

Terminal Services Gateway

EventTracker v9.2 and above

Abstract

The purpose of this document is to help users to monitor Microsoft Windows **Terminal Services Gateway** by deploying Windows Agent.

Scope

The configuration details in this guide are consistent with **EventTracker** version 9.2 and later, **Terminal Services Gateway**.

Audience

Administrators who want to monitor the **Terminal Services Gateway** using **EventTracker**.

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. Pre-requisite	3
3. EventTracker Agent configuration	3
4. EventTracker Knowledge Pack	7
4.1 Categories	7
4.2 Reports.....	7
4.3 Alerts	9
4.4 Dashboards	9
5. Importing knowledge pack into EventTracker	14
5.1 Categories	15
5.2 Alerts.....	16
5.3 Token Templates	17
5.4 Flex Reports	19
5.5 Knowledge Objects	20
5.6 Dashboards	22
6. Verifying knowledge pack in EventTracker	23
6.1 Categories	23
6.2 Alerts.....	24
6.3 Token Templates	25
6.4 Flex Reports	25
6.5 Knowledge Objects	26
6.6 Dashboards	27

1. Introduction

Windows Server 2008 Terminal Services Gateway (TS Gateway) is a role service that enables authorized remote users to connect to resources on an internal corporate or private network, from any Internet-connected device that can run the Remote Desktop Connection (RDC) client. The network resources can be terminal servers, terminal servers running RemoteApp programs, or computers with Remote Desktop enabled.

EventTracker gathers and examines acquired logs to identify terminal server configurations, terminal server connections, terminal server desktop host activity. It generates reports for terminal services user session connected, user session disconnected, user authentication success, user authentication failed, and network traffic activity. It displays authentication success and failed with username's, user session connected, and network traffic by systems. It alerts the users when terminal services gateway is shutting down and user authentication fails.

2. Pre-requisite

Prior to configuring Windows Server 2008 and later and EventTracker 9.2 and later, ensure that you meet the following prerequisites.

- Administrative access on EventTracker.
- User should have Administrative rights on Microsoft Windows Terminal Server.

3. EventTracker Agent configuration

1. Deploy EventTracker Agent in Terminal Services Server, please follow the steps mentioned in [How to Install EventTracker and Change Audit](#).
2. Click **Start >All Programs>Prism Microsystems> EventTracker**.
3. In **EventTracker Control Panel**, double-click **EventTracker Agent Configuration**.
4. Select **Event Filters** tab, and then click the **Filter Exception** button.

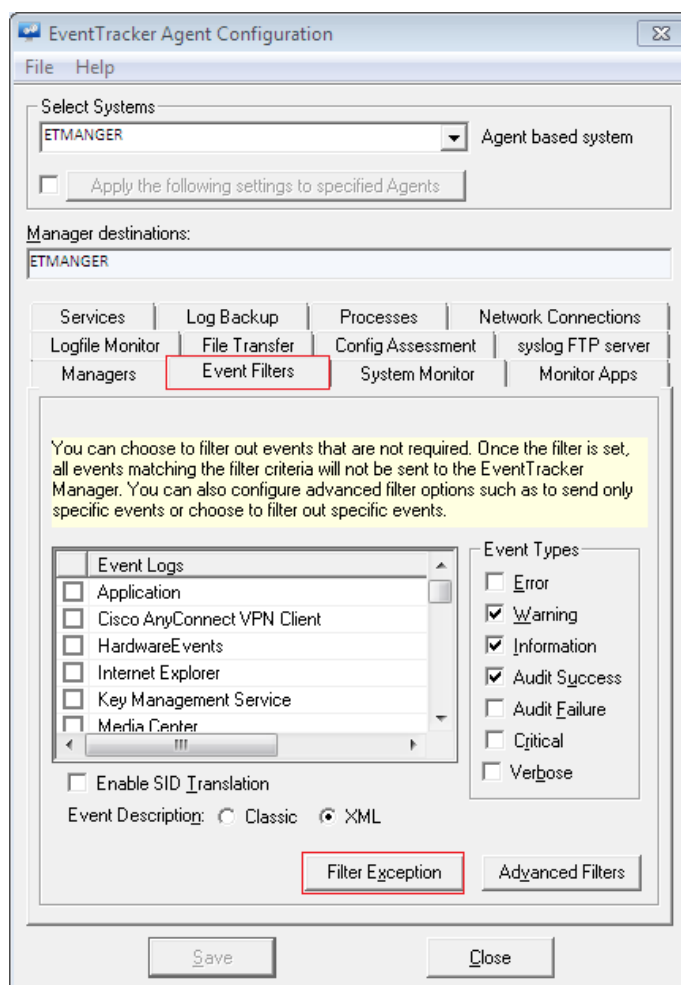


Figure 1

5. Filter Exception window displays. Click **New**.

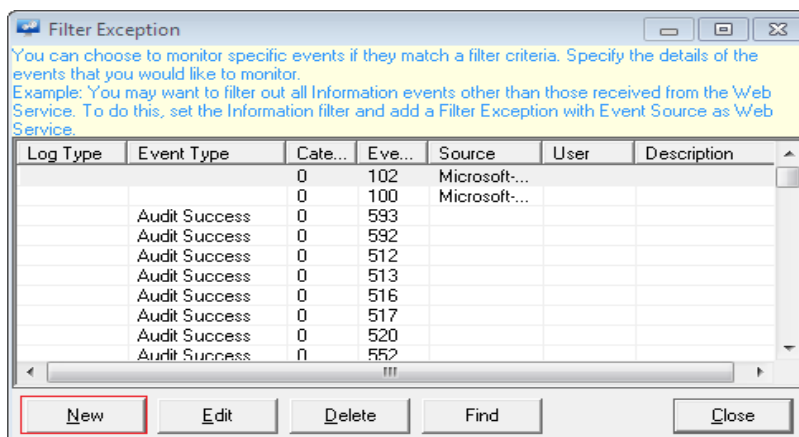


Figure 2

6. Event Details window opens. In **Match in Source** box enter '**Microsoft-Windows-TerminalServices-Gateway**'.

The screenshot shows the 'Edit Event Details' dialog box. It has a title bar with a close button. Below the title bar is a section titled 'Event Details (empty field implies all matches)'. This section contains several fields: 'Log Type' (a dropdown menu), 'Event Type' (a dropdown menu), 'Event ID' (a text box), 'Category' (a text box containing '0'), 'Match in User' (a text box), 'Match in Source' (a text box containing 'Microsoft-Windows-TerminalServices-G.'), and 'Match in Event Descr' (a text box). Below these fields is a yellow-highlighted text area containing instructions: '"Match in Event Descr", "Match in User" and "Match in Source" field can take multiple strings separated with && or ||. && stands for AND condition. || stands for OR condition. For negating the result of match operation, prefix the string with "\$NOT\$". If there are multiple strings, then the result of the whole expression is negated. Only one "\$NOT\$" should be used in the string. Example: The string "\$NOT\$Logon Type: 4||Logon Type: 5" will match all events that DO NOT contain "Logon Type: 4" or "Logon Type: 5" in the description. For more information click here.' At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Figure 3

7. Click **OK**.
8. **Save** the configuration and **Close** the EventTracker Agent Configuration window.

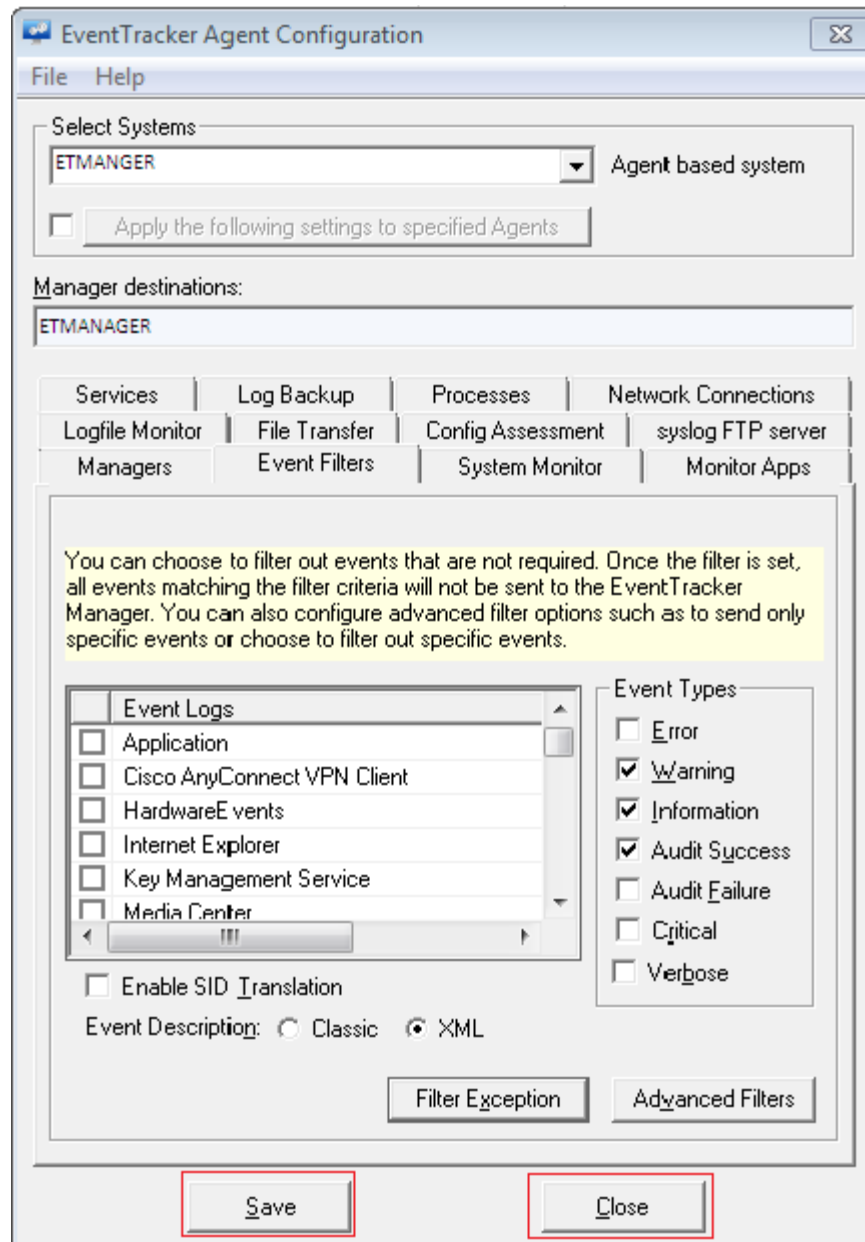


Figure 4

4. EventTracker Knowledge Pack

Once logs are received in to EventTracker, categories and reports can be configured into EventTracker.

4.1 Categories

Terminal Services Gateway: Authentication success – This category provides information related to authentication successfully allowed for user.

Terminal Services Gateway: Authentication failed – This category provides information related to authentication failed for user.

Terminal Services Gateway: Inbound traffic – This category provides information related to inbound network traffic logs.

Terminal Services Gateway: Outbound traffic – This category provides information related to outbound network traffic logs.

Terminal Services Gateway: Session connected – This category provides information related to users successfully connected to resources, authentication method, and protocol detail logs will present.

Terminal Services Gateway: Session disconnected - This category provides information related to users disconnected to resources logs will present.

4.2 Reports

Terminal Services Gateway - Authentication success – This report provides information related to authentication success for a user, IP address, username, etc.

Log Considered

The user "DOMAIN\kenneth", on client computer "1.22.47.13", met connection authorization policy requirements and was therefore authorized to access the RD Gateway server. The authentication method used was: "NTLM" and connection protocol used: "HTTP".

Sample Report

LogTime	Computer	User Name	Authentication Method	Protocol	Reason	Client IP Address
06/23/2020 05:43:07 PM	WKSTRTL12\TERMINAL_SERVICE_GATEWAY	DOMAIN\maya	NTLM	HTTP	met connection authorization policy requirements and was therefore authorized to access the RD Gateway server	1.22.32.45

Figure 5

Terminal Services Gateway - Authentication failed - This report provides information related to authentication failure for a user, reason for failure, device name, username, and IP address.

Log Considered

The user "DOMAIN\david", on client computer "13.61.12.41", did not meet connection authorization policy requirements and was therefore not authorized to access the RD Gateway server. The authentication method used was: "NTLM" and connection protocol used: "HTTP". The following error occurred: "23003".

Sample Report

LogTime	Computer	User Name	Authentication Method	Protocol	Client IP Address	Reason
06/24/2020 11:13:30 AM	WKSTRTL432\TERMINAL_SERVICE_GATEWAY	DOMAIN\david	NTLM	HTTP	12.32.67.41	did not meet connection authorization policy requirements and was therefore not authorized to access the RD Gateway server

Figure 6

Terminal Services Gateway - Network resource connected or disconnected – This report provide information related to session connected and disconnected to network resources, username, network resource name, IP address, data transferred, data downloaded, etc.

Log Considered

The user "DOMAIN\maya", on client computer "23.27.47.19", connected to resource "DaemonsecureX". Connection protocol used: "HTTP".

The user "DOMAIN\maxx", on client computer "13.18.32.21", disconnected from the following network resource: "Tallydox". Before the user disconnected, the client transferred 3037339 bytes and received 12588518 bytes. The client session duration was 794 seconds. Connection protocol used: "HTTP".

Sample Report

LogTime	Computer	User Name	Client IP Address	Network Resource	Protocol	Client Transferred	Client Received	Message	Session Duration
06/23/2020 05:43:01 PM	WKSTRTL323\TERMINAL_SERVICE_GATEWAY	DOMAIN\maya	12.56.35.62	Daemonsecure	HTTP			connected to resource "Daemonsecure"	
06/23/2020 05:43:02 PM	WKSTRTL564\TERMINAL_SERVICE_GATEWAY	DOMAIN\maxx	81.26.240.25	Taxserverbaup	HTTP	2185895 bytes	8461413 bytes	disconnected from the following network resource: "Taxserverbaup"	1287 seconds

Figure 7

Terminal Services Gateway - Network traffic detail – This report provides information related to network inbound and outbound traffic, IP address, username, etc.

Log Considered

The user "maya", on client computer "14.33.173.138:60172", has initiated an outbound connection. This connection may not be authenticated yet.

The user "kenneth", on client computer "214.23.3.138:60173", has initiated an inbound connection. This connection may not be authenticated yet.

Sample Report

LogTime	Computer	User Name	Client IP Address	Port	Message
06/23/2020 05:43:01 PM	WKSTRTL32\TERMINAL_SERVICE_GATEWAY	maya	13.24.36.34	53355	has initiated an outbound connection. This connection may not be authenticated yet.
06/23/2020 05:43:01 PM	NTPLDTBLR46\TERMINAL_SERVICE_GATEWAY	kenneth	21.36.59.236	52458	has initiated an inbound connection. This connection may not be authenticated yet.

Figure 8

4.3 Alerts

Terminal Services Gateway: User authentication failed – This alert will trigger whenever user tries to authenticate but fails.

Terminal Service Gateqay: Gateway service shutdown – This alert will trigger whenever RD gateway service is shutting down.

4.4 Dashboards

Terminal Services Gateway – Authentication success by user: This dashboard displays authentication success by username.

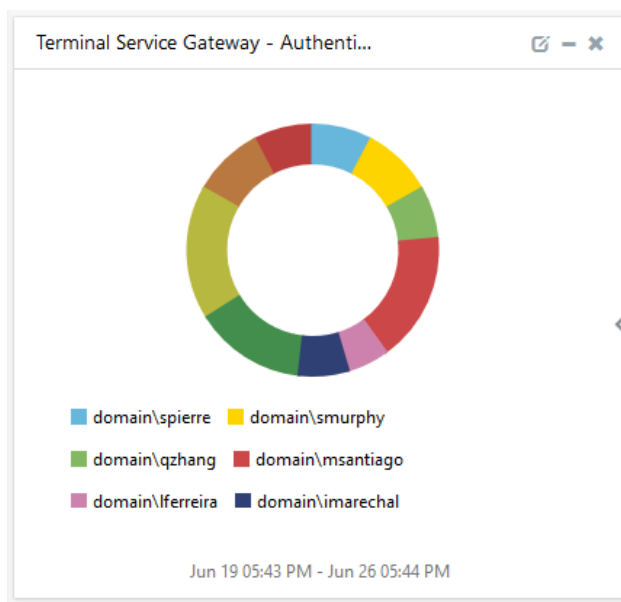


Figure 9

Terminal Services Gateway – Authentication failure by user: This dashboard displays authentication failure by username.

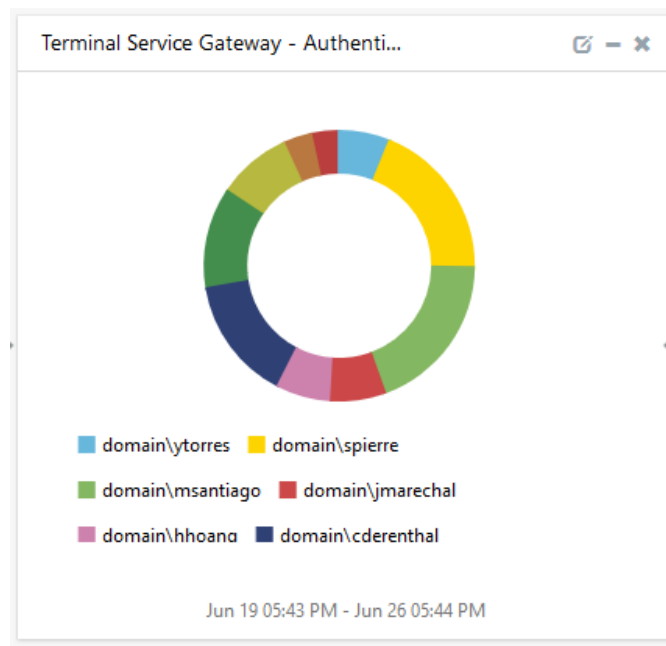


Figure 10

Terminal Services Gateway – Authentication success by trend: This dashboard displays user authentication success by trend.

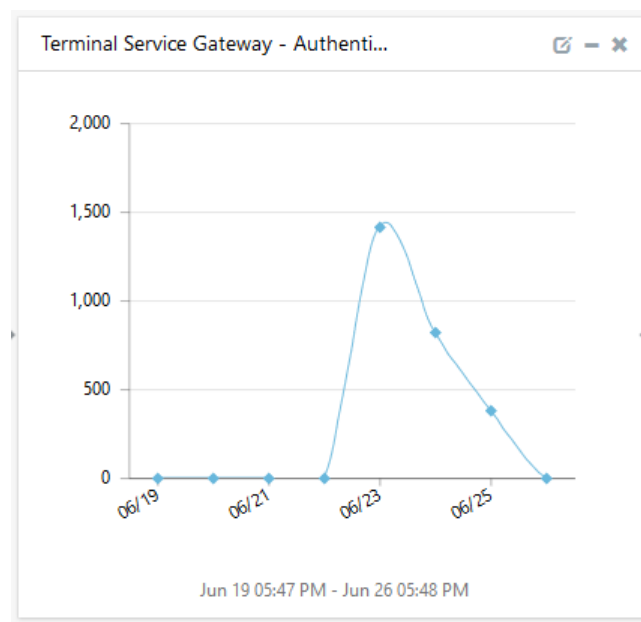


Figure 11

Terminal Services Gateway – Authentication failure by user: This dashboard displays user authentication failure by trend.

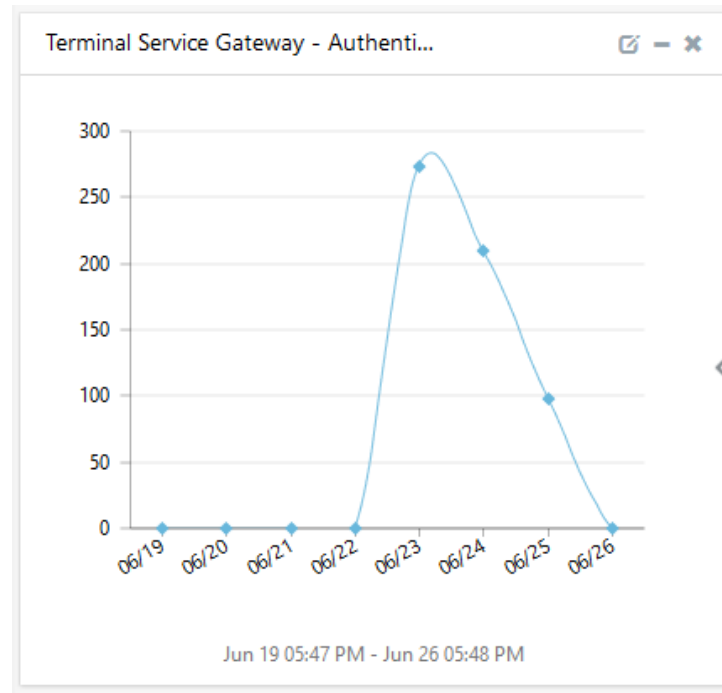


Figure 12

Terminal Services Gateway - Session connected by country - this dashboard displays user connection success to network resources by country.



Figure 13

Terminal Services Gateways - Network resources connection success by user- This dashboard displays network resource names and user names.

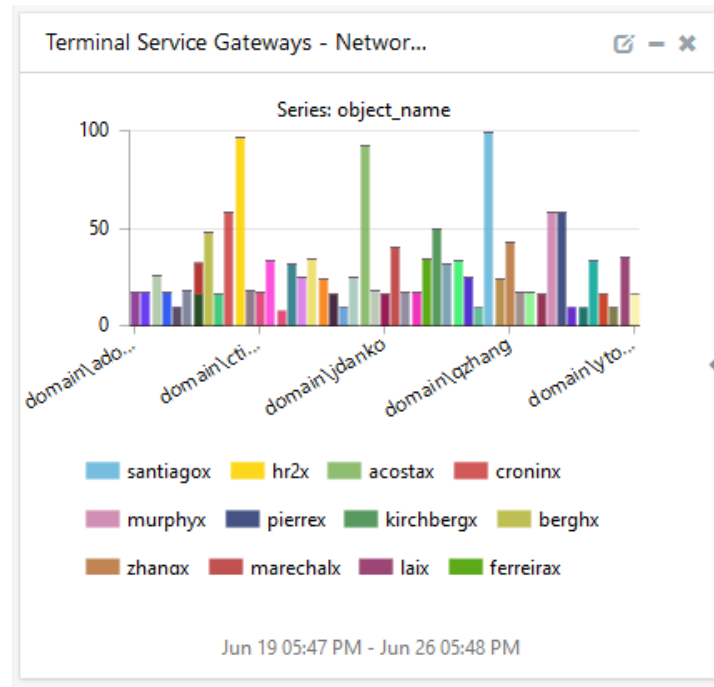


Figure 14

Terminal Services Gateway - Network Inbound traffic by client IP - This dashboard displays network inbound traffic accepted by client IP address.

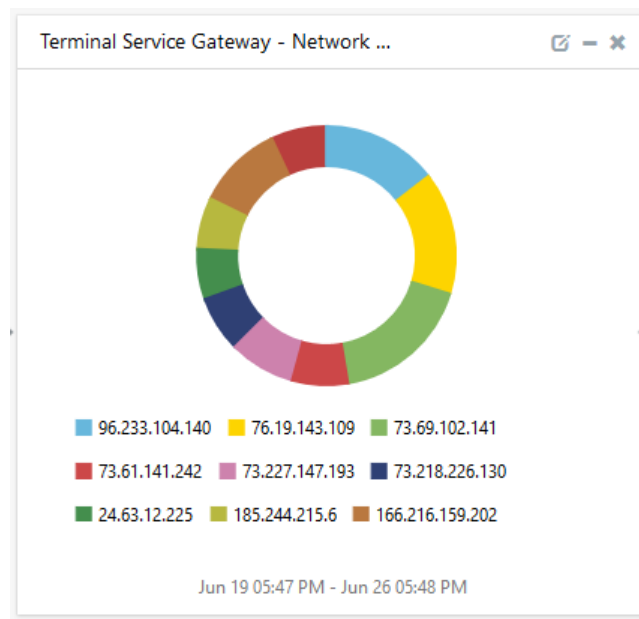


Figure 15

Terminal Services Gateway - Network outbound traffic by Client IP - This dashboard displays network outbound traffic initiated by client IP address.

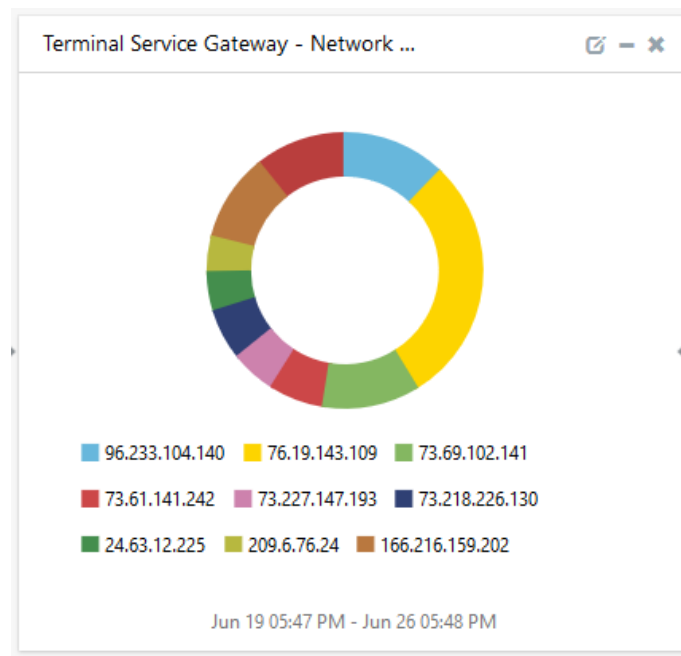


Figure 16

Terminal Services Gateway - Inbound traffic by trend – This dashboard displays network inbound traffic by trend.

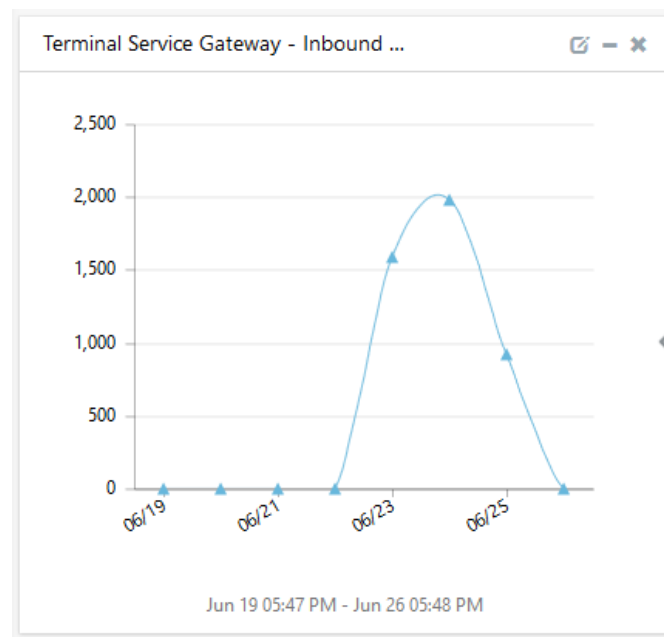


Figure 17

Terminal Services Gateway - Outbound traffic by trend - This dashboard displays network outbound traffic by trend.

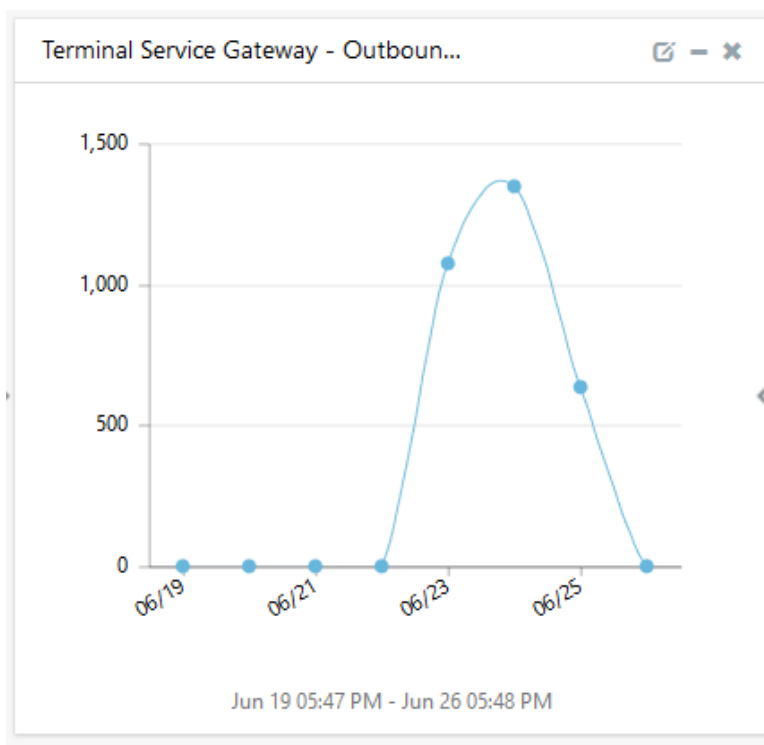


Figure 18

5. Importing knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
 - Alerts
 - Token Template/ Parsing Rules
 - Flex Reports
 - Knowledge Objects
 - Dashboards
1. Launch the **EventTracker Control Panel**.
 2. Double click **Export-Import Utility**.

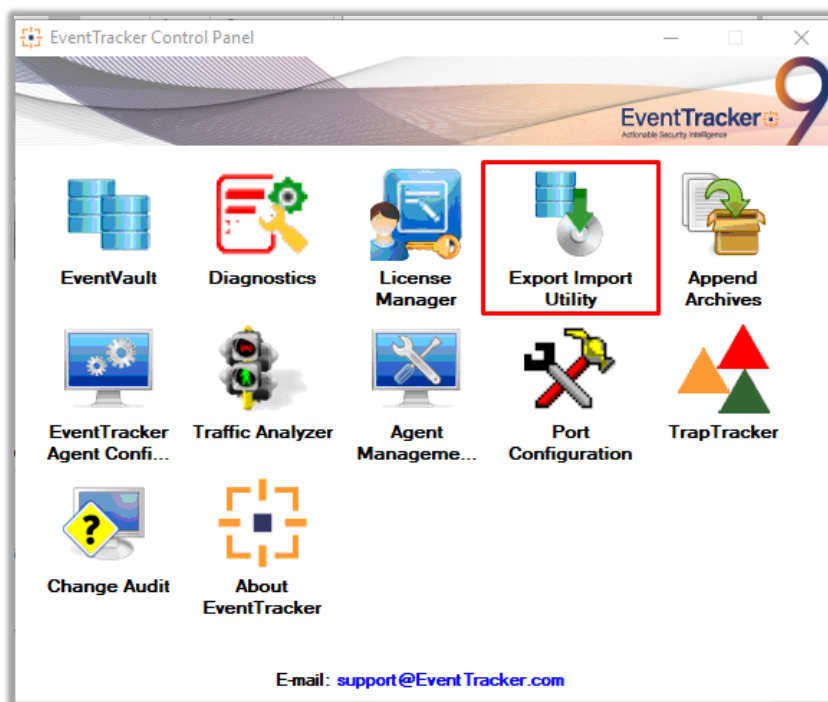


Figure 19

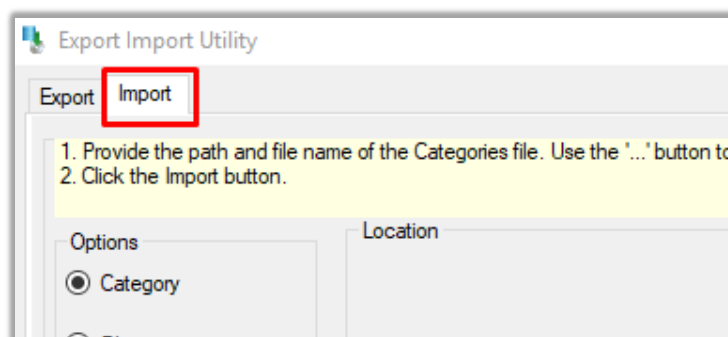



Figure 20

3. Click the **Import** tab.

5.1 Categories

1. Once you have opened “**Export-Import Utility**” via “**EventTracker Control Panel**”, click the **Category** option, and then click Browse .
2. Navigate to the knowledge pack folder and select the file with the extension “.iscat”, like “**Categories_Terminal Services Gateway. iscat**” and then click “**Import**”.

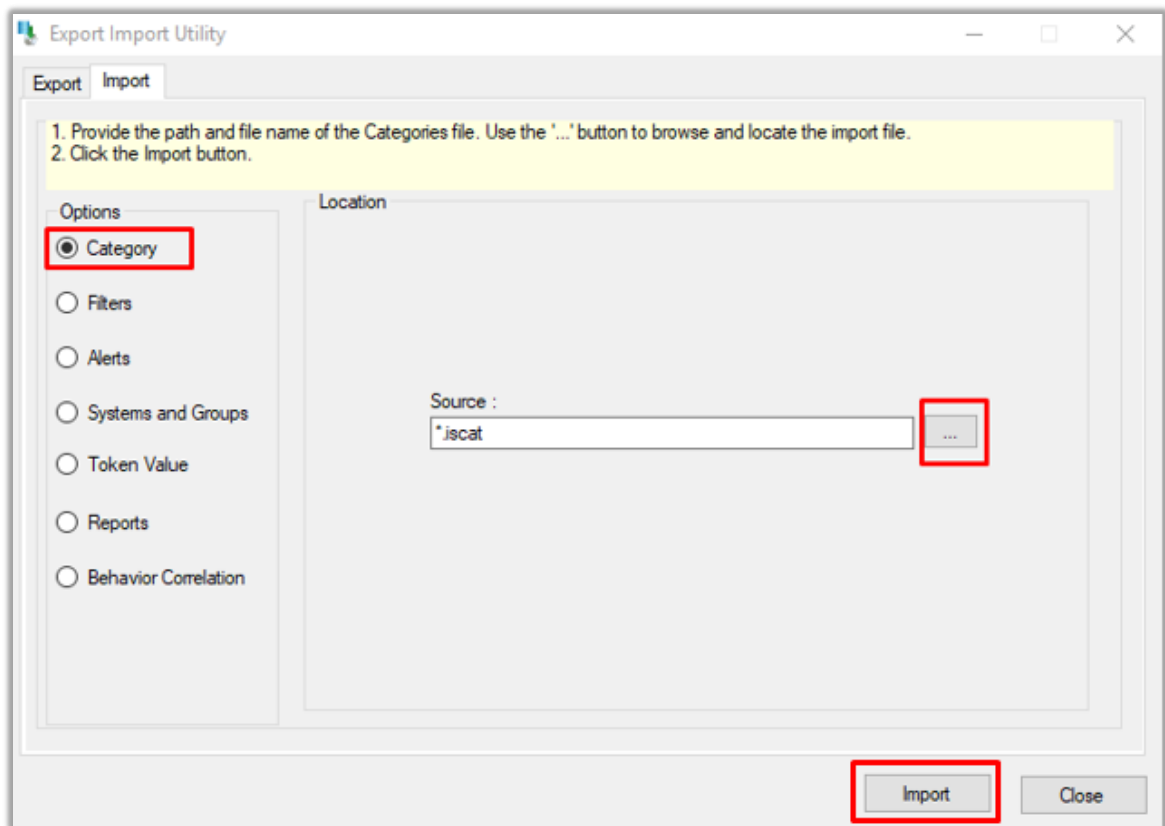


Figure 21

EventTracker displays a success message:

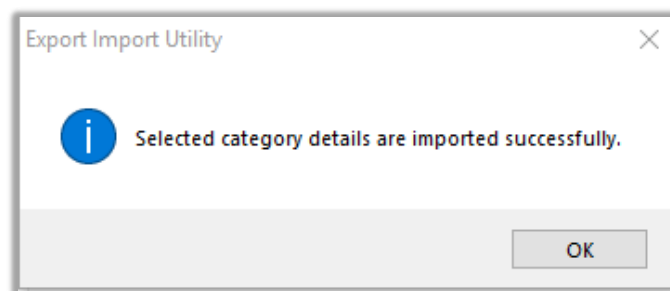


Figure 22

5.2 Alerts

1. Once you have opened “**Export-Import Utility**” via “**EventTracker Control Panel**”, click **Alert** option, and then click **Browse**.
2. Navigate to the knowledge pack folder and select the file with the extension “**.isalt**”, e.g. “**Alerts_Terminal Services Gateway.isalt**” and then click “**Import**”.

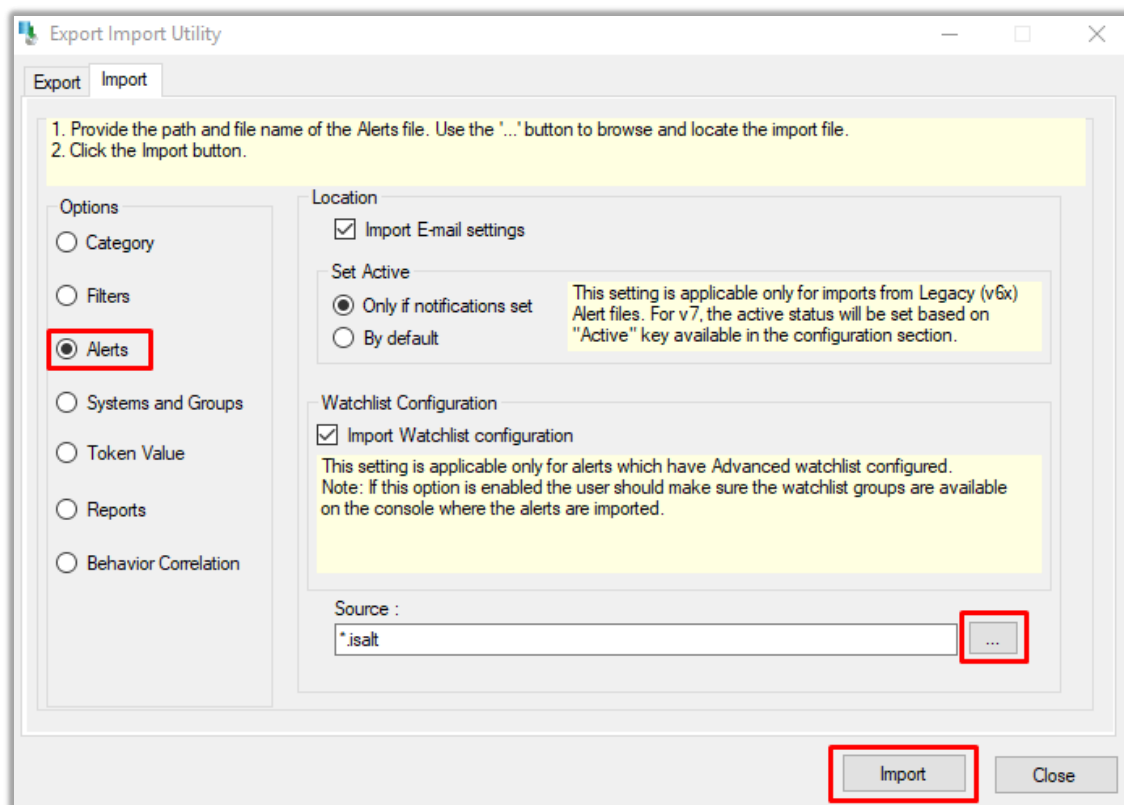


Figure 23

EventTracker displays a success message.

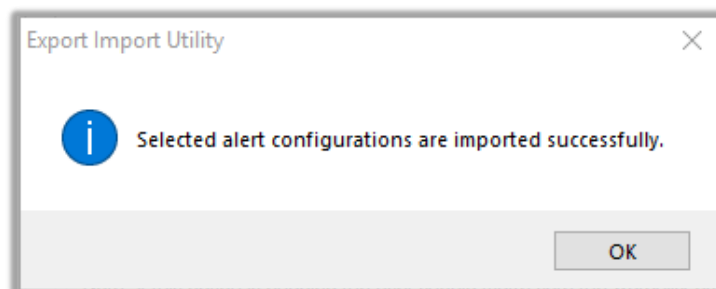


Figure 24

5.3 Token Templates

For importing **"Token Template"**, navigate to the **EventTracker manager** web interface.

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager web interface.

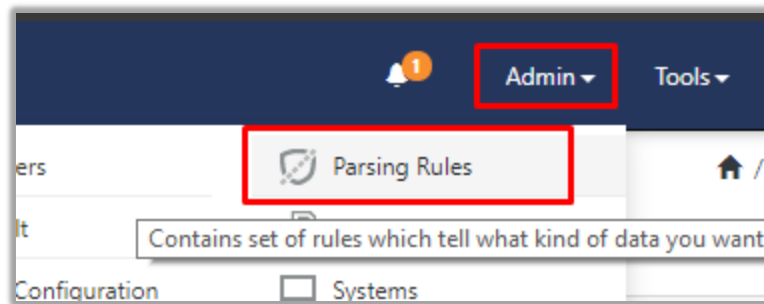


Figure 25

- Click the **“Template”** tab and then click **“Import Configuration”**.

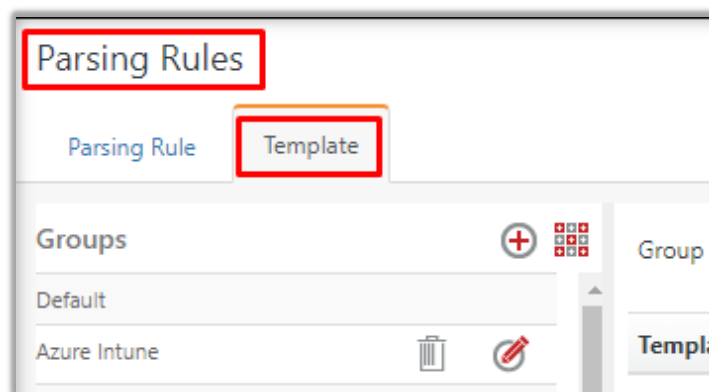


Figure 26

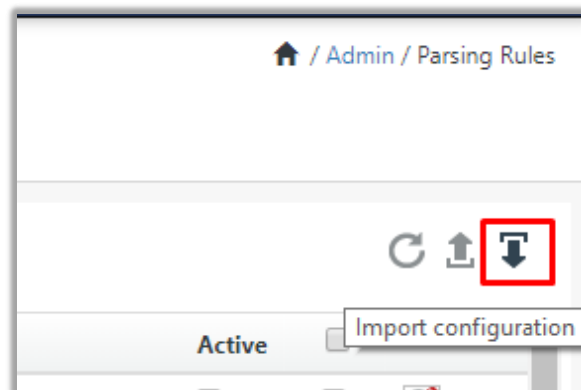


Figure 27

- Now, click **“Browse”** and navigate to the knowledge packs folder (type **C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs** in the navigation bar) where **“.ettd”**, e.g. **“Templates_Terminal Services Gateway.ettd”** file is located. Wait for a few seconds, as templates will be loaded. Once you see the templates, click desired templates and click **“Import”**.

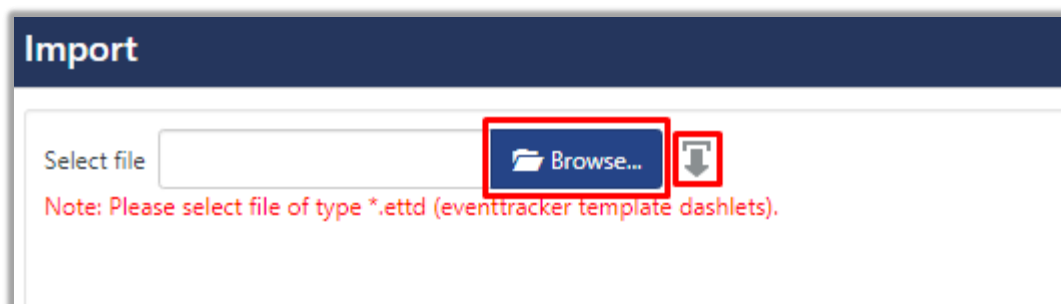


Figure 28

5.4 Flex Reports

1. In the EventTracker control panel, select **“Export/ Import utility”** and select the **“Import tab”**. Then, click **Reports** option, and choose **“New (*.etcrx)”**:

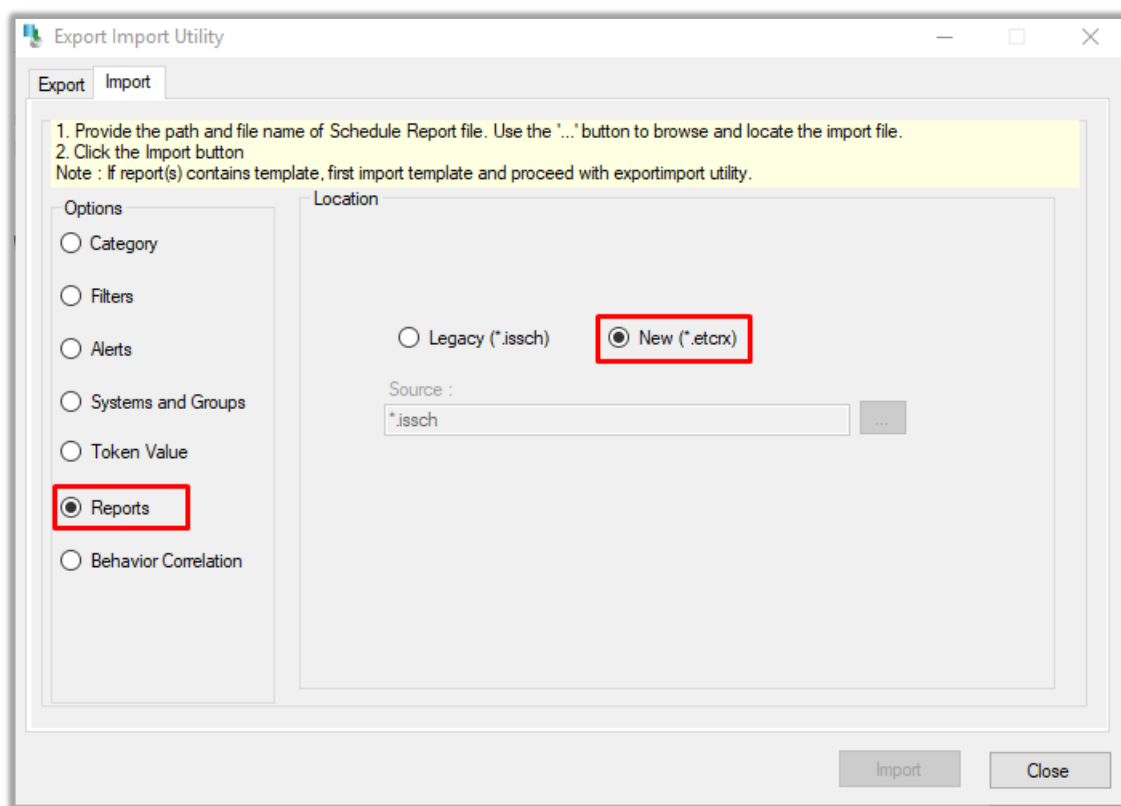


Figure 29

2. Once you have selected **“New (*.etcrx)”**, a new pop-up window will appear. Click the **“Select File”** button and navigate to the knowledge pack folder and select file with the extension **“.etcrx”**, e.g. **“Reports_Terminal Services Gateway.etcrx”**.

Figure 30


- Wait while reports are being populated in the below tables. Now, select all the relevant reports and then click **Import** .

Figure 31

EventTracker displays a success message:

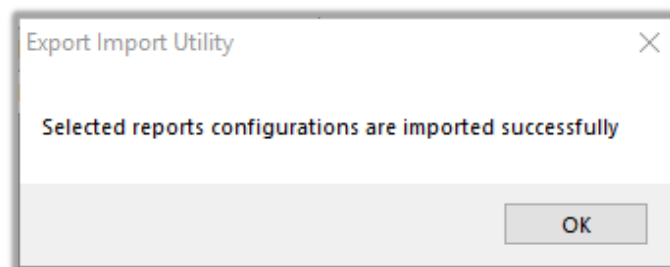


Figure 32

5.5 Knowledge Objects

- Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.

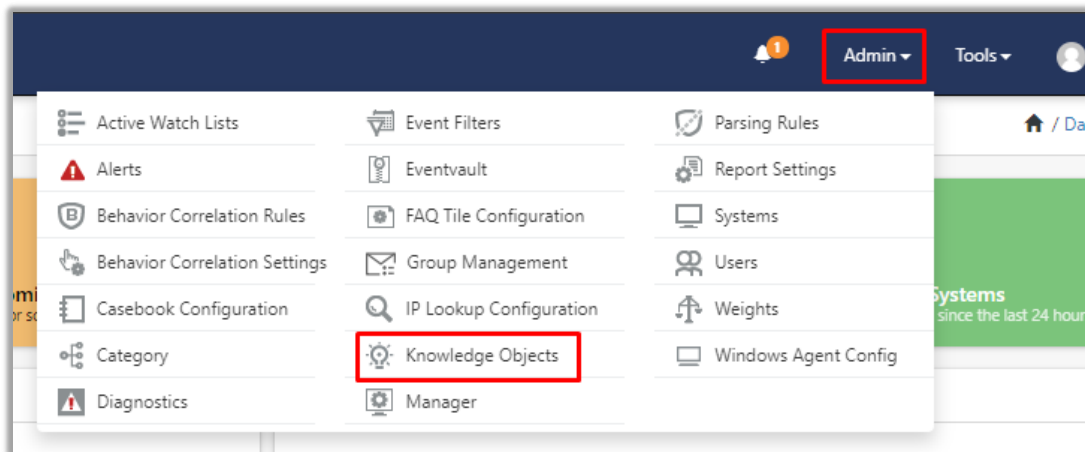


Figure 33

2. Click the “import object” icon.

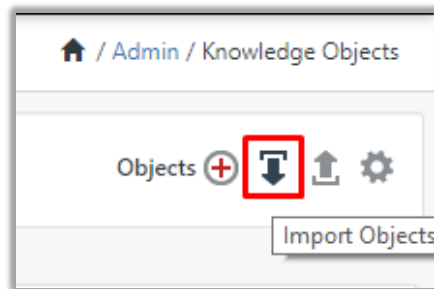


Figure 34

3. A pop-up box will appear, click “Browse” in that and navigate to the knowledge packs folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) with the extension “.etko”, e.g. “KO_Terminal Services Gateway.etko” and then click “Upload”.

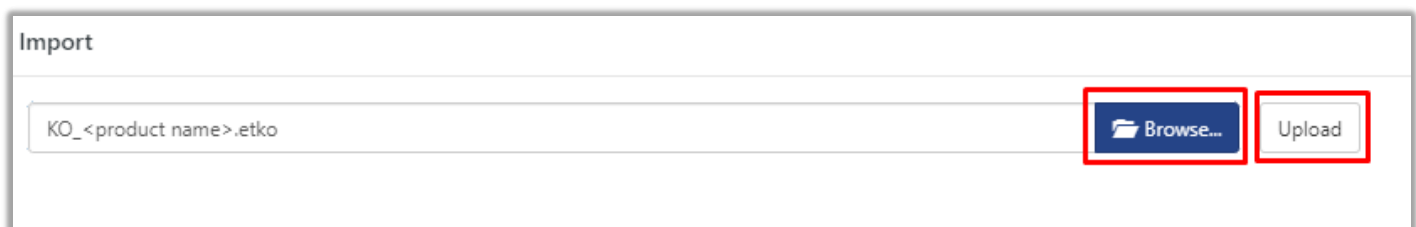


Figure 35

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click “Import”.



Figure 36

5.6 Dashboards

1. Login to the **EventTracker** web interface.
2. Navigate to **Dashboard** → **My Dashboard**.
3. In “My Dashboard”, Click **Import Button**:

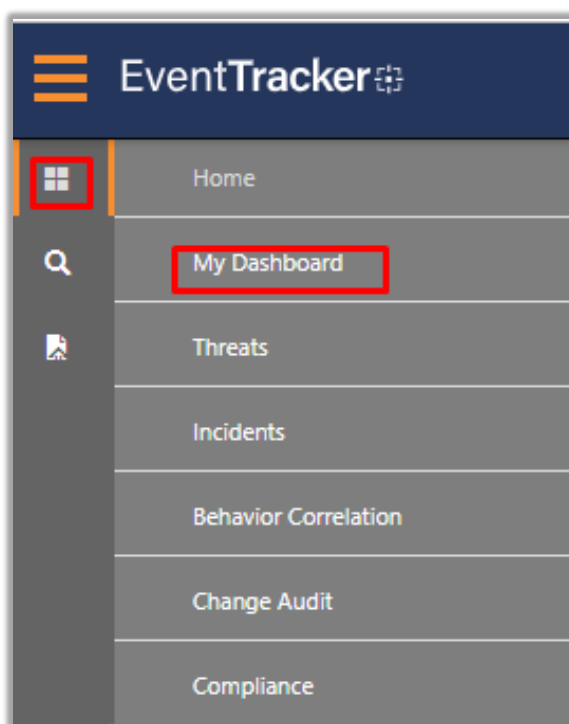


Figure 37

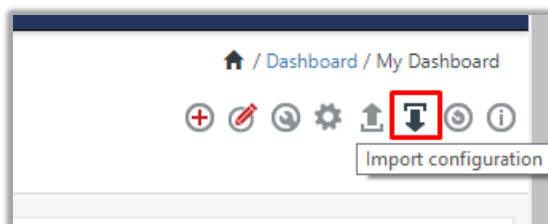


Figure 38

4. Select **Browse** and navigate to the knowledge pack folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) where “.etwd”, e.g. “Dashboard_Terminal Services Gateway.etwd” is saved and click “Upload”.
5. Wait while EventTracker populates all the available dashboards. Now, choose “Select All” and click “Import”.

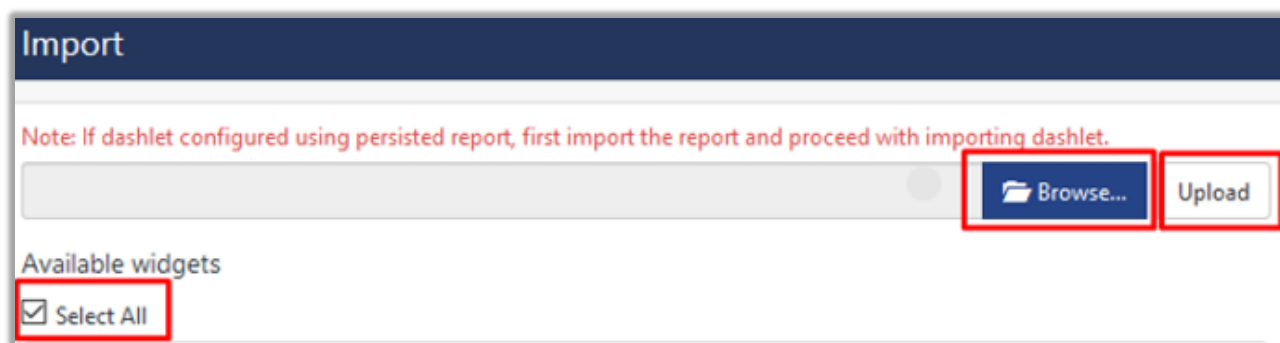


Figure 39



Figure 40

6. Verifying knowledge pack in EventTracker

6.1 Categories

1. Login to the **EventTracker web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, please click on “**Search**” and search with the “**Terminal Services Gateway**”. You will see the below results:

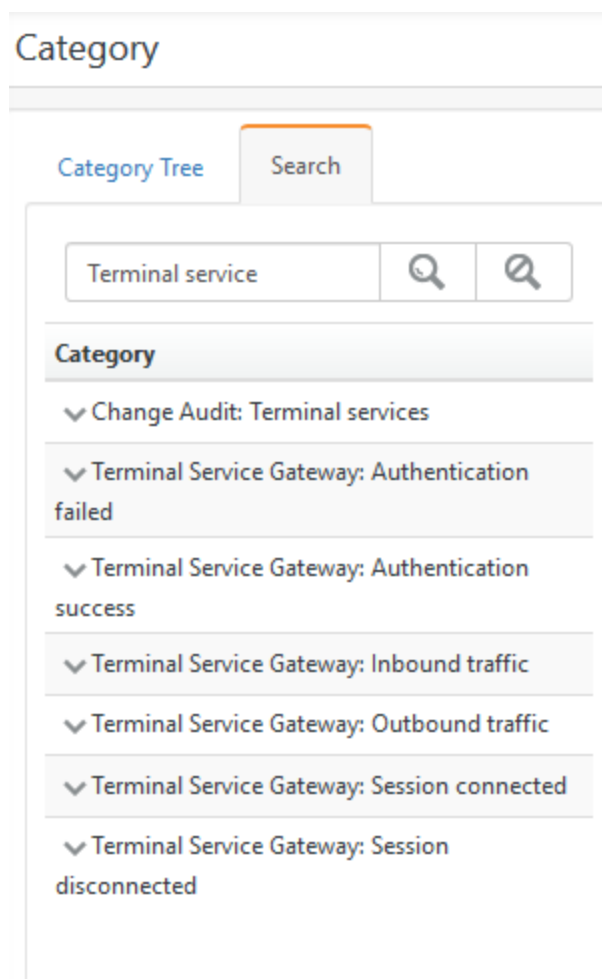


Figure 41

6.2 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In search box enter **“Terminal Services Gateway”** and then click **Search**.
EventTracker displays an alert related to Terminal Services Gateway.

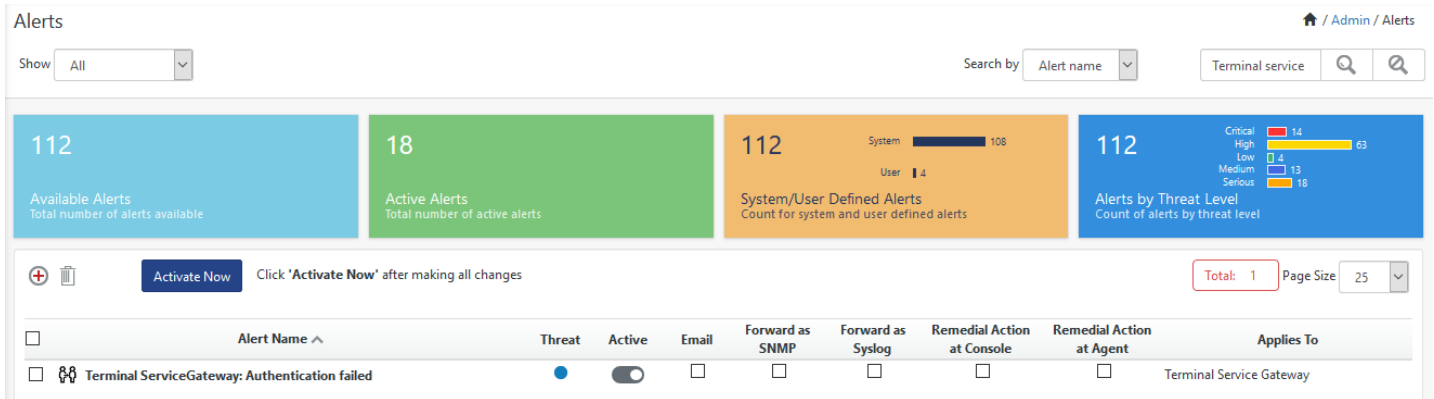


Figure 42

6.3 Token Templates

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click “**Parsing Rules**”.
2. In the “**Template**” tab, click on the “**Terminal Services Gateway**” group folder to view the imported Token.

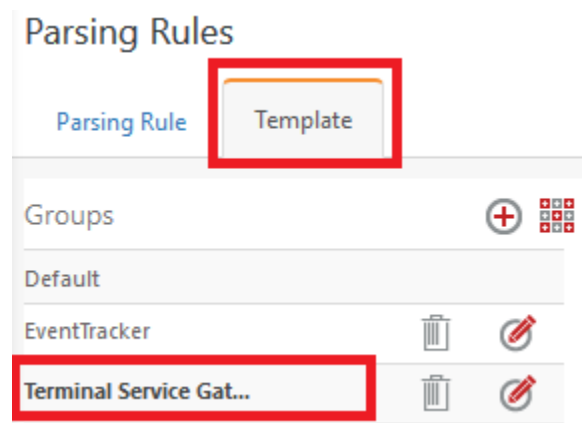


Figure 43

6.4 Flex Reports

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

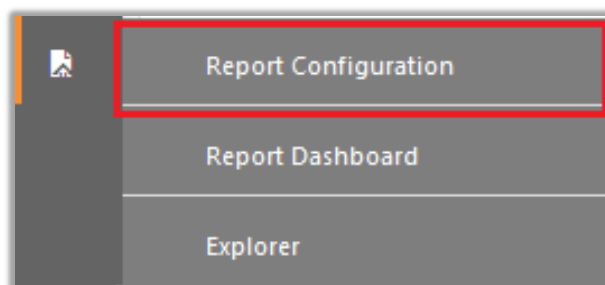


Figure 44

2. In **Reports Configuration** pane, select the **Defined** option.
3. Click on the “**Terminal Services Gateway**” group folder to view the imported reports.

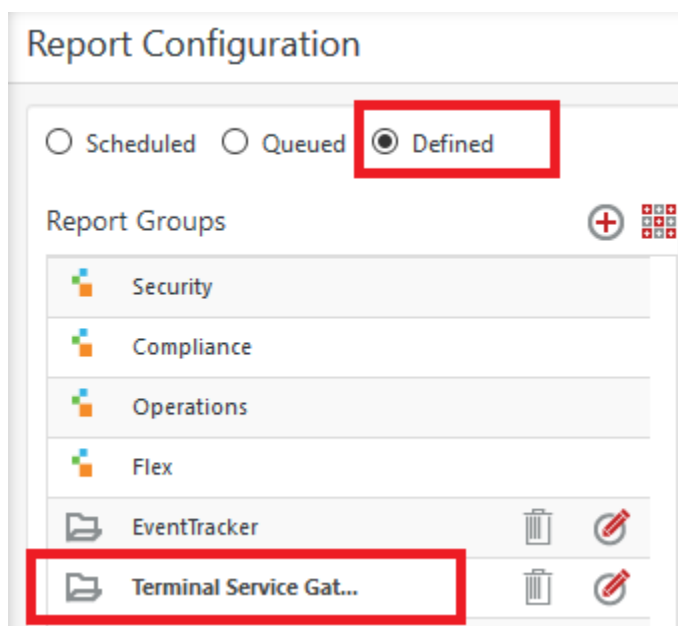


Figure 45

6.5 Knowledge Objects

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Knowledge Objects**.
2. In the **Knowledge Object** tree, expand the “**Terminal Services Gateway**” group folder to view the imported Knowledge objects.

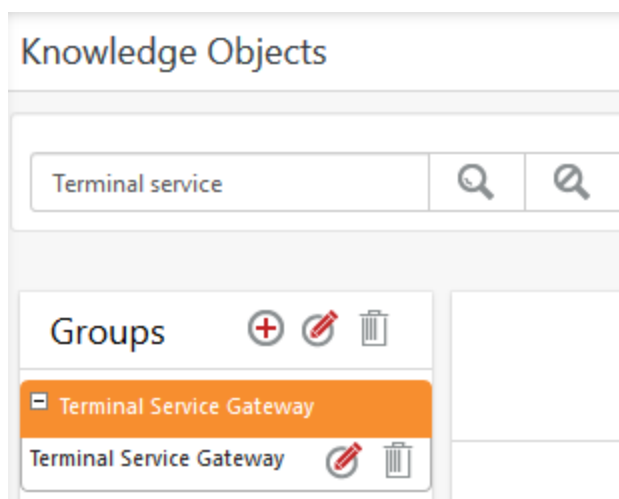


Figure 46

6.6 Dashboards

1. In the EventTracker web interface, Click **Home**  and select **"My Dashboard"**.

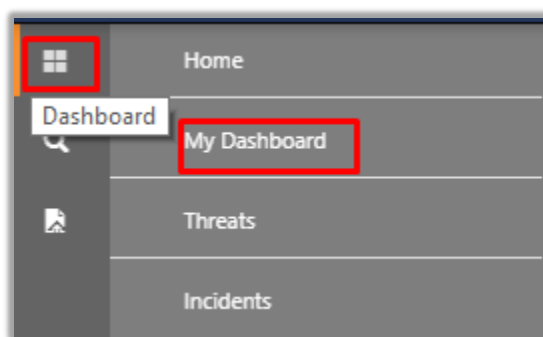


Figure 47

2. In **"Terminal Services Gateway"** dashboard you should be now able to see something like this.

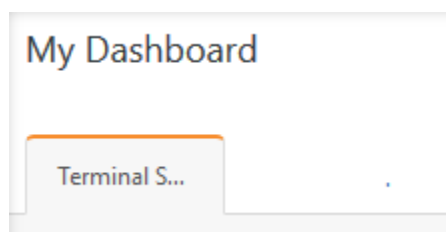


Figure 48