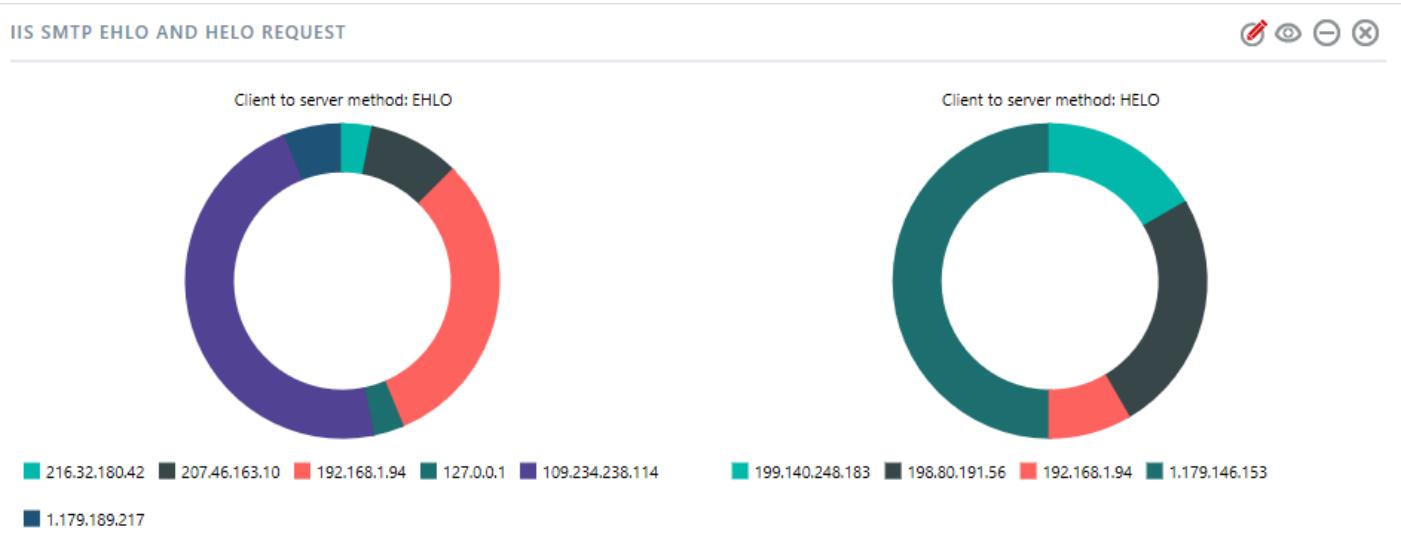


Figure 38

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

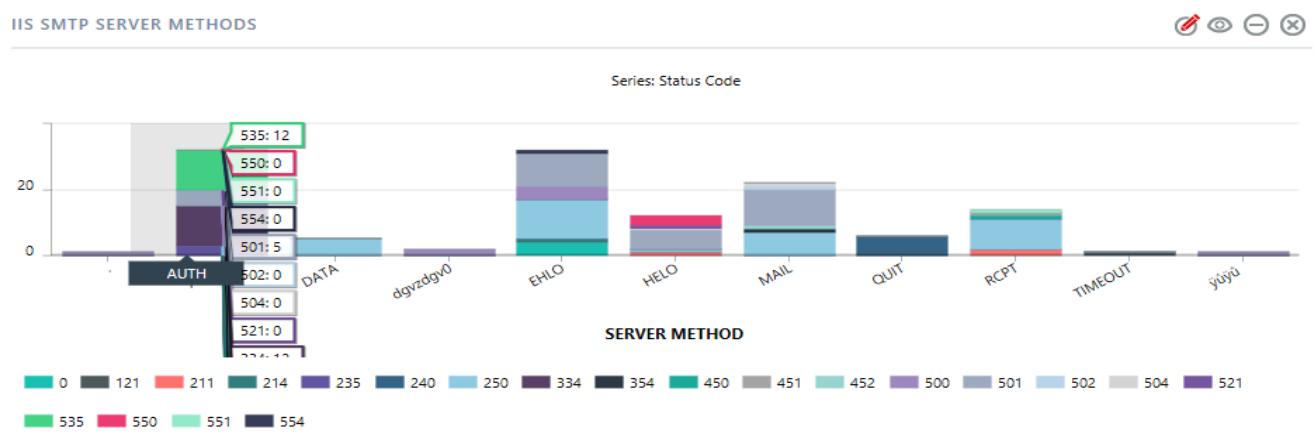


Figure 39

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

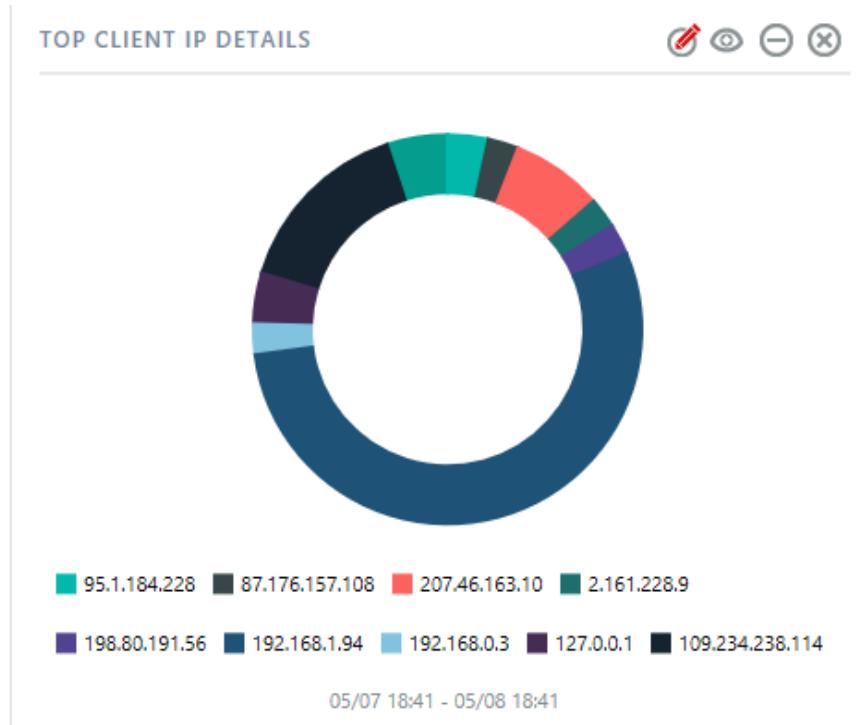


Figure 40