

Integrate AudioCodes

EventTracker v9.2 and above

Abstract

This guide will facilitate an AudioCodes user to send logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker 9.2 or later and AudioCodes SBC's (VE) v7.2.

Audience

Administrators who want to monitor the AudioCodes 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
1.1	Pre-requisites.....	3
1.2	Integration of AudioCodes events to EventTracker	3
1.2.1	Enabling syslog	3
2.	EventTracker Knowledge Pack	5
2.1	Categories	5
2.2	Alerts.....	5
2.3	Report	5
2.4	Dashboards	7
3.	Importing knowledge pack into EventTracker	12
3.1	Categories	13
3.2	Alerts.....	14
3.3	Token Template	15
3.4	Flex Reports	16
3.5	Knowledge Objects	18
3.6	Dashboards	19
4.	Verifying knowledge pack in EventTracker	20
4.1	Categories	20
4.2	Alerts.....	21
4.3	Token Template	21
4.4	Flex Reports	22
4.5	Knowledge Objects	23
4.6	Dashboards	23

1. Introduction

AudioCodes Ltd is a leading vendor of advanced voice networking and media processing solutions for the digital workplace. AudioCodes's SBC is a device that protects data and voice over a VoIP network. It has multiple deployment methods, one of which is, Mediant VE (built for deployment in virtualized data centers, public clouds, and NFV environments).

EventTracker can be integrated with AudioCodes using its syslog. It helps you to monitor the outgoing and incoming call activities by the client based on user geolocation, username, and login attributes which helps you to find the unauthorized access attempt to the login page.

EventTracker also alerts you if any unauthorized access attempts to the login page and IP address are added to the blacklist.

EventTracker generates a schedule report for user login activities, incoming and outgoing calls in AudioCodes. It displays incoming and outgoing calls by location and call activities by source and destination IP address, etc.

1.1 Pre-requisites

- The host machine should have installed the **EventTracker agent**.
- Administrator privilege for AudioCodes web interface.
- AudioCodes SBC's (VE) v7.2 should be installed.

1.2 Integration of AudioCodes events to EventTracker

1.2.1 Enabling syslog

1. Connect to the SBC web interface, and then log in using the default credentials.
2. Open the Logging Settings page (**TROUBLESHOOT > Logging > Logging Settings**).
3. Configure the following parameters.
 - a. From the '**Enable Syslog**' drop-down list, select "**Enable**".

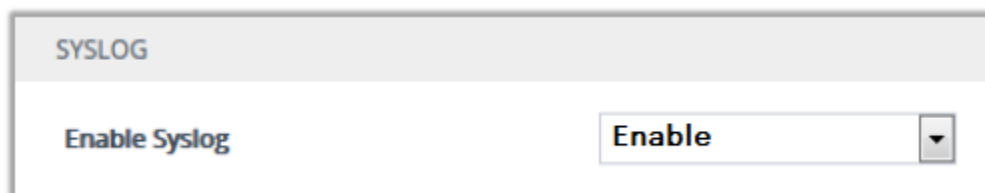
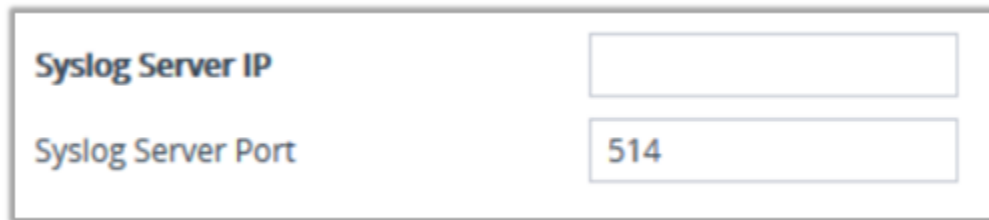


Figure 1

- b. Please fill the below information.

In the '**Syslog Server IP**' field, enter the "**EventTracker IP address**".

In the '**Syslog Server Port**' field, enter the port number **514**.



The image shows a configuration form with two input fields. The first field is labeled 'Syslog Server IP' and is empty. The second field is labeled 'Syslog Server Port' and contains the value '514'.

Figure 2

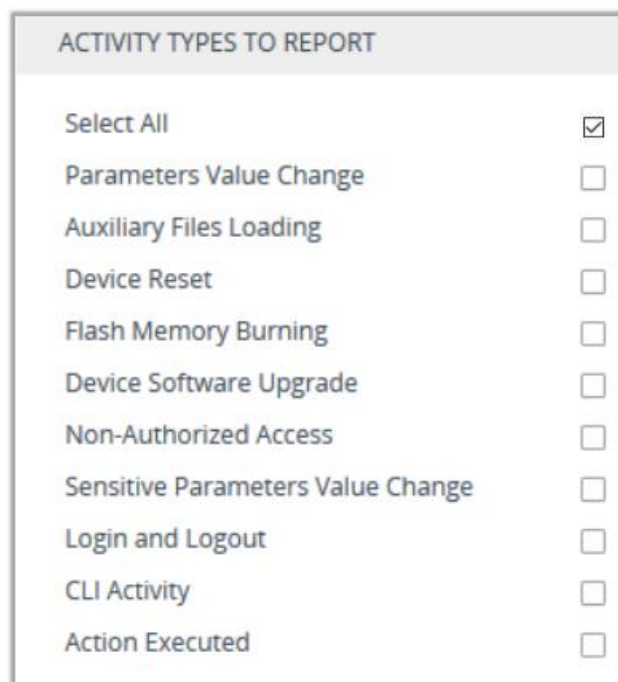
- c. In the '**Log Severity Level**' drop-down list, select the severity level, "**Informational**".



The image shows a drop-down menu labeled 'Log Severity Level'. The selected option is 'Informational', which is highlighted in yellow. A small downward arrow is visible on the right side of the menu.

Figure 3

- d. To configure reporting of management user activities, under the "**Activity Types to Report group**", select the actions to report to the syslog server. Choose, "**Select All**".



The image shows a list titled 'ACTIVITY TYPES TO REPORT'. The list contains the following items with checkboxes to their right:

ACTIVITY TYPES TO REPORT	
Select All	<input checked="" type="checkbox"/>
Parameters Value Change	<input type="checkbox"/>
Auxiliary Files Loading	<input type="checkbox"/>
Device Reset	<input type="checkbox"/>
Flash Memory Burning	<input type="checkbox"/>
Device Software Upgrade	<input type="checkbox"/>
Non-Authorized Access	<input type="checkbox"/>
Sensitive Parameters Value Change	<input type="checkbox"/>
Login and Logout	<input type="checkbox"/>
CLI Activity	<input type="checkbox"/>
Action Executed	<input type="checkbox"/>

Figure 4

4. Click **Apply** to apply your settings.

2. EventTracker Knowledge Pack

Once AudioCodes events are received in EventTracker alerts, and reports can be configured in EventTracker.

The following knowledge packs are available in EventTracker to support AudioCodes monitoring.

2.1 Categories

AudioCodes: User login success - This category provides information related to AudioCodes web console login success.

AudioCodes: User logout – This category provides information related to user logout from AudioCodes web console.

AudioCodes: IDS activities – This category provides information related to IDS detects blocklist IP addresses.

AudioCodes: Incoming SIP Calls – This category provides information related to incoming call details like source IP address, destination IP address, etc.

AudioCodes: Outgoing SIP Calls – This category provides information related to outgoing call details like source IP address, destination IP address, etc.

2.2 Alerts

AudioCodes: Unauthorized access attempt to login – This alert is triggered when the unauthorized access to the AudioCodes login page is made.

AudioCodes: IP added to blacklist – This alert is triggered when the IP is added to the blacklist.

2.3 Report

AudioCodes - Incoming Calls – This report provides information related to the incoming call-initiated details like caller id, destination IP, destination port, source IP, source port, protocol type, interface, etc.

Log Considered

```
Aug 19 12:15:39 81.144.28.83 Aug 19 11:15:39 sbc-bra01.bt.management.local [S=324082] [SID=88e9cc:10:242939] ( sip_stack)( 461020) ---- Incoming SIP Message from 200.47.131.38:5060 to SIPInterface #1 (DSIP-Trunk) UDP TO(#1) --
-- #012OPTIONS sip:104.41.49.240:5060 SIP/2.0 #012Max-Forwards: 70 #012To: <sip:104.41.49.240> #012From:
<sip:200.47.131.38>;tag=3806824538-1402146024 #012Call-ID: 4292541-3806824538-1919166543@S3-BT-
01.comsat.com.ar #012CSeq: 1 OPTIONS #012Allow:
PUBLISH,MESSAGE,UPDATE,SUBSCRIBE,REFER,INFO,NOTIFY,REGISTER,OPTIONS,BYE,INVITE,ACK,CANCEL #012Via:
SIP/2.0/UDP 200.47.131.38:5060;branch=z9hG4bK0be518b89f02f7027108c599cf01ef73 #012Contact:
<sip:200.47.131.38:5060> #012Content-Length: 0 #012 #012 #012( sip_stack)( 461021) ---- Outgoing SIP Message
```

```
to 200.47.131.38:5060 from SIPInterface #1 (DSIP-Trunk) UDP TO(#1) ---- #012SIP/2.0 200 OK #012Via: SIP/2.0/UDP
200.47.131.38:5060;branch=z9hG4bK0be518b89f02f7027108c599cf01ef73 #012From:
<sip:200.47.131.38>;tag=3806824538-1402146024 #012To: <sip:104.41.49.240>;tag=1c1758818554 #012Call-ID:
4292541-3806824538-1919166543@S3-BT-01.comsat.com.ar #012CSeq: 1 OPTIONS #012Contact:
<sip:tgrp=PSTNTrunk;trunk-context=sipt.bt.com@104.41.49.240:5060> #012Server: Mediant VE SBC/v.7.20A.204.789
#012Content-Length: 0 #012 #012 #012 [Time:19-08@11:15:34.745]
```

Sample_Report

LogTime	Allow	branch	Call ID	Destination IP	Destination port	Interface	Source IP	Source Port	Transport	Via
08/24/2020 11:06:42 AM	MESSAGE,REFER,INFO,OPTIONS,BYE,INVITE,ACK,CANCEL	z9hG4bK2dbfc546ade8ff359bf84fa7dfb92a3c;alias	942312175-3806824291-588932658@SBC9-CHC-US.bt.com	63.250.128.140	5061	SOTI-Trunk	52.183.1.111	5060	TLS	SIP/2.0/TLS 63.250.128.140:5061
08/24/2020 11:06:42 AM	MESSAGE,SUBSCRIBE,REFER,INFO,NOTIFY,REGISTER,OPTIONS,BYE,INVITE,ACK,CANCEL	z9hG4bKaa8efec181bcd78dd9843242ba19d12;alias	489218601-3806824289-1840361450@SBC5-FFT-EU.bt.com	62.134.200.60	5061	SOTI-Trunk	23.101.51.131	5060	TLS	SIP/2.0/TLS 62.134.200.60:5061

Figure 5

AudioCodes - Outgoing Calls - This report provides information related to the outgoing call initiated details like caller id, destination IP, destination port, source IP, source port, protocol type, interface, etc.

Log Considered

```
Aug 19 12:11:33 81.144.28.83 Aug 19 11:11:33 sbc-vir05.bt.management.local [S=1845189] [SID=8d3a57:8:1342329] (
sip_stack)( 2686404) ---- Outgoing SIP Message to 52.114.76.76:5061 from SIPInterface #0 (Teams) TLS TO(#5590)
SocketID(410) ---- #012OPTIONS sip:10.11.2.7 SIP/2.0 #012Via: SIP/2.0/TLS VIR05-
001.btocmvoice.com:5067;alias;branch=z9hG4bKac1542391285 #012Max-Forwards: 70 #012From:
<sip:10.11.2.7>;tag=1c1758203382 #012To: <sip:10.11.2.7> #012Call-ID: 10144927951982020111131@VIR05-
001.btocmvoice.com #012CSeq: 1 OPTIONS #012Contact: <sip:VIR05-001.btocmvoice.com:5067;transport=tls>
#012Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE #012User-
Agent: Mediant VE SBC/v.7.20A.204.789 #012Accept: application/sdp, application/simple-message-summary,
message/sipfrag #012Content-Length: 0 #012 #012 #012 [Time:19-08@11:11:31.885]
```

Sample_Report

LogTime	Accept	Allow	branch	Call ID	Destination IP	Destination port	Interface	Source IP	Transport
08/24/2020 11:06:42 AM	application/sdp, application/simple-message-summary, message/sipfrag	REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE	z9hG4bKac1297131377	20298735991982020111129@NSW02-002.btocmvoice.com	52.114.148.0	5061	Teams	10.12.2.5	tls
08/24/2020 11:06:42 AM		INVITE,ACK,OPTIONS,CANCEL,BYE,NOTIFY	z9hG4bKe4ce7059	354b73a9-6b68-49d2-b705-3a5e3b4fdafa	52.114.148.0	9793	Teams	10.12.2.5	tls
08/24/2020 11:06:42 AM	application/sdp, application/simple-message-summary, message/sipfrag	REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE	z9hG4bKac1175939149	5845480641982020111125@52.170.250.71	63.250.128.140	5061	SOTI-Trunk	10.11.2.5	tls

Figure 6

AudioCodes - User login and logout – This report provides information related to user login and logout successfully from AudioCodes console.

Log Considered

```
Aug 19 11:23:33 81.144.28.83 Aug 19 10:23:33 sbc-bra01.bt.management.local [S=322549] [BID=88e9cc:10] Activity Log: WEB: User logout. User: adm_gthomas. Session: WEB (10.5.129.1) [Time:19-08@10:23:30.007]
Aug 19 11:16:55 81.144.28.83 Aug 19 10:16:55 sbc-bra01.bt.management.local [S=322364] [BID=88e9cc:10] Activity Log: WEB: Successful login at 10.17.1.4:443. User: adm_gthomas. Session: WEB (10.5.129.1) [Time:19-08@10:16:52.384]
```

Sample_Report

LogTime	Computer	User Name	Source IP Address	Source Port	ID	Sequence Number	status
08/24/2020 11:06:42 AM	NTPLDTBLR46\AUDIOCODES-SYSLOG	adm_gthomas	10.5.129.1		262181:18	87825276	User logout
08/24/2020 11:06:42 AM	NTPLDTBLR46\AUDIOCODES-SYSLOG	adm_gthomas	10.13.1.5	443	262181:18	87825360	Successful login
08/24/2020 11:06:42 AM	NTPLDTBLR46\AUDIOCODES-SYSLOG	adm_gthomas	10.5.129.1		262181:18	87832640	User logout

Figure 7

AudioCodes - User activities – This report provides information related to user performed activities as IP profiles reset, IP profile group changed, etc.

Log Considered

```
Aug 14 10:21:35 81.144.28.83 Aug 14 09:21:35 10.5.130.3 [S=88292131] [BID=262181:18] Activity Log: "Import Trusted Certificates" was executed. User: adm_gthomas. Session: WEB (10.5.129.1) [Time:14-08@09:21:34.470]
Aug 14 10:21:35 81.144.28.83 Aug 14 09:21:35 10.5.130.3 [S=88292130] [BID=262181:18] Activity Log: Loaded File GoDaddyRoot2.cer. User: adm_gthomas. Session: WEB (10.5.129.1) [Time:14-08@09:21:34.420]
Aug 14 10:03:45 81.144.28.83 Aug 14 09:03:45 10.5.130.3 [S=88284349] [BID=262181:18] Activity Log: IP Groups row 3 - "IP Profile" was changed to "2". User: TeamsSBCAdmin. Session: WEB (10.5.129.1) [Time:14-08@09:03:43.419]
```

Sample_Report

LogTime	Computer	User Name	Action	ID	Sequence Number	Source IP Address
08/24/2020 11:06:41 AM	NTPLDTBLR46\AUDIOCODES-SYSLOG	kenneth	IP Profiles row 2 - "Reset SRTP Upon Re-key" was changed to "0"	262181:18	88267220	10.5.129.1
08/24/2020 11:06:41 AM	NTPLDTBLR46\AUDIOCODES-SYSLOG	maya	IP Groups row 3 - "IP Profile" was changed to "4"	262181:18	88284102	10.5.129.1
08/24/2020 11:06:41 AM	NTPLDTBLR46\AUDIOCODES-SYSLOG	joeb	IP Profiles row 2 - "SBC Media Security Mode" was changed to "1"	262181:18	88269891	10.5.129.1

Figure 8

2.4 Dashboards

- **AudioCodes – Login success by username:** This dashboard shows login success user names into the AudioCodes web console.

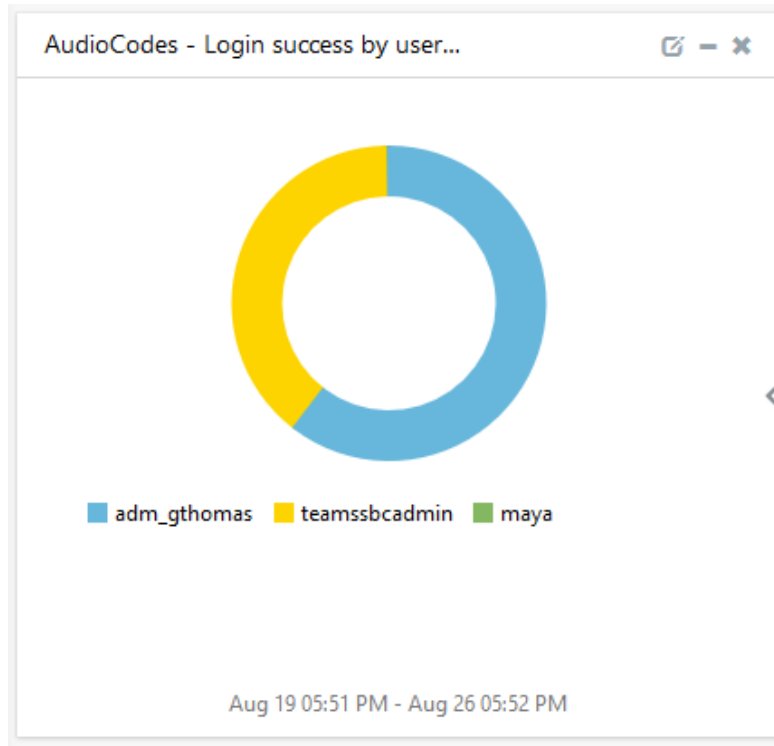


Figure 9

- **AudioCodes – Outgoing calls destination IP by country** – This dashboard shows outgoing call receivers location by destination IP address.

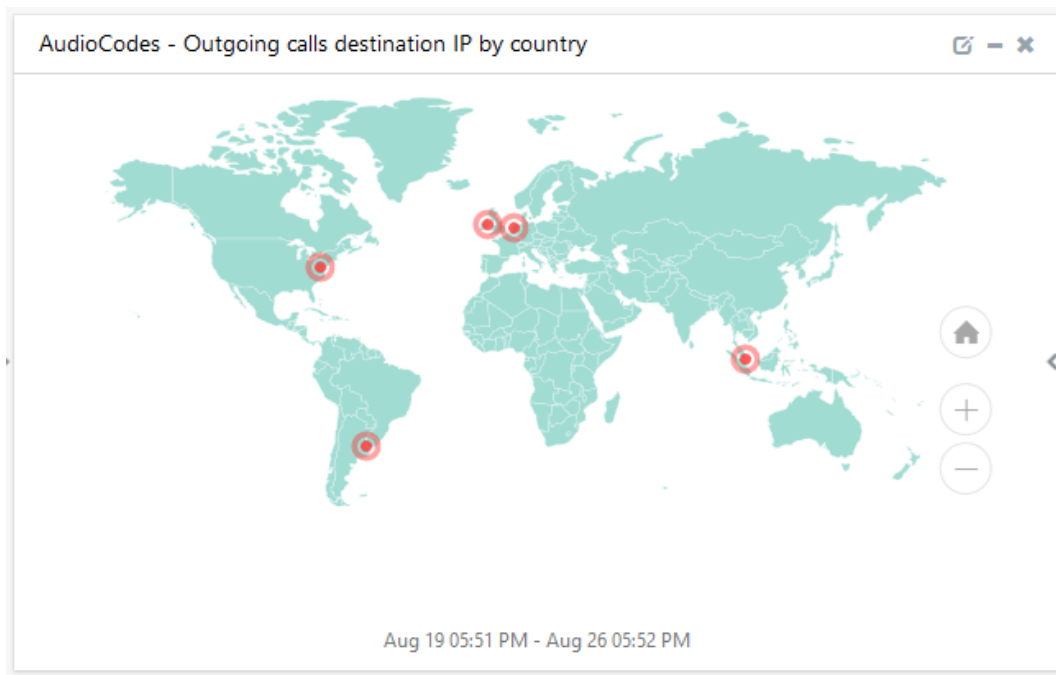


Figure 10

- **AudioCodes – IDS activities by logtype** – This dashboard shows id activities by log types like IDS rule, IDS blacklist notification, IDS counter, etc.

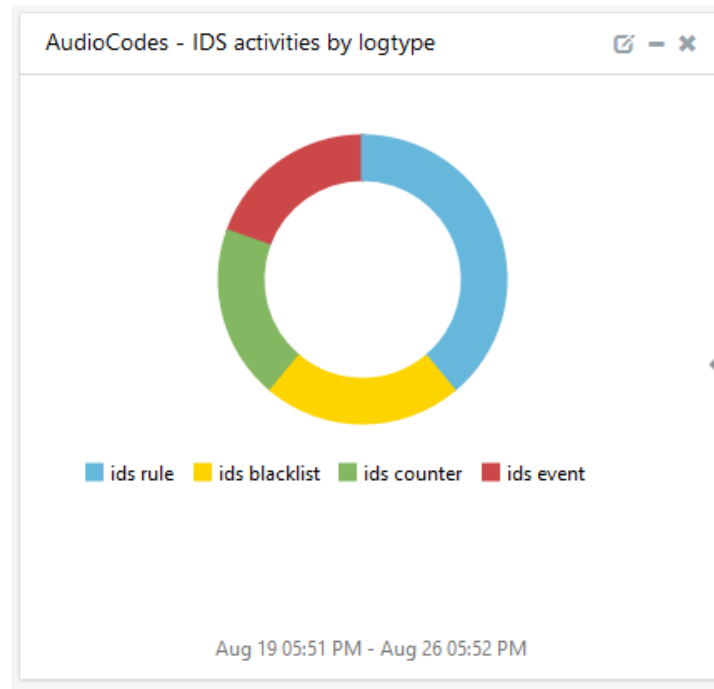


Figure 11

- **AudioCodes – Incoming calls by IP address**– This dashboard shows incoming call by source and destination IP address.

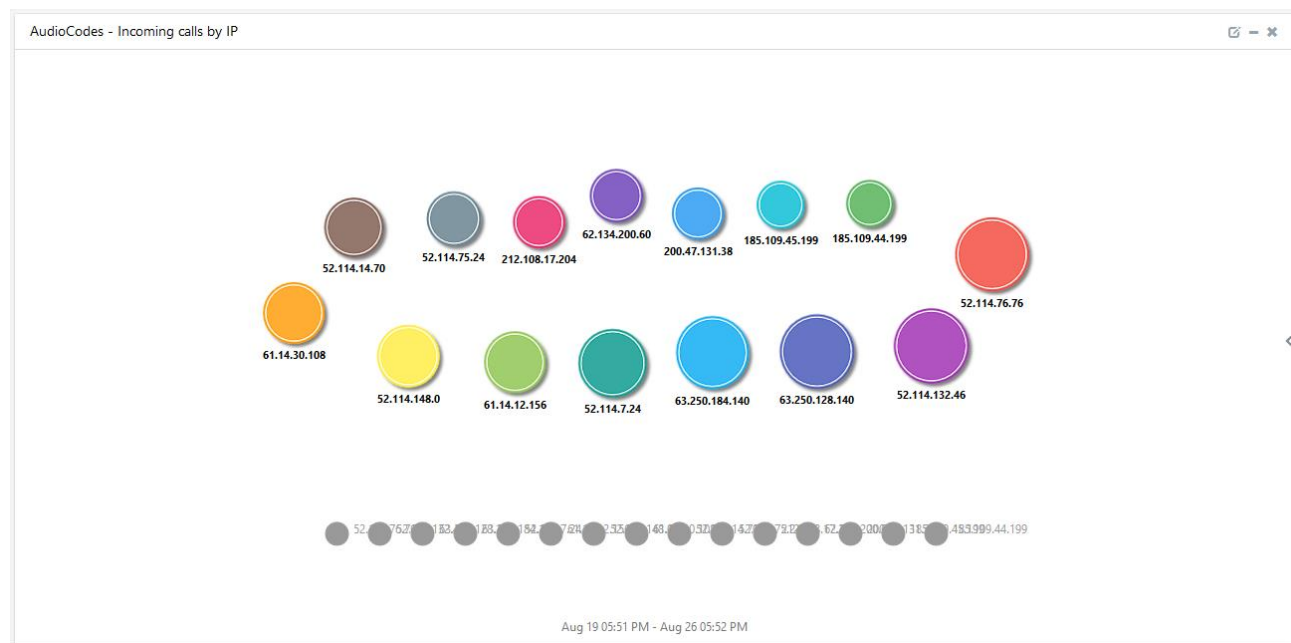


Figure 12

- **AudioCodes – Incoming calls destination IP by country** – This dashboard shows the incoming calls by destination IP address.

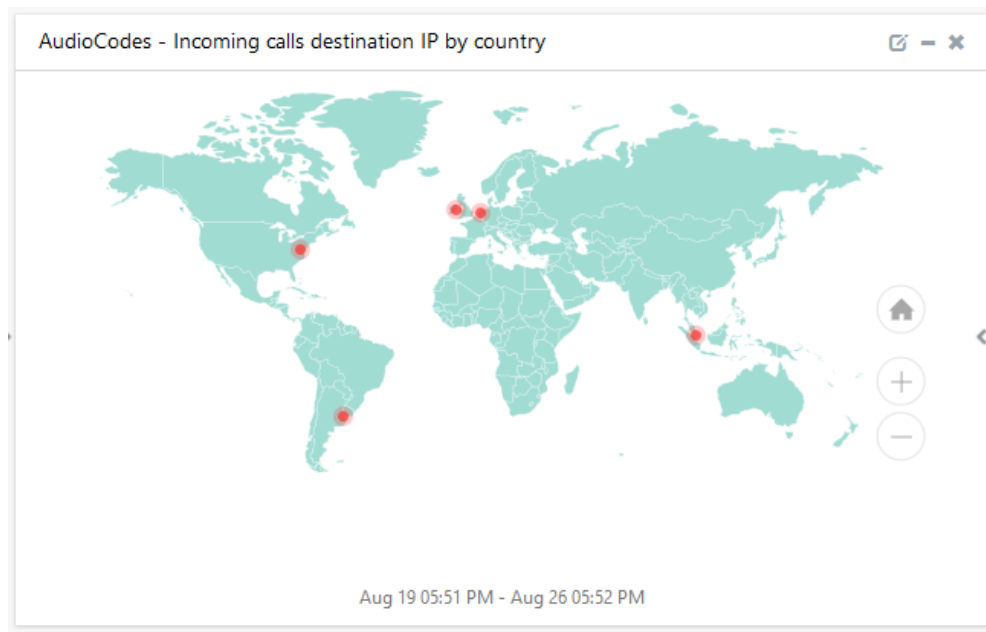


Figure 13

- **AudioCodes – Incoming calls source IP by country** – This dashboard shows the Incoming calls by source IP address.

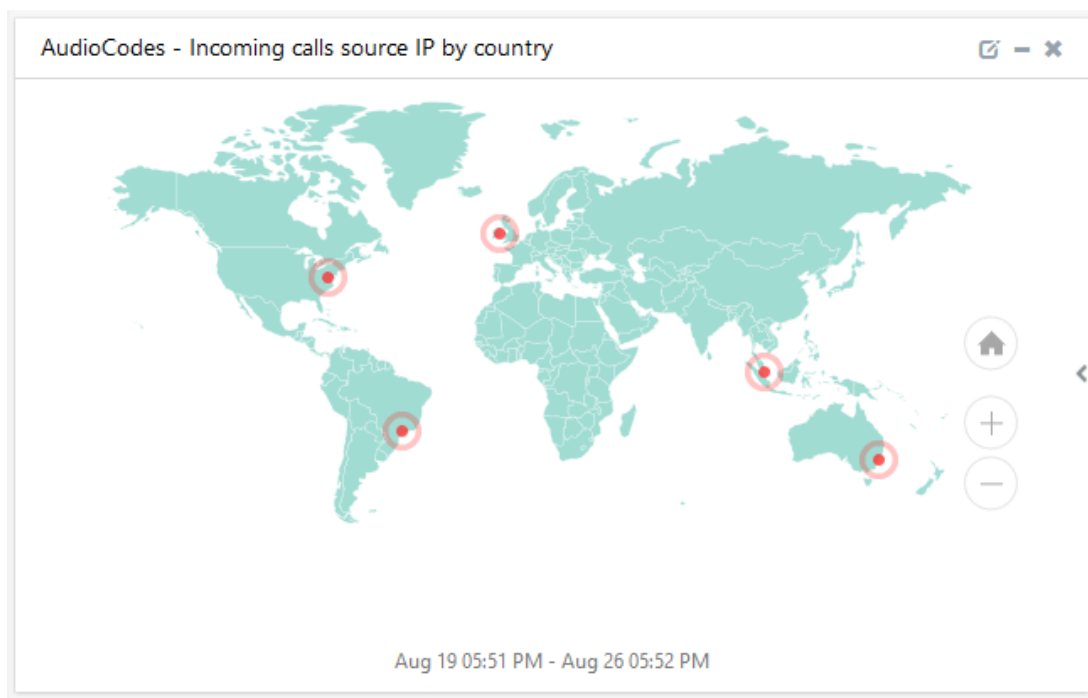


Figure 14

- **AudioCodes – Call activities by logtype** – This dashboard shows call activities by different logotypes.

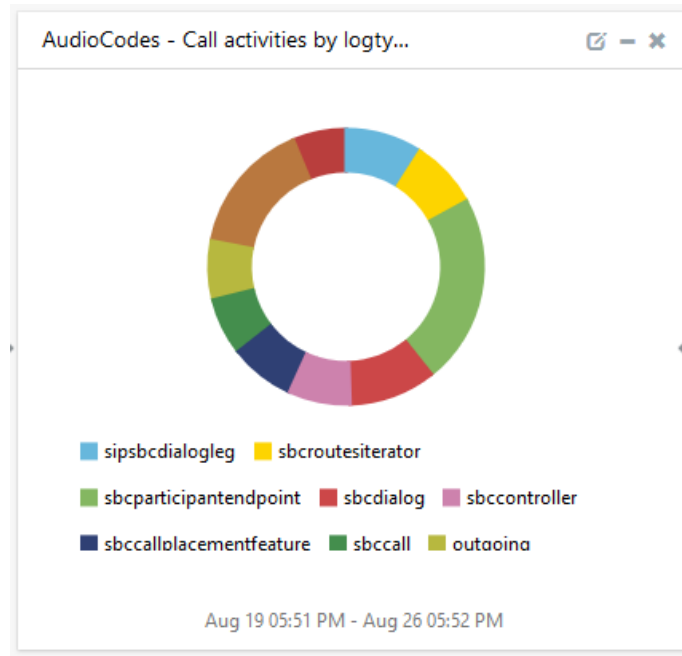


Figure 15

- **AudioCodes – Unauthorized access denied** – This dashboard shows the IP address of unauthorized users attempting to access the login page.

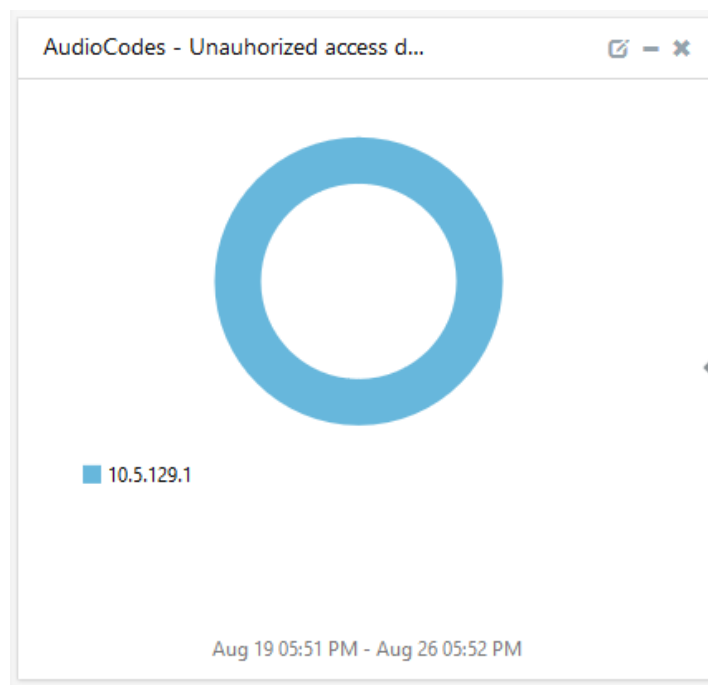


Figure 16

3. 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**.

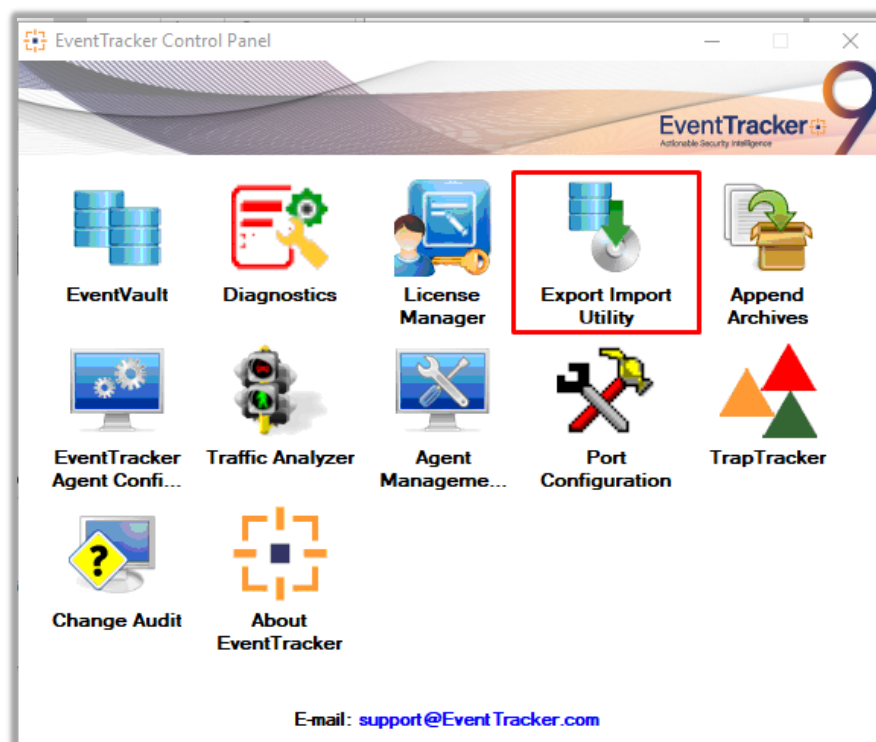


Figure 17

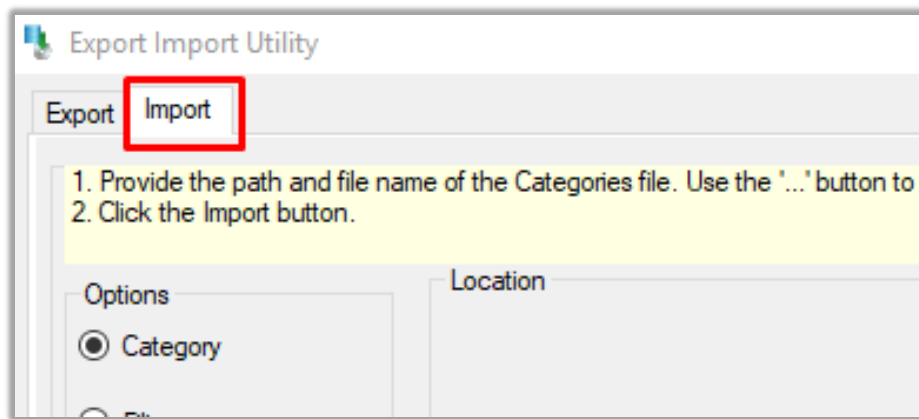


Figure 18

3. Click the **Import** tab.

3.1 Categories

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

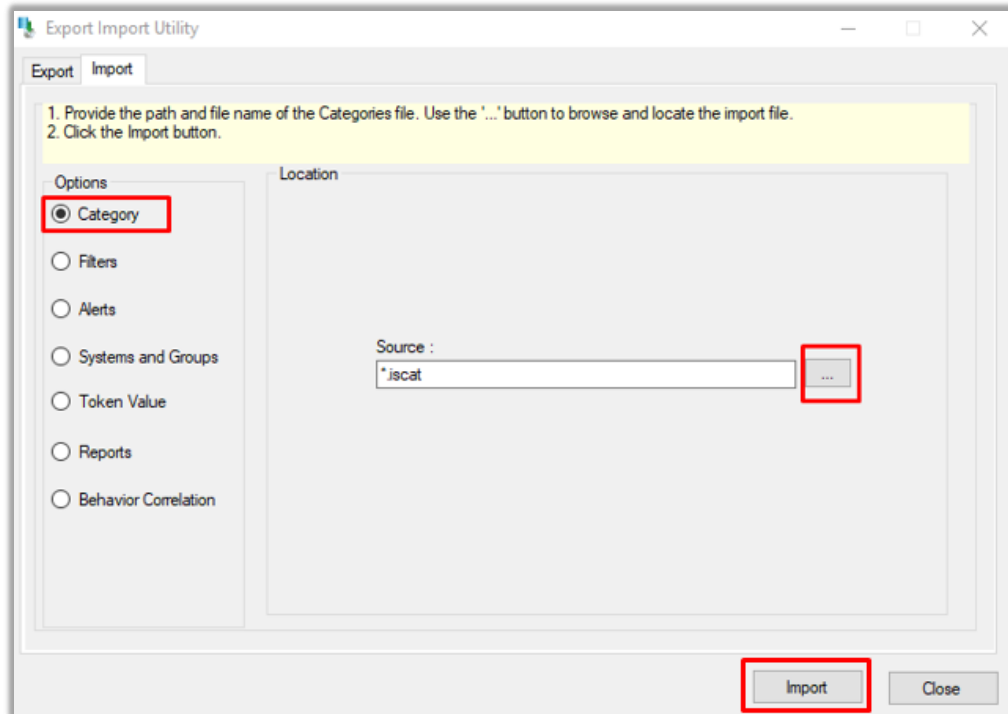


Figure 19

EventTracker displays a success message:

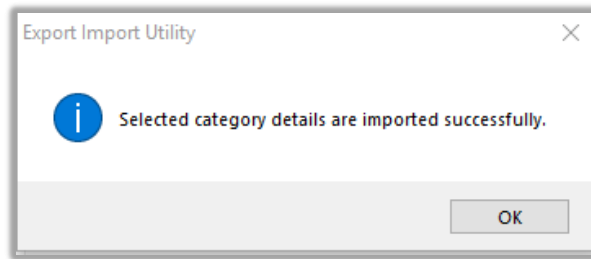


Figure 20

3.2 Alerts

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

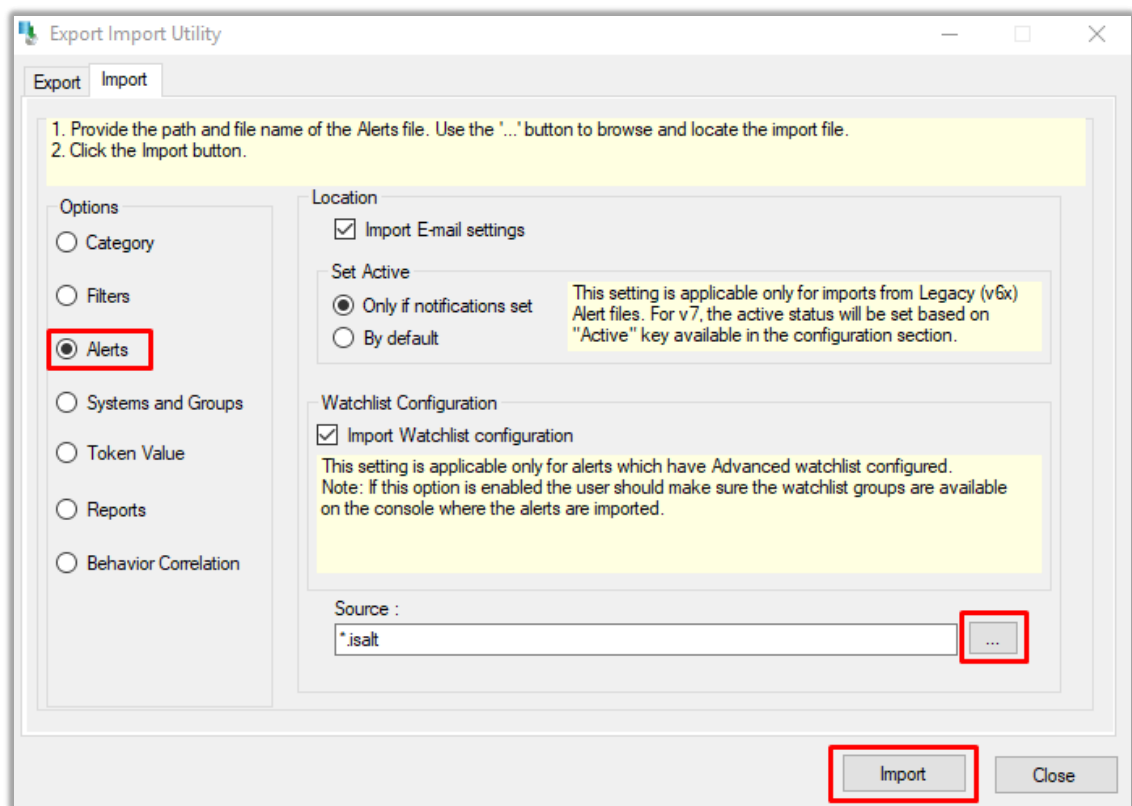


Figure 21

EventTracker displays a success message.

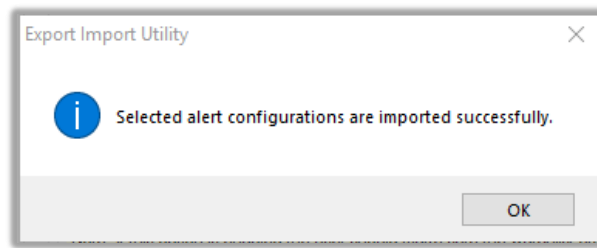


Figure 22

3.3 Token Template

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.

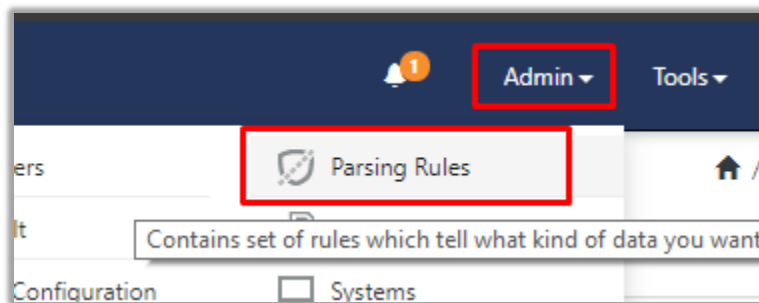


Figure 23

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

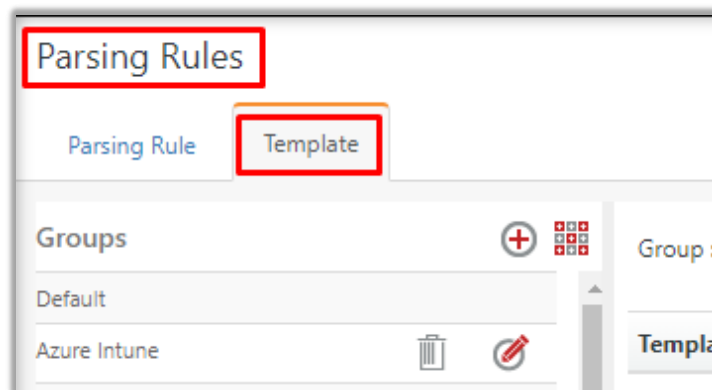


Figure 24

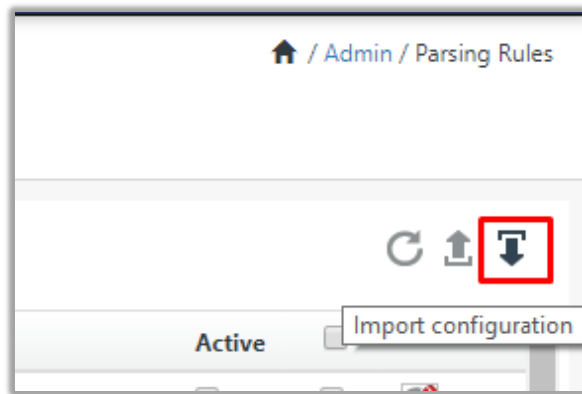


Figure 25

- 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_AudioCodes.ettd"** file is located. Wait for the templates to be loaded. Once you see the templates, choose the desired templates and click **"Import"**.

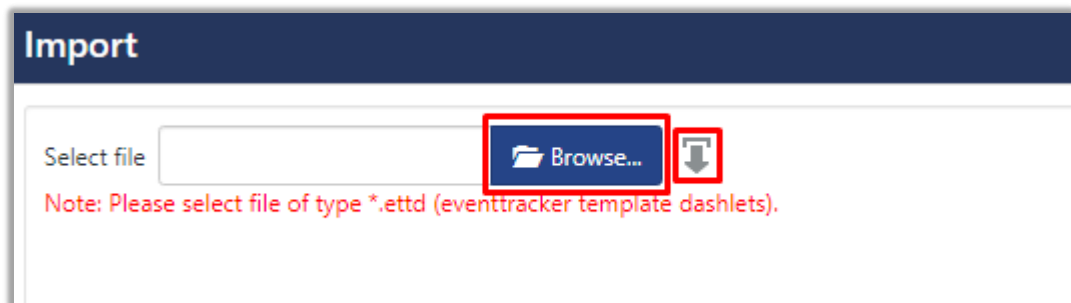


Figure 26

3.4 Flex Reports

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

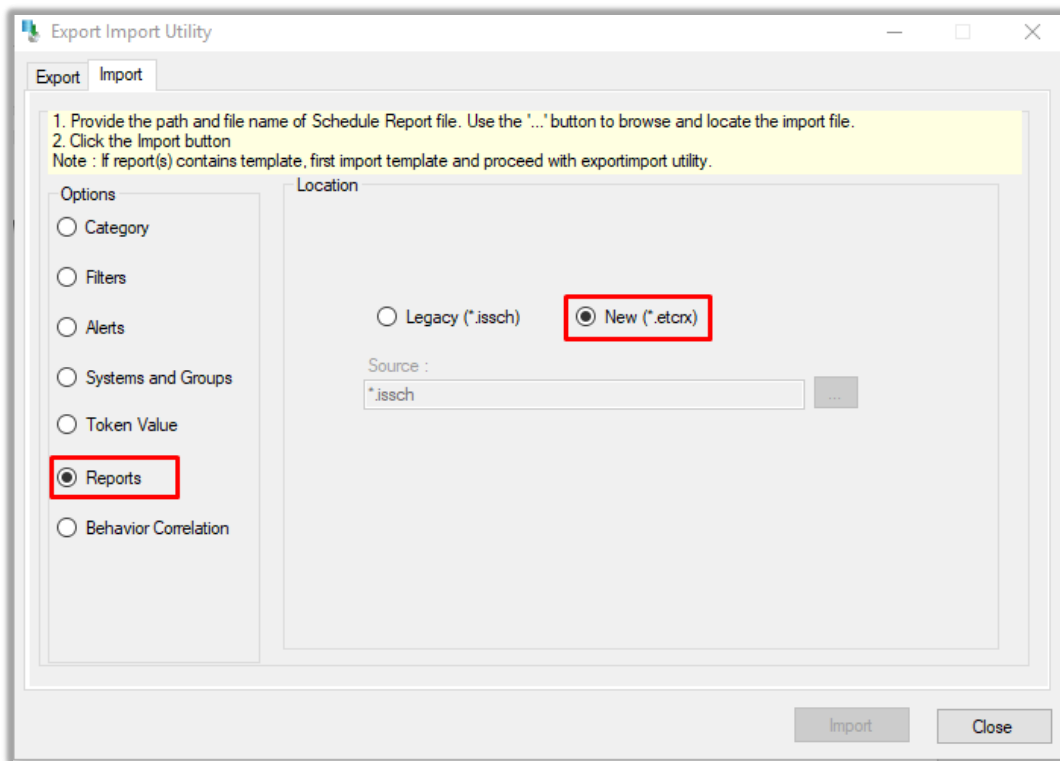


Figure 27

- 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_AudioCodes.etcrx**”.

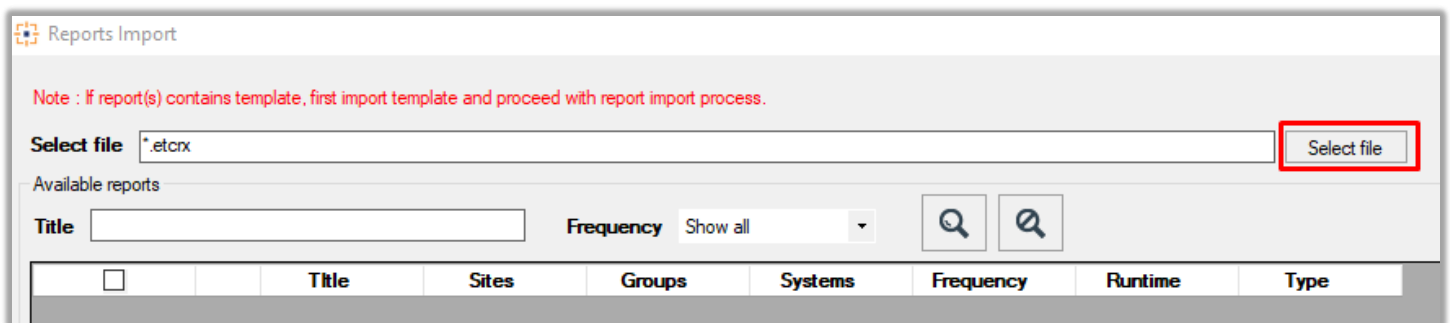



Figure 28

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

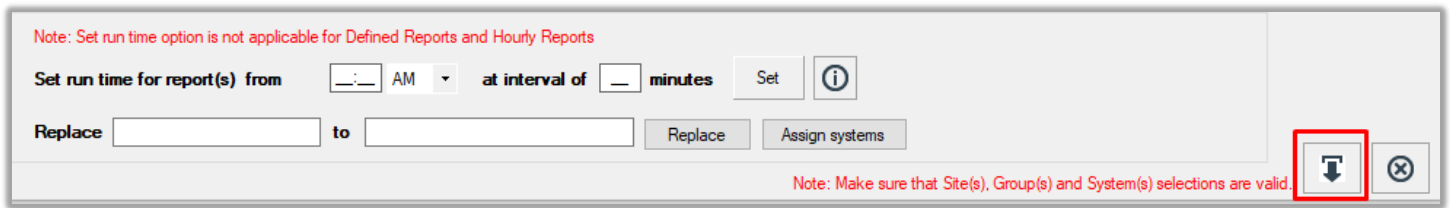


Figure 29

EventTracker displays a success message:

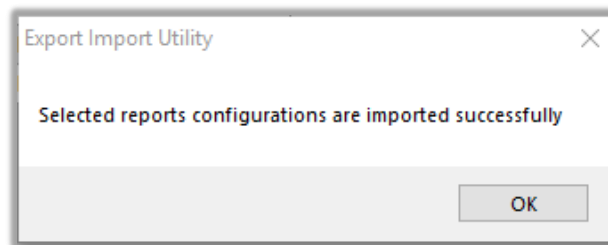


Figure 30

3.5 Knowledge Objects

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

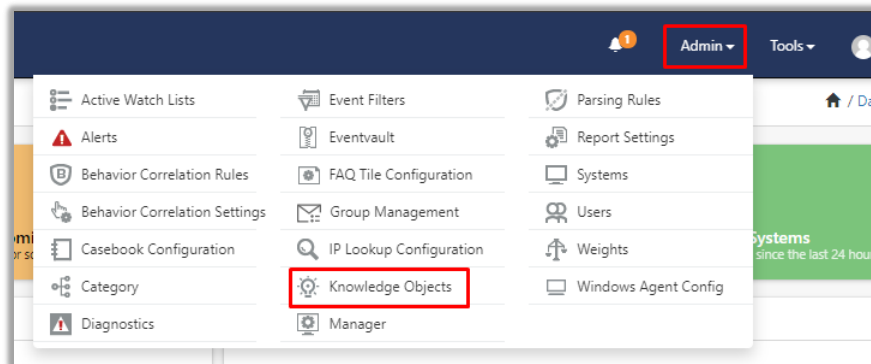


Figure 31

2. Next, click the “import object” icon.

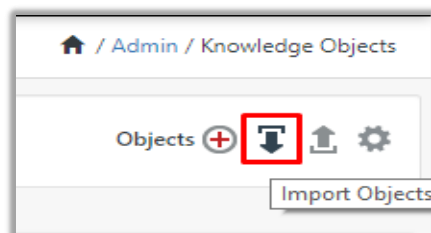


Figure 32

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_AudioCodes.etko"** and then click the **"Upload"** button.

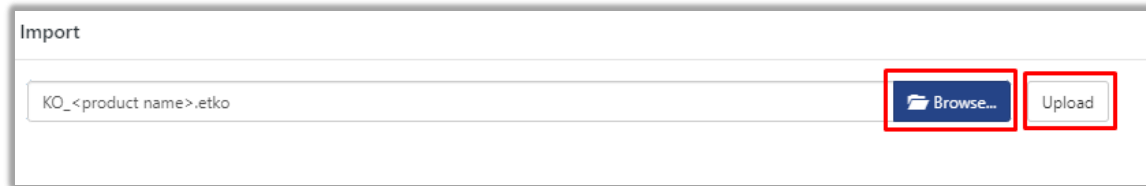


Figure 33

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click on the **"Import"** button.



Figure 34

3.6 Dashboards

1. Login to the **EventTracker** web interface.
2. Navigate to **Dashboard → My Dashboard**.
3. In **"My Dashboard"**, Click **Import**.

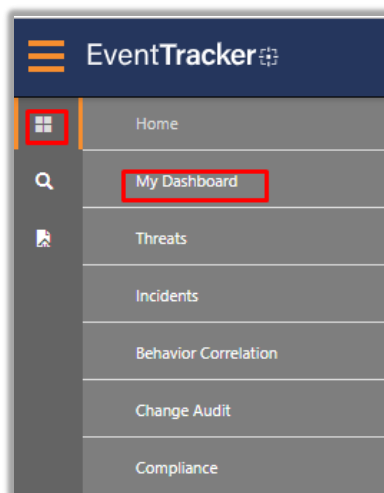


Figure 35

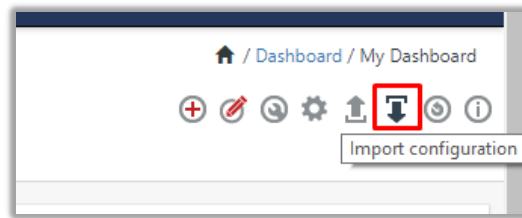


Figure 36

4. Select the **Browse** button 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_AudioCodes.etwd**" is saved and click on "**Upload**" button.
5. Wait while EventTracker populates all the available dashboards. Now, choose "**Select All**" and click on "**Import**" button.

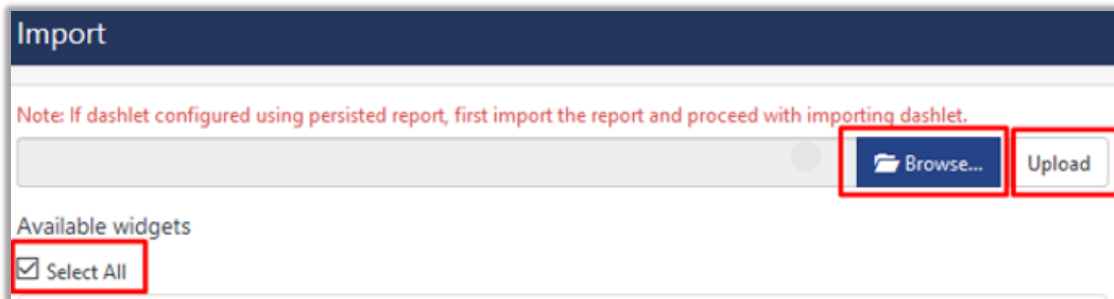


Figure 37



Figure 38

4. Verifying knowledge pack in EventTracker

4.1 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 "**AudioCodes**". You will see the below results.

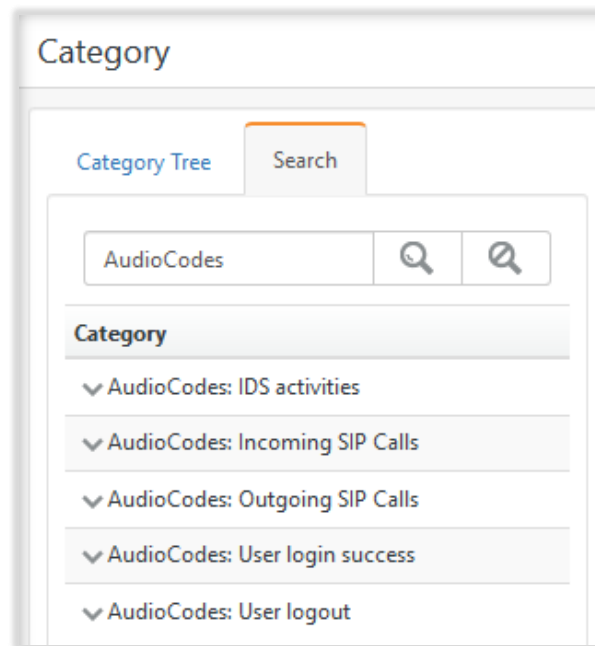


Figure 39

4.2 Alerts

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In search box enter “**AudioCodes**” and then click the **Search** button.

EventTracker displays an alert related to AudioCodes.

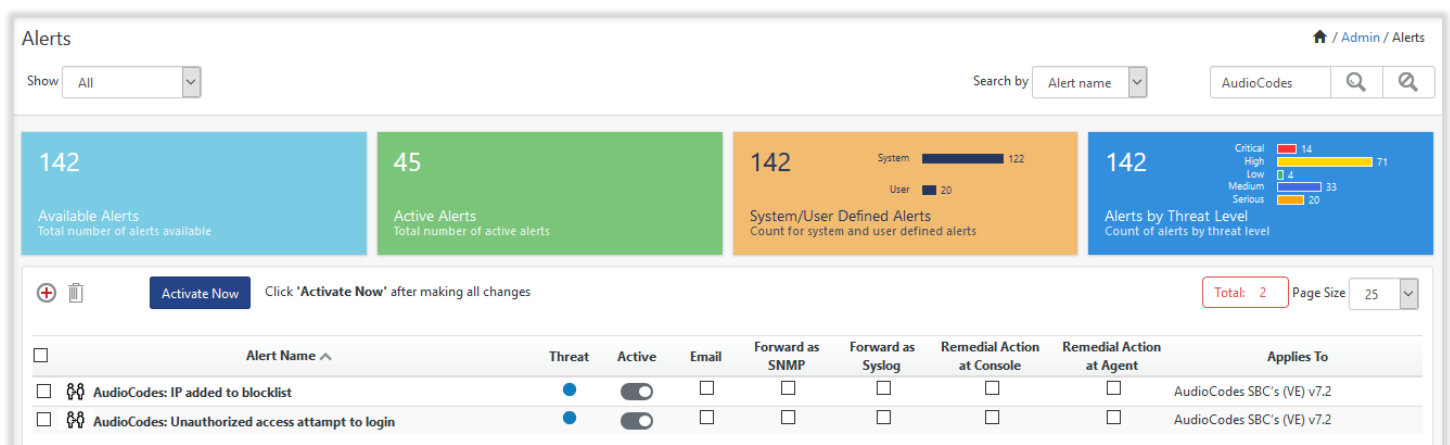


Figure 40

4.3 Token Template

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click “**Parsing Rules**”.

2. In the **“Template”** tab, click on the **“AudioCodes”** group folder to view the imported token.

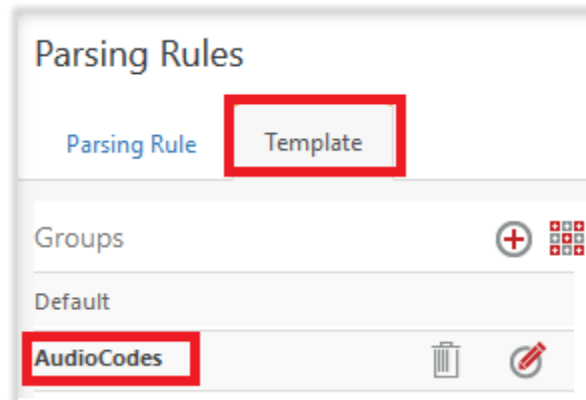


Figure 41

4.4 Flex Reports

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

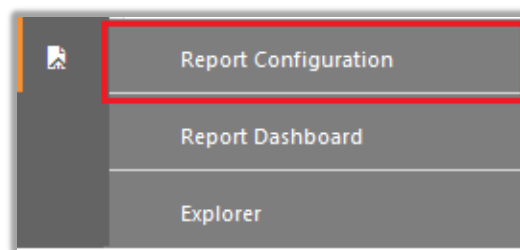


Figure 42

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

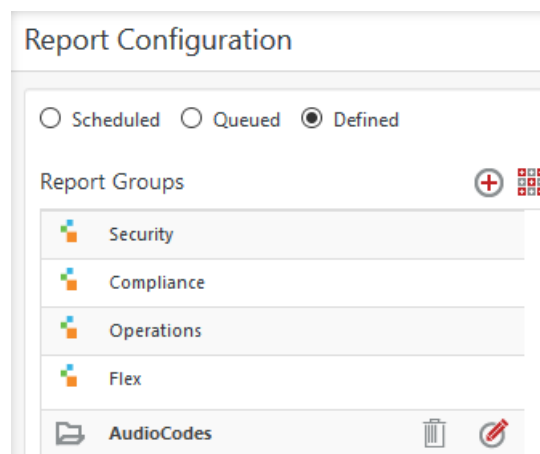


Figure 43

4.5 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 “**AudioCodes**” group folder to view the imported Knowledge objects.

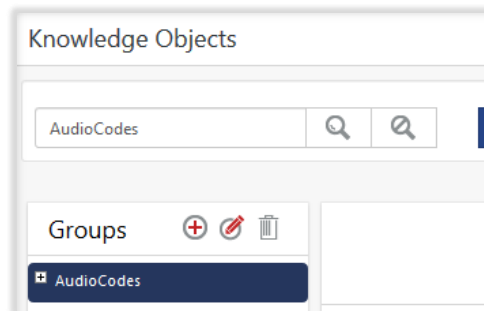


Figure 44

4.6 Dashboards

1. In the EventTracker web interface, Click on Home Button  and select “**My Dashboard**”.

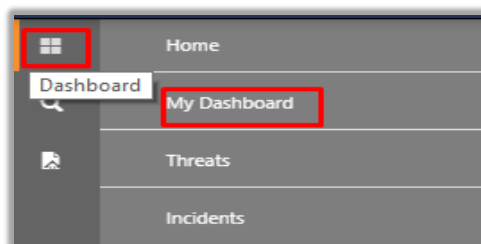


Figure 45

2. In the “**AudioCodes**” dashboard you should be now able to see something like this.

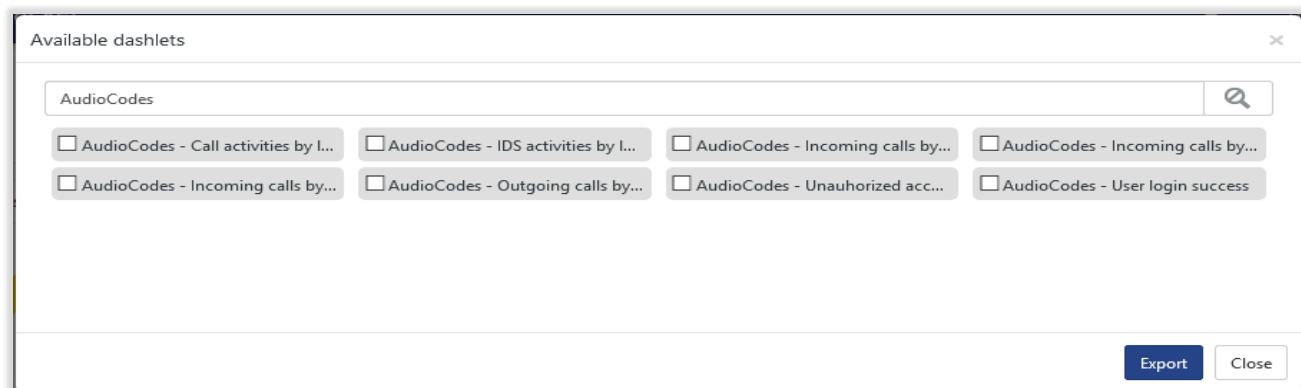


Figure 46