EventTracker

Actionable Security Intelligence

Integrate Active Directory Audit

EventTracker v8.x and above

Publication Date: April 7, 2017

Abstract

This guide helps you in configuring **Active Directory** with EventTracker to receive **Active Directory** events. In this document you will find the detailed procedures required for monitoring **Active Directory.**

Audience

Administrators who are assigned the task to monitor and manage Active Directory events using EventTracker.

Table of Contents

Overview

This guide addresses the Windows default audit policy settings, baseline recommended audit policy settings, and the more aggressive recommendations from Microsoft, for workstation and server products.

The SCM baseline recommendations shown here, along with the settings recommend to help detect compromise, are intended only to be a starting baseline guide to administrators. Each organization must make its own decisions regarding the threats they face, their acceptable risk tolerances, and what audit policy categories or subcategories they should enable. The Administrators without a thoughtful audit policy in place are encouraged to start with the settings recommended here, and then to modify and test, prior to implementing in their production environment.

Prerequisites

- EventTracker v8.x should be installed.
- Active Directory should be installed and configured.
- Recommended Audit Policies by the OS
  - Windows Server 2012
  - Windows Server 2012 R2
  - Windows Server 2008
  - Windows 8
  - Windows 7

Enabling of Active Directory Audit events

1. Open the **Run** command window, and run the command **gpedit.msc**

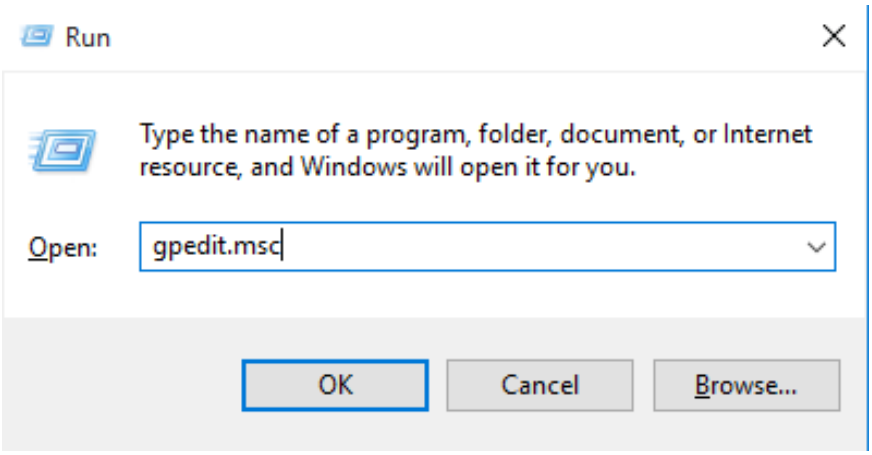

Figure 1

2. Local group policy editor window will now appear.

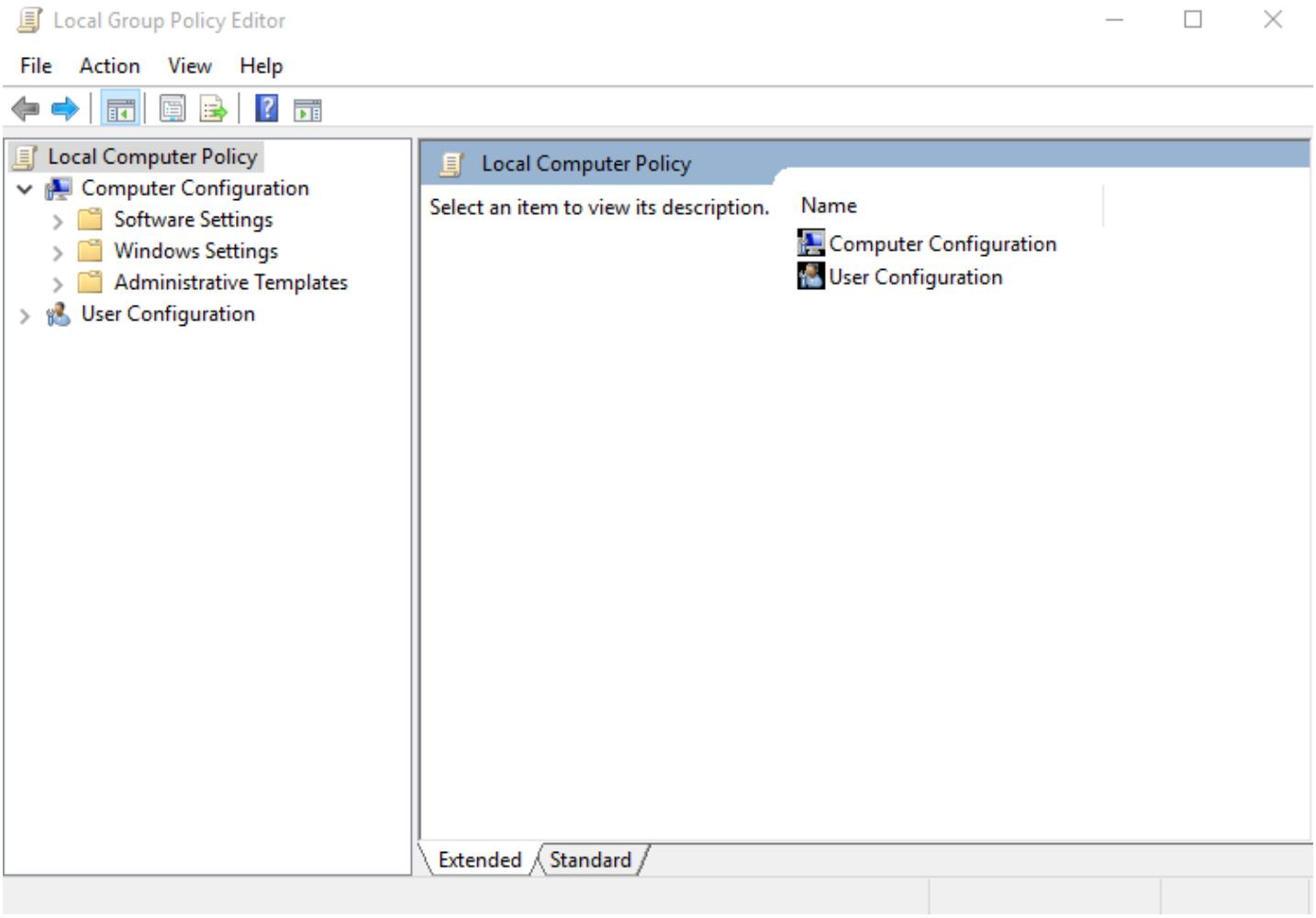

Figure 2

3. Click on **Windows Settings** dropdown under Computer Configuration and choose **Security Settings** as shown in the below image.

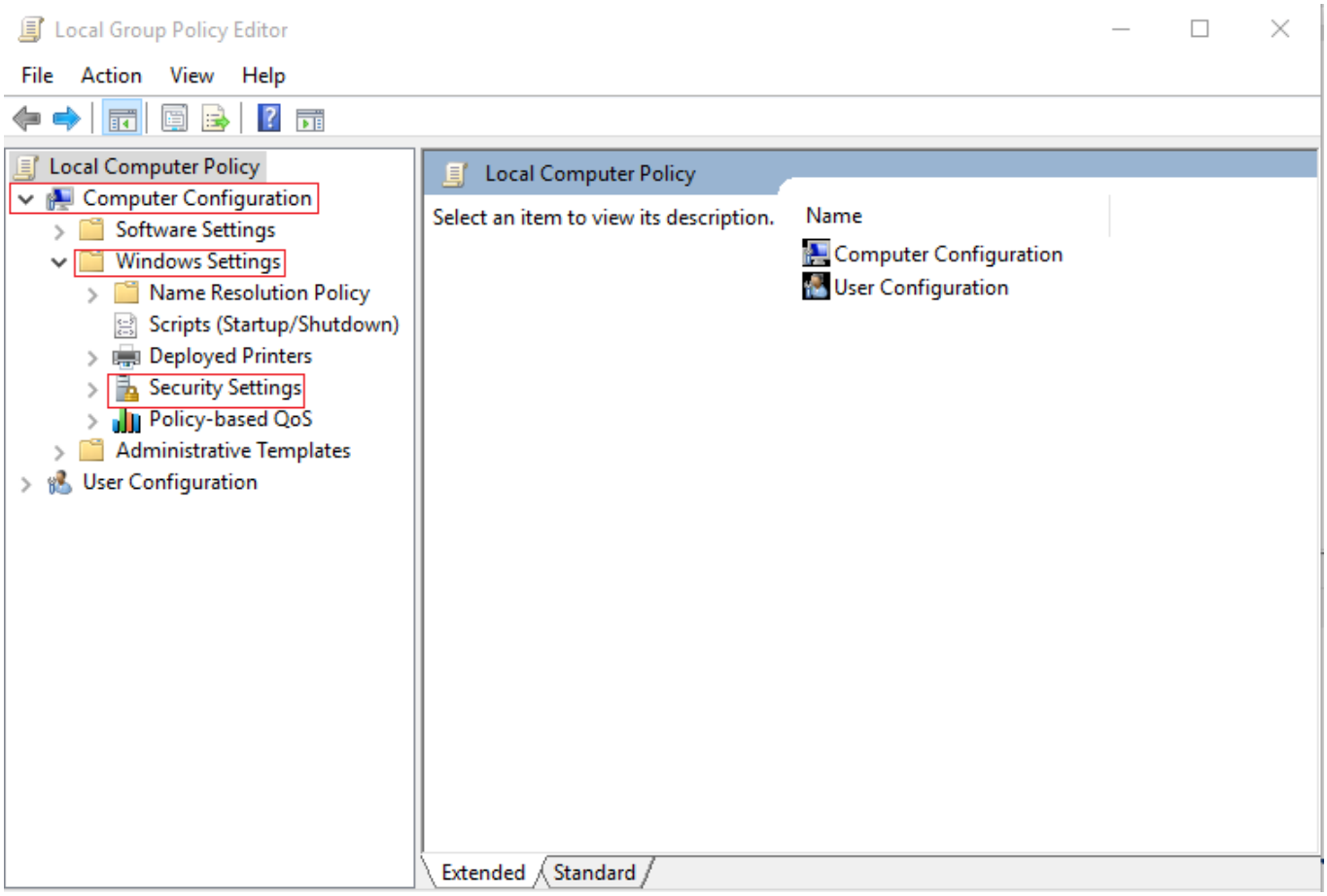

Figure 3

4. Click on **Security settings** dropdown, and click on **System Audit Policies-Local Group Policy Object.**

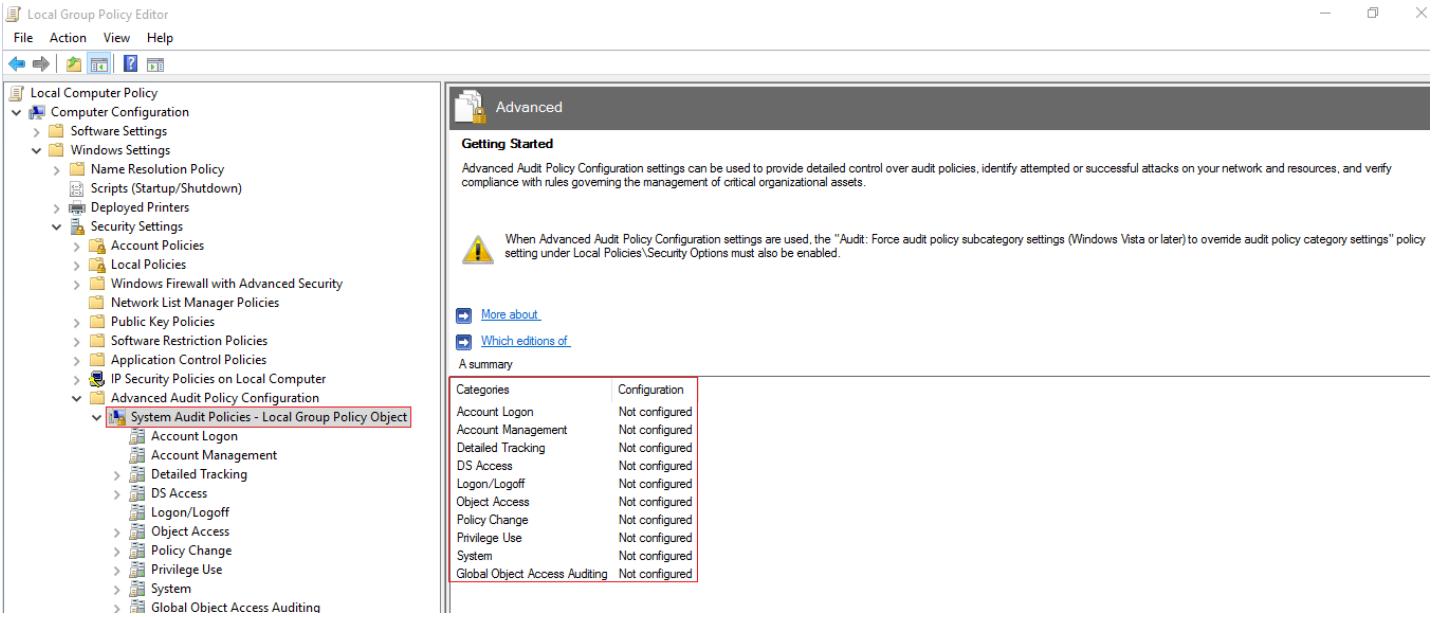

Figure 4

5. Double click on the policies that need to be enabled for auditing.
6. Auditing can be enabled for both Success/Failure events.
7. For e.g. if an **Account Logon** auditing for **Kerberos Authentication Service** needs to be enabled for Success/Failure events, highlight the **Account Logon** option and double click on **Kerberos Authentication Service** as shown in the below image.

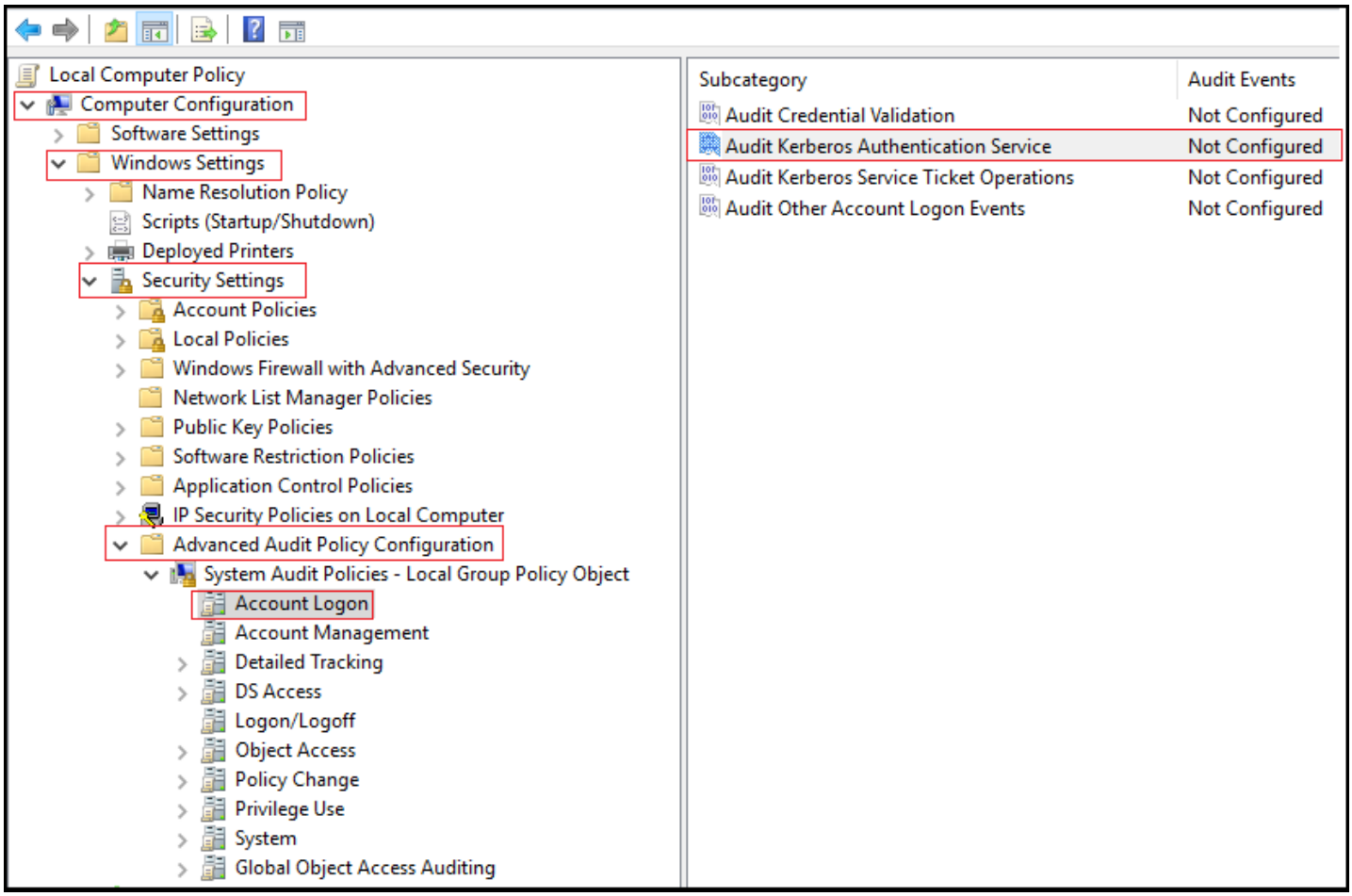

Figure 5

8. Once double clicked, another window will pop up. Click the checkbox "**Configure the following audit events"** and also the checkbox **Success** and **Failure** options as shown in the below image.

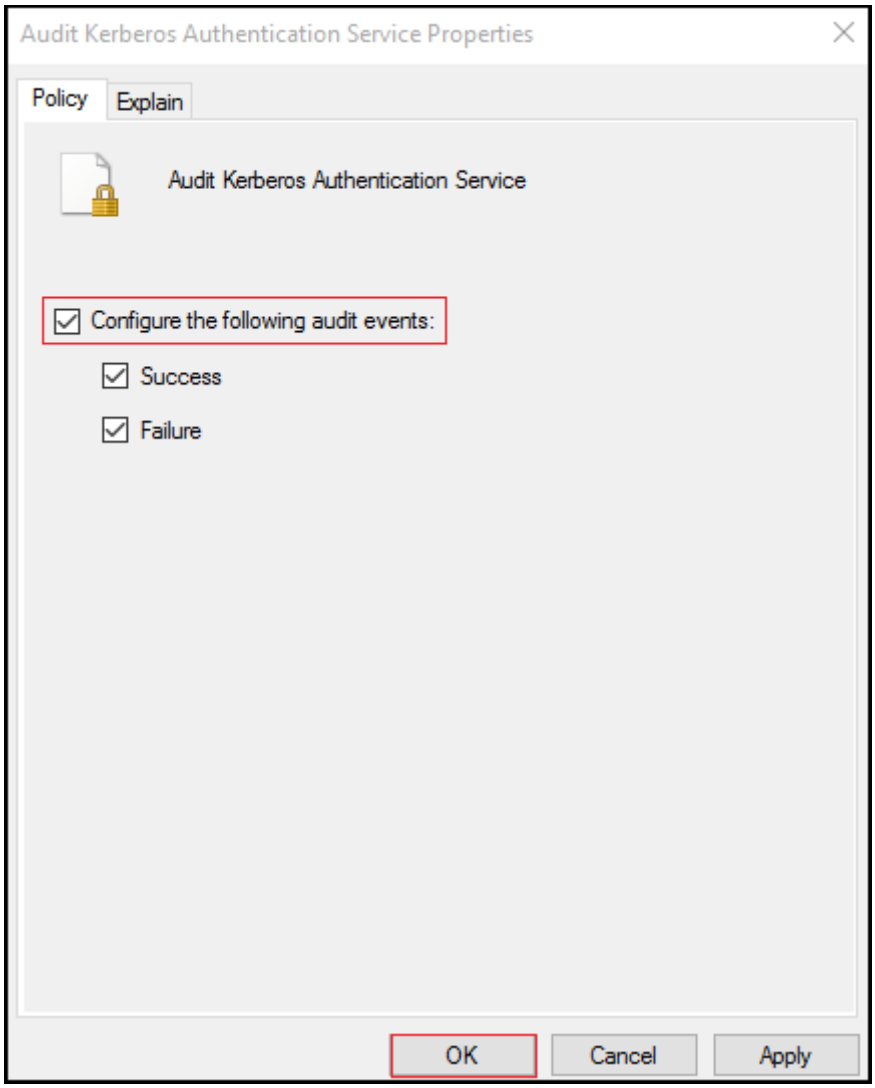

Figure 6

9. Click on **Apply** and then **OK.**
10. Now the auditing is enabled for **Kerberos Authentication Services.**
11. In the below **Flex Report** section, detailed **Category** and **Sub category** fields are provided which needs to be enabled for auditing for that specific report.
12. Enabling of auditing can be done for both the Local Computer and User Configuration in the same way as steps given above.

Configure Active Directory to send events to EventTracker

Deploy EventTracker Agent on Active Directory machine. Once the events are triggered, logs will be sent to EventTracker automatically.

Monitoring Events of Active Directory

Monitoring AD events, provides detailed information about what is happening on your Domain. Using EventTracker Enterprise, Active Directory events can be monitored which are as follows:

- **Computers**
- **Group**
- **Group Policy**
- **Local Group**
- **Objects**
- **Organizational Unit**
- **Share Folders**

EventTracker Knowledge Pack

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

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

Flex Reports

Below given are the list of reports along with the table that gives the category of Audit events which needs to be enabled.

1. **Active Directory-Account logon events:** This report provides details about all the successful logon, successful log off, special privileges logon and Logon failures done in Windows Active Directory.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
Category	Sub Category	Event ID	Audit Action
Logon/Logoff	Audit Account Lockout	4740- A User account was locked out	Enable Success/Failure
	An Account was logged off	4634- An account was logged off	
	User Initiated Log off	4647- User initiated logoff	
	User Logoff	538- User logoff	
	Special Logon	4672-Special privileges assigned to new logon	

Report Sample:

LogTime	Computer	Action	Source Security ID	Source Account Name	Source Account Domain	Target security ID	Target account name	Target account domain
03/21/2017 06:55:21 PM	PNPL-6-KP	An attempt was made to change an account's password.	WIN-R9H529RIO4Y\Administrator	Administrator	WIN-R9H529RIO4Y	WIN-R9H529RIO4Y\Administrator	Administrator	WIN-R9H529RIO4Y
03/21/2017 06:55:21 PM	PNPL-6-KP	An attempt to add SID History to an account failed.		John	Contoso	Contoso\Mike	Mike	Contoso
03/21/2017 06:55:21 PM	PNPL-6-KP	The ACL was set on accounts which are members of administrators groups.	ANONYMOUS LOGON	ANONYMOUS LOGON	NT AUTHORITY	ACME\Domain Admins	Domain Admins	DC=acme,DC=local

Figure 7

2. **Active Directory-Account management activities:** This report provides all the details about an account if it is created, deleted, changed, enabled or disabled in Windows Active Directory.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
Account Management	Audit Computer account management	4741- A computer account was created 4742- A computer account was changed 4743- A computer account was deleted	Enable Success/Failure
	Audit user account management	4720- A user account was created 4722- A user account was enabled 4725- A user account was disabled 4726- A user account was deleted 4738- A user account was changed 4740- A user account was locked out 4767- A user account was unlocked 4780- The ACL was set on accounts which are members of administrator's groups. 4794- An attempt was made to set the Directory Services Restore Mode. 5376- Credential Manager credentials were backed up 5377- Credential Manager credentials were restored from a backup	

Report Sample:

LogTime	Computer	Action	Source Account Name	Source Account Domain	Source Security ID	Target account name	Target account domain	Target security ID
03/30/2017 01:23:43 PM	PNPL-6-KP	A computer account was created.	Administrator	ACME	ACME\Administrator	WS2321$	ACME	S-1-5-21-3108364787-189202583-342365621-
03/30/2017 01:23:43 PM	PNPL-6-KP	A computer account was deleted.	Administrator	ACME	ACME\Administrator	WS2321$	ACME	S-1-5-21-3108364787-189202583-
03/30/2017 01:23:44 PM	PNPL-6-KP	A user account was enabled.	administrator	ACME-FR	ACME-FR\administrator	John.Locke	ACME-FR	ACME-FR\John.Locke
03/30/2017 01:23:44 PM	PNPL-6-KP	A user account was disabled.	Administrator	WIN-R9H529RIO4Y	WIN-R9H529RIO4Y\Administrator	bob	WIN-R9H529RIO4Y	WIN-R9H529RIO4Y\bob

Figure 8

3. **Active Directory-Audit detailed directory service replication:** This report provides the details about an Active Directory replica source naming context if it is established, removed, modified or failed.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
DS Access	Audit Detailed Directory Service Replication	4928- An Active Directory replica source naming context was established. 4929- An Active Directory replica source naming context was removed. 4930- An Active Directory replica source naming context was modified. 4931- An Active Directory replica destination naming context was modified. 4934- Attributes of an Active Directory object was replicated. 4935- Replication failure begins. 4936- Replication failure ends 4937- A lingering object was removed from a replica.	Enable Success/Failure
		Directory Services Restore Mode. 5376- Credential Manager credentials were backed up 5377- Credential Manager credentials were restored from a backup	

Report Sample:

LogTime	Computer	Action	Destination DRA	Source DRA	Source Address	Naming Context
04/03/2017 01:39:44 PM	PNPL-6-KP-WINDOWS	An Active Directory replica source naming context was established.	CN=NTDS Settings,CN=WIN-R9H529RIO4Y,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local	CN=NTDS Settings,CN=WIN-857ZZX6RQHL,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local	0b63afed-1e41-43a3-8bc2-f33dc33942ea._msdcs.acme-fr.local	CN=NTDS Settings,CN=WIN-R9H529RIO4Y,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local
04/03/2017 01:39:45 PM	PNPL-6-KP-WINDOWS	An Active Directory replica source naming context was removed.	CN=NTDS Settings,CN=WIN-R9H529RIO4Y,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local	CN=NTDS Settings,CN=WIN-857ZZX6RQHL,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local	0b63afed-1e41-43a3-8bc2-f33dc33942ea._msdcs.acme-fr.local	CN=NTDS Settings,CN=WIN-R9H529RIO4Y,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local

Figure 9

4. **Active Directory-Audit directory service changes:** This report provides all the directory configuration changes such as a directory being created, deleted, modified, moved or undeleted.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
DS Access	Audit Directory Service Changes	5136- A directory service object was modified. 5137- A directory service object was created. 5138-A directory service object was undeleted. 5139- A directory service object was moved. 5141- A directory service object was deleted.	Enable Success/Failure

Report Sample:

LogTime	Computer	Action	Source Account Name	Source Account Domain	Directory service name	Directory service type
04/03/2017 02:58:10 PM	PNPL-6-KP-WINDOWS	A directory service object was modified.	Administrator	ACME-FR	acme.com	Active Directory Domain Services
04/03/2017 02:58:10 PM	PNPL-6-KP-WINDOWS	A directory service object was created.	Administrator	ACME	acme.local	Active Directory Domain Services
04/03/2017 02:58:10 PM	PNPL-6-KP-WINDOWS	A directory service object was undeleted.	Carlos	CONTOSO	Contoso.com	Active Directory Domain Services
04/03/2017 02:58:10 PM	PNPL-6-KP-WINDOWS	A directory service object was moved.	Administrator	ACME	acme.local	Active Directory Domain Services
04/03/2017 02:58:10 PM	PNPL-6-KP-WINDOWS	A directory service object was deleted.	administrator	ACME	acme.com	Active Directory Domain Services

Figure 10

5. **Active Directory- Audit directory service replication:** This report provides all the directory service replication details.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
DS Access	Audit Directory Service Replication	4932- Synchronization of a replica of an Active Directory naming context has begun. 4933- Synchronization of a replica of an Active Directory naming context has ended.	Enable Success/Failure

Report Sample:

LogTime	Computer	Action	Source DRA	Destination DRA	Naming Context
04/03/2017 05:55:29 PM	PNPL-6-KP-WINDOWS	Synchronization of a replica of an Active Directory naming context has ended.	CN=NTDS Settings,CN=WIN-R9H529RIO4Y,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local	CN=NTDS Settings,CN=WIN-857ZZX6RQHL,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local	CN=NTDS Settings,CN=WIN-857ZZX6RQHL,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local
04/03/2017 05:55:29 PM	PNPL-6-KP-WINDOWS	Synchronization of a replica of an Active Directory naming context has begun.	CN=NTDS Settings,CN=WIN-R9H529RIO4Y,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local	CN=NTDS Settings,CN=WIN-857ZZX6RQHL,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local	CN=NTDS Settings,CN=WIN-857ZZX6RQHL,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=acme-fr,DC=local

Figure 11

6. **Active Directory-Audit DPAPI activity:** This report provides all Audit DPAPI activity.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
Detailed Tracking	Audit DPAPI Activity	4692- Backup of data protection master key was attempted. 4693- Recovery of data protection master key was attempted. 4694- Protection of auditable protected data was attempted 4695- Un-protection of auditable protected data was attempted.	Enable Success/Failure

Report Sample:

LogTime	Computer	Action	Source Security ID	Source Account Name	Source Account Domain	Key Identifier	Recovery Server
04/03/2017 06:45:53 PM	PNPL-6-KP-WINDOWS	Unprotection of auditable protected data was attempted.	WIN-R9H529RIO4Y\Administrator	Administrator	WIN-R9H529RIO4Y	ec9796fd-fa87-460d-8bf2-25e0a01ddf82	
04/03/2017 06:45:53 PM	PNPL-6-KP-WINDOWS	Backup of data protection master key was attempted.	ACME\James	James	ACME	erh49ul8-h8f5-f69t-u79e-op9hb1dg4m	UNIR9H529RIO4Y
04/03/2017 06:45:53 PM	PNPL-6-KP-WINDOWS	Recovery of data protection master key was attempted.	CONTOSO\Fred	Fred	CONTOSO	6n44cb79j8-qe89-341e-yii6-e6h4j9ks3aq	WINB6R9W6PY
04/03/2017 06:45:53 PM	PNPL-6-KP-WINDOWS	Protection of auditable protected data was attempted.	CONTOSO\Melissa	Melissa	CONTOSO	y8k7gn4et7h-ti45-961k-qa55-bn784bw5bg4	

Figure 12

7. **Active Directory-Audit process termination:** This report provides all the terminated or exited process details.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
Detailed Tracking	Audit Process Termination	4689- A process has exited.	Enable Success/Failure

Report Sample:

LogTime	Computer	Action	Source Account Name	Source Account Domain	Process Name
04/04/2017 03:00:00 PM	PNPL-6-KP-WINDOWS	A process has exited.	Edward	Contoso	C:\Windows\System32\conhost.exe
04/04/2017 03:00:00 PM	PNPL-6-KP-WINDOWS	A process has exited.	Zoe	Contoso	C:\Program Files (x86)\Microsystems\TrackerWeb\bin\sm.Tracker.IPresolver.exe

Figure 13

8. **Active Directory-Audit Kerberos authentication service:** This report provides details about all the Kerberos authentication services.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
Account Logon	Audit Kerberos Authentication Service	4678- A Kerberos authentication ticket (TGT) was requested 4771- Kerberos pre-authentication failed 4772- A Kerberos authentication ticket request failed	Enable Success/Failure

Report Sample:

LogTime	Computer	Action	Source Account Name	Source Domain Name	User ID	Service ID	Client Address
03/15/2017 05:51:42 PM	PNPL-6-KP	A Kerberos authentication ticket (TGT) was requested.	Dave	neon-sw	NEON-SW\DAVE	NEON-SW\krbtgt	192.168.1.118
03/15/2017 05:51:42 PM	PNPL-6-KP	A Kerberos authentication ticket request failed.	Basil	Contoso-us	Contoso-us\Basil	krbtgt/contoso-us	172.14.129.56
03/15/2017 05:51:42 PM	PNPL-6-KP	Kerberos pre-authentication failed.	Administrator	ACME	ACME\administrator	krbtgt/acme-fr	10.42.42.224

Figure 14

9. **Active Directory-Audit Kerberos service ticket operation:** This report provides details about all the Kerberos service ticket operations, whether it was requested or renewed.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
Account Logon	Audit Kerberos Service Ticket Operation	4769- A Kerberos service ticket was requested 4770- A Kerberos service ticket was renewed	Enable Success/Failure

Report Sample:

LogTime	Computer	Action	Source Account Name	Source Domain Name	Client Address	Service Name	Service ID
03/16/2017 11:59:01 AM	PNPL-6-KP	A Kerberos service ticket was requested.	bob@ACME.COM	ACME.COM	172.168.42.136	WIN-PY3ZJZTXPIL$	ACME\WIN-PY3ZJZTXPIL$
03/16/2017 11:59:01 AM	PNPL-6-KP	A Kerberos service ticket was renewed.	UNI-6E45GW8ERG7E8R7G$@ACME-FR.LOCAL	ACME-FR.LOCAL	172.168.44.101	krbtgt	ACME-FR\krbtgt

Figure 15

10. **Active Directory-Audit RPC events:** This report provides details about all the RPC events that were attempted.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
Detailed Tracking	Audit RPC Events	5712- A Remote Procedure Call (RPC) was attempted.	Enable Success/Failure

Report Sample:

LogTime	Computer	Action	Source Account Name	Source Account Domain	Process Name	Remote IP Address
04/04/2017 03:56:54 PM	PNPL-6-KP-WINDOWS	A Remote Procedure Call (RPC) was attempted.	wewdrr	WERESDF	C:\Windows\System32 otepad.exe	192.12.4.42
04/04/2017 03:56:54 PM	PNPL-6-KP-WINDOWS	A Remote Procedure Call (RPC) was attempted.	randyor	RFCINL	C:\Windows\System32\powershell.exe	192.168.1.118

Figure 16

11. **Active Directory-Audit other accounts logon events:** This report provides details about all the account logon events.

Audit Events that needs to be enabled:

System Audit Policies-Local Group Policy Object			
Account Logon	Audit Other Account Logon Events	4649- A replay attack was detected 4778- A session was reconnected to a Window Station 4779- A session was disconnected from a Window Station 4800- The workstation was locked 4801- The workstation was unlocked 4802- The screen saver was invoked 4803- The screen saver was dismissed 5378- The requested credentials delegation was disallowed by policy 5632- A request was made to authenticate to a wireless network 5633- A request was made to authenticate to a wired network	Enable Success/Failure

Report Sample:

LogTime	Computer	Action	Security ID	Source Account Name	Source Account Domain	Session Name	Mac address	Client Name	Client Address
04/04/2017 04:59:00 PM	PNPL-6-KP-WINDOWS	A session was disconnected to a Window Station.		Administrator	WIN-R9H529RIO4Y	RDP-Tcp#0		XPEDIT	10.42.42.211
04/04/2017 04:59:00 PM	PNPL-6-KP-WINDOWS	A session was reconnected to a Window Station.		Administrator	WIN-R9H529RIO4Y	RDP-Tcp#0		XPEDIT	10.42.42.211
04/04/2017 04:59:01 PM	PNPL-6-KP-WINDOWS	A request was made to authenticate to a wireless	Contoso\Rooney	Rooney	Contoso		2e:33:d7:ff:6a:c2		

Figure 17

Alerts

1. **Active Directory-Account management activities:** This alert is generated when any account is created, deleted, changed, enabled or disabled in Windows Active Directory.
2. **Active Directory-Account logon events:** This alert is generated when any successful logon, successful log off, special privileges logon or Logon failures is done in Windows Active Directory.
3. **Active Directory-Audit detailed directory service replication:** This alert is generated when an Active Directory replica source naming context is established, removed, modified or failed.
4. **Active Directory-Audit Dpapi activity:** This alert is generated when backup or recovery of data protection master key is attempted.
5. **Active Directory-Audit Kerberos authentication:** This alert is generated when a Kerberos authentication ticket is requested or failed.

Import Active Directory knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Token templates
- Flex Reports
- Alerts

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

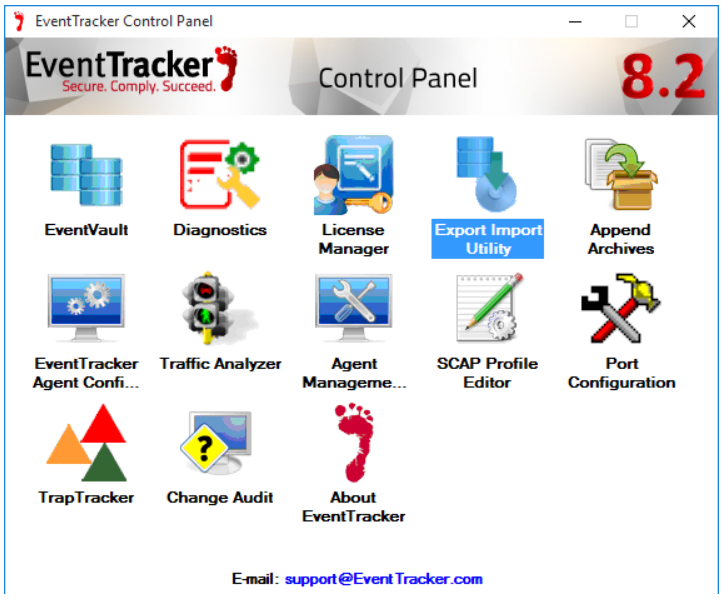

Figure 18

3. Click the **Import** tab.

Parsing Rule

1. Click **Token Value** option, and then click the browse  button.
2. Locate the **All Active Directory group of Token Value.issch** file, and then click the **Open** button.

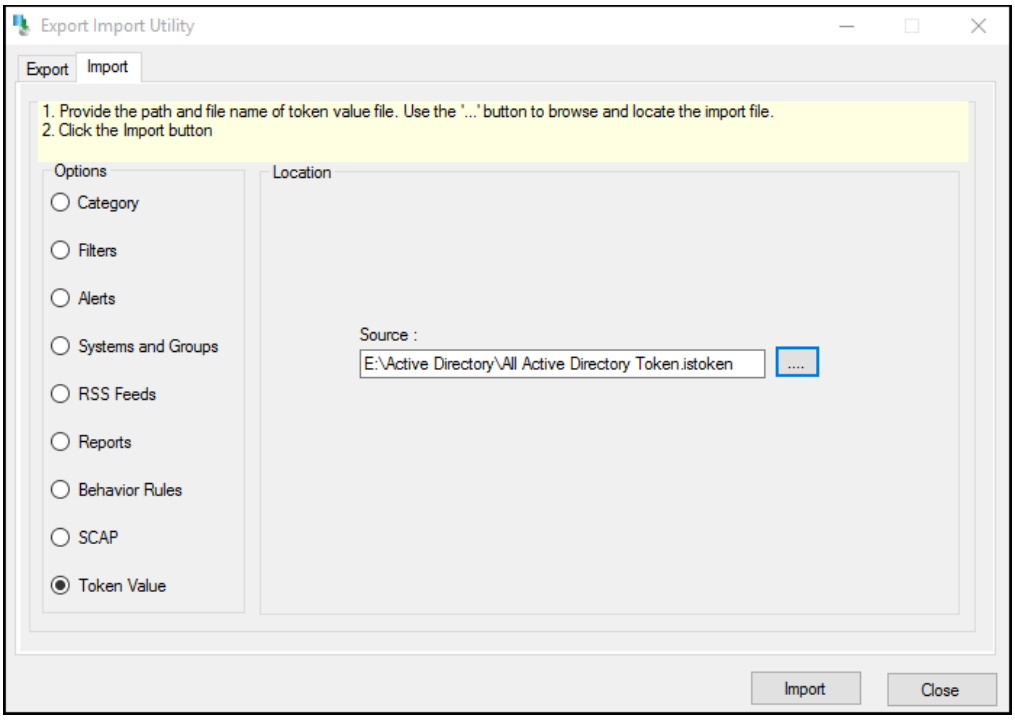

Figure 19

3. Click the **Import** button to import the tokens. EventTracker displays success message.

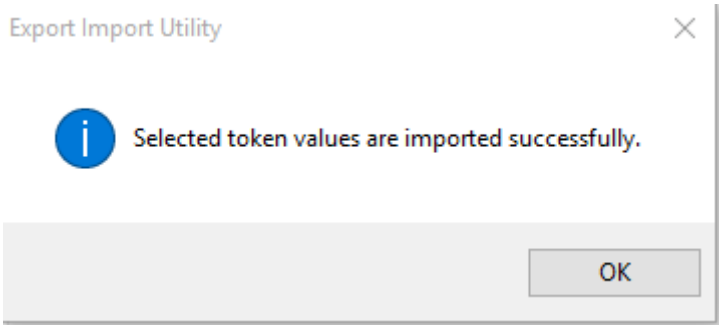

Figure 20

Flex Reports

1. Click **Reports** option, and then click the browse ... button.
2. Locate the **All Active Directory group of flex reports.issch** file, and then click the **Open** button.

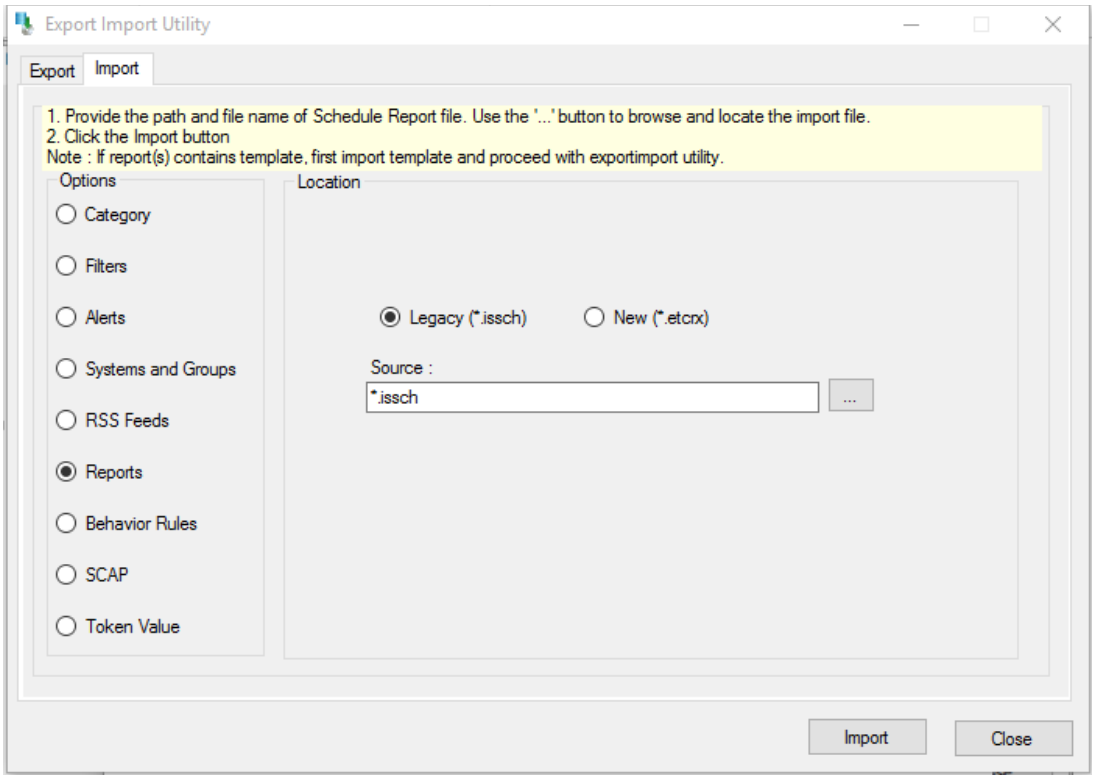

Figure 21

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

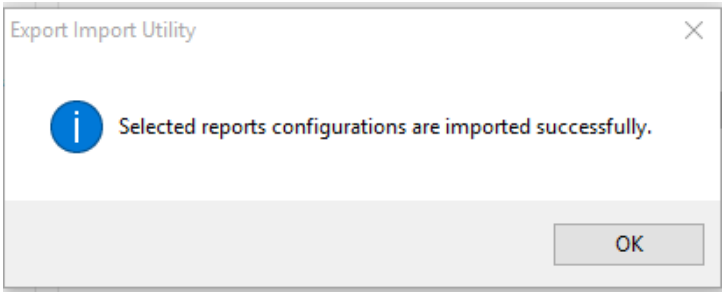

Figure 22

Alerts

1. Click **Alerts** option, and then click the browse  button.
2. Locate the **All Active Directory.isalt** file, and then click the **Open** button.

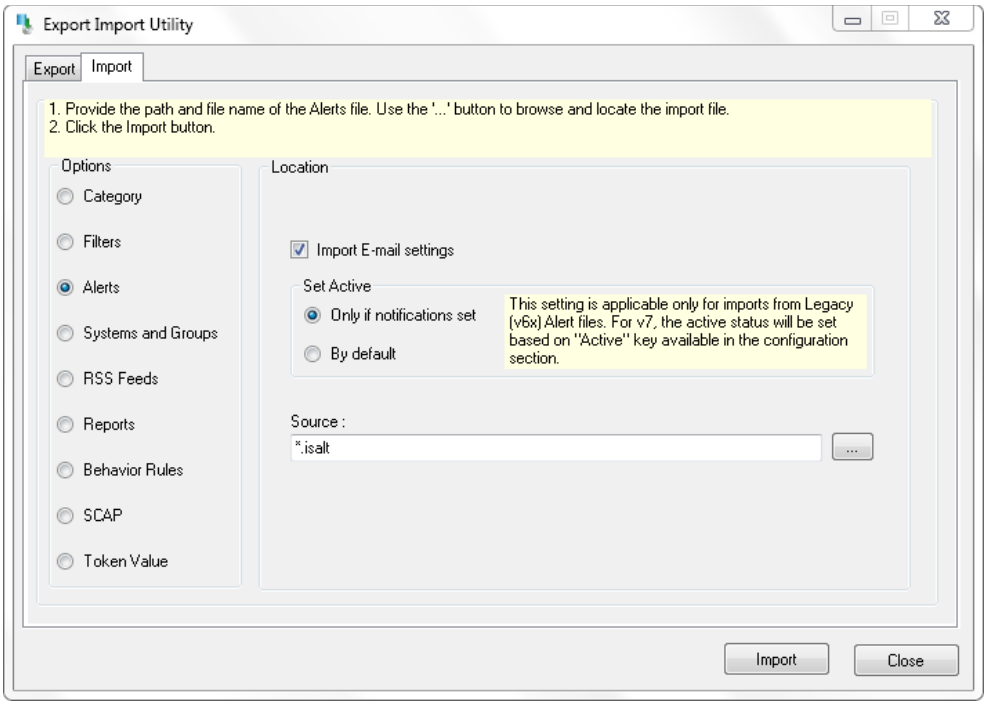

Figure 23

2. To import alerts, click the **Import** button.
   EventTracker displays success message.

Figure 24

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

Verify Active Directory knowledge pack in EventTracker

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In the **Search** field, type **Active Directory**, and then click **Go** button.
3. Alert Management page will display the imported **Active Directory** alert.

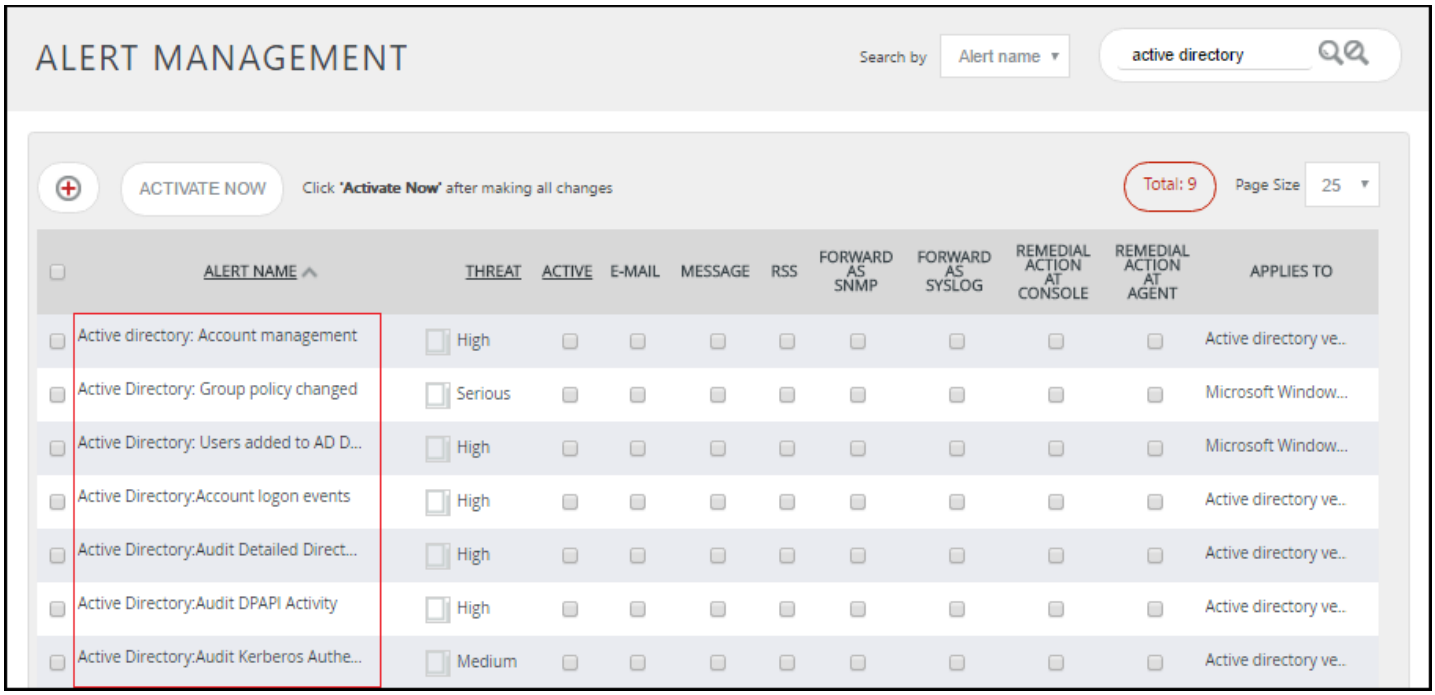

Figure 25

4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

Figure 26

5. Click the **OK** button, and then click the **Activate now** button.

NOTE:

- You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter '**Active Directory**, and then click the **Search** button.

EventTracker displays Flex reports of '**Active Directory.**

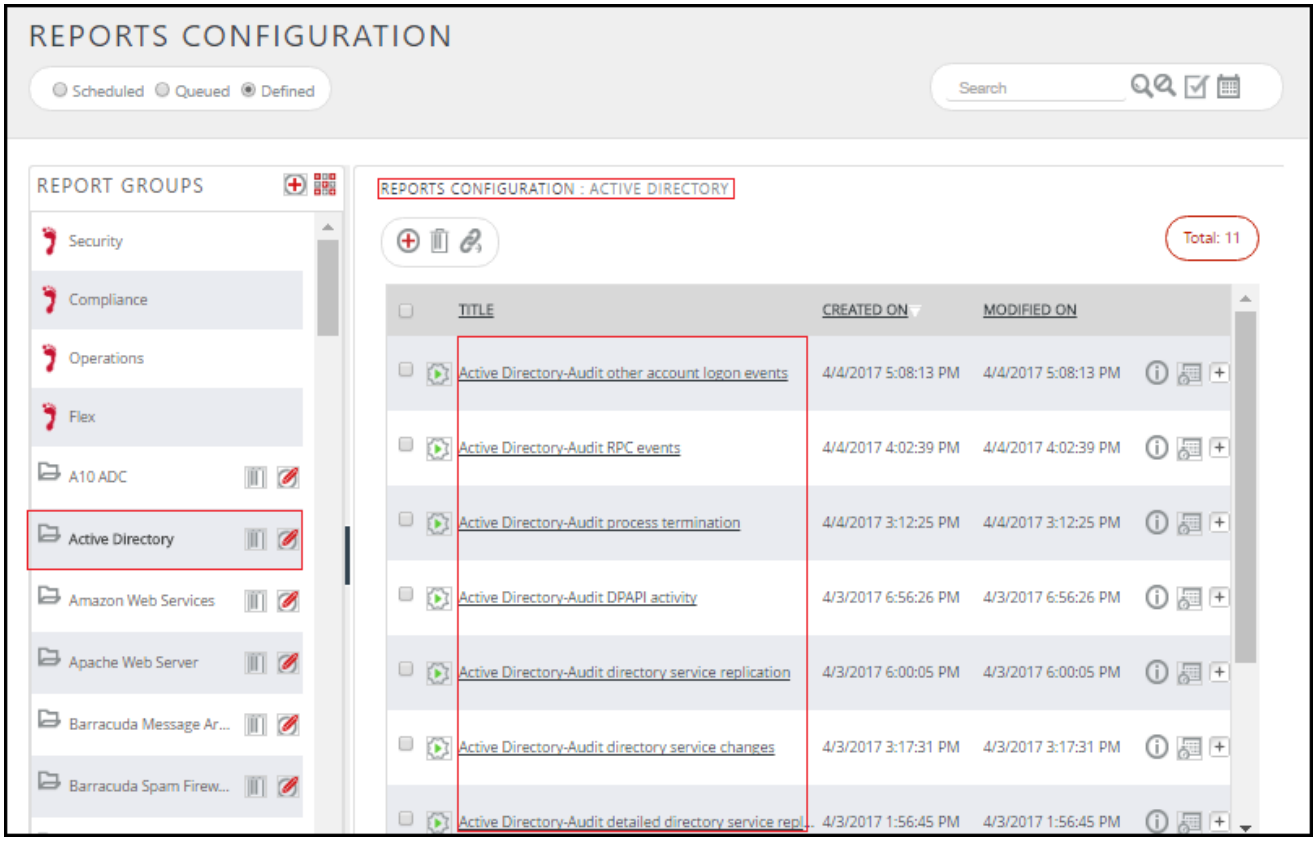

Figure 27

Template

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules.**

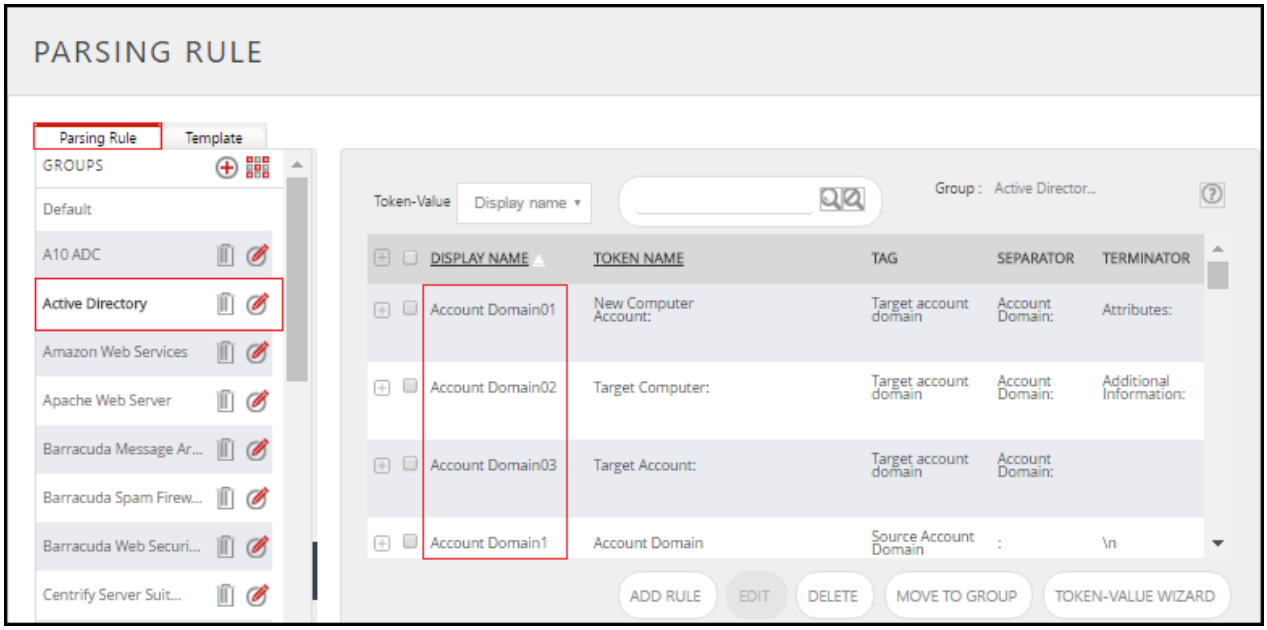

Figure 28

Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

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

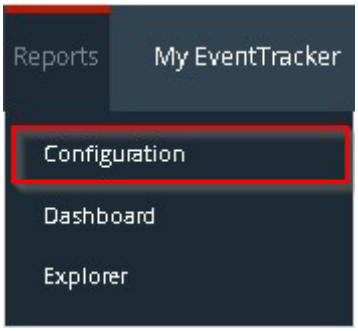

Figure 29

2. Navigate to **Reports>Configuration**.
3. Select **Active Directory** in report groups. Check **Defined** dialog box.

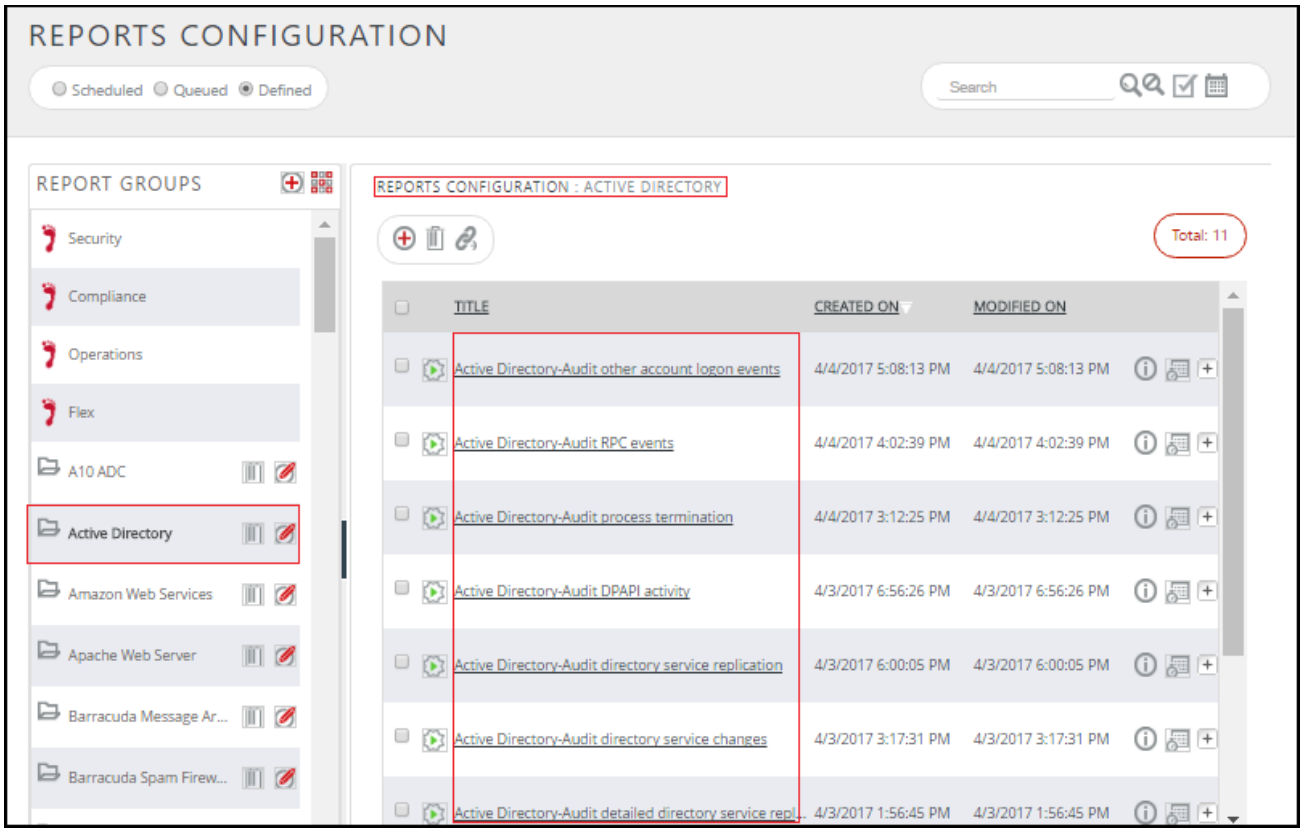

Figure 30

4. Click on '**schedule**'  to plan a report for later execution.
5. Click **Next** button to proceed.
6. In review page, check **Persist data in EventVault Explorer** option.

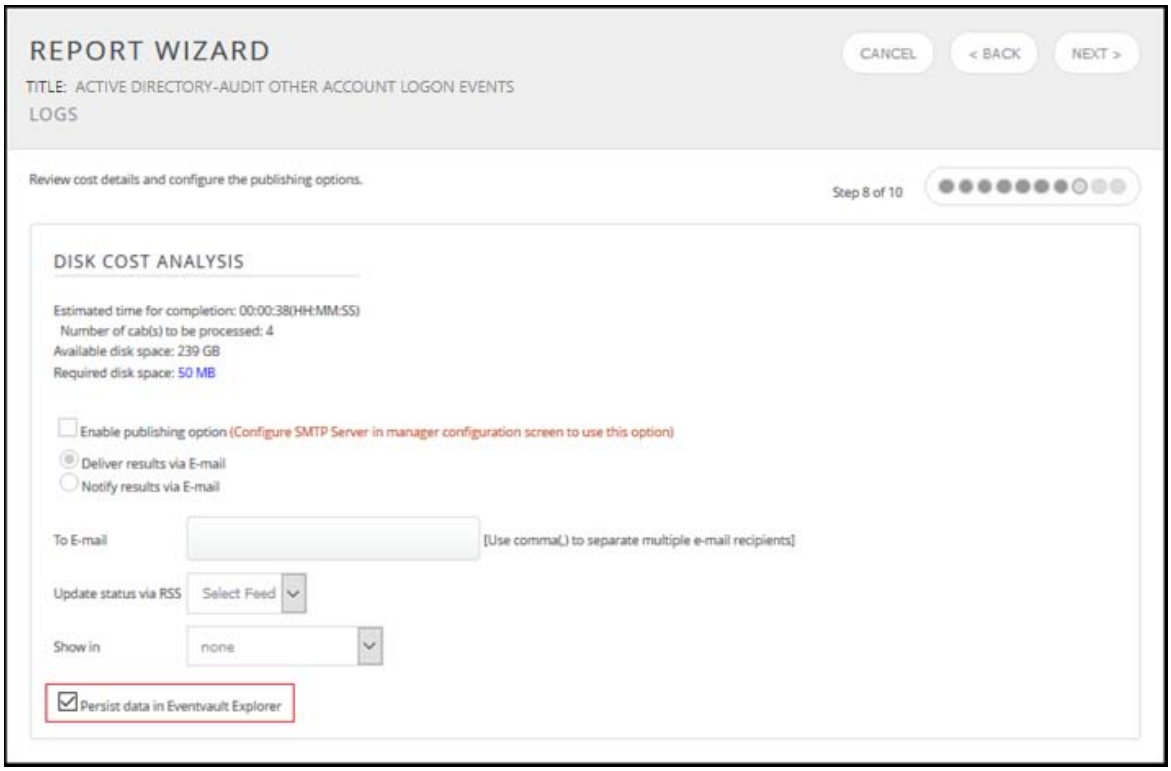

Figure 31

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

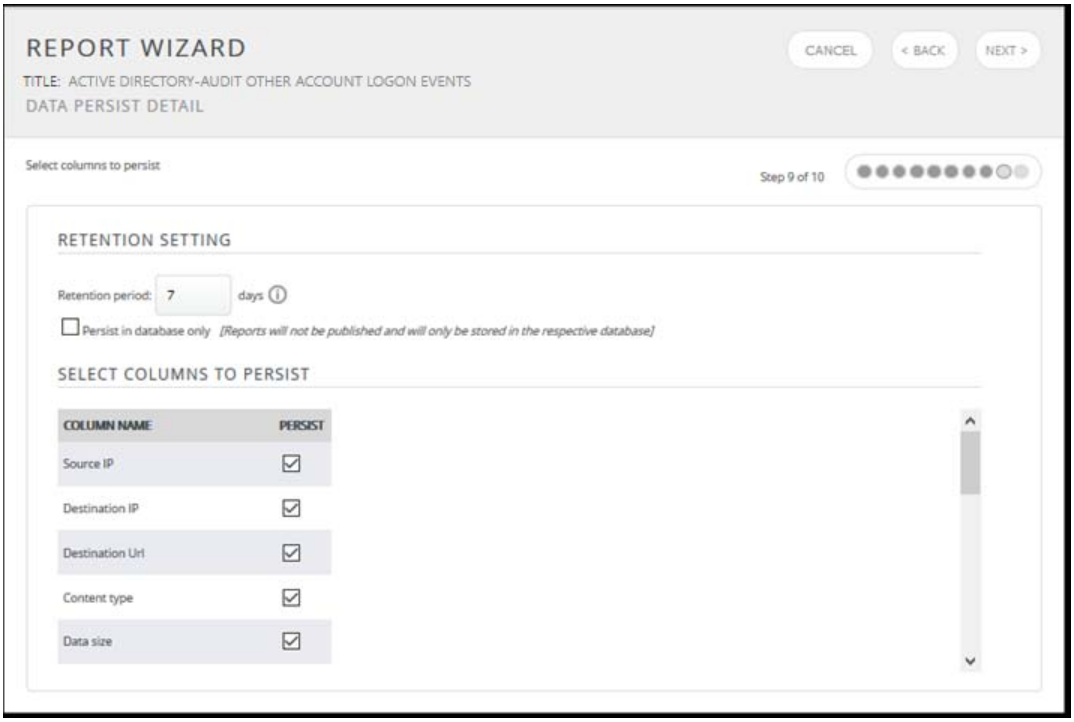

Figure 32

8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

Create Dashlets

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

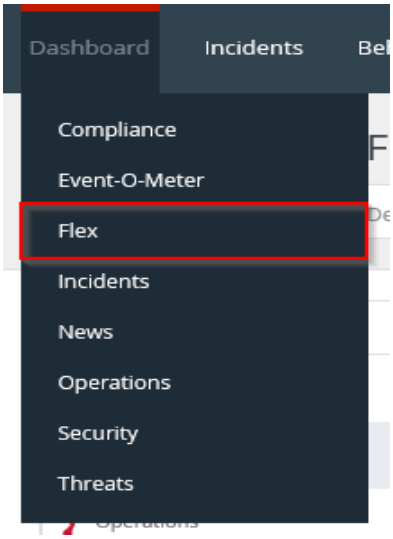

Figure 33

2. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

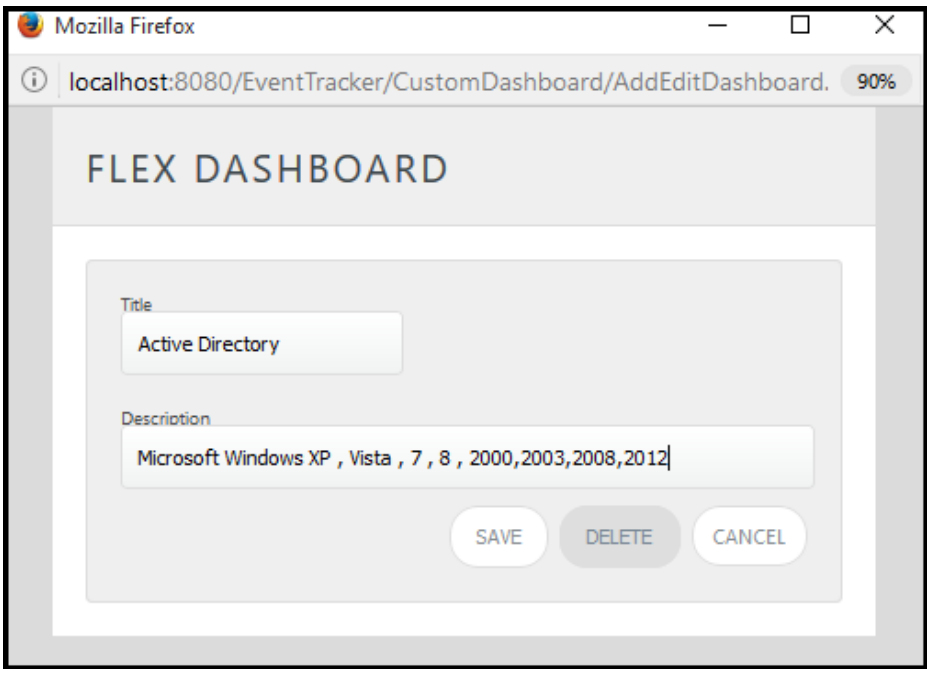

Figure 34

3. Fill suitable title and description and click **Save** button.
4. Click to configure a new flex dashlet. Widget configuration pane is shown.

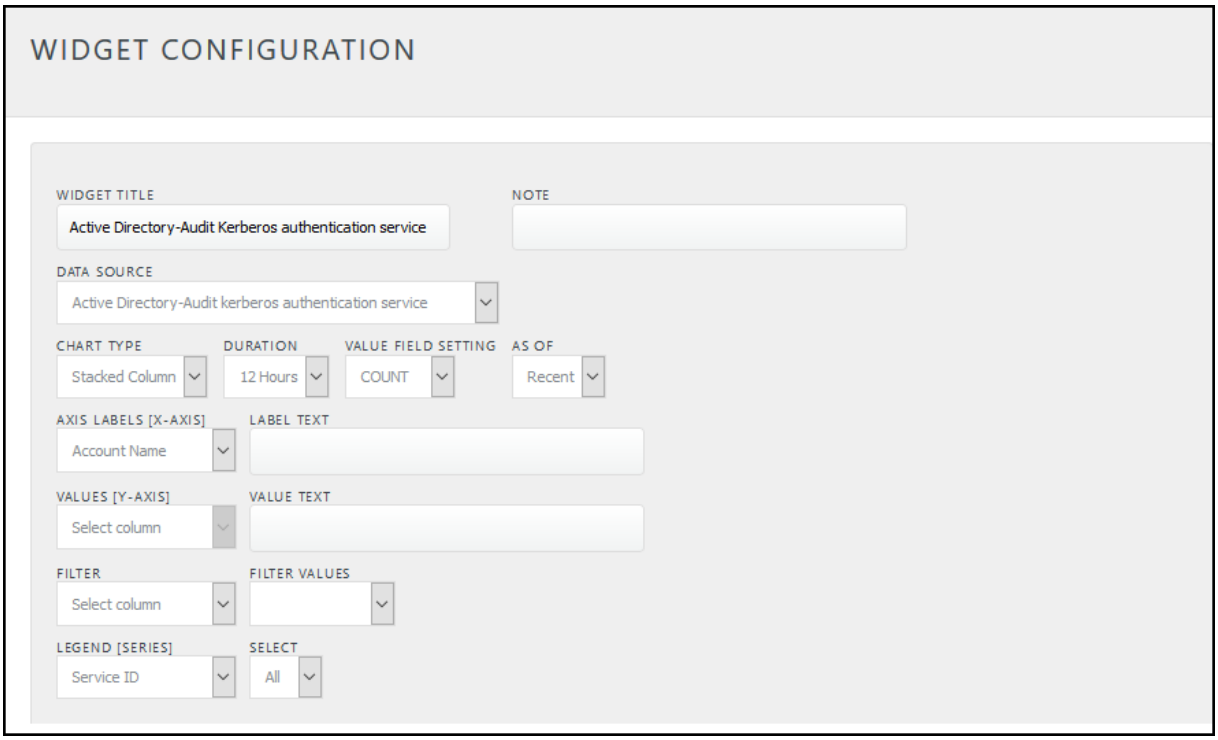

Figure 35

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

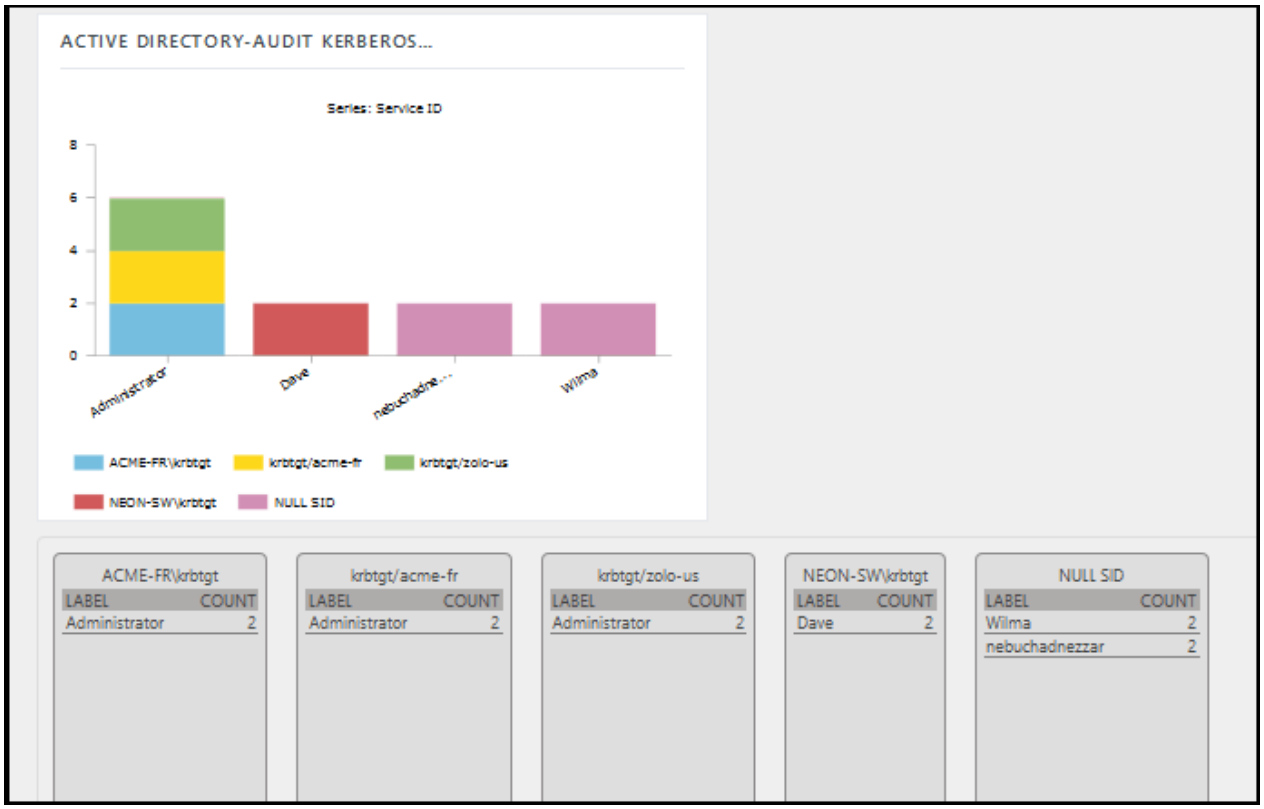

Figure 36

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

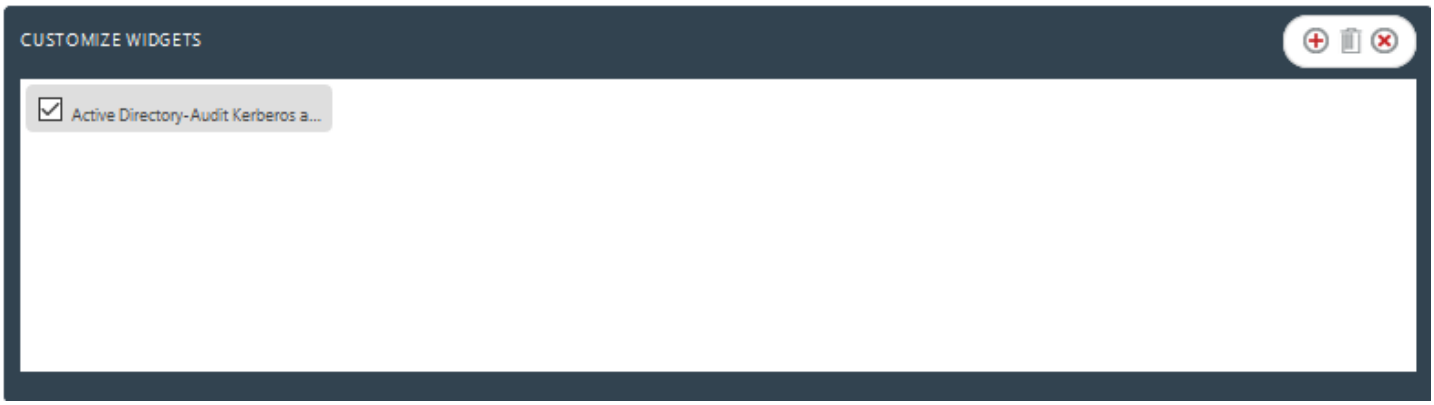

Figure 37

15. Click 'customize' to locate and choose created dashlet.
16. Click to add dashlet to earlier created dashboard.

Sample Flex Dashboards

- **WIDGET TITLE:** Active Directory-Account management Activity
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Account Name
  LEGEND[SERIES]: Action

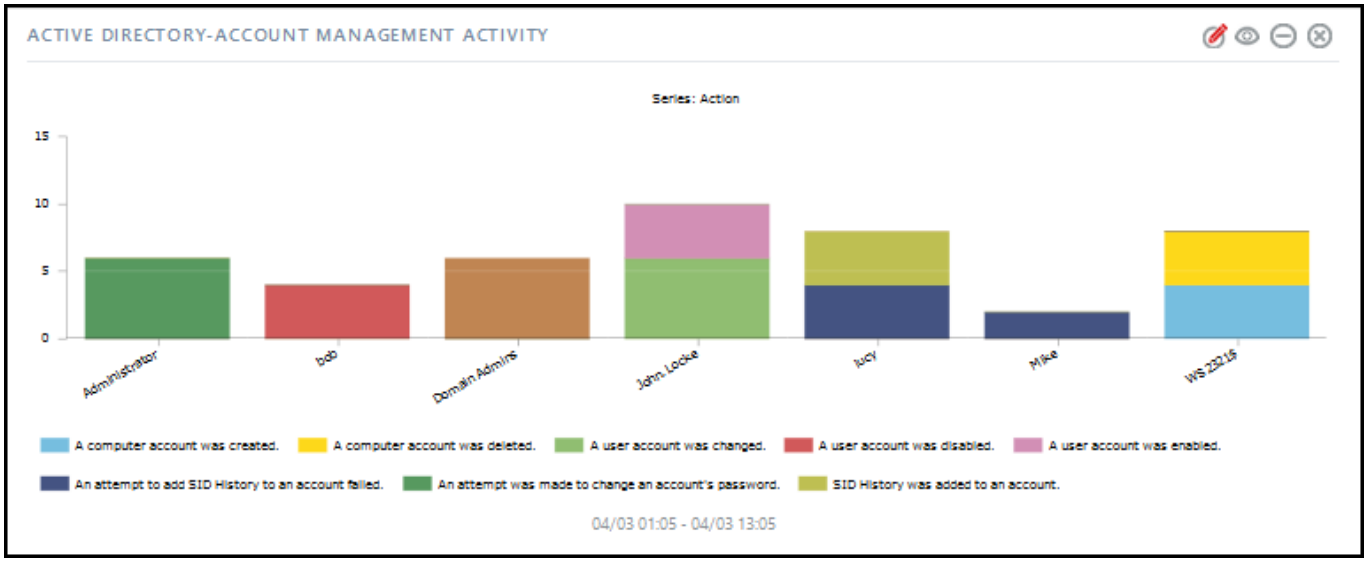

Figure 38

- **WIDGET TITLE:** Active Directory-Audit Dpapi activity
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Account Name
  LEGEND [SERIES]: Action

Figure 39

- **WIDGET TITLE:** Active Directory-Audit detailed directory services
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Action

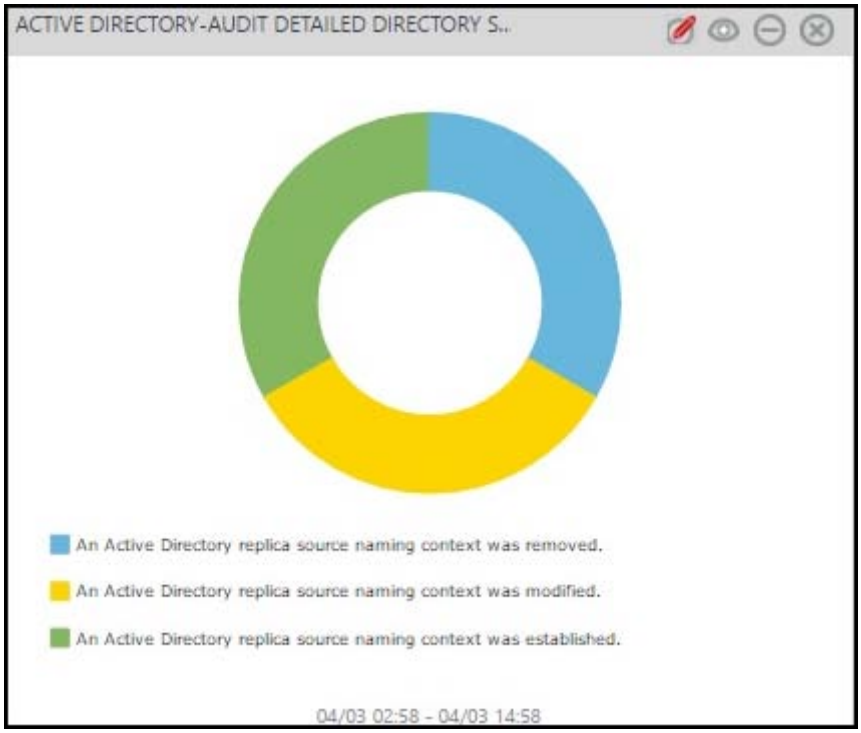

Figure 40

- **WIDGET TITLE:** Active Directory-Audit directory service replication
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Action
  LEGEND [SERIES]: Computer

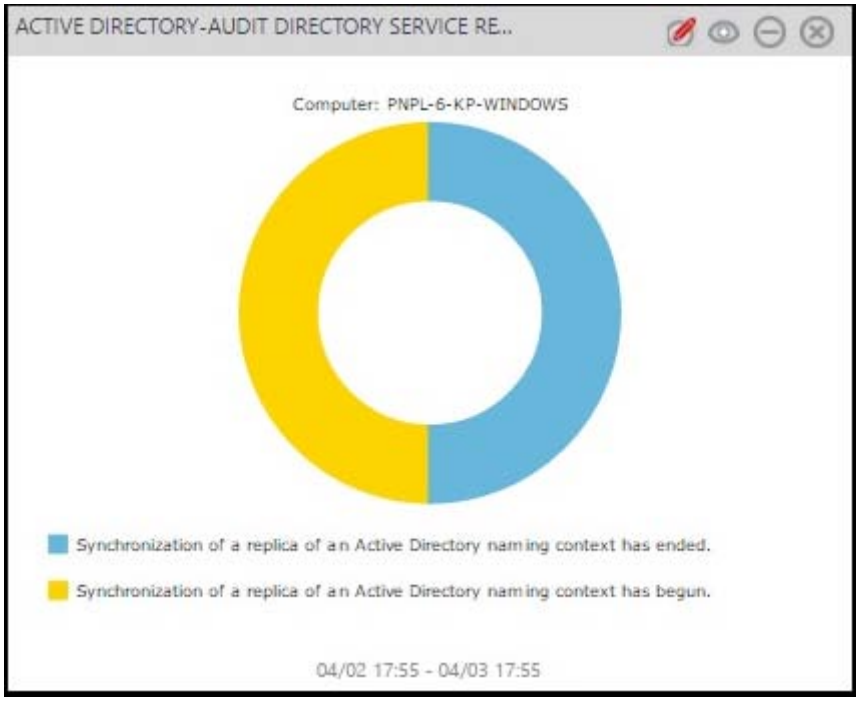

Figure 41

- **WIDGET TITLE:** Active Directory-Audit directory service changes
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Account Name
  LEGEND [SERIES]: Computer

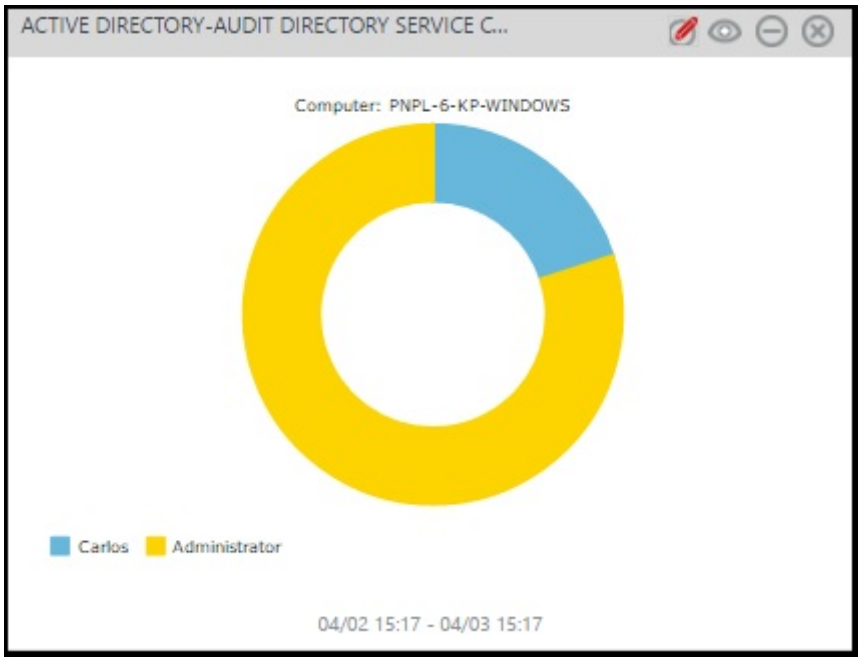

Figure 42

- **WIDGET TITLE:** Active Directory-Audit Kerberos service ticket operation
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Account Name
  LEGEND[SERIES]: Service Name

Figure 43

- **WIDGET TITLE:** Active Directory-Audit process termination
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Account Name
  LEGEND[SERIES]: Action

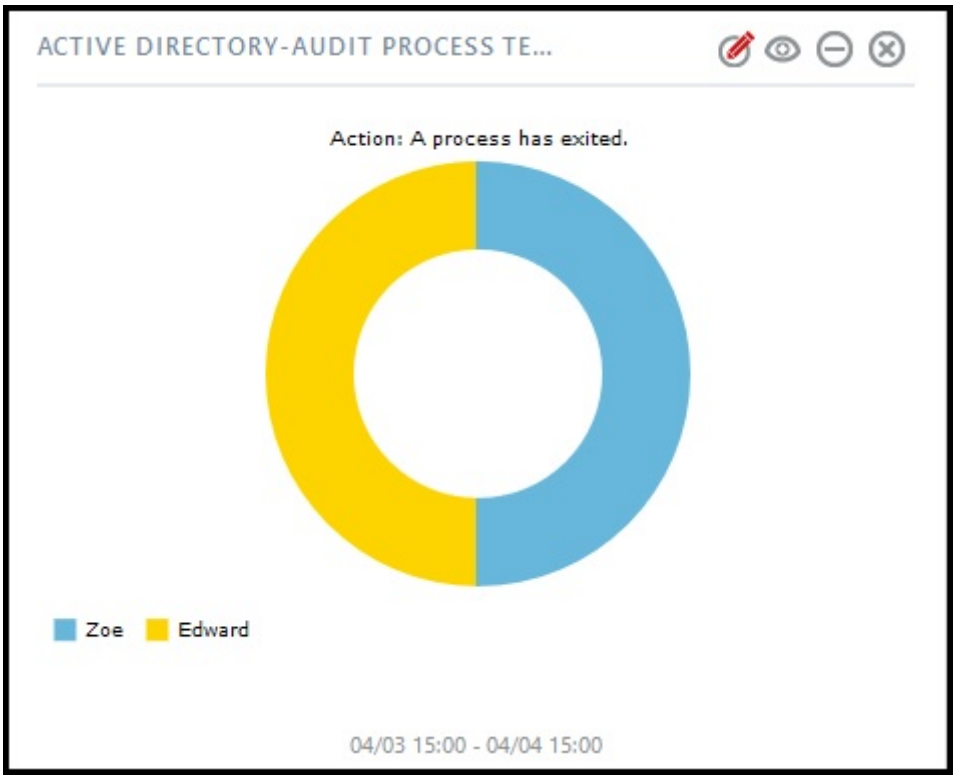

Figure 44

- **WIDGET TITLE:** Active Directory-Audit other account logon events
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Account Name
  LEGEND [SERIES]: Source Account Domain

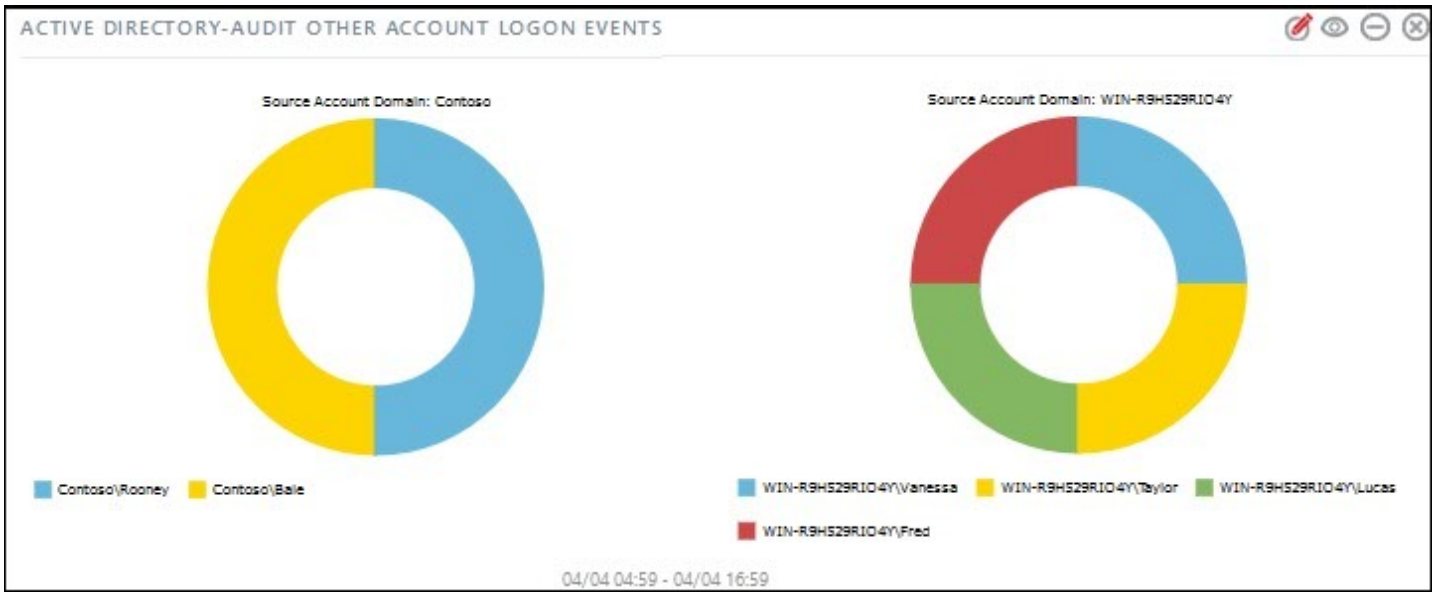

Figure 45