

Integrate Routing and Remote Access Service (RRAS)

EventTracker v8.x and above

Abstract

This guide provides instructions to configure Routing and Remote Access Service (RRAS) to send the windows based events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, and Microsoft Windows Server 2008 and later.

Audience

Routing and Remote Access Service (RRAS) users, who wish to forward windows based messages to EventTracker manager.

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
Scope	1
Audience.....	1
Introduction.....	3
Prerequisites.....	3
Configuration.....	3
Forward RRAS Logs to EventTracker by deploying the Agent.....	5
Import RRAS VPN logs into EventTracker via LFM	6
EventTracker Knowledge Pack (KP).....	13
Flex Reports	13
Categories and Saved Searches.....	16
Import RRAS knowledge pack into EventTracker	16
Token Templates:	16
Flex Reports:.....	17
Verify RRAS Knowledge Pack in EventTracker	19
Verify RRAS Token Templates	19
Verify RRAS Flex Reports	19

Introduction

RRAS stands for Routing and Remote Access Service. It is a Microsoft API and server software that makes it possible to create applications to administer the routing and remote access service capabilities of the operating system, to function as a network router.

An RRAS server provides two different types of remote access connectivity:

- **Virtual private networking** - A virtual private network (VPN) is a secured, point-to-point connection across a public network, such as the Internet. A VPN client uses TCP/IP-based tunneling protocols to make a connection to a port on a remote VPN server.
- **Dial-up networking** - In dial-up networking, a remote access client makes a dial-up telephone connection to a physical port on a remote access server by using the service of a telecommunication provider, such as analog telephone or ISDN.

Prerequisites

Prior to configuring Routing and Remote Access Service (RRAS) and EventTracker, ensure that you meet the following prerequisites:

- Microsoft Windows Server 2008 or above version should be installed.
- Proper access permissions to make configuration changes.
- EventTracker agent should be installed in Windows Server.
- Administrative access on EventTracker.

Configuration

You must enable and configure logging on Routing and Remote Access Service (RRAS) prior to configuring EventTracker.

To configure logging in RRAS,

1. In the **Routing and Remote Access MMC snap-in**, in the navigation pane, right-click the server used, and then click **Properties**. If you are using Server Manager, right-click **Routing and Remote Access**, and then click **Properties**.

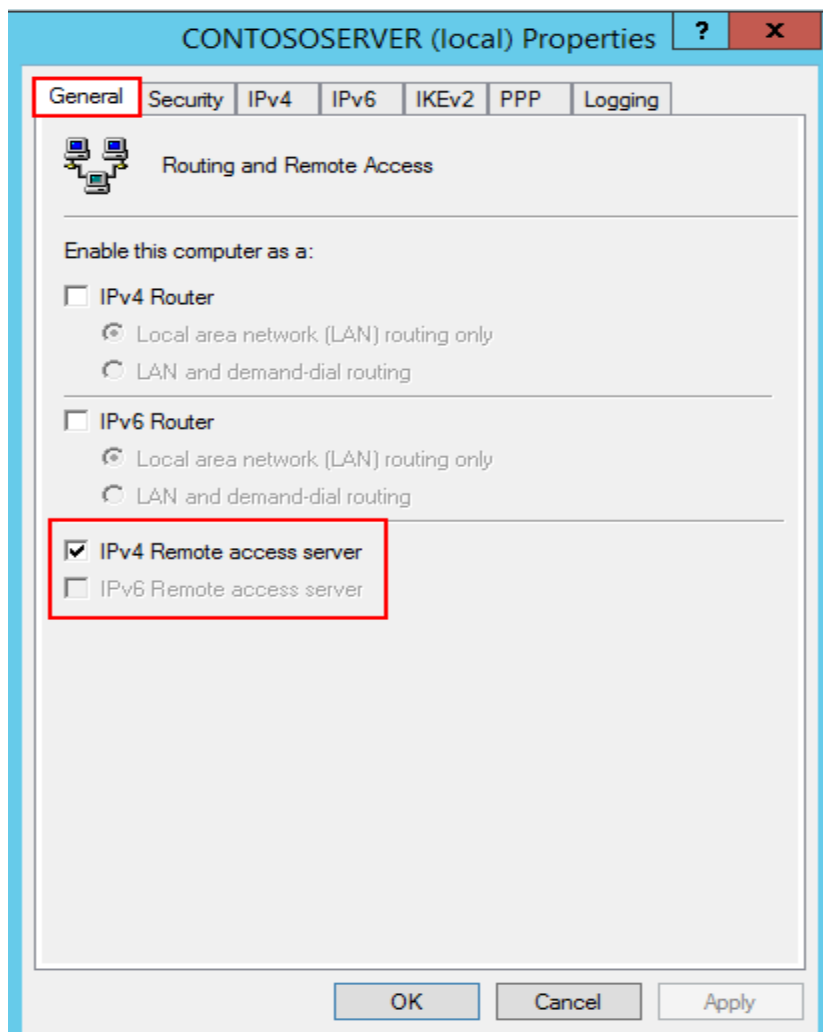


Figure 1

2. On the **Logging** tab, choose **Log errors and warnings** option

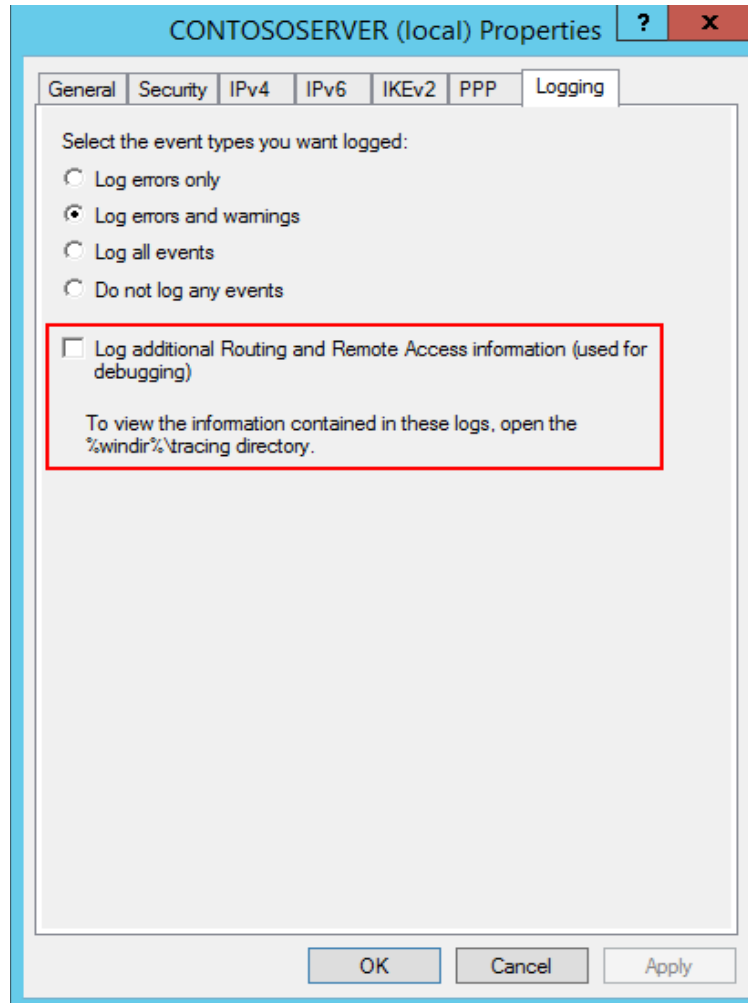


Figure 2

3. Click **Apply**, and then click the **OK** button to save changes.

It will forward the logs to Event Viewer.

Forward RRAS Logs to EventTracker by deploying the Agent

VPN log is stored in a separate file path (i.e. C:\Windows\System32\LogFiles\IN1408.log) and RRAS operation is displayed in EventViewer.

1. Open **Routing and Remote Access**.
2. Double-click **Routing and Remote Access**, and then double-click the server name on which you want to configure logging.
3. In the console tree, right-click **Remote Access Logging & Policies** and then select **Launch NPS**.
4. In left pane, click **Accounting**, click **Change Log File properties** and then select **Log File** tab.

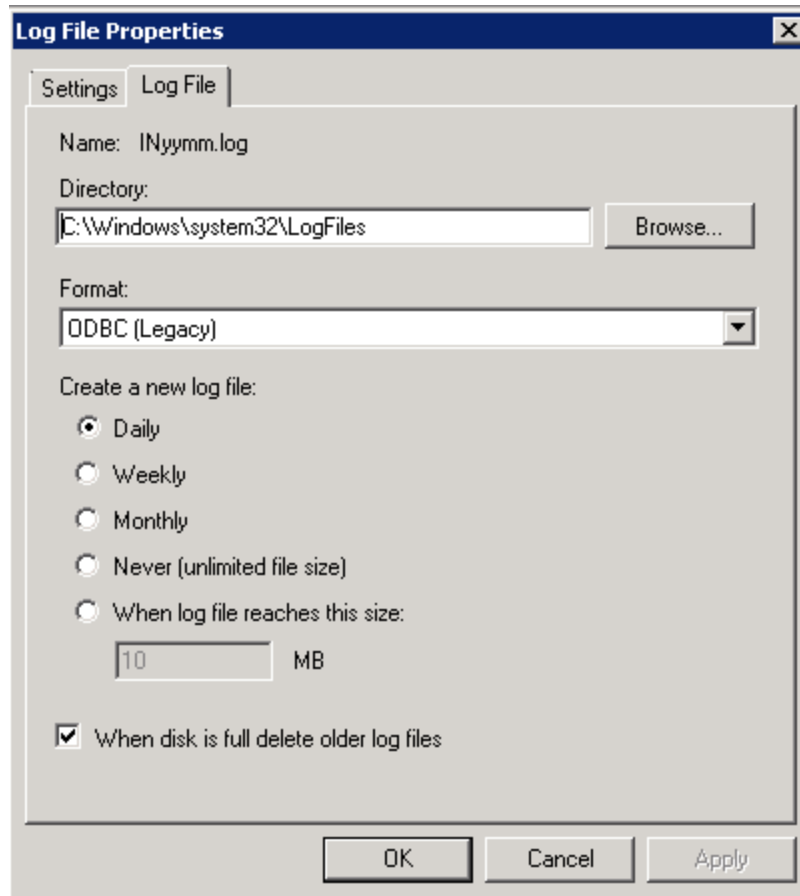


Figure 3

5. Change the log file **Directory:** and log **Format:** (ODBC recommended) as per requirement.
6. Click **Apply** and then click **OK** button to save the changes.

Import RRAS VPN logs into EventTracker via LFM

1. Go to the EventTracker installation file path and search for **etaconfig** application.
2. Then right click on the application icon and **Run as Administrator**.
3. Select **Logfile Monitor** tab.

EventTracker opens the 'Logfile Monitor' tab.

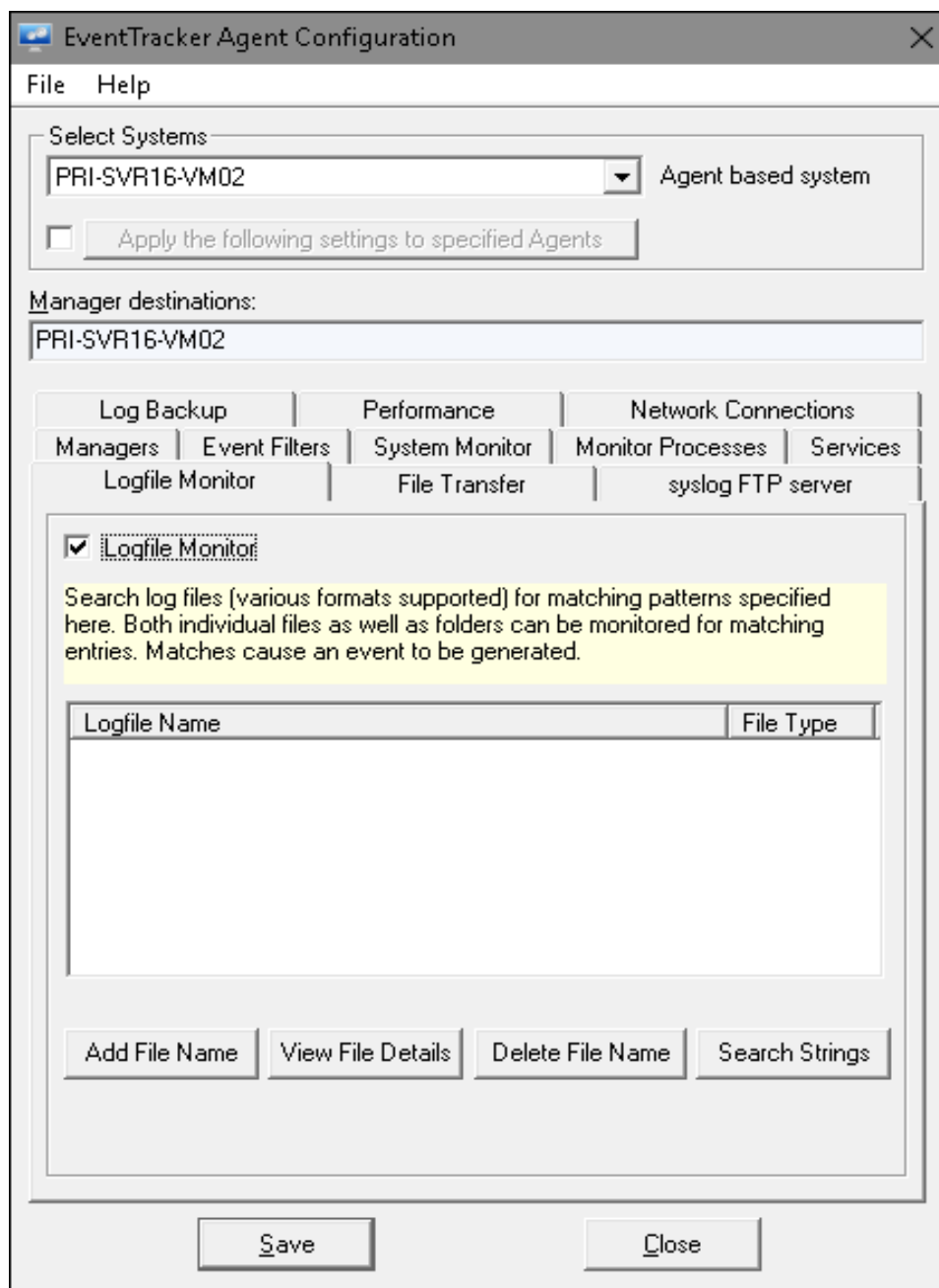


Figure 4

4. Click the **Add File Name** button.
EventTracker displays the 'Enter File Name' window.

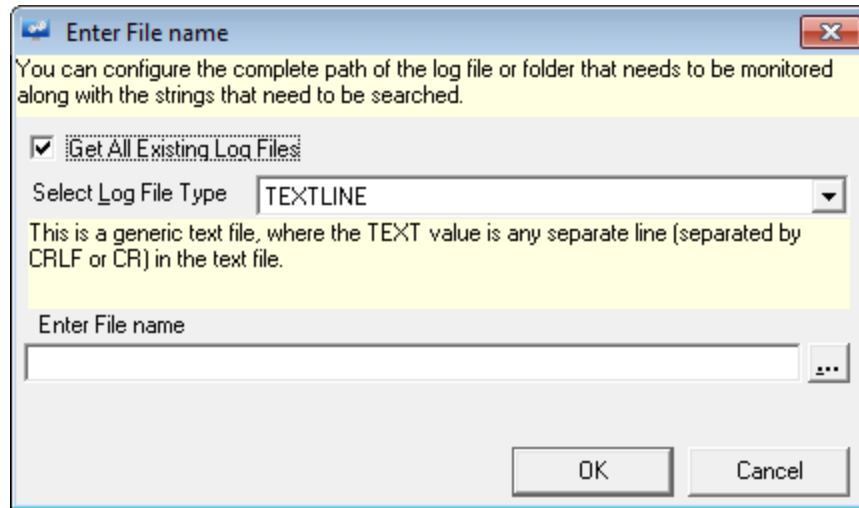


Figure 5

5. Click the **Get All Existing Log Files** checkbox, if you want all the existing files prior to this configuration and the files that are logged after this configuration.
6. Select the logfile type as **TEXTLINE** from the **Select Logfile Type** drop-down list.
7. Click the **Enter File Name** path option.
EventTracker displays the 'Select Folder/File Name' window.

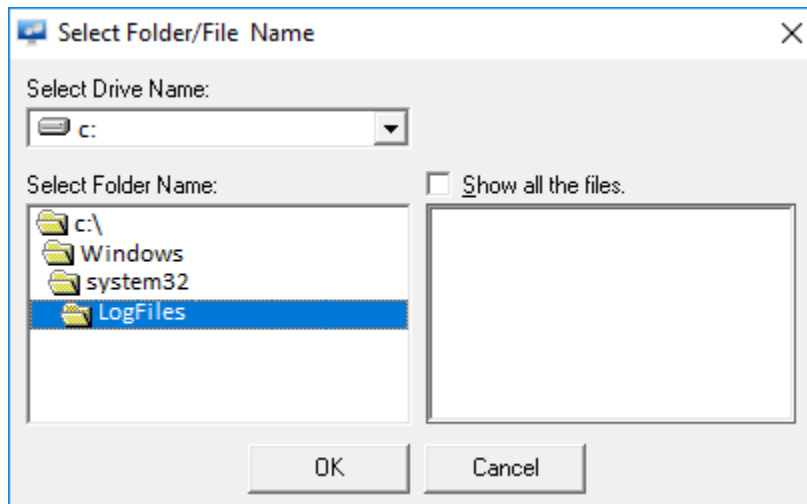


Figure 6

8. In **Select Folder name**: Select appropriate folder associated with selected Log File Type.
9. Click **OK**.
EventTracker displays the '**Select file extension**' window.

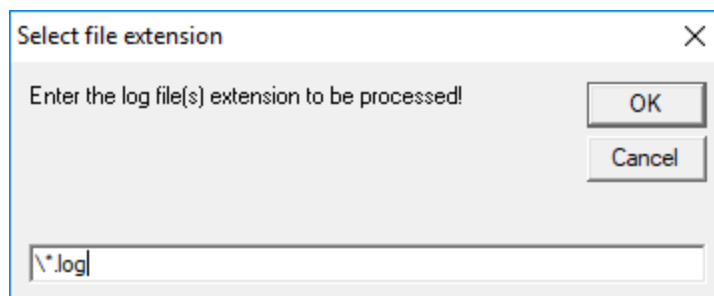


Figure 7

10. Type ***.log** and click **OK**.

EventTracker displays the 'Enter File name' window.

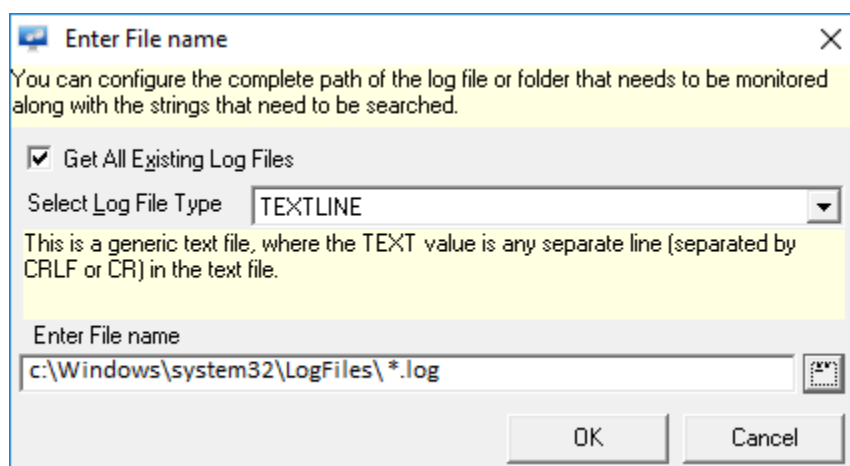


Figure 8

11. Click **OK**.

EventTracker displays the 'EventTracker Agent Configuration' message box.

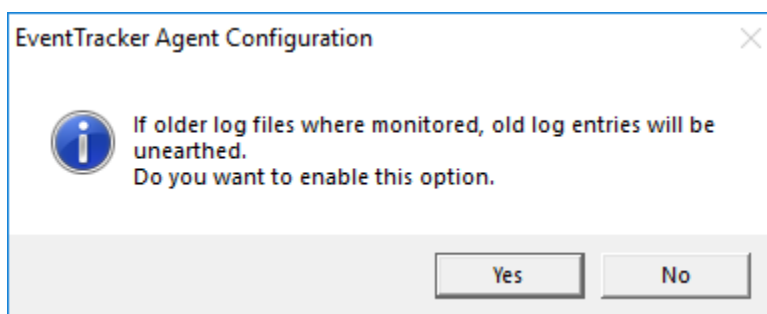


Figure 9

12. Click **Yes**.

EventTracker displays the Search String dialog box.

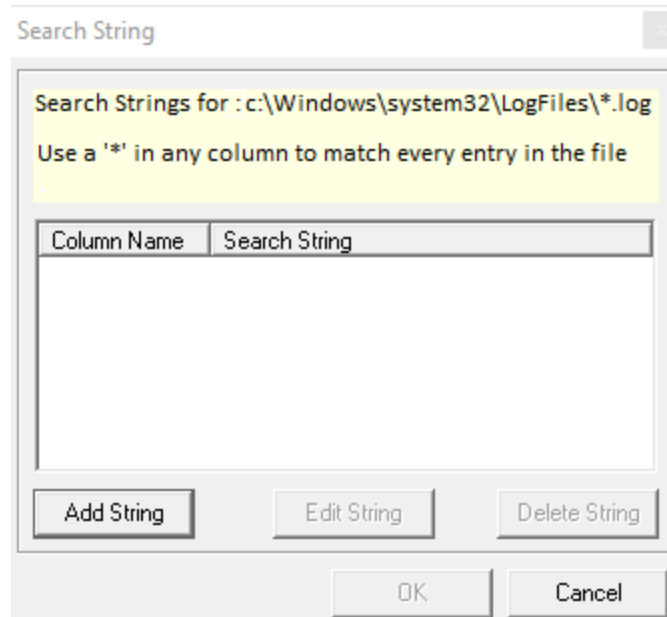


Figure 10

13. Click the **Add String** button.

EventTracker displays the 'Enter Search String' dialog box.

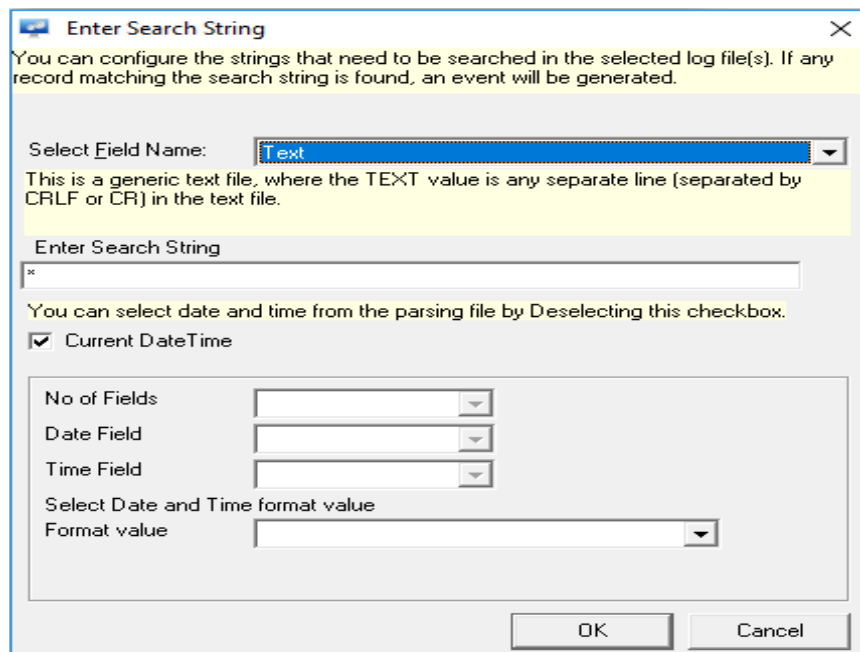


Figure 11

14. Select the file name as **TEXT** from the **Select Field Name** drop-down list.

15. Type "*" in the **Enter Search String** field.

16. Click the **Current DateTime**

17. Click **OK**.

EventTracker displays the Search String dialog box.

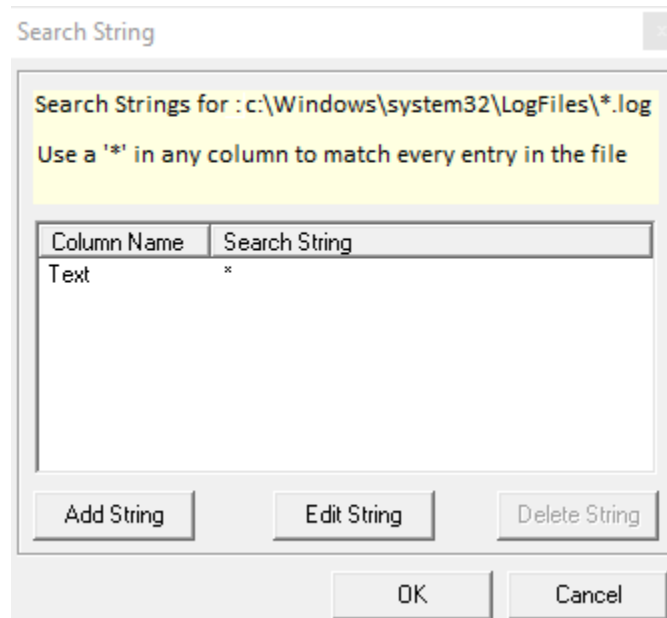


Figure 12

18. Click **OK**.

EventTracker displays the 'Agent Configuration' window with the newly added Logfile entry.

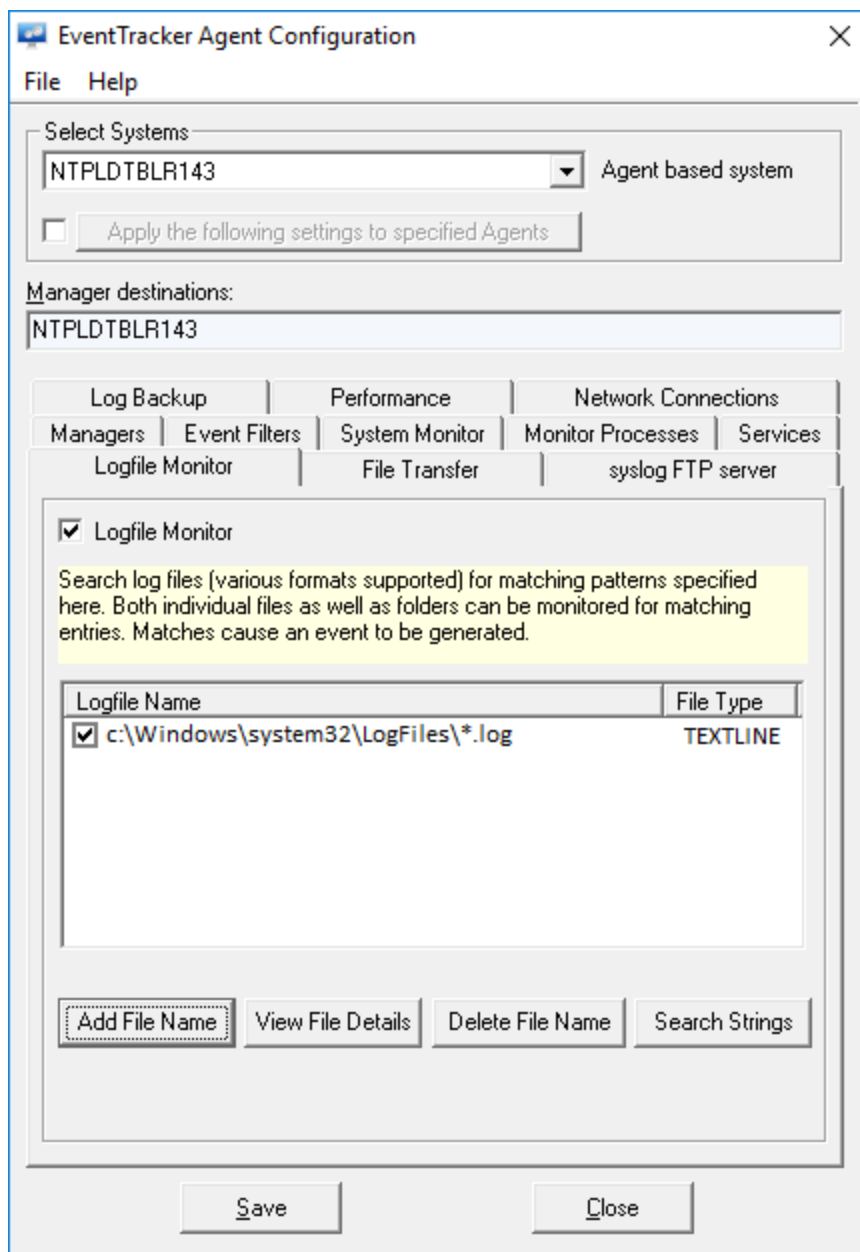


Figure 13

19. Click the **S**ave button.

EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v8.x to support Microsoft Windows Routing and Remote Access Service (RRAS) monitoring.

Flex Reports

- **MS RRAS-Access request** - This report provides information related to all access request send for VPN connection.

LogTime	Computer	Client Computer Name	Username	Packet Type	Source IP Address	NAS IP address	Client IP address
06/21/2018 01:23:08 PM	RRAS	A0090	mkr.domain/KU Users/Active/smith	1	10.25.99.12	62.44.1.43	10.225.99.123
06/21/2018 01:23:08 PM	RRAS	A0089	mkr.domain/KU Users/Active/kenny	1	10.25.99.12	10.61.17.20	10.225.99.122
06/21/2018 01:23:08 PM	RRAS	A0088	mkr.domain/KU Users/Active/John	4	10.25.99.17	19.6.14.101	10.225.99.117

Figure 14

Sample logs:

Time	Description
Jun 21 01:25:11 PM	ENTRY:"A00254","RAS",06/13/2018,06:28:41,4,"mcr995",,"12.223.22.55",,"55.32.2.110",,"11.23.5.2",,"A00254",,"12.223.22.55",385,,,"12.223.22.55",,"A...
event_log_type	+ - Application
event_type	+ - Information
event_id	+ - 3230
event_source	+ - EventTracker
event_user_domain	+ - N/A
event_computer	+ - RRAS
event_user_name	+ - N/A
event_description	ENTRY:"A00254","RAS",06/13/2018,06:28:41,4,"mcr995",,"12.223.22.55",,"55.32.2.110",,"11.23.5.2",,"A00254",,"12.223.22.55",385,,,"12.223.22.55",,"A00254",1528864119,,5,,1,2,,0,"311 1 12.223.22.55 05/17/2018 04:07:23 5350",,,,,,2,,42450954,252890902,"5351",3,2426,148984,224932,1,"3705",1,,3,1,"55.32.2.110",,"12.223.22.55",,,,,,"MSRASV5.20",311,,,"0x01534349454E4345",4,,,"Microsoft Routing and Remote Access Service Policy",1,,,"MSRAS-0-GB11024",,"MSRASV5.20" FILE:C:\Windows\System32\LogFiles\IN1806.log TYPE:TEXTLINE FIELD: *

Figure 15

- **MS RRAS-Access failure** - This report provides information related to failure client access request.

LogTime	Computer	Client Computer Name	Packet Type	Username	Source IP Address
06/21/2018 01:23:10 PM	RRAS	A00250	3	SCIENCE\gzf555	10.25.99.13
06/21/2018 01:23:10 PM	RRAS	A00250	3	SCIENCE\gzf542	10.25.9.23
06/21/2018 01:23:10 PM	RRAS	A00250	3	SCIENCE\gzf589	10.25.98.30

Figure 16

Sample logs:

Time	Description
Jun 21 01:23:11 PM	ENTRY:"A00250","RAS",06/13/2018,23:05:01,3,,"SCIENCE\fk259".....4,16,"311 1 12.223.22.55 05/17/2018 04:05:52 4583"....."Micr...
<i>event_log_type</i>	+ - Application
<i>event_type</i>	+ - Information
<i>event_id</i>	+ - 3230
<i>event_source</i>	+ - EventTracker
<i>event_user_domain</i>	+ - N/A
<i>event_computer</i>	+ - RRAS
<i>event_user_name</i>	+ - N/A
<i>event_description</i>	ENTRY:"A00250","RAS",06/13/2018,23:05:01,3,,"SCIENCE\fk259".....4,16,"311 1 12.223.22.55 05/17/2018 04:05:52 4583"....."Micro soft Routing and Remote Access Service Policy",1,.... FILE:C:\Windows\System32\LogFiles\IN1806.log TYPE:TEXTLINE FIELD: *

Figure 17

- **MS RRAS-Access success** - This report provides information related to successful client access request.

LogTime	Computer	Client Computer Name	Username	Packet Type	Source IP Address
06/21/2018 01:23:08 PM	RRAS	A00250	science.domain/KU Users/Active/lkL4	1	10.25.9.13
06/21/2018 01:23:08 PM	RRAS	A00257	science.domain/KU Users/Active/pg22	1	10.5.9.22
06/21/2018 01:23:08 PM	RRAS	A00253	science.domain/KU Users/Active/lp2	4	13.5.99.11
06/21/2018 01:23:08 PM	RRAS	A00250	science.domain/KU Users/Active/kp225	2	13.5.99.23

Figure 18

Sample logs:

Time	Description
Jun 21 01:25:13 PM	ENTRY:"A00257","RAS",06/13/2018,05:39:07,1,"science hb499","science.domain/KU Users/Active/thb499","12.223.22.55","55.32.2.110",,"A00257","12.22..
event_log_type	+ Application
event_type	+ Information
event_id	+ 3230
event_source	+ EventTracker
event_user_domain	+ N/A
event_computer	+ RRAS
event_user_name	+ N/A
event_description	ENTRY:"A00257","RAS",06/13/2018,05:39:07,1,"science hb499","science.domain/KU Users/Active/thb499","12.223.22.55","55.32.2.110",,"A00257","12.223.22.55",259,"12.223.22.55",,"A00257",,"5,,1,2,5,"SEC-NAT-VPN-PLN_Klientnetadgang",0,"311 1 12.223.22.55 05/14/2018 04:21:06 6231",,"6232",,"3,1,"55.32.2.110","12.223.22.55",,"MSRASV5.20",311,,"Microsoft Routing and Remote Access Service Policy",1,,"MSRAS-0-PB10636",,"MSRASV5.20" FILE:C:\Windows\System32\LogFiles\IN1806.log TYPE:TEXTLINE FIELD: *

Figure 19

- **MS RRAS- Accounting request** - This report provides information related to client status for the accounting request.

LogTime	Computer	Username	Client IP Address	Client Workstation
06/21/2018 01:23:08 PM	RRAS	vjc28	76.7.15.12	MSRAS-0-PB13132
06/21/2018 01:23:08 PM	RRAS	vjc26	76.7.15.10	MSRAS-0-PB13132
06/21/2018 01:23:09 PM	RRAS	mktrg430	19.61.37.80	MSRAS-0-PB09261

Figure 20

Sample logs:

Time	Description
Jun 21 01:23:59 PM	ENTRY:"A00257","RAS",06/13/2018,14:50:00,4,"science\wkp253",,"12.223.22.55",,"55.32.2.110",,"11.23.5.2",,"A00257",,"12.223.22.55",262,,,"12.223.22..
event_log_type	+ Application
event_type	+ Information
event_id	+ 3230
event_source	+ EventTracker
event_user_domain	+ N/A
event_computer	+ RRAS
event_user_name	+ N/A
event_description	ENTRY:"A00257","RAS",06/13/2018,14:50:00,4,"science\wkp253",,"12.223.22.55",,"155.122.22.2",,"11.23.5.2",,"A00257",,"12.223.22.55",262,,,"12.223.22.55",,"A00257",1528894200,5,,1,2,,0,"311 1 12.223.22.55 05/14/2018 04:21:06 6361",,"1,,"6362",3,,"4799",1,,3,1,"155.122.22.23",,"12.223.22.55",,"MSRASV5.20",311,,,"0x01534349454E4345",4,,,"Microsoft Routing and Remote Access Service Policy",1,,"MSRAS-0-PB10517",,"MSRASV5.20" FILE:C:\Windows\System32\LogFiles\IN1806.log TYPE:TEXTLINE FIELD: *

Figure 21

Categories and Saved Searches


- **MS RRAS: Accept Request-** This category provides information related to client access request for VPN.
- **MS RRAS: Access Accept-** This category provides information related to client access accept.
- **MS RRAS: Access Reject-** This category provides information related to client access reject.
- **MS RRAS: Accounting Type-** This category provides information related to accounting type.
- **MS RRAS: Authentication Failure-** This category provides information related to authentication failure.
- **MS RRAS: Request Discard-** This category provides information related to client request discard.

Import RRAS knowledge pack into EventTracker

Import knowledge pack items in the following sequence:

- Token Templates
- Flex Reports

Token Templates:

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Parsing rule**.
3. Select the **Template** tab option and click the  button.
4. Locate the **All RRAS Token Template .ettd files** and click the **Open** button.

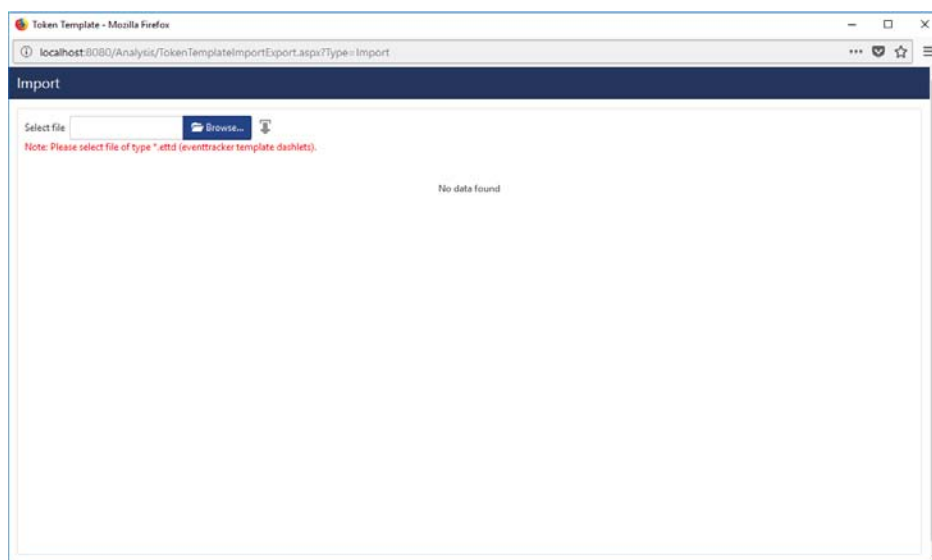


Figure 22

- To import token templates, click the **Import** button.
EventTracker displays success message.

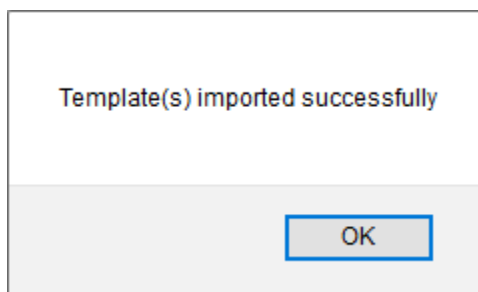


Figure 23

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

Flex Reports:

- Go to the EventTracker installation path and search for **ETControlPanel** application.
- Then right click on the application icon and **Run as Administrator**.
- Double click **Export Import Utility** and click **Import** tab.

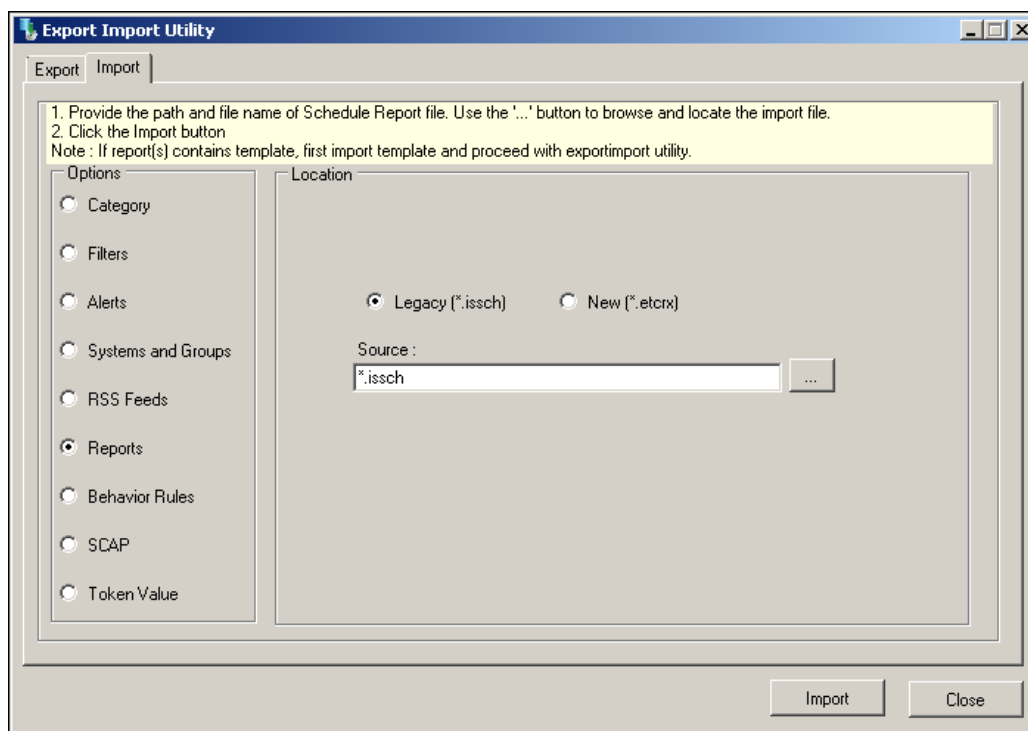



Figure 24

4. Click **Report** option, select the **New (.etcrx)** and then click the  button.

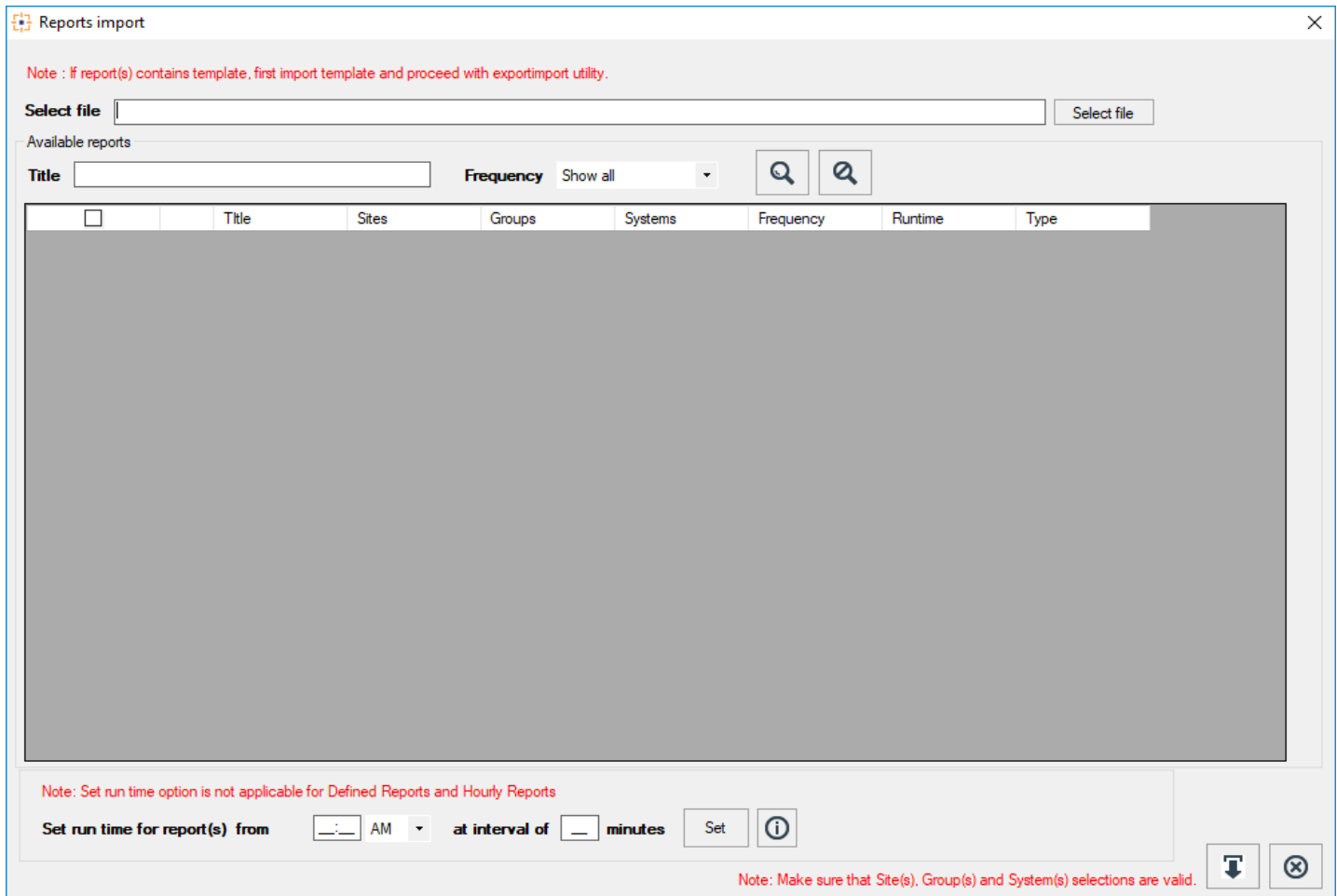



Figure 25

5. Locate the **All RRAS group of Report.etcrx** file, and then click the **Open** button.
 6. Click  button to import the scheduled reports.

EventTracker displays success message.

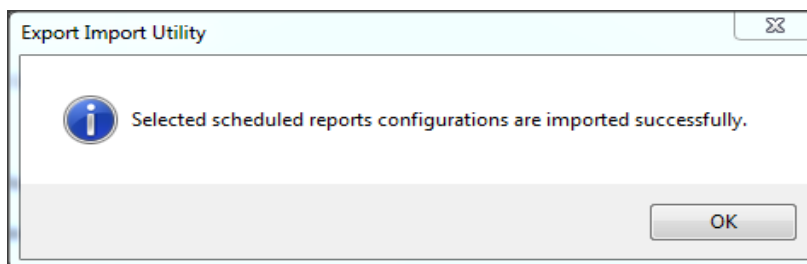


Figure 26

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

Verify RRAS Knowledge Pack in EventTracker

Verify RRAS Token Templates

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Parsing Rules**.
3. Imported RRAS tokens added in **Microsoft RRAS Groups** list at left side of **Template** tab of EventTracker Enterprise (as shown in below figure).

The screenshot shows the 'Parsing Rules' interface in EventTracker Enterprise. The 'Template' tab is selected. On the left, under the 'Groups' section, 'Microsoft RRAS' is highlighted with a red box. On the right, a table displays the templates for the 'Microsoft RRAS' group, also highlighted with a red box. The table has columns for Template Name, Template Description, Added By, and Added Date.

Template Name	Template Description	Added By	Added Date
MS RRAS -Access failure	Microsoft RRAS	ETAdmin	Mar 05 03:46:03 PM
MS RRAS -Access request	Microsoft RRAS	ETAdmin	Mar 05 03:46:03 PM
MS RRAS -Access success	Microsoft RRAS	ETAdmin	Mar 05 03:46:03 PM
MS RRAS -Accounting request	Microsoft RRAS	ETAdmin	Mar 05 03:46:03 PM
MS RRAS -Authentication type	Microsoft RRAS	ETAdmin	Mar 05 03:46:03 PM

Figure 27

Verify RRAS Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu. Select **Configuration**.
3. In the **Reports Configuration**, select **Defined** from radio button.
EventTracker displays **Defined** page.
4. Select the '**Microsoft RRAS**' Groups.

EventTracker displays Flex reports of RRAS.

Report Configuration

Scheduled Queued Defined

Search...

Report Groups

- Security
- Compliance
- Operations
- Flex
- Cb Defense
- EventTracker
- Microsoft RRAS**
- NtopNG
- Office 365
- Synology
- UniFi AP AC Pro
- Windows

Reports configuration: Microsoft RRAS

<input type="checkbox"/>	Title	Created on	Modified on
<input type="checkbox"/>	MS RRAS-Accounting request	Mar 05 03:47:38 PM	Jan 01 05:30:00 AM
<input type="checkbox"/>	MS RRAS-Access success	Mar 05 03:47:38 PM	Jan 01 05:30:00 AM
<input type="checkbox"/>	MS RRAS-Access failure	Mar 05 03:47:38 PM	Jan 01 05:30:00 AM
<input type="checkbox"/>	MS RRAS-Access request	Mar 05 03:47:38 PM	Jan 01 05:30:00 AM

Figure 28