

## Integrate EZproxy

## Abstract

This guide provides instructions to configure EZproxy to send the critical events to EventTracker.

## Scope

The configurations detailed in this guide are consistent with **EventTracker** version **7.x and later**, and **EZproxy** **6.x or later**.

## Audience

Administrators, who are responsible for monitoring EZproxy using 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
Overview.....	3
Prerequisites.....	3
Configure EZproxy to send events to EventTracker .....	3
EZProxy syslog configuration.....	3
EZProxy audit log configuration .....	4
EventTracker DLA configuration.....	5
EventTracker Knowledge Pack (KP).....	8
Reports .....	8
Categories.....	9
Knowledge Objects.....	9
Import EZproxy Knowledge Pack into EventTracker .....	9
Import Parsing Rules .....	10
Import Token Templates .....	11
Import Flex Reports.....	13
Import Knowledge Object .....	14
Verify EZproxy knowledge pack in EventTracker .....	16
Verify Parsing Rules.....	16
Verify Token Templates.....	16
Verify Flex Reports .....	17
Verify Knowledge Object.....	18
Create Dashboards in EventTracker .....	19
Schedule Reports.....	19
Create Dashlets .....	21
Sample Dashboards.....	25
Sample Reports .....	27

## Overview

**EZproxy** is a web proxy server used by organizations to give access from outside the cooperation's computer network to restricted-access websites that authenticate users by IP address.

EventTracker collects and analyzes critical events to provide an administrator insight on client traffic, user behavior and intrusion attempts.

## Prerequisites

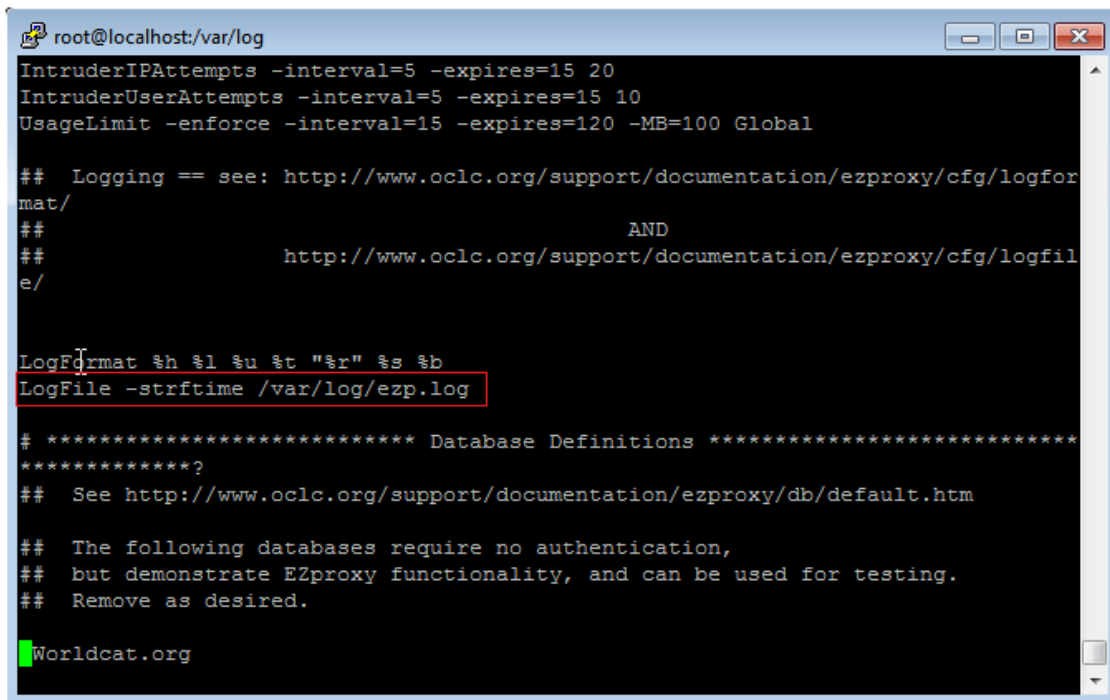
- **EventTracker v7.x or later** should be installed.
- **EZproxy v6.X or later** should be installed on Linux.

## Configure EZproxy to send events to EventTracker

### EZProxy syslog configuration

Following are the steps for forwarding usage logs from EZProxy to EventTracker machine using syslog.

1. First, check the location of EZproxy log file through **/usr/local/ezproxy/conf.txt**



```

root@localhost:/var/log
IntruderIPAttempts -interval=5 -expires=15 20
IntruderUserAttempts -interval=5 -expires=15 10
UsageLimit -enforce -interval=15 -expires=120 -MB=100 Global

## Logging == see: http://www.oclc.org/support/documentation/ezproxy/cfg/logfor
mat/
##
##          AND
##
##          http://www.oclc.org/support/documentation/ezproxy/cfg/logfil
e/

LogFormat %h %l %u %t "%r" %s %b
LogFile -strftime /var/log/ezp.log

# ***** Database Definitions *****
*****?
## See http://www.oclc.org/support/documentation/ezproxy/db/default.htm

## The following databases require no authentication,
## but demonstrate EZproxy functionality, and can be used for testing.
## Remove as desired.

Worldcat.org

```

Figure 1

2. Make an entry in the `/etc/rsyslog.conf` file as shown:

```
*.info /var/log/ezp.log
```

3. Make entry in the end of `/etc/rsyslog.conf` file as shown:

```
*.* @EventTracker Machine IP or hostname
```

**NOTE**-To generate and consume audit events, the additional directives are added to `config.txt` and the EventTracker DLA is configured.

## EZProxy audit log configuration

1. To enable **audit and intrusion logging** add following directives to `config.txt` file in EZproxy installation directory. As tabulated:

Event	Directive
Login Events	Audit Login.Denied Login.Success Login.Success.Groups Login.Failure
Intrusion Events	IntruderIPAttempts -interval=5 -expires=15 20
	IntruderUserAttempts -interval=5 -expires=15 10

Table 1

2. To transfer audit log files to EventTracker server, use the following script.

```
#!/bin/sh
USERNAME="your-ftp-user-name"
PASSWORD="your-ftp-password"
SERVER="your-ftp.server.com"

# EZproxy local directory to pickup *.txt file
FILE="/var/EZproxy"

# EventTracker remote server directory to upload file
LOGDIR="/Ezproxy"

# login to remote server
ftp -n -i $SERVER <<EOF
user $USERNAME $PASSWORD
mkdir $LOGDIR
cd $LOGDIR
mput $FILE/*.txt
quit
EOF
```

3. Set a **cron** job for running above mentioned script at specific intervals.

```
30 15 * * * /path/to/ftp.exproxy.script.sh
```

## EventTracker DLA configuration

1. Open **EventTracker** in browser and logon.

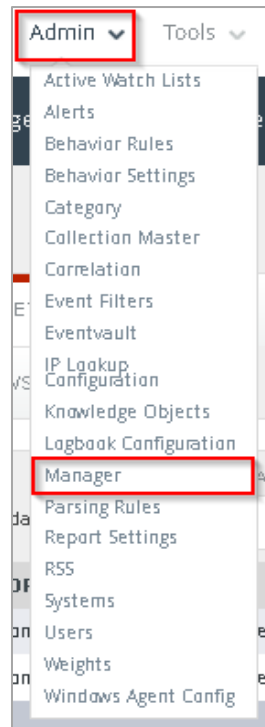


Figure 2

2. In EventTracker Enterprise, click the **Admin** drop-down, select **Manager**.  
Manager Configuration pane is shown:

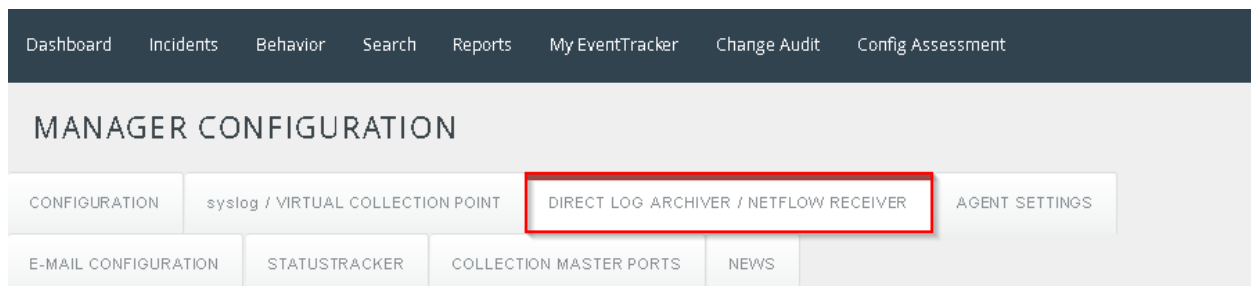


Figure 3

3. Select **Direct Log Archiver/Netflow Receiver** tab.
4. Select **Direct log file archiving from external sources** checkbox.

MANAGER CONFIGURATION

CONFIGURATION    syslog / VIRTUAL COLLECTION POINT    **DIRECT LOG ARCHIVER / NETFLOW RECEIVER**    AGENT SETTINGS

E-MAIL CONFIGURATION    STATUSTRACKER    COLLECTION MASTER PORTS    NEWS

Direct log file archiving from external sources    Purge files after  days    14505

ASSOCIATED VIRTUAL COLLECTION POINT

LOG FILE FOLDER	CONFIGURATION NAME	LOG FILE EXTENSION	FIELD SEPARATOR	LOG TYPE
D:\MS Office 365\Non Empty	0365	csv	Comma - [Fields containing comma are wrapped in double quotes]	
D:\Mainwarninglogs	Fairwarning	csv	Comma - [Fields containing comma are wrapped in double quotes]	

Figure 4

- Click the **Add** button.  
Direct Archiver Configuration pane is shown.

Direct Archiver Configuration

Type:

Logfile Extension:

Configuration Name:

Log File Folder:

Single Line     Multi Line

Field Separator:

Starting Line Offset:

Extract field names from header:

Figure 5

6. Select **Others** from **Type** dropdown.
7. Type **txt** as **Logfile Extension**.
8. Type an appropriate **Configuration Name**.
9. Click the **Browse** button and select path of EZproxy log folder created by above mentioned script.
10. Select **Single Line** dialog box.
11. Select **TAB FROM** field separator dropdown.
12. Select **Extract fields from header** checkbox.
13. Click the **Configure** button.

Direct archiver configuration pane is shown.

The screenshot shows the 'Direct Archiver Configuration' window. The 'Log file configuration' section is active. The 'Log Source' field is highlighted with a red box and contains the text 'EZ'. The 'Computer Name' field contains 'huey' and the 'Computer IP' field contains '192.168.1.94'. A 'GET IP' button is located to the right of the IP field. Below these fields, there are dropdown menus for 'System Type' (set to 'Win 7') and 'Log File Format' (set to 'Custom Log File Format'). There are also radio buttons for 'Entire Row as Description' and 'Formatted Description' (selected). At the bottom, there are 'ADD' and 'REMOVE' buttons for the 'Message Fields' section.

Figure 6

14. Type a fitting **Log Source** name.
15. Select desired **Computer Name**, **Computer IP** and **System Type**.
16. Scroll down and Click the **Save & Close** button.



Saved configuration is shown in DLA pane.

MANAGER CONFIGURATION

CONFIGURATION | syslog / VIRTUAL COLLECTION POINT | **DIRECT LOG ARCHIVER / NETFLOW RECEIVER** | AGENT SETTINGS

E-MAIL CONFIGURATION | STATUSTRACKER | COLLECTION MASTER PORTS | NEWS

Direct log file archiving from external sources | Purge files after  days | ASSOCIATED VIRTUAL COLLECTION POINT: 14505

LOG FILE FOLDER	CONFIGURATION NAME	LOG FILE EXTENSION	FIELD SEPARATOR	LOG TYPE
D:\MS Office 365\Non Empty	O365	csv	Comma - [Fields containing comma are wrapped in double quotes]	
D:\fairwarning\logs	Fairwarning	csv	Comma - [Fields containing comma are wrapped in double quotes]	
D:\EZProxy	EZ	txt	TAB	

ADD EDIT REMOVE

Figure 7

17. Click the **Save** button to consolidate changes.

## EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and Reports can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support EZproxy monitoring.

### Reports

1. **EZproxy - Allowed Traffic Details** – This report provides information related to web traffic allowed by EZproxy which includes device name, client address bytes transferred, request type, requested URI, requested URL, user agent type and user agent details fields.
2. **EZproxy - Denied Traffic Details** – This report provides information related to web traffic denied by EZproxy which includes device name, client address, error type and error details fields.
3. **EZproxy - User Logon Details** – This report provides information related to user logon/logoff events which includes user name, source address, logon status and logon details fields.
4. **EZproxy - Intrusion Details** – This report provides information related to intrusion attempts detected which includes user name, source address and attack type fields.

## Categories

1. **EZproxy - Audit Log Purged** - This category briefs an administrator about purging of EZproxy audit logs.
2. **EZproxy - System Startup/Shutdown** - This category briefs an administrator about EZproxy startup and shutdown.

## Knowledge Objects

1. **EZproxy - Allowed Traffic** - This KO assists in analysis of web traffic allowed through EZproxy.
2. **EZproxy - Denied Traffic** - This KO assists in analysis of web traffic denied through EZproxy.

## Import EZproxy Knowledge Pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**, and then click the **Import** tab.

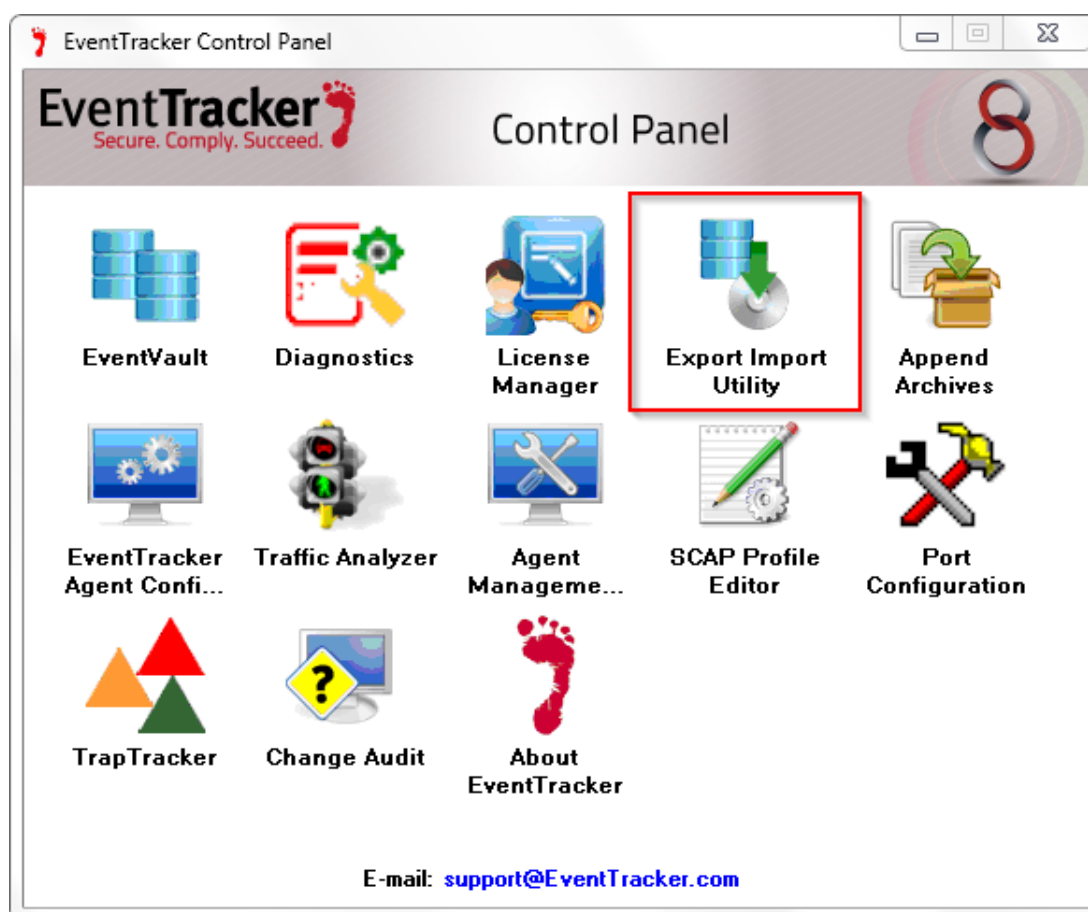



Figure 8

Import **Categories, Alerts, and Reports** as given below.

## Import Parsing Rules

1. Click **Token Value** option, and then click the browse  button.
2. Locate **All EZproxy group of tokens.istoken** file, and then click the **Open** button.

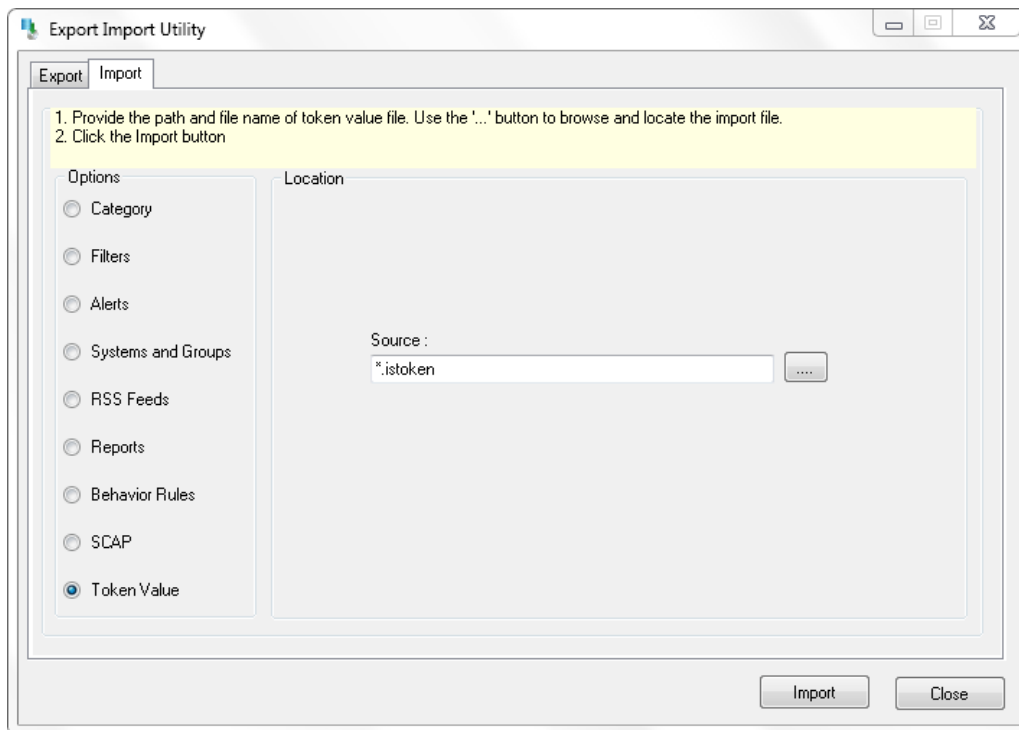


Figure 9

3. To import token value, click the **Import** button.  
EventTracker displays success message.

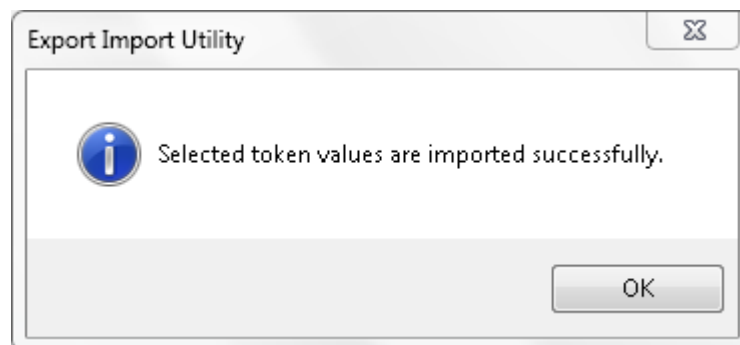

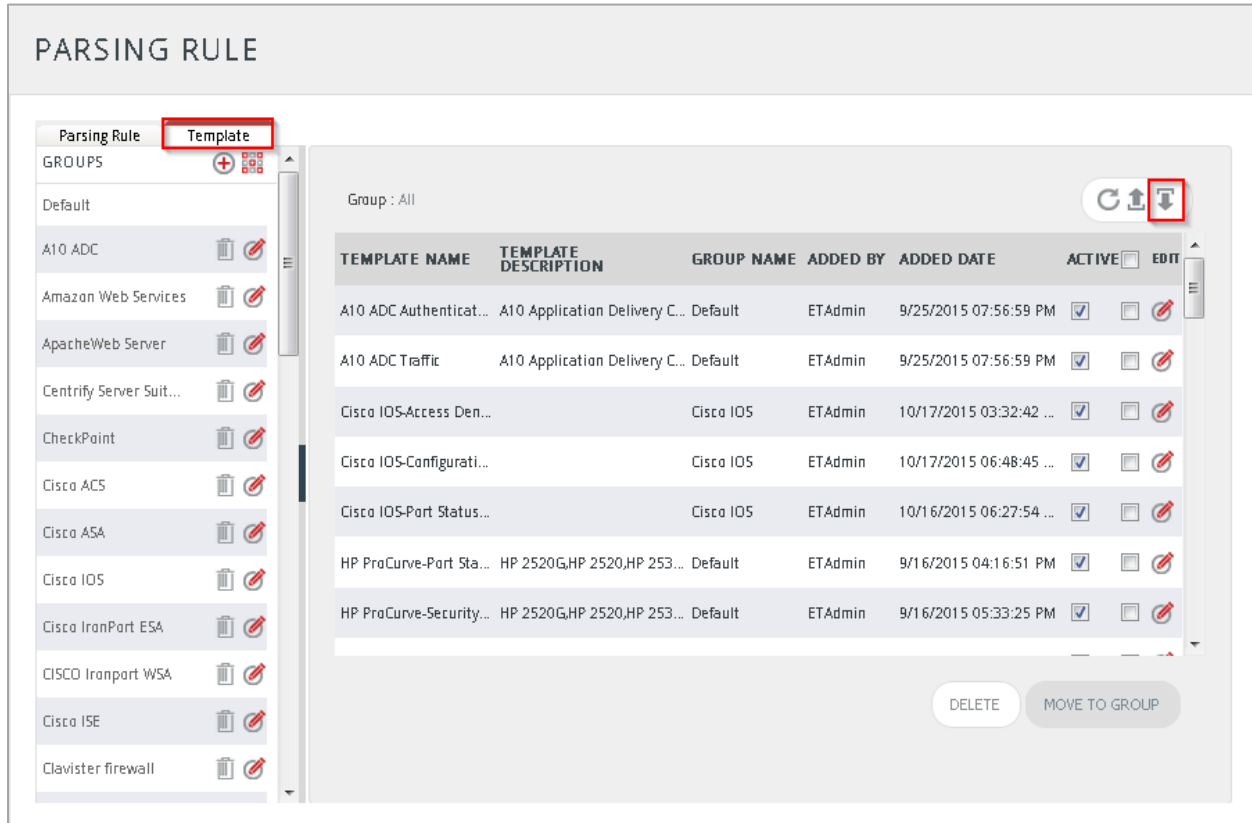


Figure 10

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

## Import Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on  'Import' option.

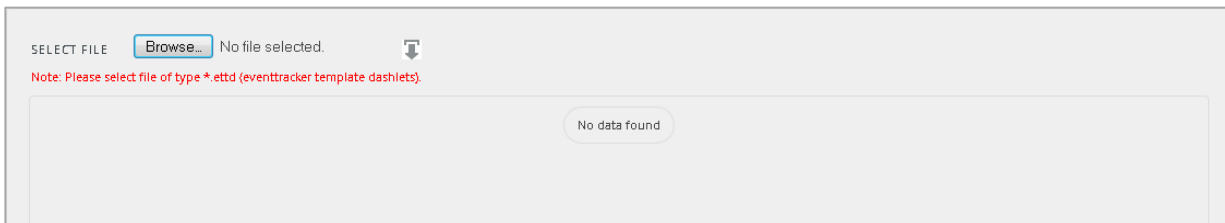


The screenshot shows the 'PARSING RULE' interface. On the left, the 'Template' tab is selected and highlighted with a red box. The main area displays a table of templates. At the top right of the table area, the 'Import' icon (a downward arrow) is highlighted with a red box. Below the table are 'DELETE' and 'MOVE TO GROUP' buttons.

TEMPLATE NAME	TEMPLATE DESCRIPTION	GROUP NAME	ADDED BY	ADDED DATE	ACTIVE	EDIT
A10 ADC Authenticat...	A10 Application Delivery C...	Default	ETAdmin	9/25/2015 07:56:59 PM	<input checked="" type="checkbox"/>	
A10 ADC Traffic	A10 Application Delivery C...	Default	ETAdmin	9/25/2015 07:56:59 PM	<input checked="" type="checkbox"/>	
Cisco IOS-Access Den...		Cisco IOS	ETAdmin	10/17/2015 03:32:42 ...	<input checked="" type="checkbox"/>	
Cisco IOS-Configurati...		Cisco IOS	ETAdmin	10/17/2015 06:48:45 ...	<input checked="" type="checkbox"/>	
Cisco IOS-Part Status...		Cisco IOS	ETAdmin	10/16/2015 06:27:54 ...	<input checked="" type="checkbox"/>	
HP ProCurve-Part Sta...	HP 2520G,HP 2520,HP 253...	Default	ETAdmin	9/16/2015 04:16:51 PM	<input checked="" type="checkbox"/>	
HP ProCurve-Security...	HP 2520G,HP 2520,HP 253...	Default	ETAdmin	9/16/2015 05:33:25 PM	<input checked="" type="checkbox"/>	

Figure 11

3. Click on **Browse** button.



The screenshot shows a file selection interface. At the top, it says 'SELECT FILE' followed by a 'Browse...' button and 'No file selected.' Below this, a red note reads: 'Note: Please select file of type \*.ettd (eventtracker template dashlets)'. In the center, there is a 'No data found' button.

Figure 12

4. Locate **EZproxy token template.ettd** file, and then click the **Open** button.

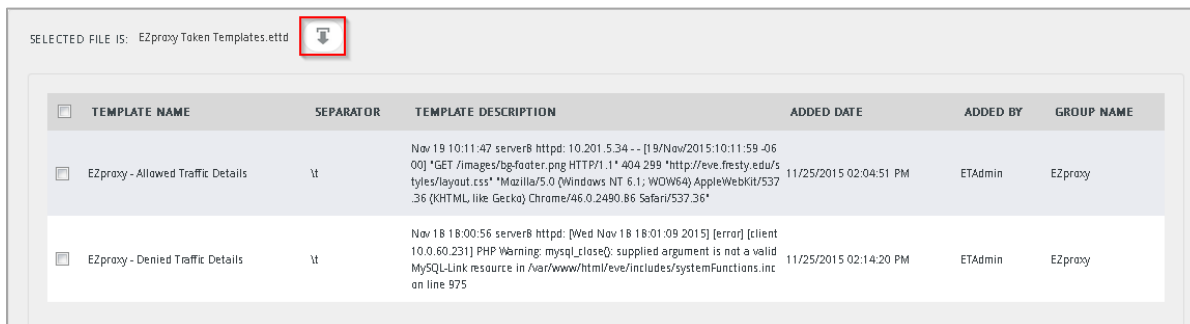


Figure 13

5. Now select the check box and then click on **Import** option  
EventTracker displays success message.

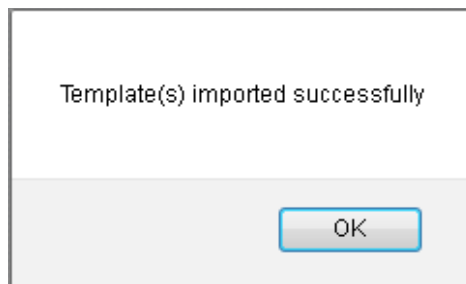



Figure 14

6. Click on **OK** button.

## Import Flex Reports

1. Click **Reports** option, and then click the '**browse**'  button.
2. Locate **All EZproxy group reports.issch** file, and then click the **Open** button.

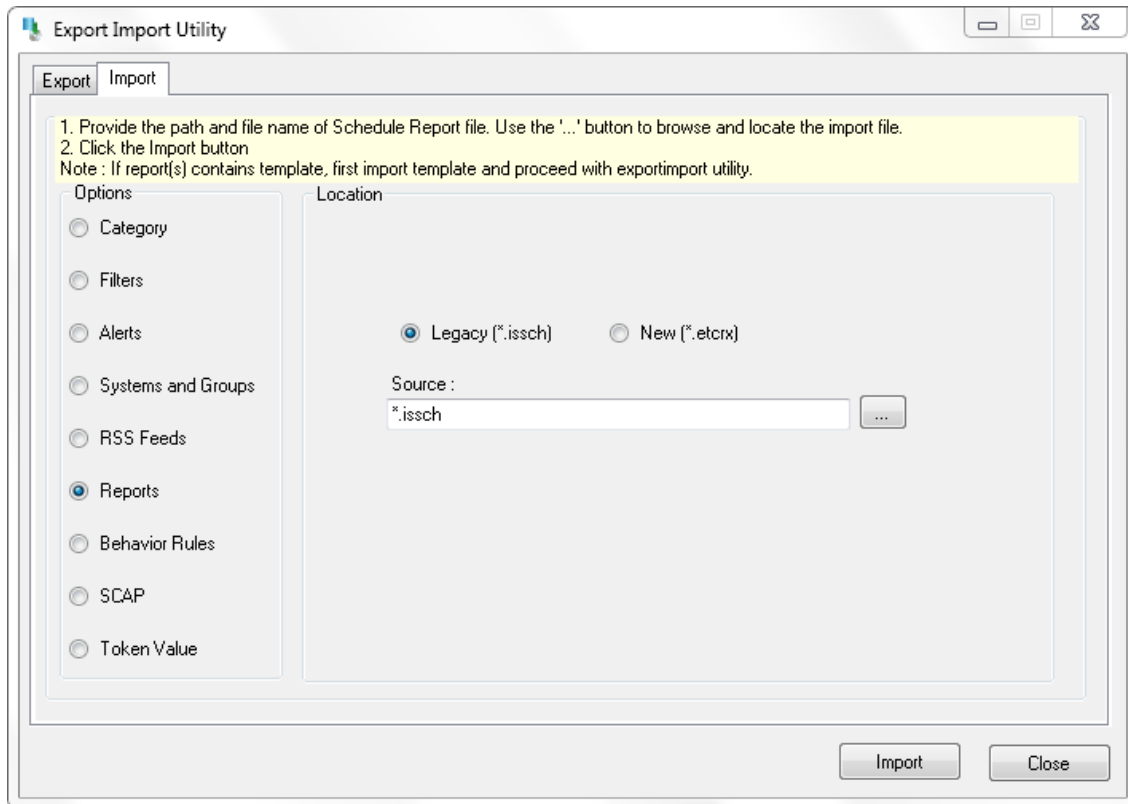


Figure 15

3. To import scheduled reports, click the **Import** button.
   
EventTracker displays success message.

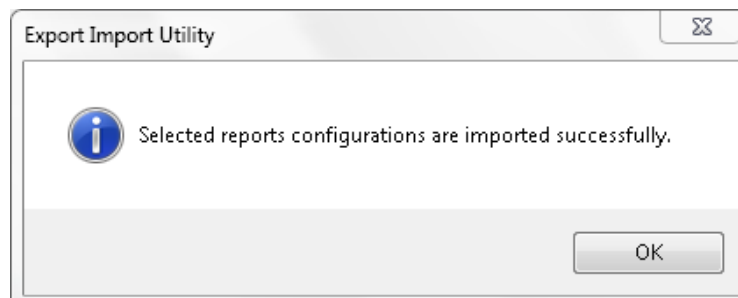


Figure 16

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

## Import Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on **Import** option.

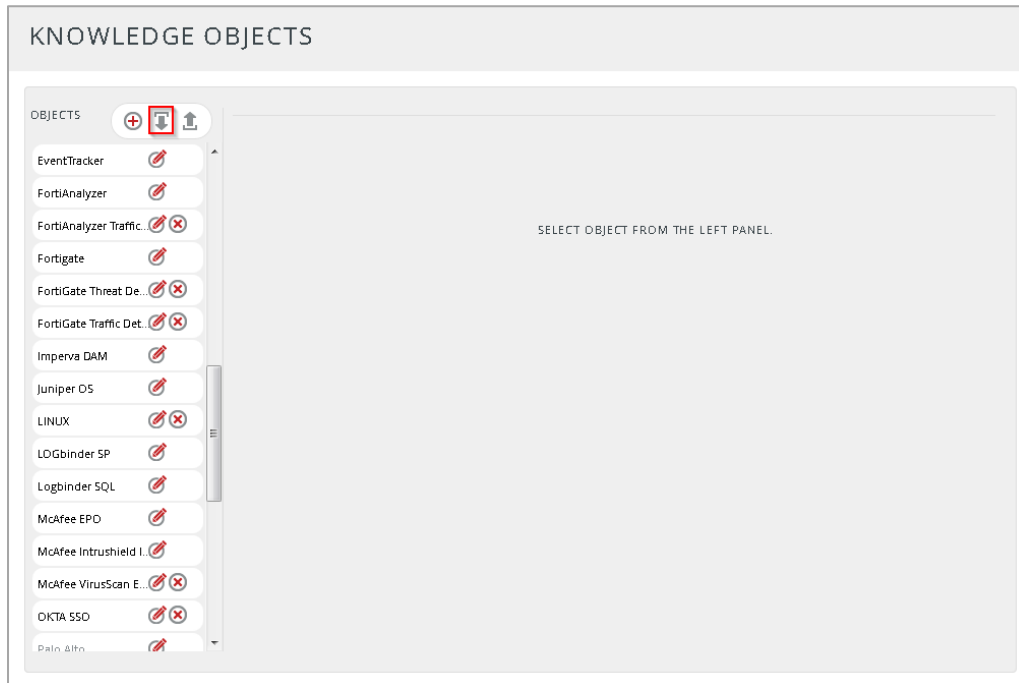


Figure 17

3. In **IMPORT** pane click on **Browse** button.

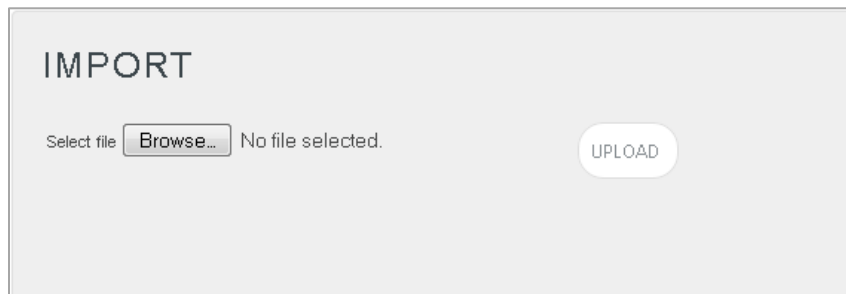


Figure 18

4. Locate **EZproxy KO.etko** file, and then click the **UPLOAD** button.

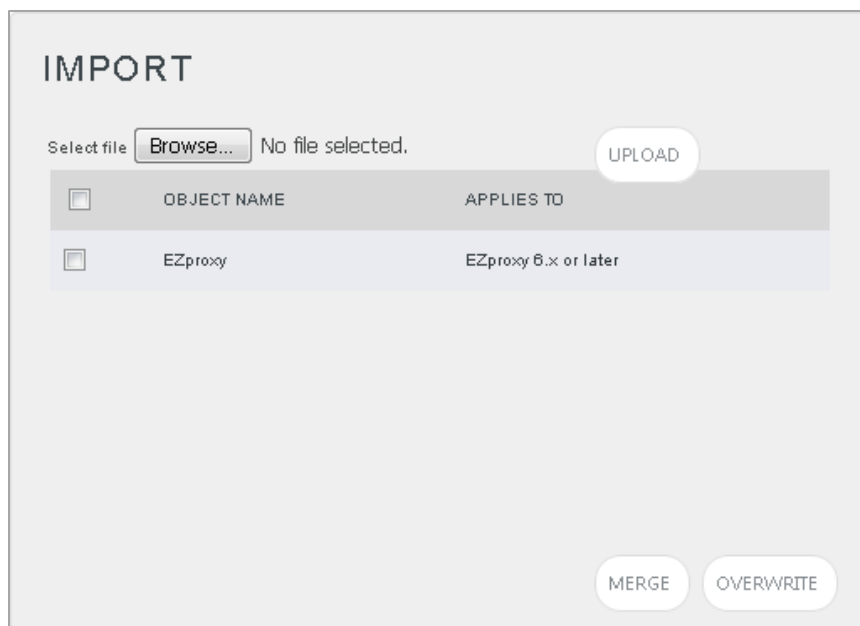


Figure 19

- Now select the check box and then click on '**MERGE**' option. EventTracker displays success message.

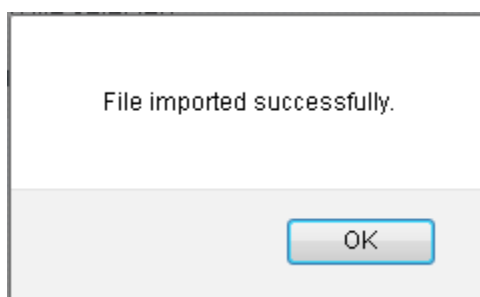


Figure 20

- Click on **OK** button.



# Verify EZproxy knowledge pack in EventTracker

## Verify Parsing Rules

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Parsing Rules**.
3. In **Token Value Group Tree** to view imported token values, scroll down and click **EZproxy group** folder.

Token values are displayed in the token value pane.

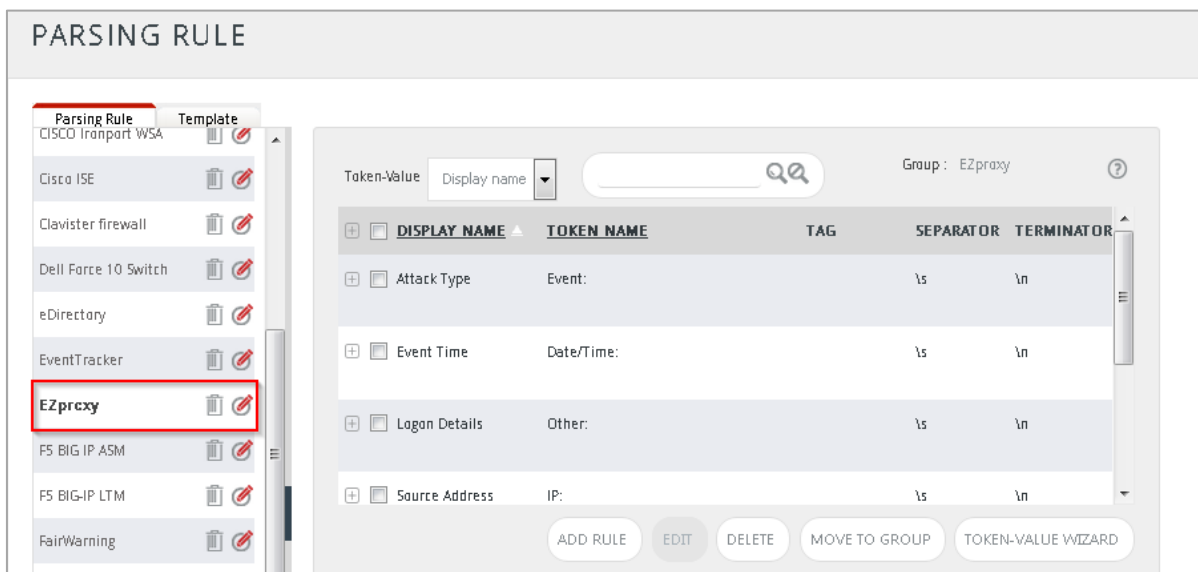


Figure 21

## Verify Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab.
3. In **Token Value Group Tree** to view imported token values, scroll down and click **EZproxy group** folder.

Imported token template is displayed in the template pane.

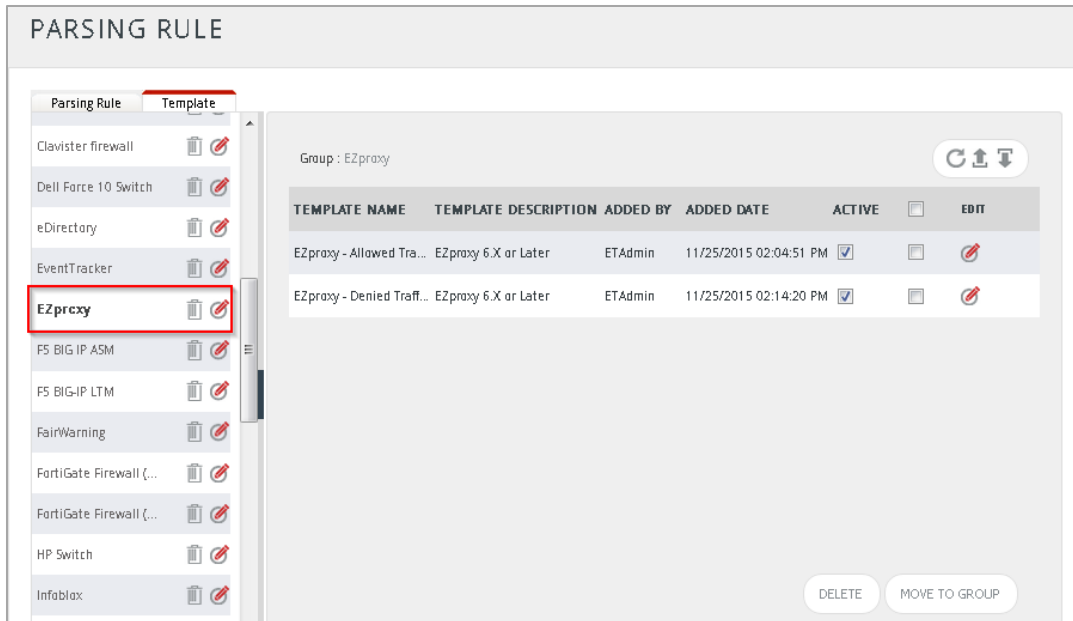


Figure 22

## Verify Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported flex reports, scroll down and click **EZproxy group** folder. Imported reports are displayed in the Reports Configuration pane.

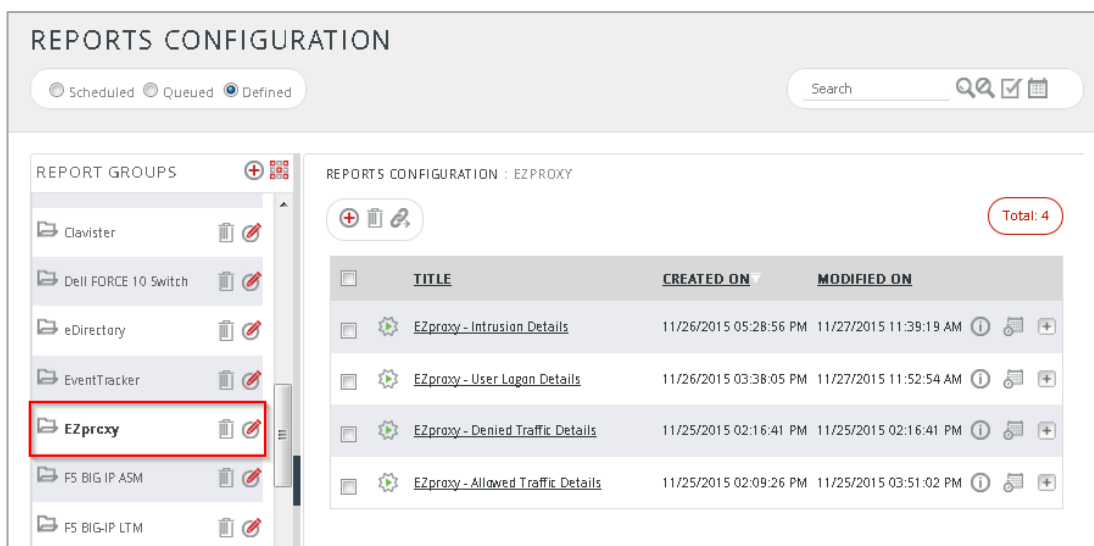


Figure 23

**NOTE:** Please specify appropriate **systems** in **report wizard** for better performance.



# Create Dashboards in EventTracker

## Schedule Reports

1. Open **EventTracker** in browser and logon.

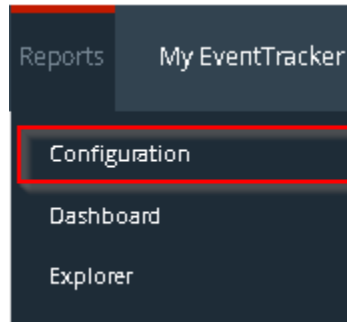


Figure 25

2. Navigate to **Reports>Configuration**.

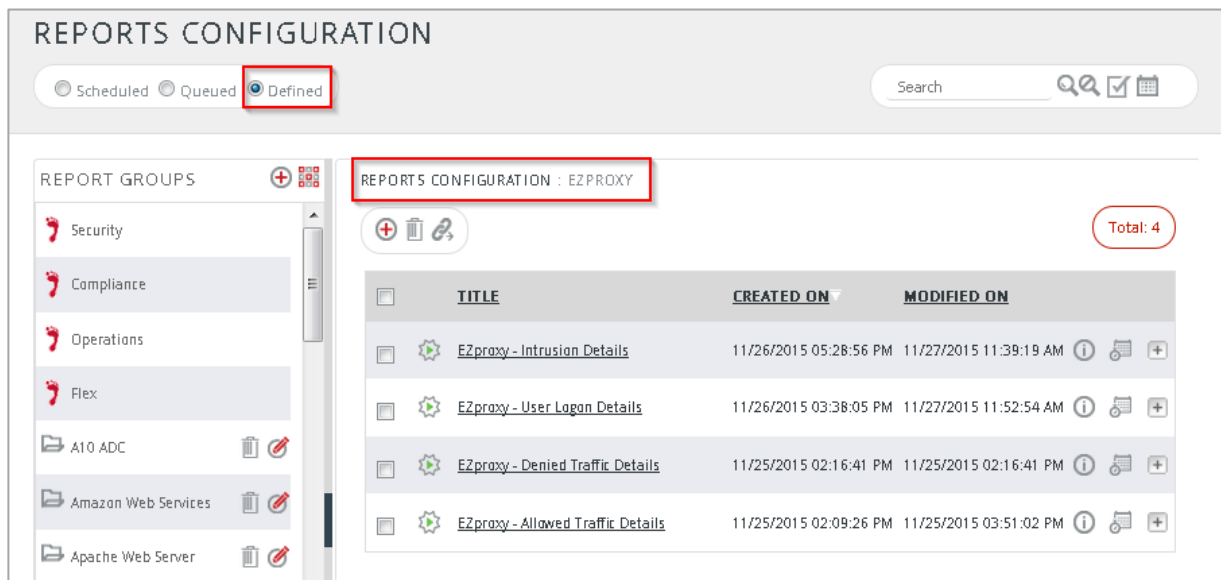



Figure 26

3. Select **EZproxy** in report groups. Check **defined** dialog box.
4. Click on 'schedule'  to plan a report for later execution.

**REPORT WIZARD** CANCEL < BACK NEXT >

TITLE: EZPROXY - ALLOWED TRAFFIC DETAILS  
LOGS

Review cost details and configure the publishing options. Step 8 of 10

**DISK COST ANALYSIS**

Estimated time for completion: 00:00:40(HH:MM:SS)  
Number of cab(s) to be processed: 5  
Available disk space: 195 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:  [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS:  ▼

Show in:  ▼

Persist data in Eventvault Explorer

Figure 27

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault explorer** box.

**REPORT WIZARD** CANCEL < BACK NEXT >

TITLE: EZPROXY - ALLOWED TRAFFIC DETAILS  
DATA PERSIST DETAIL

Select columns to persist Step 9 of 10

**RETENTION SETTING**

Retention period:  days ⓘ

Persist in database only *[Reports will not be published and will only be stored in the respective database]*

**SELECT COLUMNS TO PERSIST**

COLUMN NAME	PERSIST
Event Time	<input checked="" type="checkbox"/>
Device Name	<input checked="" type="checkbox"/>
Client Address	<input checked="" type="checkbox"/>
Bytes Transferred	<input checked="" type="checkbox"/>
Request Type	<input checked="" type="checkbox"/>

Figure 28

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
7. Proceed to next step and click **Schedule** button.
8. Wait for scheduled time or generate report manually.

## Create Dashlets

1. **EventTracker 8** is required to configure flex dashboard.
2. Open **EventTracker** in browser and logon.

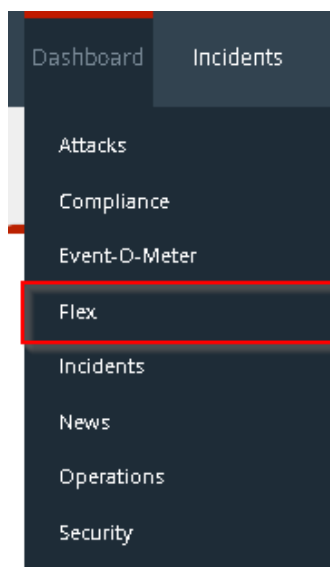


Figure 29

3. Navigate to **Dashboard>Flex**.

Flex Dashboard pane is shown.

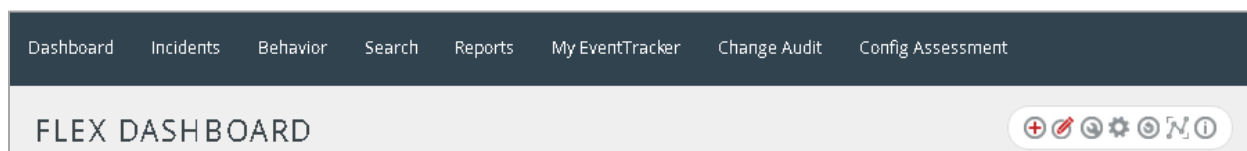




Figure 30

4. Click  to add a new dashboard.

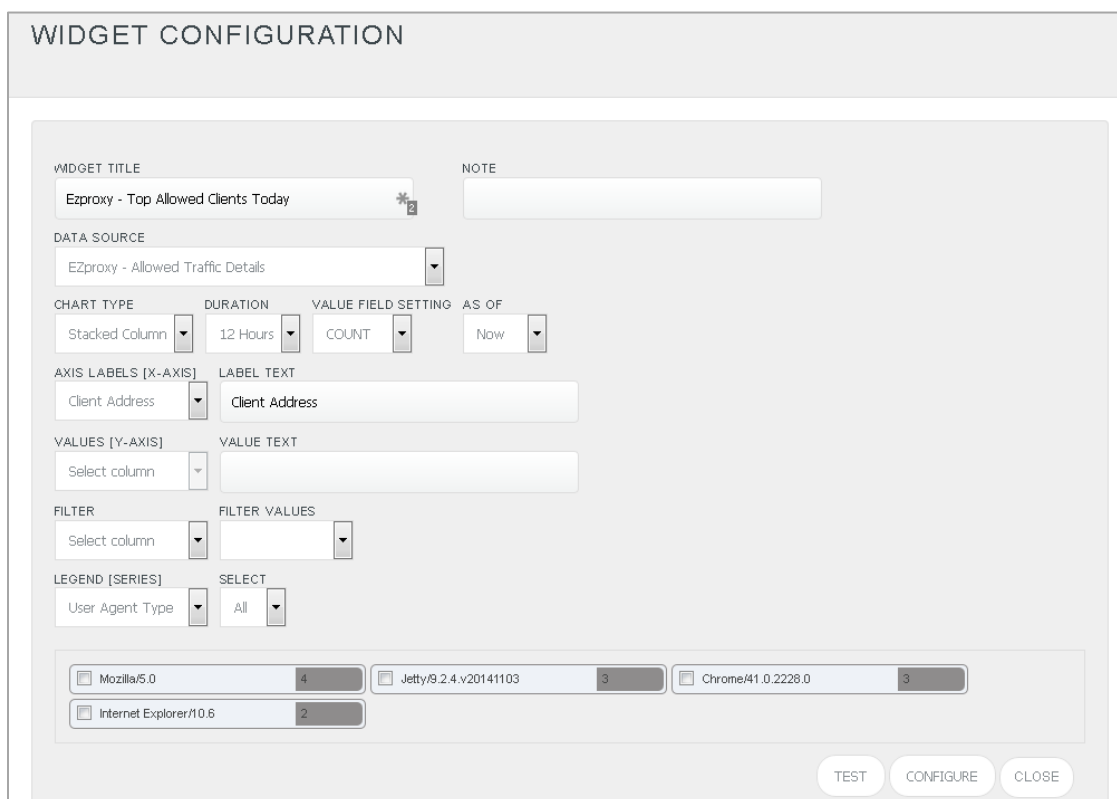
Flex Dashboard configuration pane is shown.

 The configuration pane is titled 'FLEX DASHBOARD'. It contains two input fields: 'Title' with the value 'EZproxy' and 'Description' with the value 'EZproxy 6.X or Later'. At the bottom right, there are three buttons: 'SAVE', 'DELETE', and 'CANCEL'.


Figure 31

5. Fill fitting title and description and click **Save** button.
6. Click  to configure a new flex dashlet.

Widget configuration pane is shown.



WIDGET CONFIGURATION

WIDGET TITLE: Ezproxy - Top Allowed Clients Today 

NOTE: [Empty text input]

DATA SOURCE: EZproxy - Allowed Traffic Details

CHART TYPE: Stacked Column

DURATION: 12 Hours

VALUE FIELD SETTING: COUNT

AS OF: Now

AXIS LABELS [X-AXIS]: Client Address

LABEL TEXT: Client Address

VALUES [Y-AXIS]: Select column

VALUE TEXT: [Empty text input]

FILTER: Select column

FILTER VALUES: [Empty dropdown]

LEGEND [SERIES]: User Agent Type

SELECT: All

<input type="checkbox"/> Mozilla/5.0	4	<input type="checkbox"/> Jetty/9.2.4.v20141103	3	<input type="checkbox"/> Chrome/41.0.2228.0	3
<input type="checkbox"/> Internet Explorer/10.6	2				

TEST CONFIGURE CLOSE

Figure 32

7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.



Evaluated chart is shown.

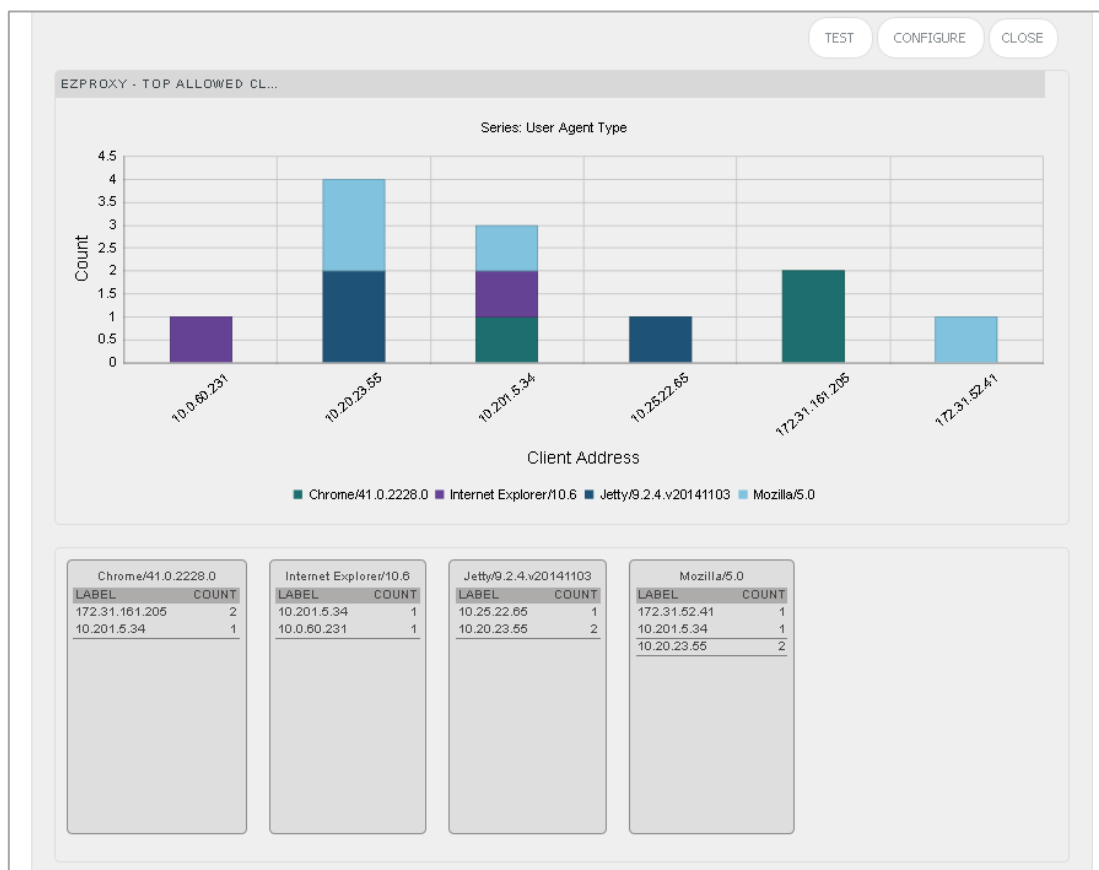


Figure 33

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

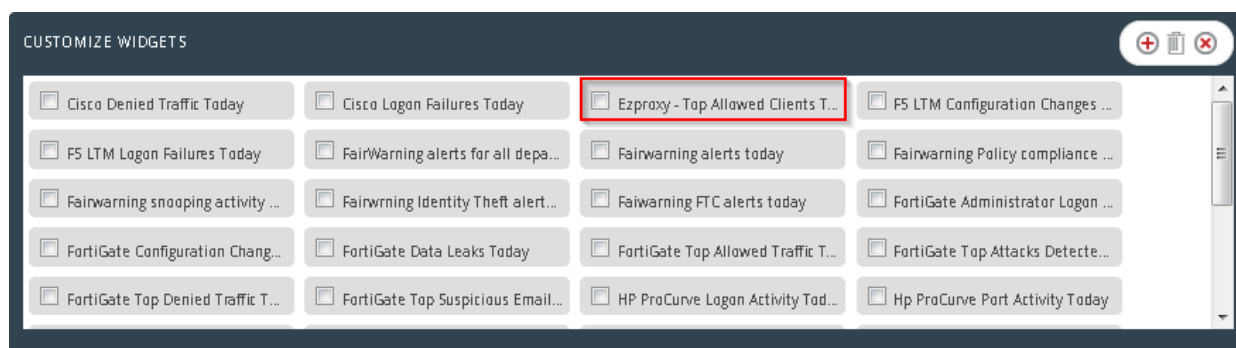




Figure 34

17. Click 'customize'  to locate and choose created dashlet.

18. Click  to add dashlet to earlier created dashboard.

# Sample Dashboards

- EZproxy User Logons Events Today

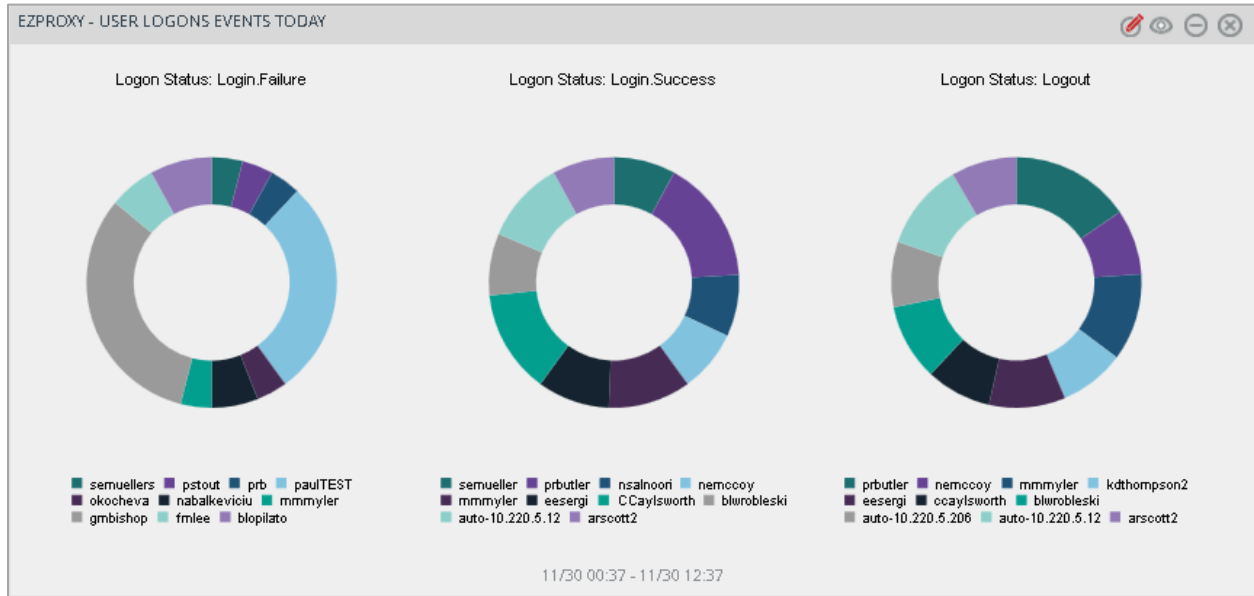


Figure 35

- EZproxy Top Intrusion Attempts Today

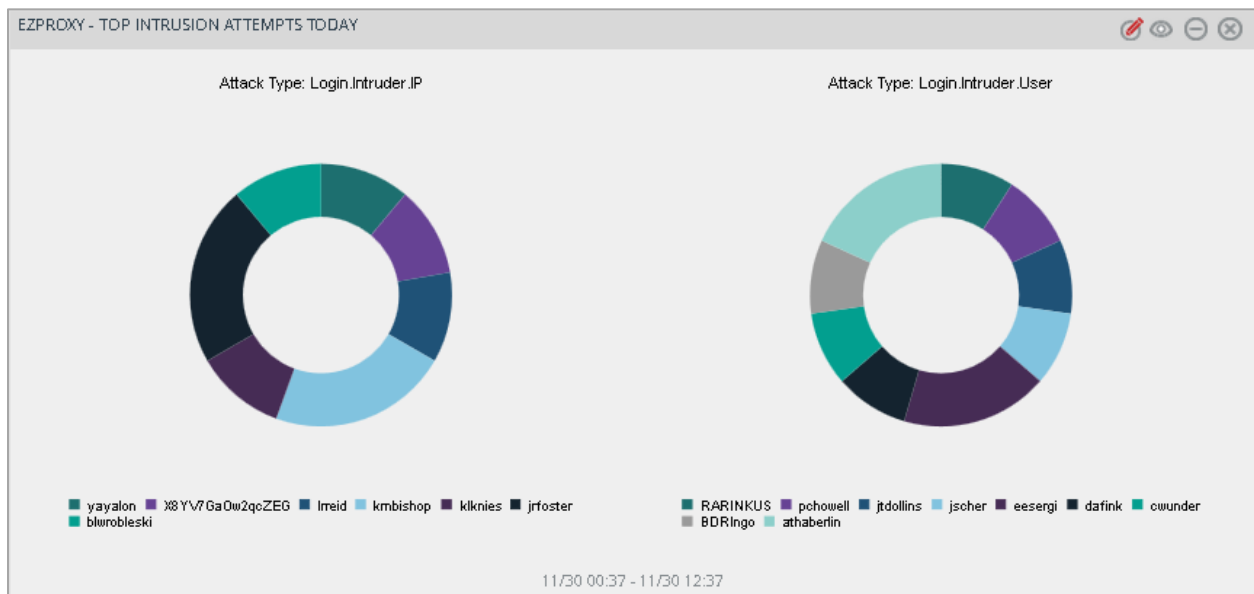


Figure 36

- **EZproxy Top Denied Clients Today**

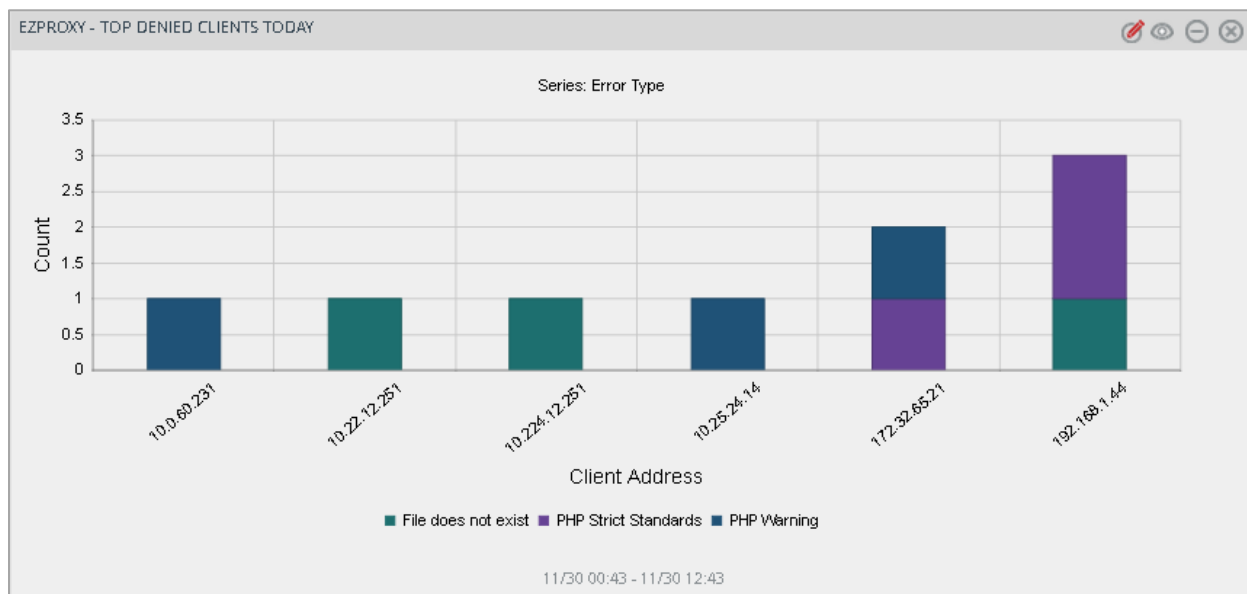


Figure 37

- **EZproxy Top Allowed Clients Today**

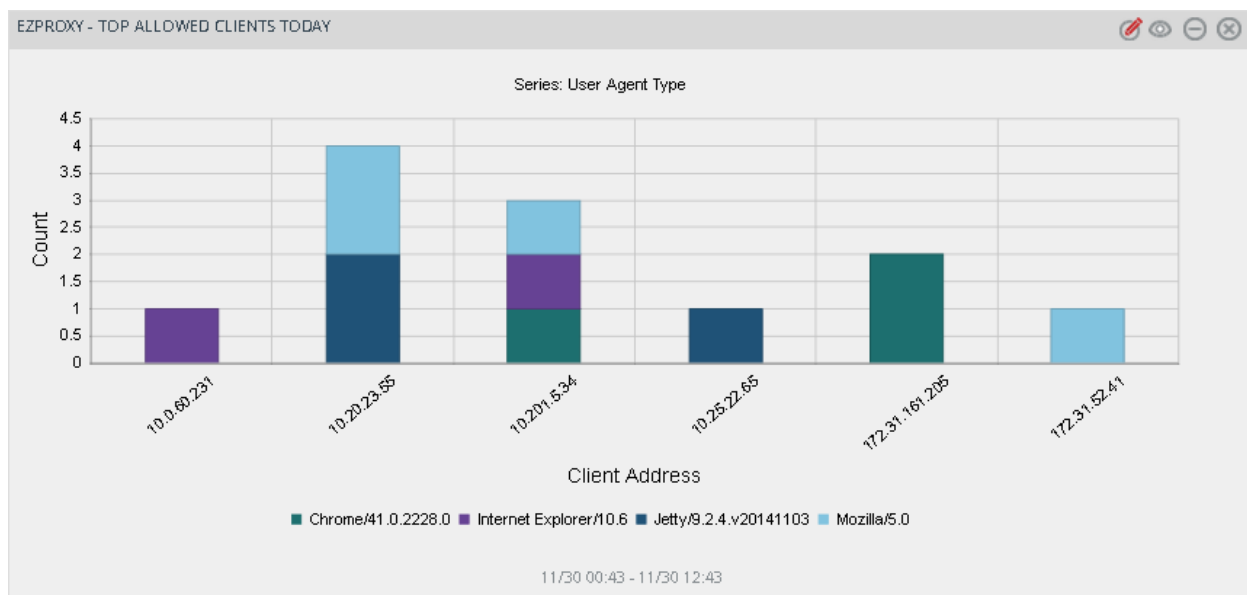


Figure 38

## Sample Reports

- EZproxy-User Logon Details

EZproxy - Allowed Traffic Details									
Event Time	Device Name	Client Address	Bytes Transferred	Request Type	Requested URI	Requested URL	User Agent Type	User Agent Details	Status Code
18/Nov/2015:18:07:50	server8	172.31.161.205	303	GET	/	http://library.triky.edu/	Mozilla/5.0	(Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/600.5.17	302
19/Nov/2015:18:11:59	server8	10.201.5.34	299	GET	/images/bg-footer.png	http://eve.triky.edu/styles/layout.css	Mozilla/5.0	(Windows NT 6.1; WOW64) AppleWebKit/537.36	404
18/Nov/2015:18:08:25	server8	172.31.161.205	303	HEAD	/	-	Mozilla/5.0	(Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/600.5.17	302
19/Nov/2015:18:12:47	server8	10.201.5.34	299	GET	/images/bg-footer.png	http://eve.triky.edu/styles/layout.css	Mozilla/5.0	(Windows NT 6.1; WOW64) AppleWebKit/537.36	404
18/Nov/2015:18:17:50	server8	172.31.161.205	303	GET	/	http://library.triky.edu/	Mozilla/5.0	(Macintosh; Intel Mac OS X 10_10_3) AppleWebKit/600.5.17	302

Figure 39

- EZproxy-User Logon Details

EZproxy - Denied Traffic Details				
Event Time	Device Name	Client Address	Error Type	Error Details
Wed Nov 18 15:43:11 2015	server8	10.224.12.251	File does not exist	/var/www/html/eve/images/bg-footer.png, referer: http://eve.samford.edu/
Wed Nov 18 17:21:16 2015	server8	5.9.83.211	PHP Strict Standards	mktime() [ <a href="#">function.mktime()</a> ]: It is not safe to rely on the system's timezone settings. Please use the date.timezone setting, the TZ environment variable or the date_default_timezone_set() function. In case you used any of those methods and you are still getting this warning, you most likely misspelled the timezone identifier. We selected "America/Chicago" for "CST-6.0/no DST" instead in /var/www/html/eve/includes/systemFunctions.inc on line 628
Wed Nov 18 18:01:09 2015	server8	10.0.60.231	PHP Warning	mysql_close(): supplied argument is not a valid MySQL-Link resource in /var/www/html/eve/includes/systemFunctions.inc on line 975

Figure 40

- EZproxy-User Logon Details

EZproxy - User Logon Details					
Event Time	Computer	Logon Status	User Name	Source Address	Logon Details
2015-26-11 00:08:25	HUEY-DLA	Logout	lrreid		Expired
2015-26-11 00:36:55	HUEY-DLA	Logout	klknies		Expired
2015-26-11 00:22:55	HUEY-DLA	Logout	jzhu3		Expired
2015-26-11 00:21:55	HUEY-DLA	Logout	amwiggins		Expired
2015-26-11 00:20:55	HUEY-DLA	Login.Failure	mepugh	14.21.25.33	
2015-26-11 00:18:55	HUEY-DLA	Logout	Ancruz		Expired
2015-26-11 00:18:00	HUEY-DLA	Login.Success	mmcgee	98.226.171.49	
2015-26-11 00:14:25	HUEY-DLA	Logout	kawilson2		Expired
2015-26-11 00:13:27	HUEY-DLA	Login.Success	srayat	99.71.120.85	
2015-26-11 00:12:12	HUEY-DLA	Login.Success	gmbishop	162.236.189.108	
2015-26-11 00:11:25	HUEY-DLA	Logout	slwetly		Expired
2015-26-11 00:10:55	HUEY-DLA	Logout	jpark2		Expired
2015-26-11 00:10:55	HUEY-DLA	Logout	mkleavell		Expired
2015-26-11 00:09:30	HUEY-DLA	Login.Success	emtedtman	50.178.206.178	
2015-26-11 00:39:25	HUEY-DLA	Logout	klchappelow		Expired
2015-26-11 00:04:25	HUEY-DLA	Logout	gcdewitt		Expired
2015-26-11 00:00:25	HUEY-DLA	Logout	mlheller		Expired
2015-26-11 00:00:25	HUEY-DLA	Logout	sdegler		Expired
2015-26-11 00:00:53	HUEY-DLA	Login.Success	jblynch	98.223.214.70	

Figure 41

- EZproxy-User Logon Details

EZproxy - Intrusion Details				
Event Time	Computer	Attack Type	User Name	Source Address
2015-26-11 15:38:55	HUEY-DLA	Login.Intruder.IP	lrreid	108.210.118.82
2015-26-11 16:14:36	HUEY-DLA	Login.Intruder.IP		108.210.118.82
2015-26-11 17:27:56	HUEY-DLA	Login.Intruder.IP	jzhu3	108.210.118.82
2015-26-11 19:35:14	HUEY-DLA	Login.Intruder.User	amwiggins	
2015-26-11 15:38:57	HUEY-DLA	Login.Intruder.IP	mepugh	108.210.118.82
2015-26-11 19:14:38	HUEY-DLA	Login.Intruder.User	Ancruz	
2015-26-11 15:38:58	HUEY-DLA	Login.Intruder.IP	mmcgee	108.210.118.82
2015-26-11 19:14:39	HUEY-DLA	Login.Intruder.IP	kawilson2	108.204.148.82
2015-26-11 15:38:59	HUEY-DLA	Login.Intruder.IP		108.210.118.82
2015-26-11 19:14:40	HUEY-DLA	Login.Intruder.User	gmbishop	
2015-26-11 15:38:60	HUEY-DLA	Login.Intruder.IP	slwetly	108.210.118.82
2015-26-11 19:14:41	HUEY-DLA	Login.Intruder.User	jpark2	
2015-26-11 15:38:61	HUEY-DLA	Login.Intruder.IP		108.210.118.82
2015-26-11 19:14:42	HUEY-DLA	Login.Intruder.User	emtedtman	
2015-26-11 15:38:62	HUEY-DLA	Login.Intruder.User	klchappelow	
2015-26-11 19:14:43	HUEY-DLA	Login.Intruder.User	gcdewitt	
2015-26-11 15:38:63	HUEY-DLA	Login.Intruder.IP	mlheller	108.210.118.82
2015-26-11 19:14:44	HUEY-DLA	Login.Intruder.User	sdegler	
2015-26-11 15:38:64	HUEY-DLA	Login.Intruder.IP	jblynch	108.210.118.82

Figure 42