EventTracker
Secure. Comply. Succeed.

Integrate IBM AIX

EventTracker Enterprise

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Publication Date: April 6, 2016

About this Guide

This guide will facilitate an **IBM AIX** user to send logs to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise 7.x or later and IBM AIX 6.1 and 7.1.**

Audience

Administrators who want to monitor **IBM AIX** using EventTracker Enterprise.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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 Prism Microsystems, 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.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Introduction

AIX (Advanced Interactive eXecutive, pronounced ‘a i ex”) is a series of proprietary UNIX operating system developed and sold by IBM for several of its computer platforms.

Pre-requisites

- **EventTracker 7.x or later** should be installed.
- User should have administrator privileges to IBM AIX server.

Configuring IBM AIX for Auditing

The audit logger constructs the audit record and appends it to the kernel audit trail. From there, it can be written in one or both of the following modes:

- BIN mode Written in two binary files.
- STREAM mode Written synchronously via an audit pseudo-device

To enable STREAM mode auditing and select audit events:

1. Start:

   ```
   streammode = on
   cmds = /etc/security/audit/streamcmds
   ```

IBM AIX syslog configuration

1. Login to the IBM AIX Unix machine as root.
2. Open Terminal Window.
3. Open syslog.conf in VI Editor. Vi /etc/syslog.conf.
4. Add the below mentioned line in file syslog.conf at last.

   ```
   *.info@IP address of EventTracker Enterprise machine
   ```

5. Save the file using :wq
6. Run refresh –s syslogd

EventTracker Knowledge Pack

Once IBM AIX is configured events are received in EventTracker; Alerts and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support IBM AIX.

Categories

- **IBM AIX: Account management**
  This category provides information related to system accounting, being enabled or disabled by the admin.

- **IBM AIX: Administrator logon activity**
  This category provides information related to successful user logon attempts.

- **IBM AIX: Audit configuration**
  This category provides information when an administrator performs auditing on process control events, security events and privilege required events.

- **IBM AIX: Backup and restore activity**
  This category provides information related to backup, restore and export activity.

- **IBM AIX: Cron activity**
  This category provides information related to cron that tasks running automatically in the background at regular intervals.

- **IBM AIX: Device management**
  This category provides information related to device configuration, device create, delete, remove, start and stop details.

- **IBM AIX: File access control changes**
  This category provides information related to access control list that defines the access rights to the object.

- **IBM AIX: File management**
  This category provides information related to file management that performs read, write, rename, change of mode and ownership.

- **IBM AIX: File system activity**
  This category provides information related to file system that make, remove, change of directory and root.

- **IBM AIX: General activity**
  This category provides information related to port locked, port changed, enqueuing request to shared resources and installs, updates and maintenance of the available software products.

- **IBM AIX: Group management**
  This category provides information related to group name, checks the existence of the users that are listed as group administrators in the group database files and also checks for valid admin attribute for each group.

- **IBM AIX: Kernel process activity**
  This category provides information related to the state of each active processes and threads in the system.

- **IBM AIX: Logical volume management activity**
  This category provides information related to logical volume management and locally attached disk drives operations.

- **IBM AIX: Password changed**
  This category provides information related to change of user's password, administrator password and verifies the correctness of local authentication information.

- **IBM AIX: Security objects audit**
  This category provides information related to the environment attributes allowing admin to read, write and execute operations on security objects.

- **IBM AIX: Security roles management**
  This category provides information related to role based access control allowing the creation, change and removal of roles for system by administrator.

- **IBM AIX: System resource controller**
  This category provides information related to start and stop of the system resource controller and changes in the subserver and subsystem definition in the object class.

- **IBM AIX: System start and stop**
  This category provides information related to server startup and shutdown.

- **IBM AIX: TCPIP activity**
  This category provides information related to changes in TCP/IP interfaces, routes and system time via network.

- **IBM AIX: User authentication failed**
  This category provides information related to authentication failure for user due to incorrect password or insufficient permission.

- **IBM AIX: User management**
  This category provides information related to user create, change, remove and user access to the shell.

Alerts

- **IBM AIX: Account disabled**
  This alert is generated when administrator disables the system accounting.

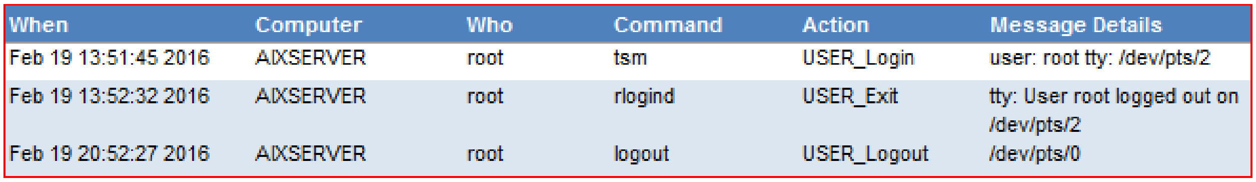
- **IBM AIX: Device removed**
  This alert is generated when administrator removes the device from the server.

- **IBM AIX: Security role changed**
  This alert is generated when administrator create, change and remove the security roles.

- **IBM AIX: System rebooted**
  This alert is generated when administrator reboots the server.

Flex Reports

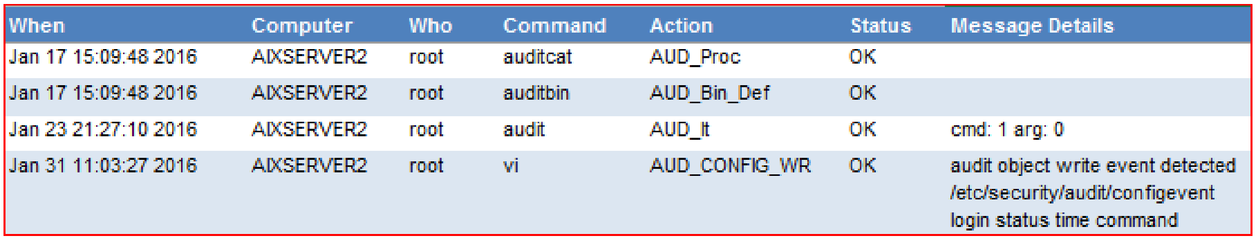
- **IBM AIX: Administrator logon activity**
  This report provides information related to user logon activity, that is, whoever has logged in, logged out or exited from the server.



When	Computer	Who	Command	Action	Message Details
Feb 19 13:51:45 2016	AIXSERVER	root	tsm	USER_Login	user: root tty: /dev/pts/2
Feb 19 13:52:32 2016	AIXSERVER	root	rlogind	USER_Exit	tty: User root logged out on /dev/pts/2
Feb 19 20:52:27 2016	AIXSERVER	root	logout	USER_Logout	/dev/pts/0

```
USER_Login   root    OK   Wed Jan 31 13:51:45 2007  tsm user: root tty: /dev/pts/2

USER_Logout root    OK    Tue Jan 23 20:52:27 2007 logout /dev/ pts/0

USER_Exit      root    OK    Wed Jan 31 13:52:32 2007 rlogind tty: User root logged out on /dev/pts/2
```

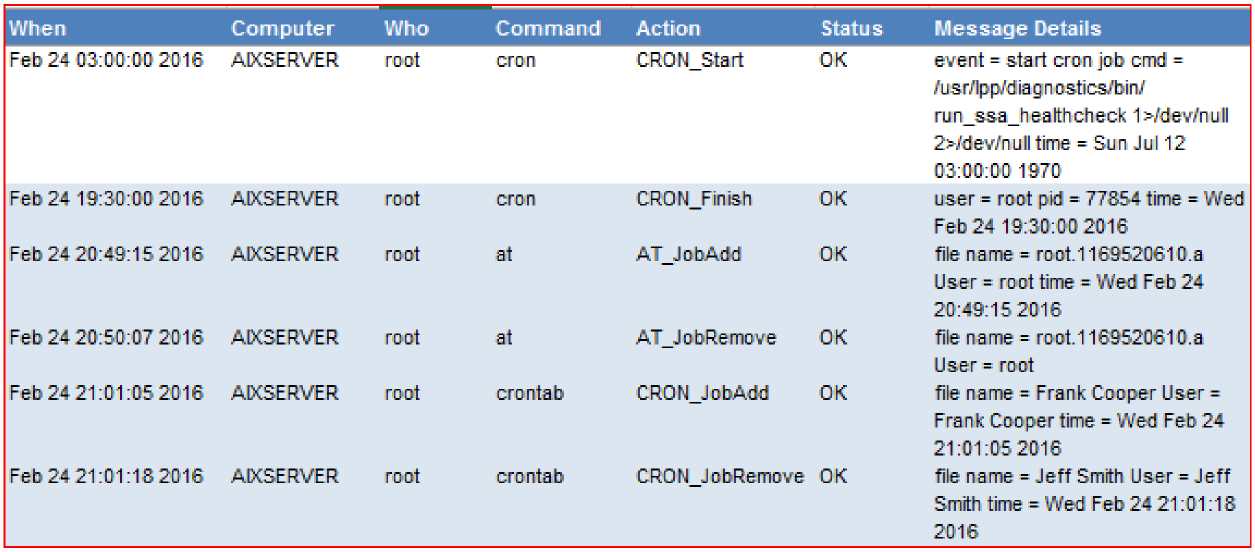
- **IBM AIX: Audit configuration**
  This report provides the information related to the events and objects, which are audited.



When	Computer	Who	Command	Action	Status	Message Details
Jan 17 15:09:48 2016	AIXSERVER2	root	auditcat	AUD_Proc	OK	
Jan 17 15:09:48 2016	AIXSERVER2	root	auditbin	AUD_Bin_Def	OK	
Jan 23 21:27:10 2016	AIXSERVER2	root	audit	AUD_It	OK	cmd: 1 arg: 0
Jan 31 11:03:27 2016	AIXSERVER2	root	vi	AUD_CONFIG_WR	OK	audit object write event detected /etc/security/audit/configevent login status time command

```
  AUD_CONFIG_WR root OK Wed Jan 31 11:03:27 2007 vi audit object write event detected
/etc/security/audit/configevent login status time command

AUD_It root OK Tue Jan 23 21:27:10 2007 audit cmd: 1 arg: 0

AUD_Bin_Def root OK Wed Jan 17 15:09:48 2007 auditbin

AUD_Proc root OK Wed Jan 17 15:09:48 2007 auditcat
```

- **IBM AIX:Cron activity**
  This report provides information related to scheduling the tasks to be executed at a specified time.

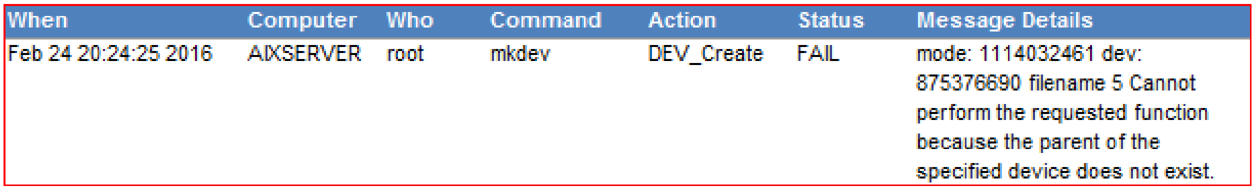


When	Computer	Who	Command	Action	Status	Message Details
Feb 24 03:00:00 2016	AIXSERVER	root	cron	CRON_Start	OK	event = start cron job cmd = /usr/lpp/diagnostics/bin/ run_ssa_healthcheck 1>/dev/null 2>/dev/null time = Sun Jul 12 03:00:00 1970
Feb 24 19:30:00 2016	AIXSERVER	root	cron	CRON_Finish	OK	user = root pid = 77854 time = Wed Feb 24 19:30:00 2016
Feb 24 20:49:15 2016	AIXSERVER	root	at	AT_JobAdd	OK	file name = root.1169520610.a User = root time = Wed Feb 24 20:49:15 2016
Feb 24 20:50:07 2016	AIXSERVER	root	at	AT_JobRemove	OK	file name = root.1169520610.a User = root
Feb 24 21:01:05 2016	AIXSERVER	root	crontab	CRON_JobAdd	OK	file name = Frank Cooper User = Frank Cooper time = Wed Feb 24 21:01:05 2016
Feb 24 21:01:18 2016	AIXSERVER	root	crontab	CRON_JobRemove	OK	file name = Jeff Smith User = Jeff Smith time = Wed Feb 24 21:01:18 2016

```
CRON_JobRemove root OK Mon Jan 22 21:01:18 2016 crontab file name = Frank Cooper User = Frank Cooper
time = Mon Jan 22 21:01:18 2016

CRON_JobAdd root OK Mon Jan 22 21:01:05 2016 crontab file name = Jeff Smith User = Jeff Smith time =
Mon Jan 22 21:01:05 2016

CRON_Start root OK Sun Jul 12 03:00:00 1970 cron □ event = start cron job cmd = /usr/lpp/diagnostics/bin/
run_ssa_healthcheck 1>/dev/null 2>/dev/null time = Sun Jul 12 03:00:00 1970
```

```
CRON_Finish root OK Mon Jan 22 19:30:00 2016 cron user = root pid = 77854 time = Mon Jan 22 19:30:00
2016

AT_JobRemove root OK Mon Jan 22 20:50:07 2016 at file name = root.1169520610.a User = root

AT_JobAdd root OK Mon Jan 22 20:49:15 2016 at file name = root.1169520610.a User = root time = Mon Jan
22 20:49:15 2016
```

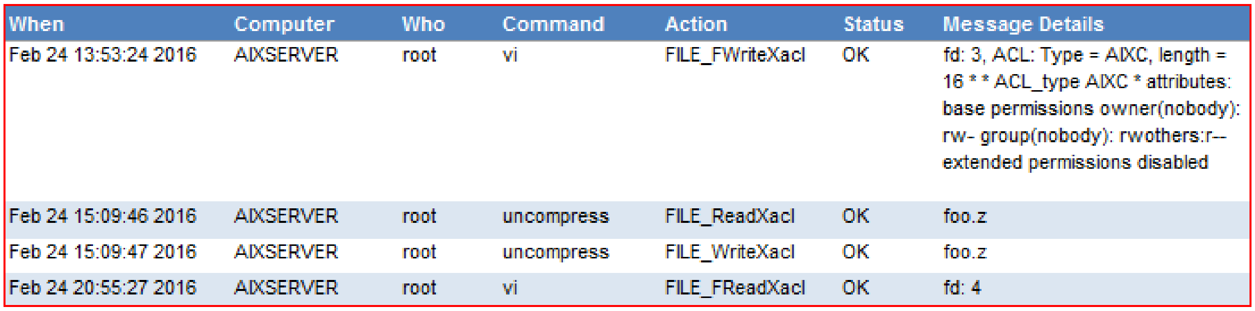
- **IBM AIX:Device management**
  This report provides the information related to device create, configure and change details.



When	Computer	Who	Command	Action	Status	Message Details
Feb 24 20:24:25 2016	AIXSERVER	root	mkdev	DEV_Create	FAIL	mode: 1114032461 dev: 875376690 filename 5 Cannot perform the requested function because the parent of the specified device does not exist.

```
DEV_Create root FAIL Mon Jan 22 20:24:25 2007 mkdev mode: 1114032461 dev: 875376690 filename 5
Cannot perform the requested function because the parent of the specified device does not exist.
```

- **IBM AIX:File access control changes**
  This report provides information related to access control list defined to files by the user.

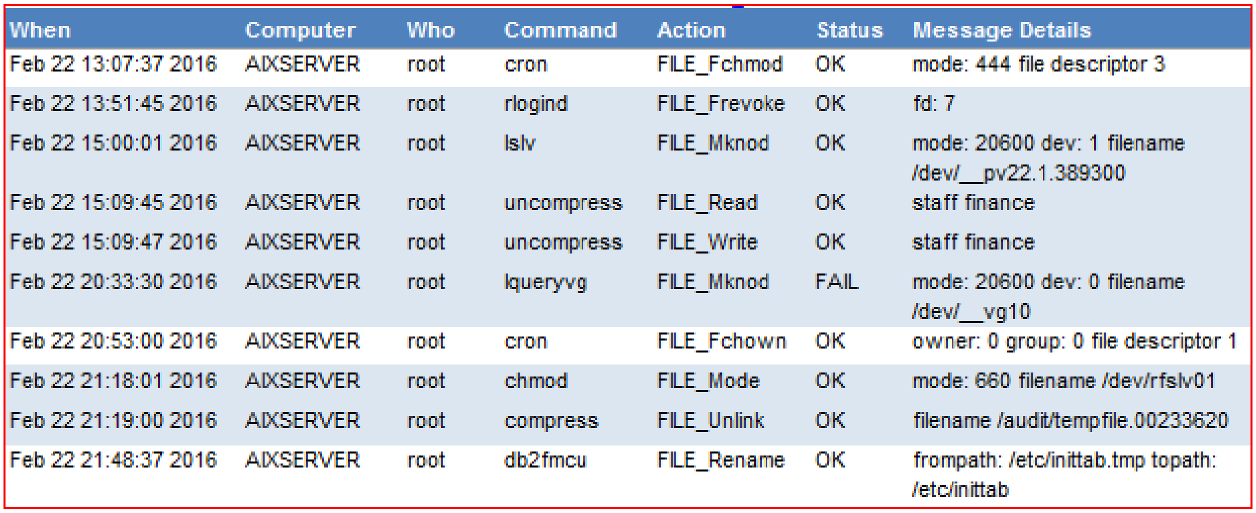


When	Computer	Who	Command	Action	Status	Message Details
Feb 24 13:53:24 2016	AIXSERVER	root	vi	FILE_FWriteXacl	OK	fd: 3, ACL: Type = AIXC, length = 16 * * ACL_type AIXC * attributes: base permissions owner(nobody): rw- group(nobody): rwothers:r-- extended permissions disabled
Feb 24 15:09:46 2016	AIXSERVER	root	uncompress	FILE_ReadXacl	OK	foo.z
Feb 24 15:09:47 2016	AIXSERVER	root	uncompress	FILE_WriteXacl	OK	foo.z
Feb 24 20:55:27 2016	AIXSERVER	root	vi	FILE_FReadXacl	OK	fd: 4

```
FILE_Acl root OK Wed Jan 31 13:51:45 2007 telnetd filename: /dev/pts/2, ACL: length: 16, mode: 0, user: 6,
group: 6, other:6

FILE_Facl root OK Wed Jan 31 13:51:45 2007 rlogind fd: 8, ACL: length: 16, mode: 0, user: 0, group: 0,
other:0

FILE_WriteXacl root OK Wed Jan 17 15:09:47 2007 uncompress foo.z

FILE_FWriteXacl root OK Wed Jan 31 13:53:24 2007 vi fd: 3, ACL: Type = AIXC, length = 16 * * ACL_type
AIXC * attributes: base permissions owner(nobody): rw- group(nobody): rw-others: r-- extended permissions
disabled
```

```
FILE_ReadXacl root OK Wed Jan 17 15:09:46 2007 uncompress

FILE_FReadXacl root OK Tue Jan 23 20:55:27 2007 vi fd: 4
```

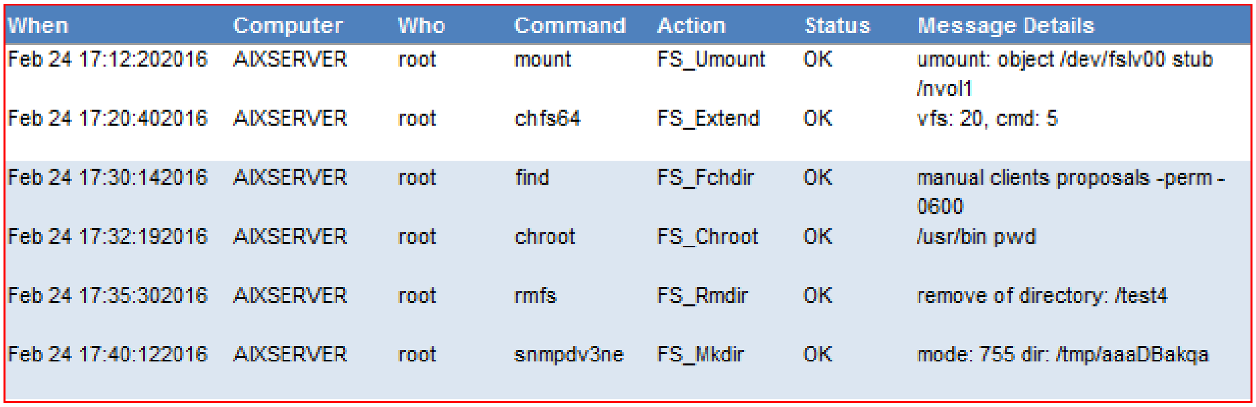
- **IBM AIX: File management**
  This report provides information related to files that are compressed, uncompressed, changing of ownership and renaming by the user.



When	Computer	Who	Command	Action	Status	Message Details
Feb 22 13:07:37 2016	AIXSERVER	root	cron	FILE_Fchmod	OK	mode: 444 file descriptor 3
Feb 22 13:51:45 2016	AIXSERVER	root	rlogind	FILE_Frevoke	OK	fd: 7
Feb 22 15:00:01 2016	AIXSERVER	root	lslv	FILE_Mknod	OK	mode: 20600 dev: 1 filename /dev/__pv22.1.389300
Feb 22 15:09:45 2016	AIXSERVER	root	uncompress	FILE_Read	OK	staff finance
Feb 22 15:09:47 2016	AIXSERVER	root	uncompress	FILE_Write	OK	staff finance
Feb 22 20:33:30 2016	AIXSERVER	root	lqueryvg	FILE_Mknod	FAIL	mode: 20600 dev: 0 filename /dev/__vg10
Feb 22 20:53:00 2016	AIXSERVER	root	cron	FILE_Fchown	OK	owner: 0 group: 0 file descriptor 1
Feb 22 21:18:01 2016	AIXSERVER	root	chmod	FILE_Mode	OK	mode: 660 filename /dev/rfslv01
Feb 22 21:19:00 2016	AIXSERVER	root	compress	FILE_Unlink	OK	filename /audit/tempfile.00233620
Feb 22 21:48:37 2016	AIXSERVER	root	db2fmcu	FILE_Rename	OK	frompath: /etc/inittab.tmp topath: /etc/inittab

```
FILE_Unlink root OK Tue Aug 18 21:19:00 1970 compress filename /audit/tempfile.00233620

FILE_Read root OK Wed Jan 17 15:09:45 2007 uncompress

FILE_Write root OK Wed Jan 17 15:09:47 2007 uncompress

FILE_Unlink root OK Tue Aug 18 21:19:00 1970 compress filename /audit/tempfile.00233620

FILE_Rename root OK Sat Aug 22 21:48:37 1970 db2fmcu frompath: /etc/inittab.tmp topath: /etc/inittab

FILE_Mode root OK Tue Jan 23 21:18:01 2007 chmod mode: 660 filename /dev/rfslv01

FILE_Fchmod root OK Wed Jan 31 13:07:37 2007 cron mode: 444 file descriptor 3

FILE_Fchown root OK Mon Jan 22 20:53:00 2007 cron owner: 0 group: 0 file descriptor 1

FILE_Mknod root FAIL Mon Jan 22 15:00:01 2007 lslv mode: 20600 dev: 1 filename /dev/__pv22.1.389300

FILE_Dupfd root OK Wed Jan 17 15:09:45 2007 sh

FILE_Utimes root OK Wed Jan 17 15:09:46 2007 uncompress

FILE_Accessx root OK Wed Jan 17 15:09:45 2007 sh

FILE_Frevoke root OK Wed Jan 31 13:51:45 2007 rlogind fd: 7
```

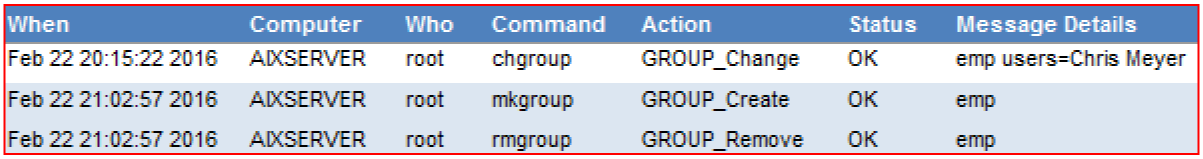
- **IBM AIX: File system activity**
  This report provides information related to files change of current root, make change and remove of directory by the user.



When	Computer	Who	Command	Action	Status	Message Details
Feb 24 17:12:202016	AIXSERVER	root	mount	FS_Umount	OK	umount: object /dev/fslv00 stub /nvol1
Feb 24 17:20:402016	AIXSERVER	root	chfs64	FS_Extend	OK	vfs: 20, cmd: 5
Feb 24 17:30:142016	AIXSERVER	root	find	FS_Fchdir	OK	manual clients proposals -perm -0600
Feb 24 17:32:192016	AIXSERVER	root	chroot	FS_Chroot	OK	/usr/bin pwd
Feb 24 17:35:302016	AIXSERVER	root	rmfs	FS_Rmdir	OK	remove of directory: /test4
Feb 24 17:40:122016	AIXSERVER	root	snmpdv3ne	FS_Mkdir	OK	mode: 755 dir: /tmp/aaaDBakqa

```
FS_Mount root OK Tue Jan 23 20:46:14 2007 mount mount: object /dev/fslv00 stub /nvol1

FS_Extend root OK Mon Jan 22 20:33:30 2007 chfs64 vfs: 20, cmd: 5

FS_Umount root OK Tue Jan 23 20:46:45 2007 mount umount: object /dev/fslv00 stub /nvol1

FS_Chdir root OK Tue Aug 18 21:30:00 1970 cron change current directory to: /

FS_Fchdir root OK Wed Jan 17 14:49:55 2007 find

FS_Rmdir root OK Wed Jan 31 13:36:01 2007 rmfs remove of directory: /test4

FS_Mkdir root OK Wed Jan 31 13:07:20 2007 snmpdv3ne mode: 755 dir: /tmp/aaaDBakqa

FILE_Utimes root OK Wed Jan 17 15:09:46 2007 uncompress
```

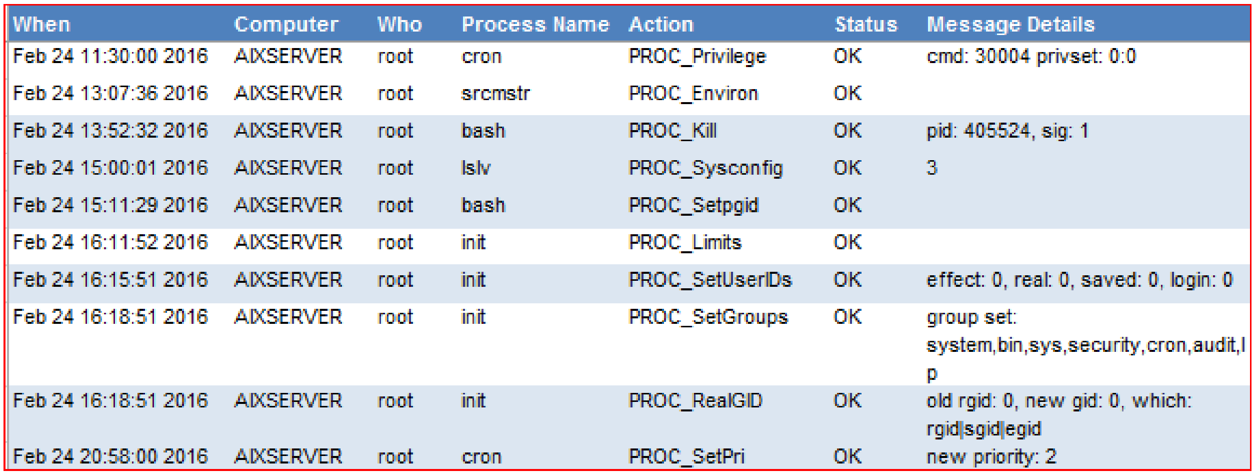
- **IBM AIX: Group management**
  This report provides information related to group changed, created and removed by the user.



When	Computer	Who	Command	Action	Status	Message Details
Feb 22 20:15:22 2016	AIXSERVER	root	chgroup	GROUP_Change	OK	emp users=Chris Meyer
Feb 22 21:02:57 2016	AIXSERVER	root	mkgroup	GROUP_Create	OK	emp
Feb 22 21:02:57 2016	AIXSERVER	root	rmgroup	GROUP_Remove	OK	emp

```
GROUP_Change root OK Mon Jan 22 20:15:22 2016 chgroup emp users=Chris Meyer

 GROUP_Create root OK Tue Jan 23 21:02:57 2016 mkgroup emp

GROUP_Remove root OK Mon Jan 22 20:18:48 2016 rmgroup emp
```

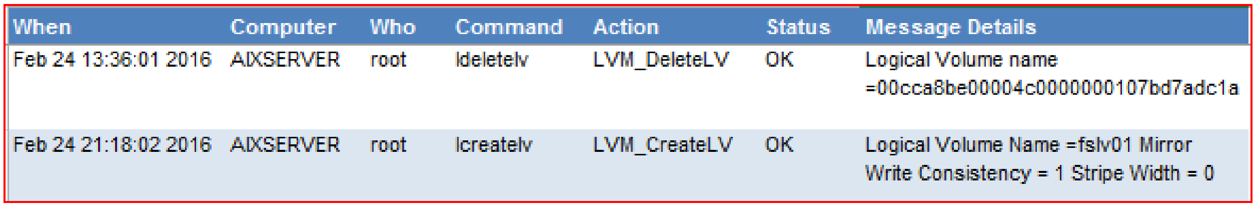
- **IBM AIX: Kernel process activity**
  This report provides information related to the list of kernel processes running on the server.



When	Computer	Who	Process Name	Action	Status	Message Details
Feb 24 11:30:00 2016	AIXSERVER	root	cron	PROC_Privilege	OK	cmd: 30004 privset: 0:0
Feb 24 13:07:36 2016	AIXSERVER	root	srcmstr	PROC_Environ	OK	
Feb 24 13:52:32 2016	AIXSERVER	root	bash	PROC_Kill	OK	pid: 405524, sig: 1
Feb 24 15:00:01 2016	AIXSERVER	root	lslv	PROC_Sysconfig	OK	3
Feb 24 15:11:29 2016	AIXSERVER	root	bash	PROC_Setpgid	OK	
Feb 24 16:11:52 2016	AIXSERVER	root	init	PROC_Limits	OK	
Feb 24 16:15:51 2016	AIXSERVER	root	init	PROC_SetUserIDs	OK	effect: 0, real: 0, saved: 0, login: 0
Feb 24 16:18:51 2016	AIXSERVER	root	init	PROC_SetGroups	OK	group set: system,bin,sys,security,cron,audit,lp
Feb 24 16:18:51 2016	AIXSERVER	root	init	PROC_RealGID	OK	old rgid: 0, new gid: 0, which: rgid|sgid|egid
Feb 24 20:58:00 2016	AIXSERVER	root	cron	PROC_SetPri	OK	new priority: 2

```
PROC_Sysconfig root OK Mon Jan 22 15:00:01 2007 lslv 3

PROC_Environ root OK Wed Jan 31 13:07:36 2007 srcmstr

PROC_Limits root OK Fri Jan 19 16:11:52 2007 init

PROC_SetPri root OK Mon Jan 22 20:58:00 2007 cron new priority: 2

PROC_Privilege root OK Thu Jan 18 11:30:00 2007 cron cmd: 30004 privset: 0:0

PROC_Kill root OK Wed Jan 31 13:52:32 2007 bash pid: 405524, sig: 1

PROC_Setpgid root OK Wed Jan 17 15:11:29 2007 bash

PROC_SetGroups root OK Fri Jan 19 16:18:51 2007 init group set: system,bin,sys,security,cron,audit,lp
```

- **IBM AIX: Logical volume management activity**
  This report provides information related to creation and deletion of logical volume.

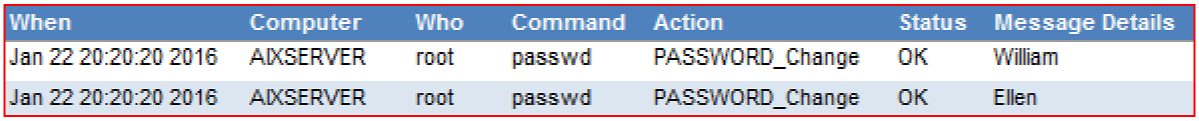


When	Computer	Who	Command	Action	Status	Message Details
Feb 24 13:36:01 2016	AIXSERVER	root	ldeletelv	LVM_DeleteLV	OK	Logical Volume name =00cca8be00004c0000000107bd7adc1a
Feb 24 21:18:02 2016	AIXSERVER	root	lcreatelv	LVM_CreateLV	OK	Logical Volume Name =fslv01 Mirror Write Consistency = 1 Stripe Width = 0

```
LVM_CreateLV root OK Tue Jan 23 21:18:02 2007 lcreatelv Logical Volume Name =fslv01 Mirror Write
Consistency = 1 Stripe Width = 0
```

```
LVM_DeleteLV root OK Wed Jan 31 13:36:01 2007 ldeletelv Logical Volume name
=00cca8be00004c0000000107bd7adc1a
```

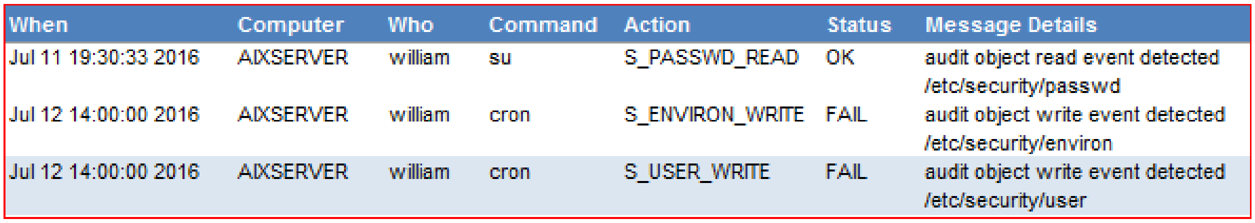
- **IBM AIX: Password changed**
  This report provides information related to password changed, that user root has changed the password for the users specified in the message details.



When	Computer	Who	Command	Action	Status	Message Details
Jan 22 20:20:20 2016	AIXSERVER	root	passwd	PASSWORD_Change	OK	William
Jan 22 20:20:20 2016	AIXSERVER	root	passwd	PASSWORD_Change	OK	Ellen

```
PASSWORD_Change root OK Mon Jan 22 20:20:20 2007 passwd William

PASSWORD_Change root OK Mon Jan 22 20:20:20 2007 passwd Ellen
```

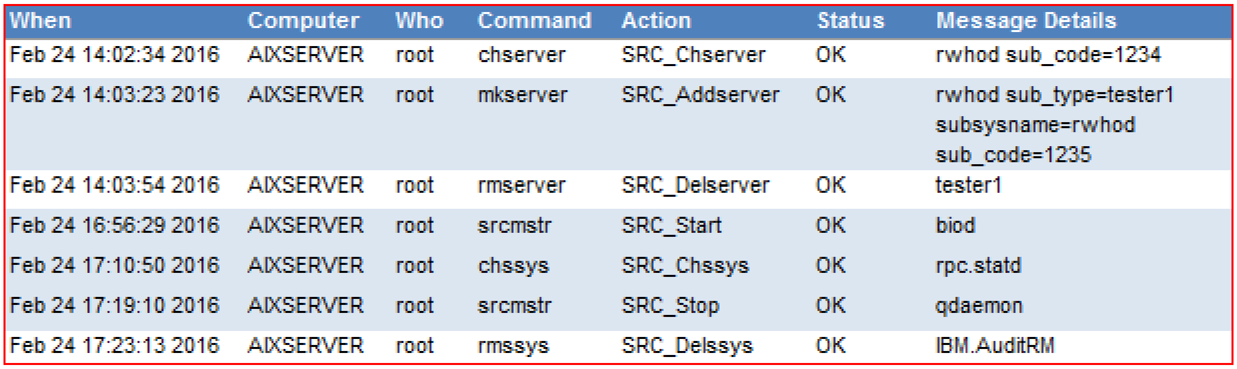
- **IBM AIX: Security objects audit**
  This report provides information related to audit being performed on the security objects by the user.



When	Computer	Who	Command	Action	Status	Message Details
Jul 11 19:30:33 2016	AIXSERVER	william	su	S_PASSWD_READ	OK	audit object read event detected /etc/security/passwd
Jul 12 14:00:00 2016	AIXSERVER	william	cron	S_ENVIRON_WRITE	FAIL	audit object write event detected /etc/security/environ
Jul 12 14:00:00 2016	AIXSERVER	william	cron	S_USER_WRITE	FAIL	audit object write event detected /etc/security/user

```
S_PASSWD_READ william OK Sat Jul 11 19:30:33 1970 su   audit object read event detected
/etc/security/passwd

S_USER_WRITE william FAIL Sun Jul 12 14:00:00 1970 cron audit object write event detected
/etc/security/user

S_ENVIRON_WRITE william FAIL Sun Jul 12 14:00:00 1970 cron  audit object write event detected
/etc/security/environ
```

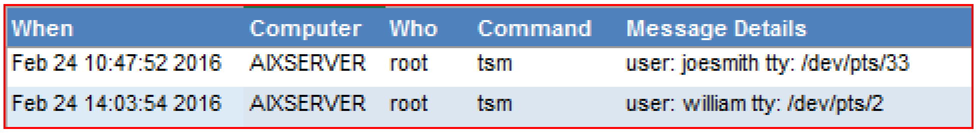
- **IBM AIX: System resource controller**
  This report provides the information related to subroutines and subsystem on the server.



When	Computer	Who	Command	Action	Status	Message Details
Feb 24 14:02:34 2016	AIXSERVER	root	chserver	SRC_Chserver	OK	rwhod sub_code=1234
Feb 24 14:03:23 2016	AIXSERVER	root	mkserver	SRC_Addserver	OK	rwhod sub_type=tester1 subsysname=rwhod sub_code=1235
Feb 24 14:03:54 2016	AIXSERVER	root	rmserver	SRC_Delserver	OK	tester1
Feb 24 16:56:29 2016	AIXSERVER	root	srcmstr	SRC_Start	OK	biod
Feb 24 17:10:50 2016	AIXSERVER	root	chssys	SRC_Chssys	OK	rpc.statd
Feb 24 17:19:10 2016	AIXSERVER	root	srcmstr	SRC_Stop	OK	qdaemon
Feb 24 17:23:13 2016	AIXSERVER	root	rmssys	SRC_Delssys	OK	IBM.AuditRM

```
SRC_Start root OK Tue Jan 30 16:56:29 2007 srcmstr biod

SRC_Stop root OK Tue Jan 30 17:19:10 2007 srcmstr qdaemon

SRC_Addssys root OK Tue Jan 30 17:23:13 2007 mkssys IBM.CSMAgentRM subsysname=IBM.CSMAgentRM
synonym= cmdargs= path=/usr/sbin/rsct/bin/ IBM.CSMAgentRMd uid=0 auditid=0 standin=/dev/console
standout=/dev/console standerr=/var/ct/ IBM.CSMAgentRM.stderr action=1 multi=0 contact=3 svrkey=0
svrmtype=0 priority=20 signorm=0 sigforce=0 display=1 waittime=20 grpname=rsct_rm

SRC_Chssys root OK Tue Jan 30 17:10:50 2007 chssys rpc.statd

SRC_Delssys root OK Tue Jan 30 17:23:13 2007 rmssys IBM.AuditRM

SRC_Delserver root OK Wed Jan 31 14:03:54 2007 rmserver tester1
```

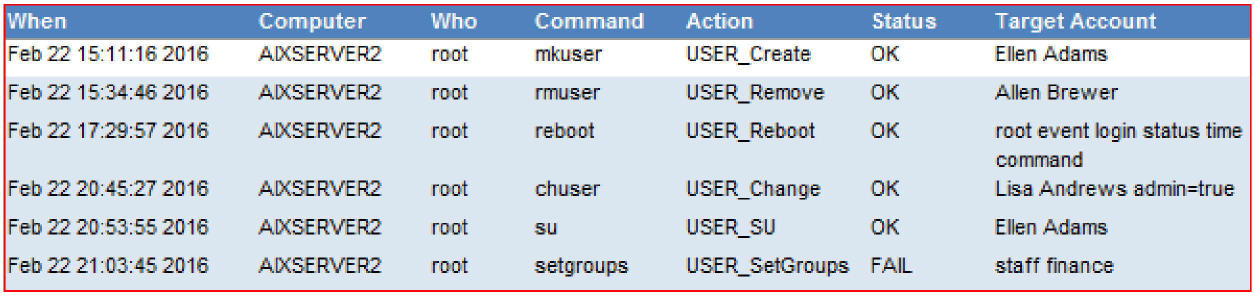
- **IBM AIX: User authentication failed**
  This report provides information related to user authentication failed logins.



When	Computer	Who	Command	Message Details
Feb 24 10:47:52 2016	AIXSERVER	root	tsm	user: joesmith tty: /dev/pts/33
Feb 24 14:03:54 2016	AIXSERVER	root	tsm	user: william tty: /dev/pts/2

```
USER_Login root FAIL_AUTH Mon Jan 07 10:47:52 2013 tsm user: joesmith tty: /dev/pts/33

USER_Login root FAIL_AUTH Mon Jan 07 10:47:52 2013 tsm user: william tty: /dev/pts/2
```

- **IBM AIX: User management**
  This report provides information related to user created, removed and changed details.



When	Computer	Who	Command	Action	Status	Target Account
Feb 22 15:11:16 2016	AIXSERVER2	root	mkuser	USER_Create	OK	Ellen Adams
Feb 22 15:34:46 2016	AIXSERVER2	root	rmuser	USER_Remove	OK	Allen Brewer
Feb 22 17:29:57 2016	AIXSERVER2	root	reboot	USER_Reboot	OK	root event login status time command
Feb 22 20:45:27 2016	AIXSERVER2	root	chuser	USER_Change	OK	Lisa Andrews admin=true
Feb 22 20:53:55 2016	AIXSERVER2	root	su	USER_SU	OK	Ellen Adams
Feb 22 21:03:45 2016	AIXSERVER2	root	setgroups	USER_SetGroups	FAIL	staff finance

USER_Change root OK Mon Jan 22 20:45:27 2007 chuser Lisa Andrews admin=true

USER_Remove root OK Wed Jan 17 15:34:46 2007 rmuser Allen Brewer

USER_Create root OK Wed Jan 17 15:11:16 2007 mkuser Ellen Adams

USER_SU root OK Tue Jan 23 20:53:55 2007 su Ellen Adams

Import Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence

- Categories
- Alerts
- Token Templates
- Flex Reports
- Knowledge Object

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

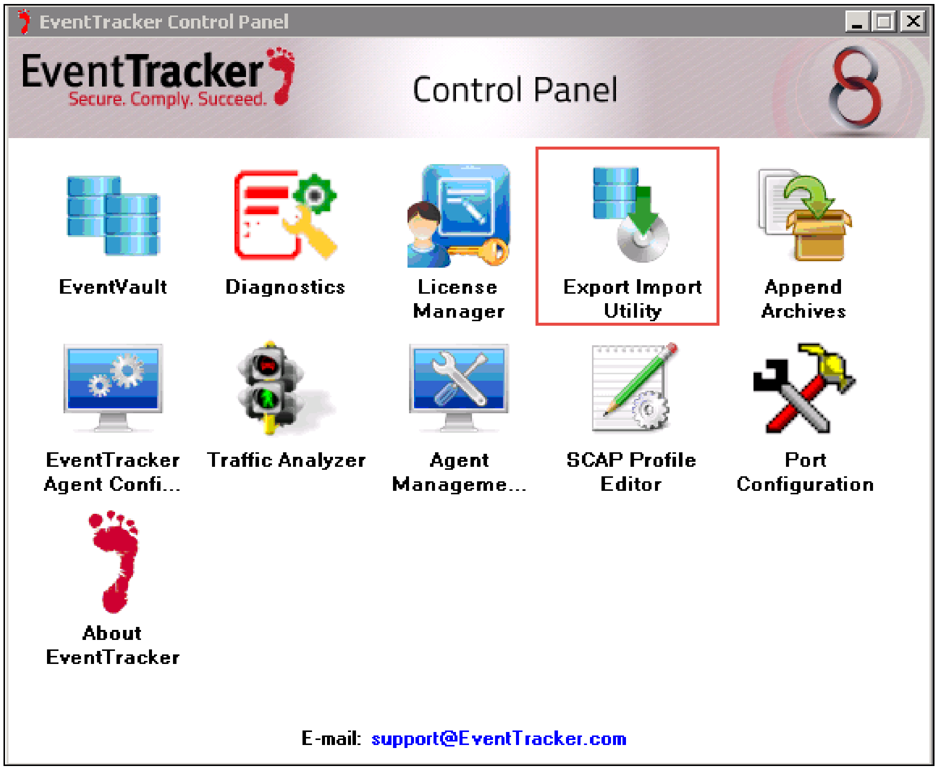
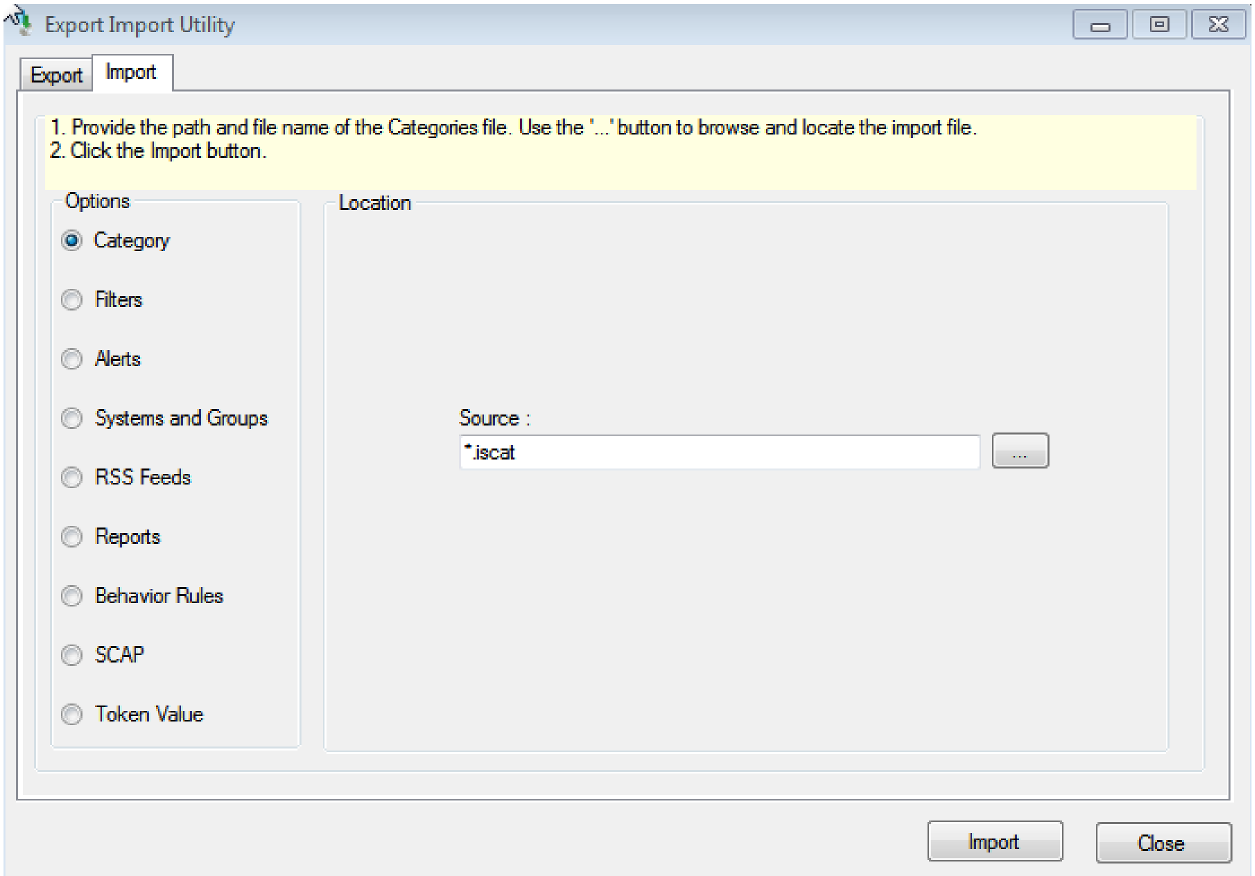


Figure 1

Import **Categories, Alerts, Flex Reports and Knowledge Objects** as given below.

Categories

1. Click **Category** option, and then click the browse [...] button.



Export Import Utility

1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

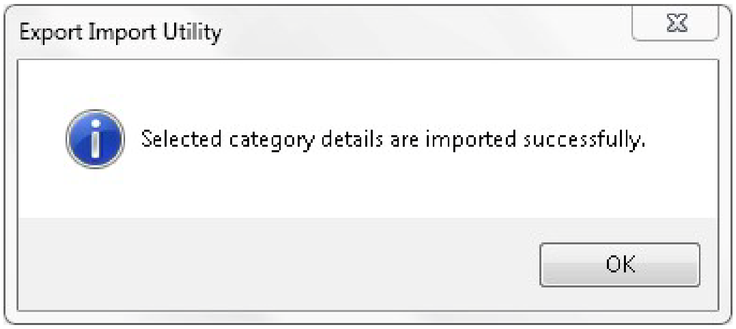
Source : *.iscat

Figure 2

2. Locate **All IBM AIX categories.iscat** file, and then click the **Open** button.

3. To import categories, click the **Import** button.

   EventTracker displays success message.



Export Import Utility

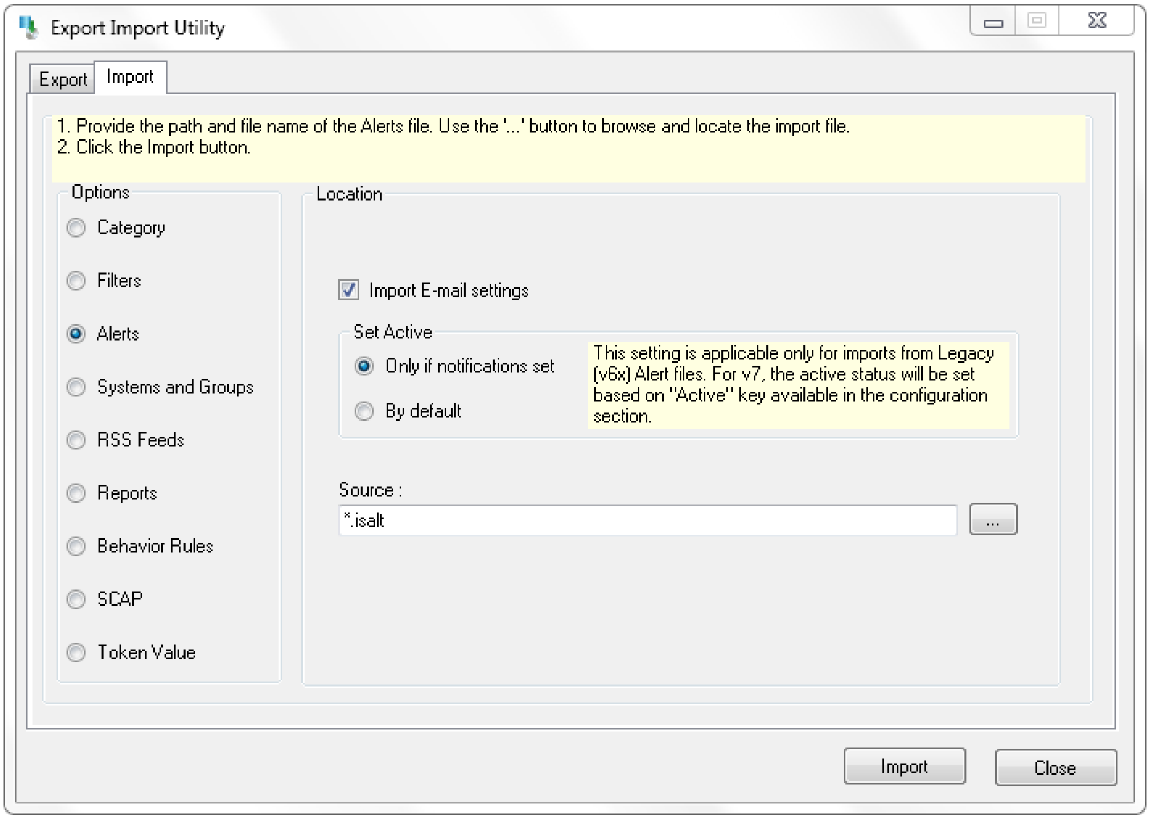
Selected category details are imported successfully.

Figure 3

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

Alerts

1. Click **Alert** option, and then click the **browse** [...] button.



1. Provide the path and file name of the Alerts file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

○ Category
○ Filters
● Alerts
○ Systems and Groups
○ RSS Feeds
○ Reports
○ Behavior Rules
○ SCAP
○ Token Value

Location

☑ Import E-mail settings

Set Active

● Only if notifications set
○ By default

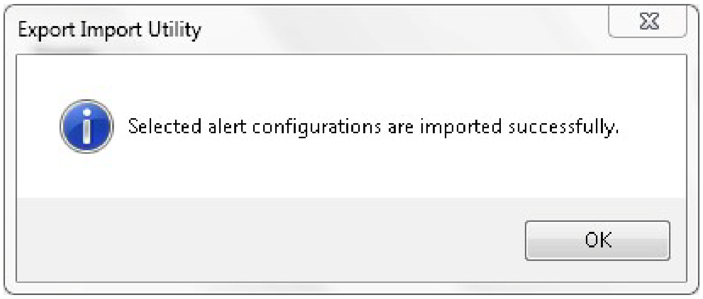
This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.

Source : *.isalt

Figure 4

2. Locate **All IBM AIX alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

   EventTracker displays success message.



Export Import Utility

Selected alert configurations are imported successfully.

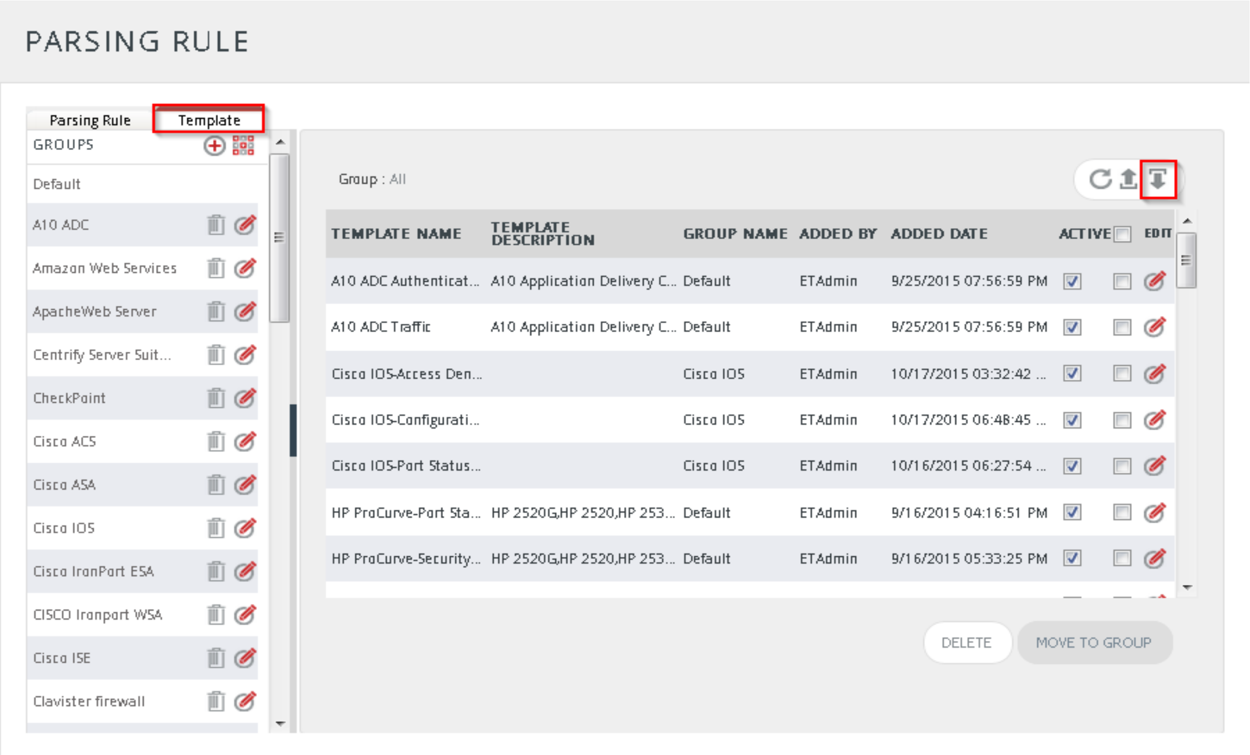
Figure 5

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

Token Templates

1. Click the **Admin** menu, and then click **Parsing rule**.

2. Select **Template** tab, and then click on ⤓ '**Import**' option.

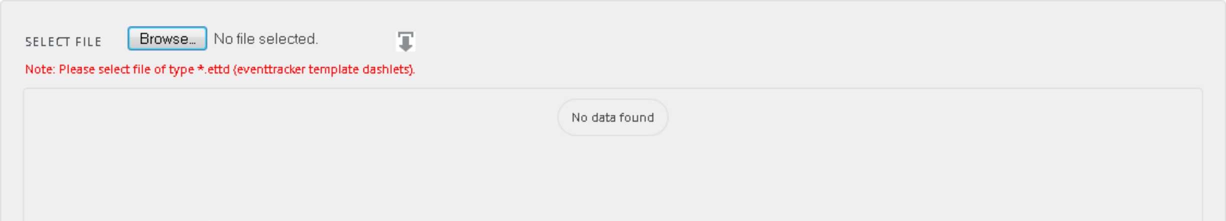


PARSING RULE

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	☑	☐	✎
A10 ADC Traffic	A10 Application Delivery C...	Default	ETAdmin	9/25/2015 07:56:59 PM	☑	☐	✎
Cisco IOS-Access Den...		Cisco IOS	ETAdmin	10/17/2015 03:32:42 ...	☑	☐	✎
Cisco IOS-Configurati...		Cisco IOS	ETAdmin	10/17/2015 06:48:45 ...	☑	☐	✎
Cisco IOS-Port Status...		Cisco IOS	ETAdmin	10/16/2015 06:27:54 ...	☑	☐	✎
HP ProCurve-Port Sta...	HP 2520G,HP 2520,HP 253...	Default	ETAdmin	9/16/2015 04:16:51 PM	☑	☐	✎
HP ProCurve-Security...	HP 2520G,HP 2520,HP 253...	Default	ETAdmin	9/16/2015 05:33:25 PM	☑	☐	✎

Figure 8

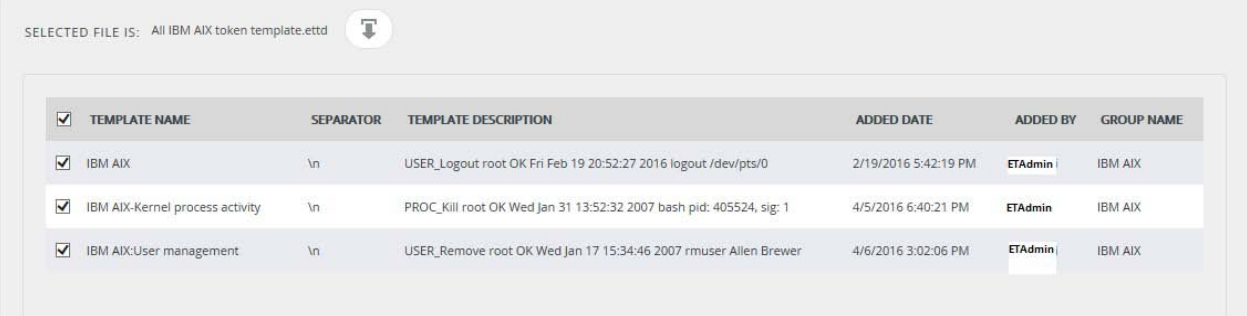
3. Click on **Browse** button.



Note: Please select file of type *.ettd (eventtracker template dashlets).

Figure 9

4. Locate **All IBM AIX token template.ettd** file, and then click the **Open** button

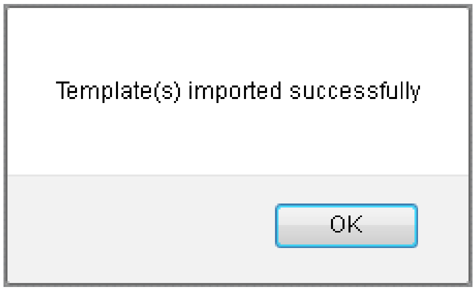


SELECTED FILE IS: All IBM AIX token template.ettd

☑	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
☑	IBM AIX	\n	USER_Logout root OK Fri Feb 19 20:52:27 2016 logout /dev/pts/0	2/19/2016 5:42:19 PM	ETAdmin	IBM AIX
☑	IBM AIX-Kernel process activity	\n	PROC_Kill root OK Wed Jan 31 13:52:32 2007 bash pid: 405524, sig: 1	4/5/2016 6:40:21 PM	ETAdmin	IBM AIX
☑	IBM AIX:User management	\n	USER_Remove root OK Wed Jan 17 15:34:46 2007 rmuser Allen Brewer	4/6/2016 3:02:06 PM	ETAdmin	IBM AIX

Figure 10

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



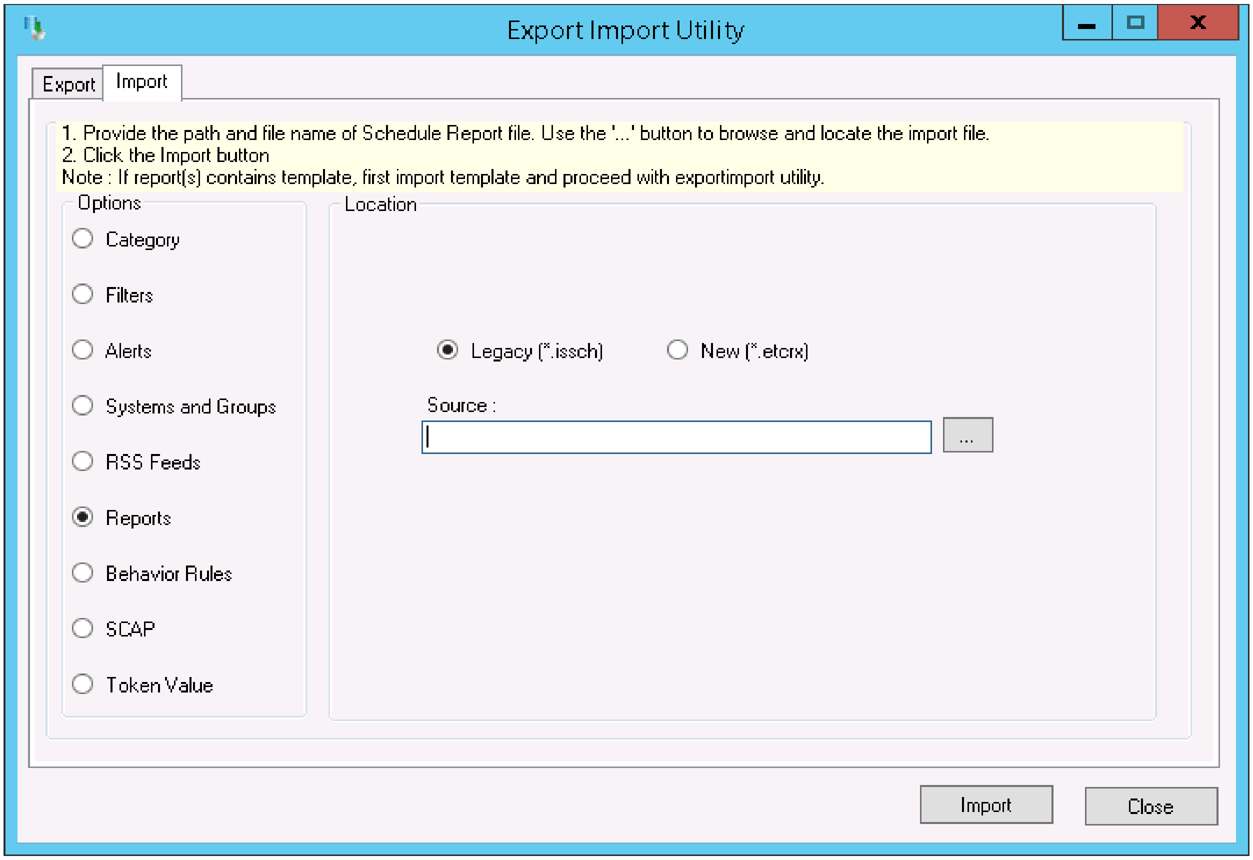
Template(s) imported successfully

Figure 11

6. Click on **OK** button.

Flex Reports

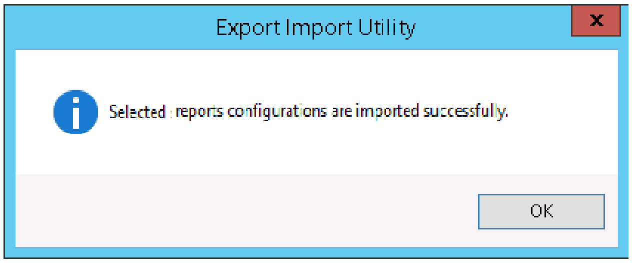
1. Click **Report** option, and then click the browse [...] button



1. Provide the path and file name of Schedule Report file. Use the '...' button to browse and locate the import file.
2. Click the Import button
Note : If report(s) contains template, first import template and proceed with exportimport utility.

Figure 12

2. Locate the **All IBM AIX flex reports.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports, EventTracker displays success message.



Selected reports configurations are imported successfully.

Figure 13

Knowledge Object

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

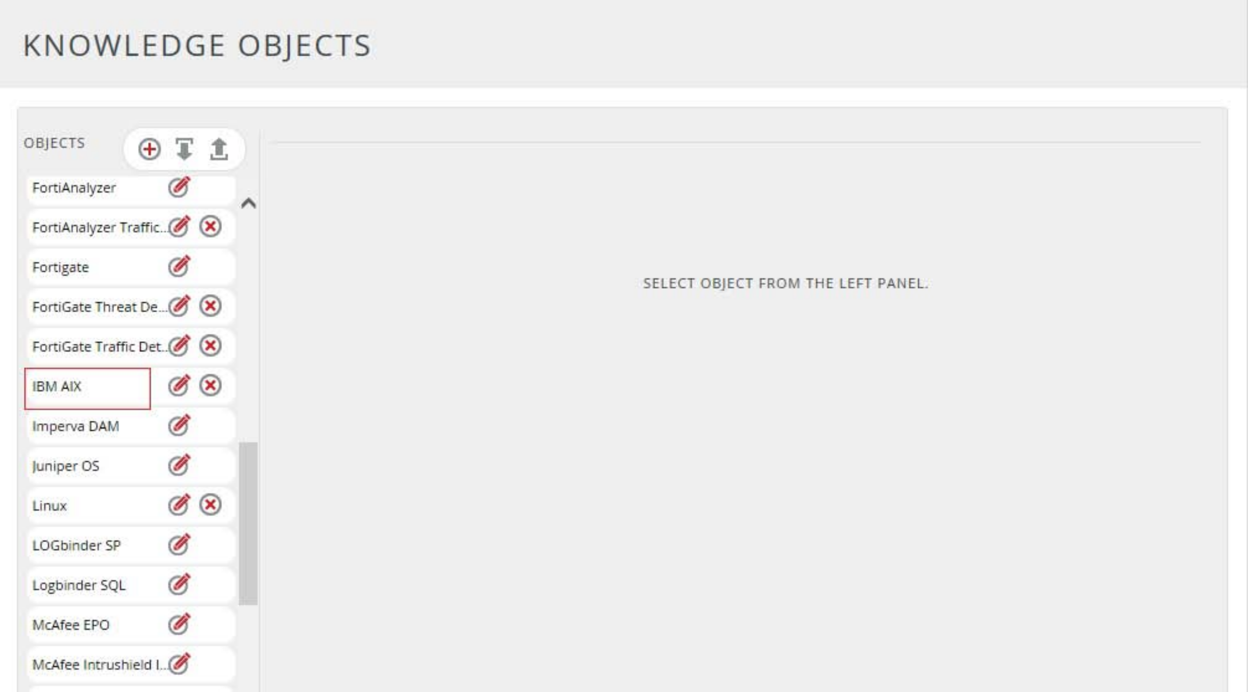


Figure 14

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

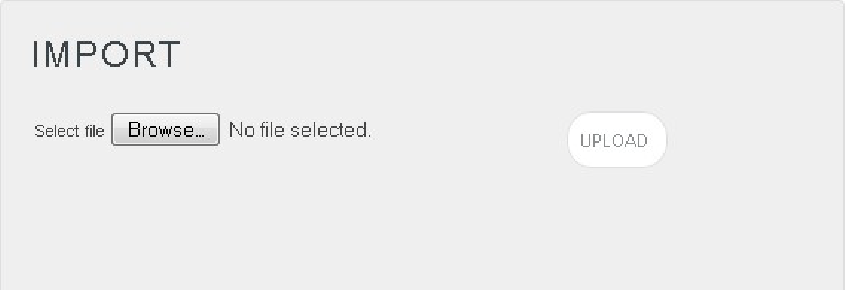
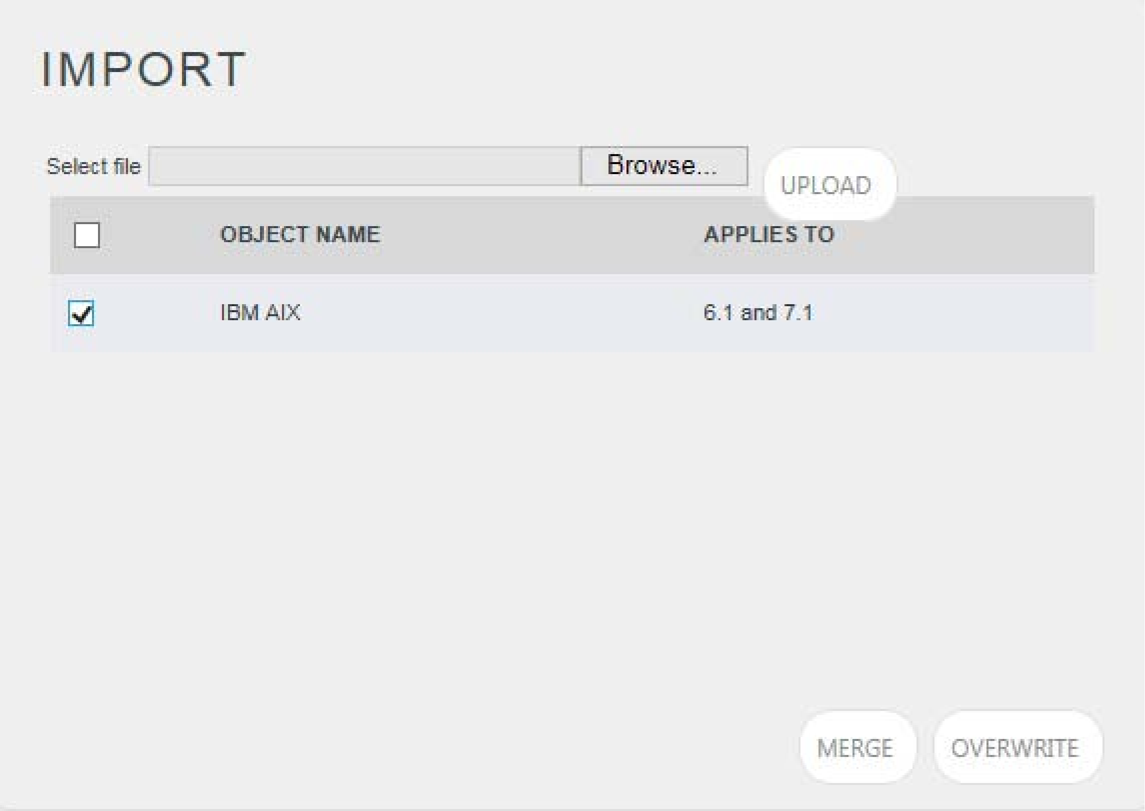


Figure 15

4. Locate **All IBM AIX knowledge object.etko** file, and then click the **UPLOAD** button.

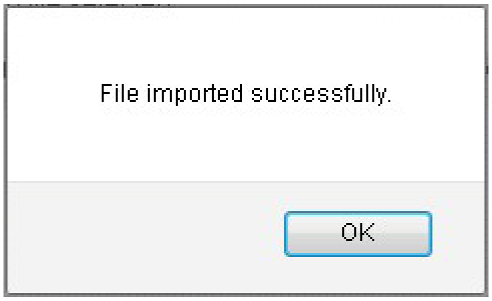


IMPORT

☐	OBJECT NAME	APPLIES TO
☑	IBM AIX	6.1 and 7.1

Figure 16

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



File imported successfully.

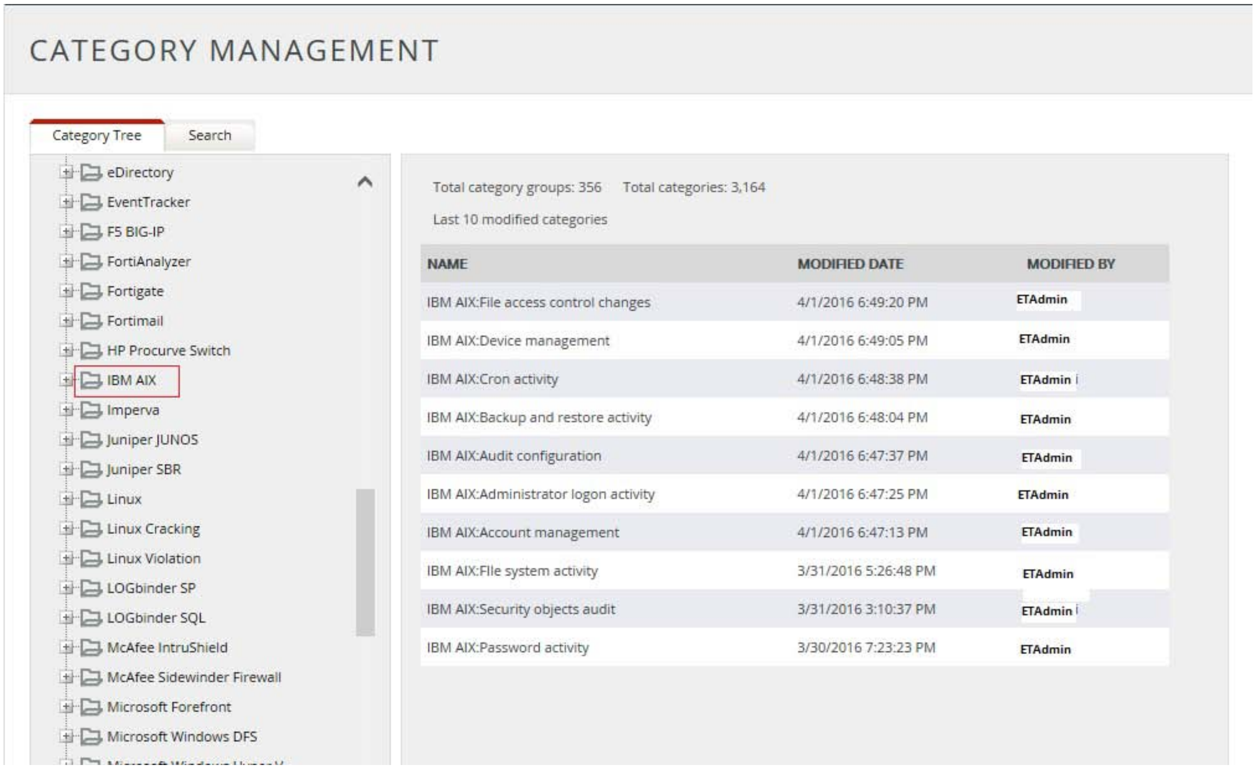
Figure 17

6. Click on **OK** button.

Verifying IBM AIX knowledge pack in EventTracker

IBM AIX Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **IBM AIX** group folder to view the imported categories.



Total category groups: 356 Total categories: 3,164

Last 10 modified categories

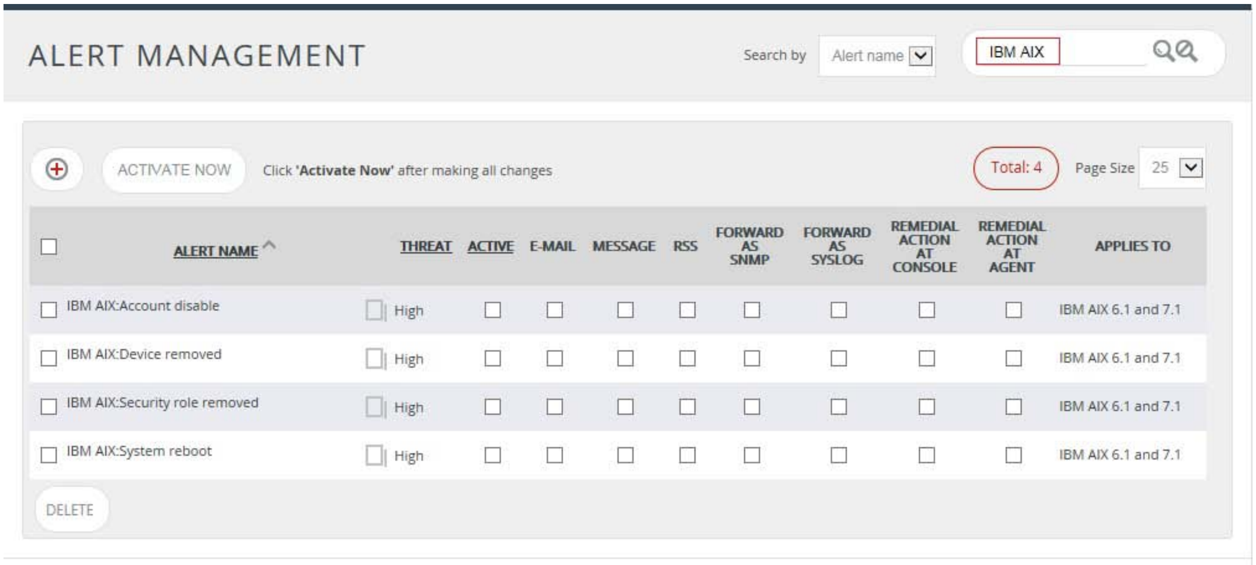
NAME	MODIFIED DATE	MODIFIED BY
IBM AIX:File access control changes	4/1/2016 6:49:20 PM	ETAdmin
IBM AIX:Device management	4/1/2016 6:49:05 PM	ETAdmin
IBM AIX:Cron activity	4/1/2016 6:48:38 PM	ETAdmin
IBM AIX:Backup and restore activity	4/1/2016 6:48:04 PM	ETAdmin
IBM AIX:Audit configuration	4/1/2016 6:47:37 PM	ETAdmin
IBM AIX:Administrator logon activity	4/1/2016 6:47:25 PM	ETAdmin
IBM AIX:Account management	4/1/2016 6:47:13 PM	ETAdmin
IBM AIX:FIle system activity	3/31/2016 5:26:48 PM	ETAdmin
IBM AIX:Security objects audit	3/31/2016 3:10:37 PM	ETAdmin
IBM AIX:Password activity	3/30/2016 7:23:23 PM	ETAdmin

Figure 18

IBM AIX Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In **Search** field, type '**IBM AIX**', and then click the **Go** button.

   Alert Management page will display all the imported IBM AIX alerts.



ALERT MANAGEMENT

Search by Alert name IBM AIX

ACTIVATE NOW Click **'Activate Now'** after making all changes

Total: 4 Page Size 25

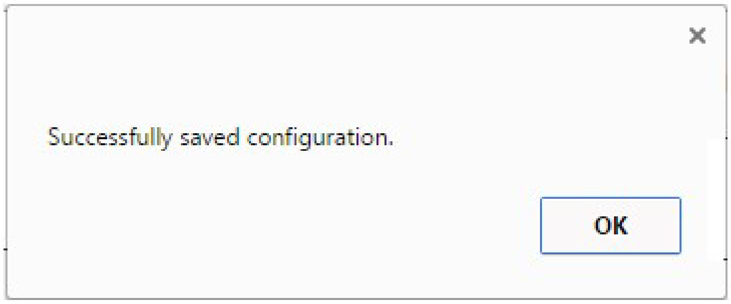
□	ALERT NAME	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
□	IBM AIX:Account disable	High	□	□	□	□	□	□	□	□	IBM AIX 6.1 and 7.1
□	IBM AIX:Device removed	High	□	□	□	□	□	□	□	□	IBM AIX 6.1 and 7.1
□	IBM AIX:Security role removed	High	□	□	□	□	□	□	□	□	IBM AIX 6.1 and 7.1
□	IBM AIX:System reboot	High	□	□	□	□	□	□	□	□	IBM AIX 6.1 and 7.1

DELETE

Figure 19

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.



Successfully saved configuration.

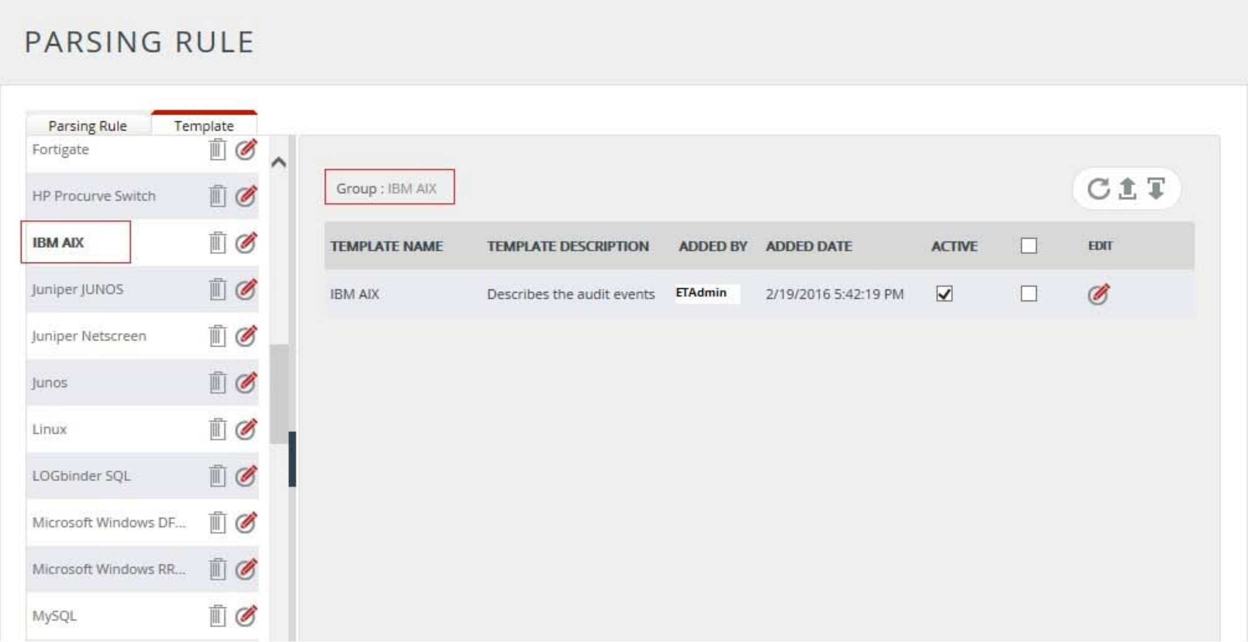
Figure 20

5. Click **OK**, 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.

IBM AIX Token Template

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



TEMPLATE NAME	TEMPLATE DESCRIPTION	ADDED BY	ADDED DATE	ACTIVE	□	EDIT
IBM AIX	Describes the audit events	ETAdmin	2/19/2016 5:42:19 PM	☑	□	

Figure 21

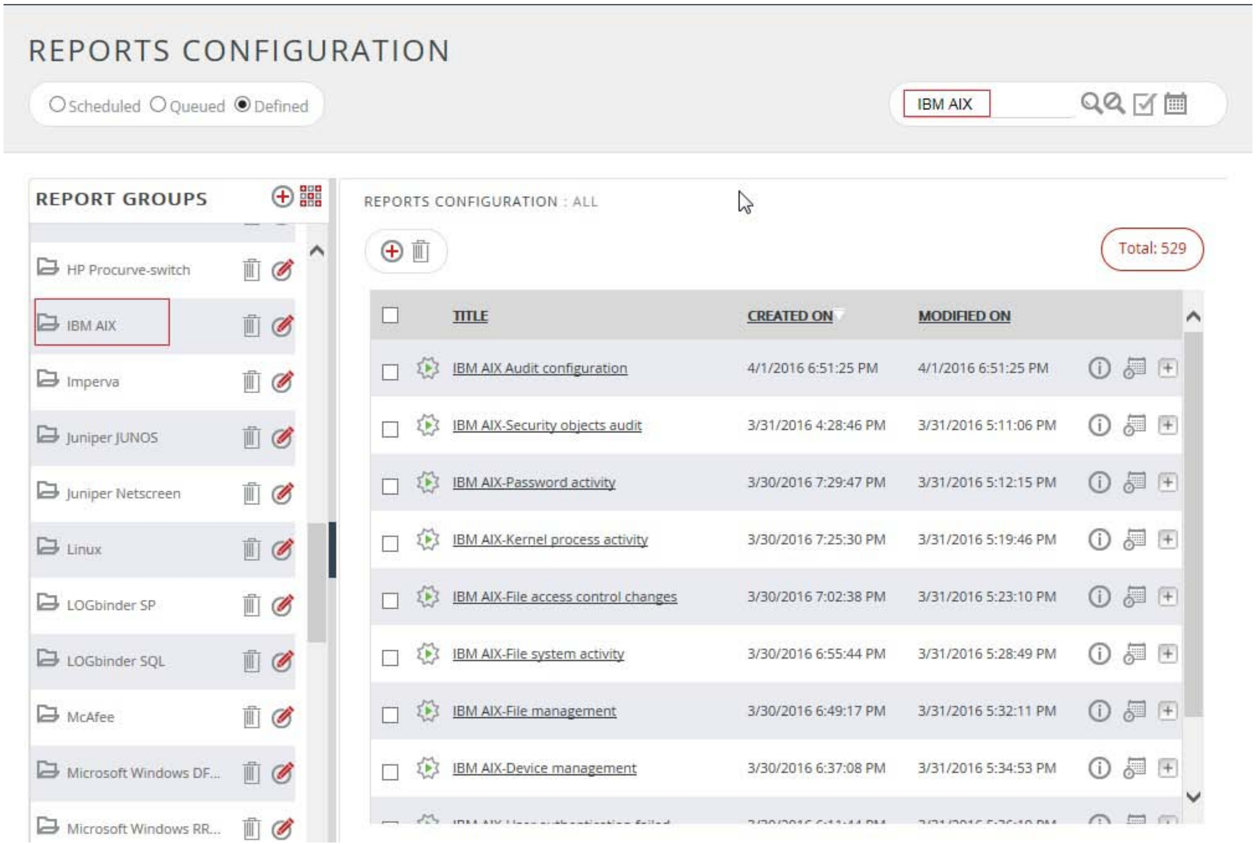
IBM AIX Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then select **Configuration**.
3. In **Reports Configuration** pane, select **Defined** option.

   EventTracker displays **Defined** page.

4. In search box enter '**IBM AIX'**, and then click the **Search** button.

   EventTracker displays Flex reports of IBM AIX

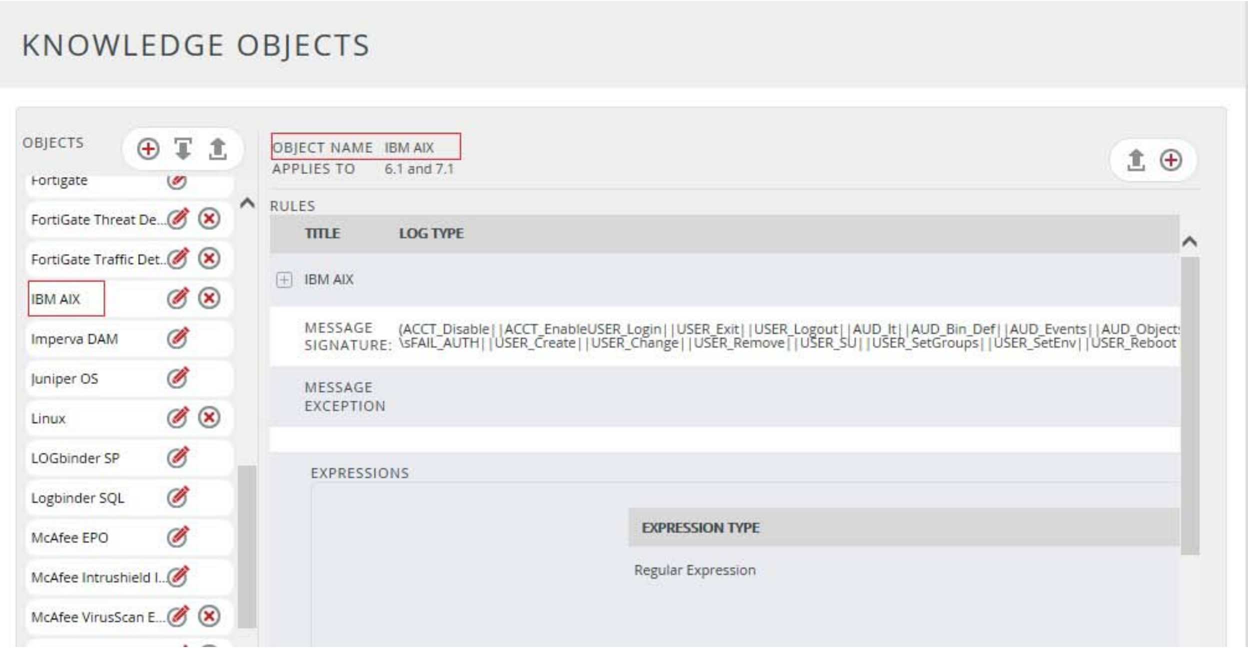


□	TITLE	CREATED ON	MODIFIED ON
□	IBM AIX Audit configuration	4/1/2016 6:51:25 PM	4/1/2016 6:51:25 PM
□	IBM AIX-Security objects audit	3/31/2016 4:28:46 PM	3/31/2016 5:11:06 PM
□	IBM AIX-Password activity	3/30/2016 7:29:47 PM	3/31/2016 5:12:15 PM
□	IBM AIX-Kernel process activity	3/30/2016 7:25:30 PM	3/31/2016 5:19:46 PM
□	IBM AIX-File access control changes	3/30/2016 7:02:38 PM	3/31/2016 5:23:10 PM
□	IBM AIX-File system activity	3/30/2016 6:55:44 PM	3/31/2016 5:28:49 PM
□	IBM AIX-File management	3/30/2016 6:49:17 PM	3/31/2016 5:32:11 PM
□	IBM AIX-Device management	3/30/2016 6:37:08 PM	3/31/2016 5:34:53 PM

Figure 22

IBM AIX Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**
2. Scroll down and select **IBM AIX** in **Objects** pane. Imported **IBM AIX** object details are shown.



OBJECT NAME IBM AIX
APPLIES TO 6.1 and 7.1

RULES

TITLE	LOG TYPE
IBM AIX	

MESSAGE SIGNATURE: (ACCT_Disable||ACCT_EnableUSER_Login||USER_Exit||USER_Logout||AUD_It||AUD_Bin_Def||AUD_Events||AUD_Object: \sFAIL_AUTH||USER_Create||USER_Change||USER_Remove||USER_SU||USER_SetGroups||USER_SetEnv||USER_Reboot

MESSAGE EXCEPTION

EXPRESSIONS

EXPRESSION TYPE
Regular Expression

Figure 23

Create Flex Dashboards in EventTracker

Schedule Reports

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

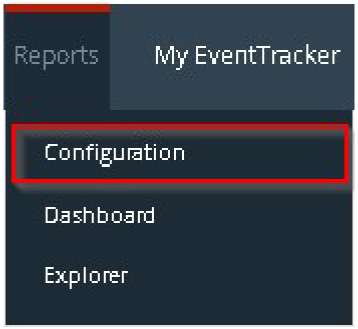
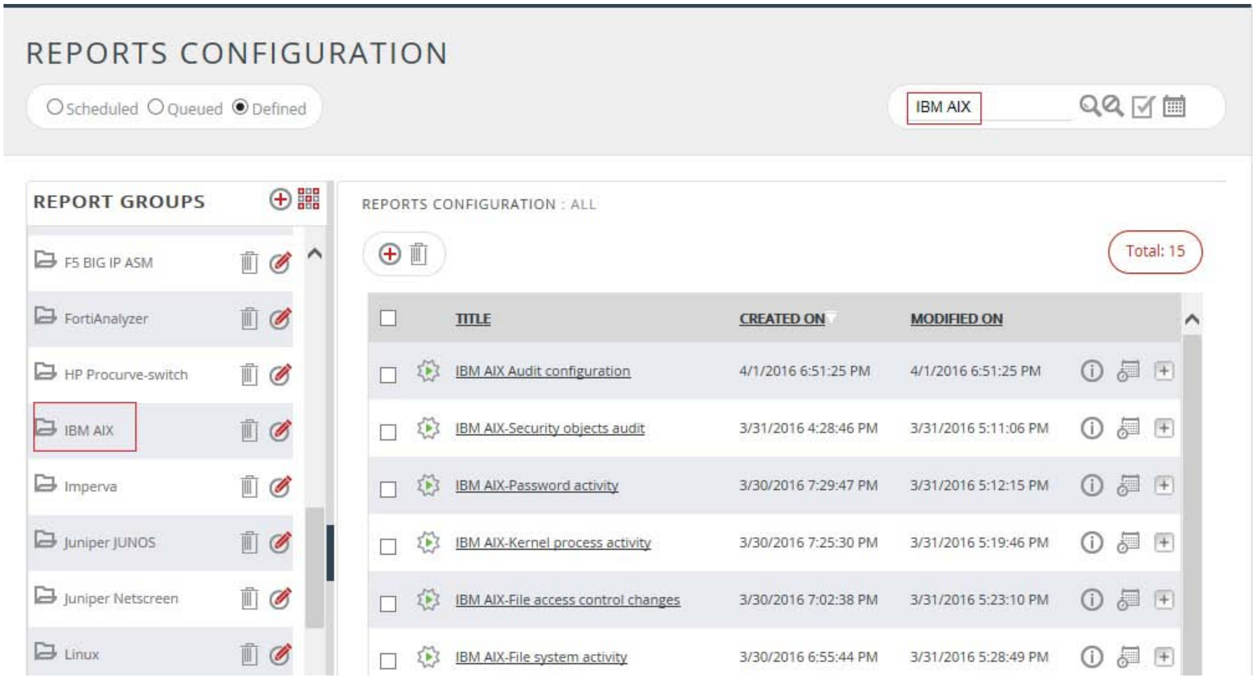


Figure 24

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



REPORTS CONFIGURATION

○ Scheduled ○ Queued ● Defined

IBM AIX

REPORT GROUPS

- F5 BIG IP ASM
- FortiAnalyzer
- HP Procurve-switch
- IBM AIX
- Imperva
- Juniper JUNOS
- Juniper Netscreen
- Linux

REPORTS CONFIGURATION : ALL

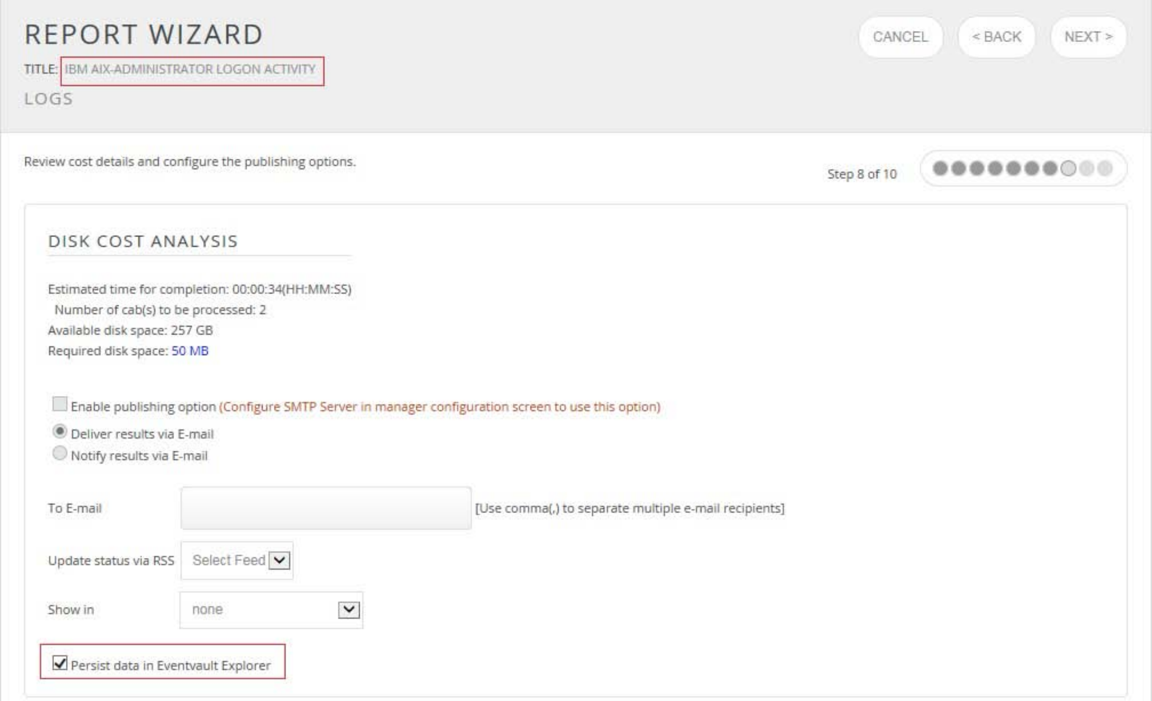
Total: 15

□	TITLE	CREATED ON	MODIFIED ON
□	IBM AIX Audit configuration	4/1/2016 6:51:25 PM	4/1/2016 6:51:25 PM
□	IBM AIX-Security objects audit	3/31/2016 4:28:46 PM	3/31/2016 5:11:06 PM
□	IBM AIX-Password activity	3/30/2016 7:29:47 PM	3/31/2016 5:12:15 PM
□	IBM AIX-Kernel process activity	3/30/2016 7:25:30 PM	3/31/2016 5:19:46 PM
□	IBM AIX-File access control changes	3/30/2016 7:02:38 PM	3/31/2016 5:23:10 PM
□	IBM AIX-File system activity	3/30/2016 6:55:44 PM	3/31/2016 5:28:49 PM

Figure 25

3. Select **IBM AIX** in report groups. Check **defined** dialog box.

4. Click on '**schedule**' to plan a report for later execution.



REPORT WIZARD

TITLE: IBM AIX-ADMINISTRATOR LOGON ACTIVITY

LOGS

Review cost details and configure the publishing options.

Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:00:34(HH:MM:SS)
Number of cab(s) to be processed: 2
Available disk space: 257 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]

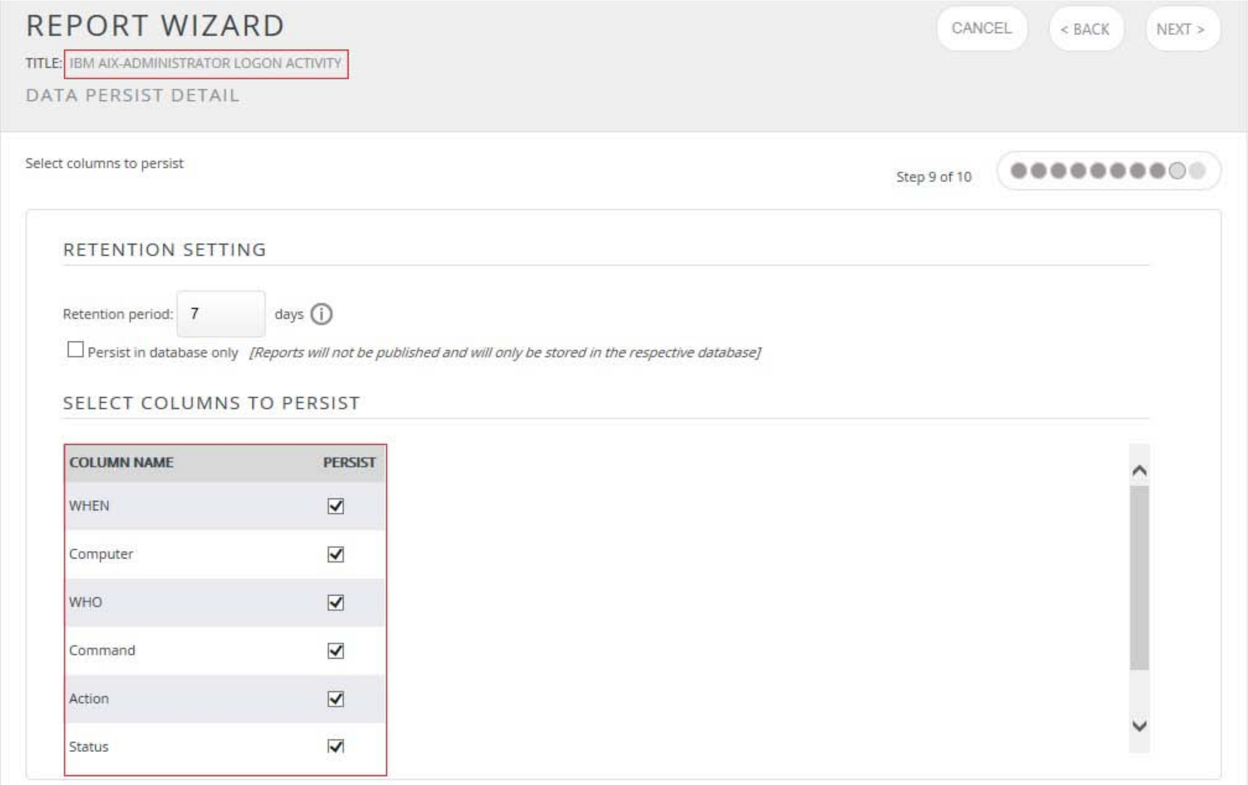
Update status via RSS: Select Feed

Show in: none

☑ Persist data in Eventvault Explorer

Figure 26

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



TITLE: IBM AIX-ADMINISTRATOR LOGON ACTIVITY

DATA PERSIST DETAIL

Select columns to persist

Step 9 of 10

RETENTION SETTING

Retention period: 7 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
WHEN	☑
Computer	☑
WHO	☑
Command	☑
Action	☑
Status	☑

Figure 27

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.

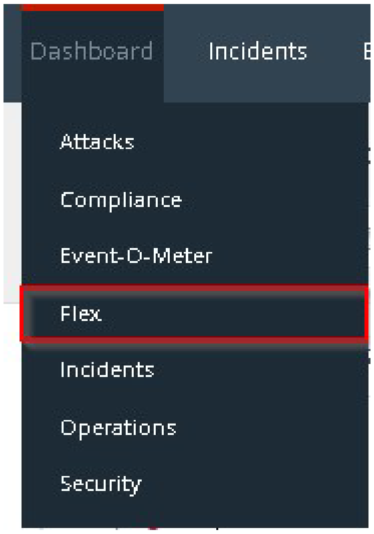
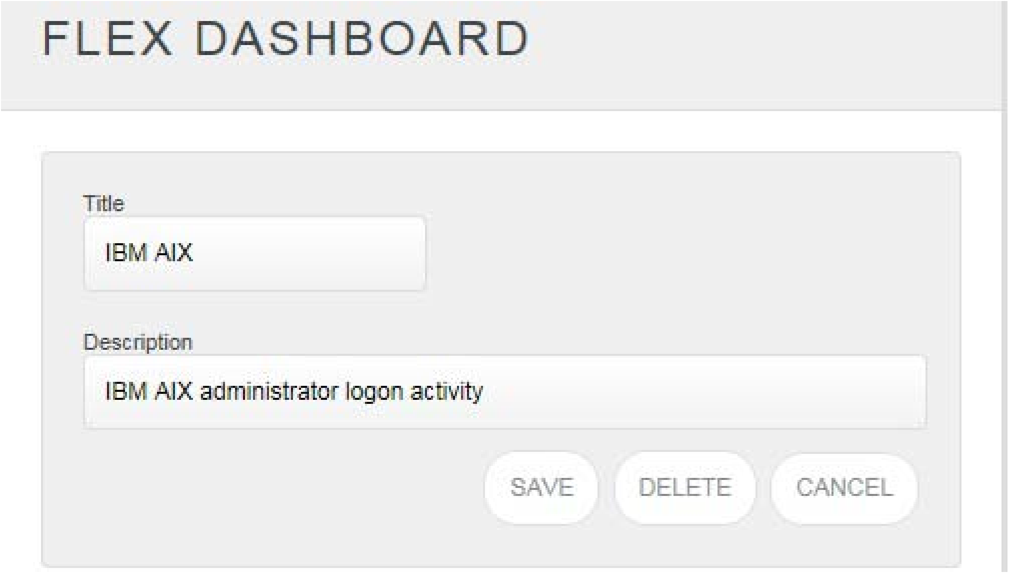


Figure 28

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



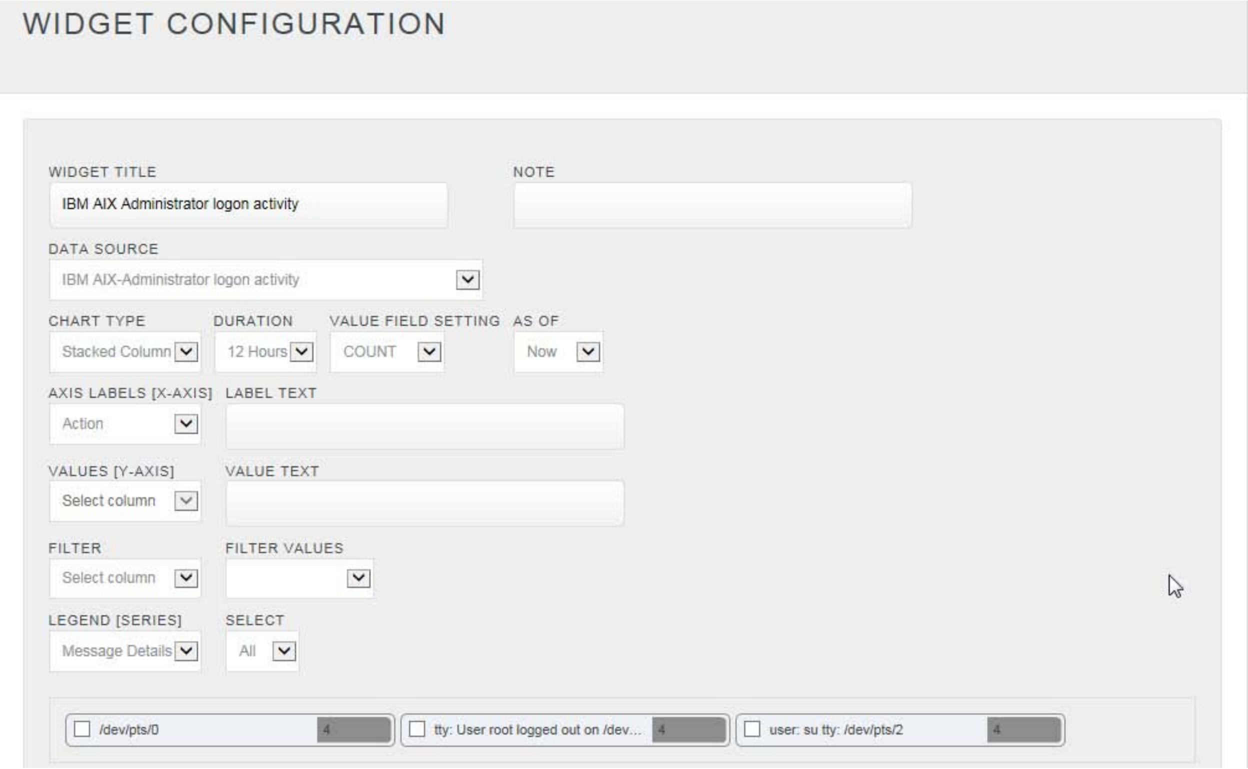
Title: IBM AIX

Description: IBM AIX administrator logon activity

Figure 29

4. Fill suitable title and description and click **Save** button.

5. Click ⚙ to configure a new flex dashlet. Widget configuration pane is shown.



WIDGET CONFIGURATION

WIDGET TITLE: IBM AIX Administrator logon activity

NOTE:

DATA SOURCE: IBM AIX-Administrator logon activity

CHART TYPE: Stacked Column

DURATION: 12 Hours

VALUE FIELD SETTING: COUNT

AS OF: Now

AXIS LABELS [X-AXIS]: Action

LABEL TEXT:

VALUES [Y-AXIS]: Select column

VALUE TEXT:

FILTER: Select column

FILTER VALUES:

LEGEND [SERIES]: Message Details

SELECT: All

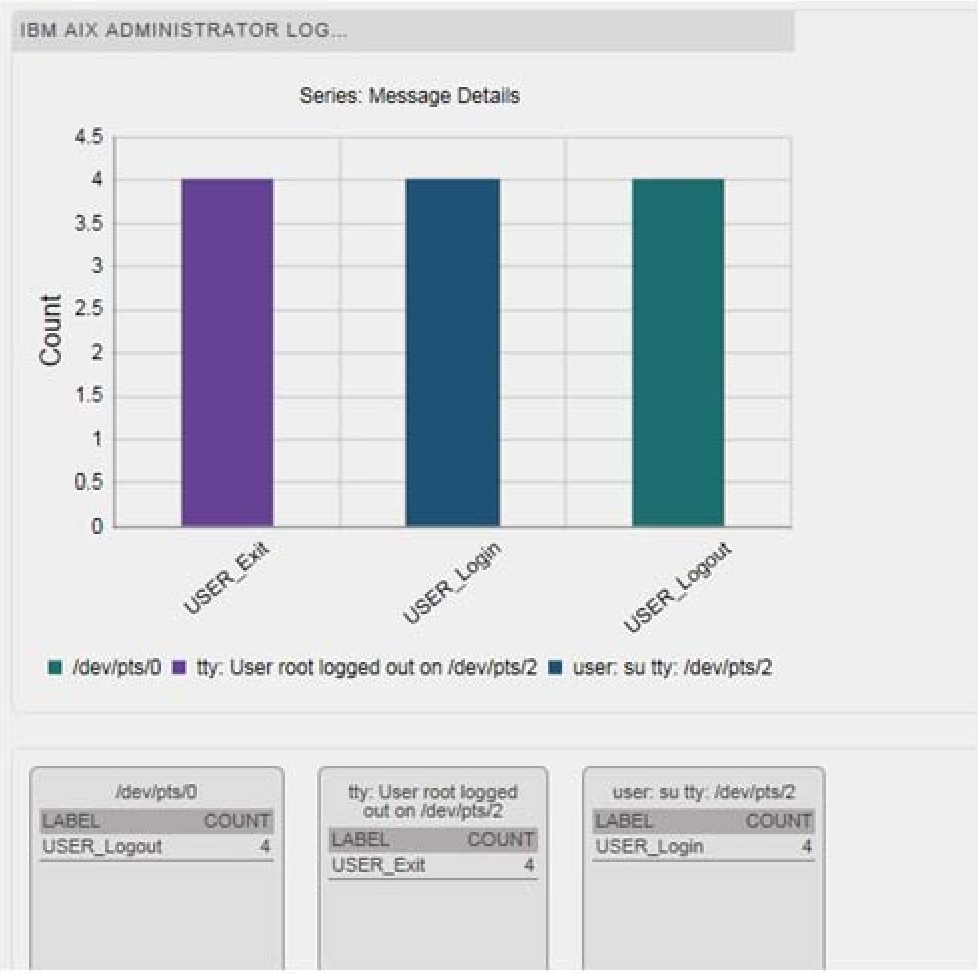
□ /dev/pts/0 4

□ tty: User root logged out on /dev... 4

□ user: su tty: /dev/pts/2 4

Figure 30

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


IBM AIX ADMINISTRATOR LOG...
Series: Message Details
Count
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
USER_Exit
USER_Login
USER_Logout
🟩 /dev/pts/0
🟪 tty: User root logged out on /dev/pts/2
🟦 user: su tty: /dev/pts/2

/dev/pts/0

LABEL	COUNT
USER_Logout	4

tty: User root logged out on /dev/pts/2

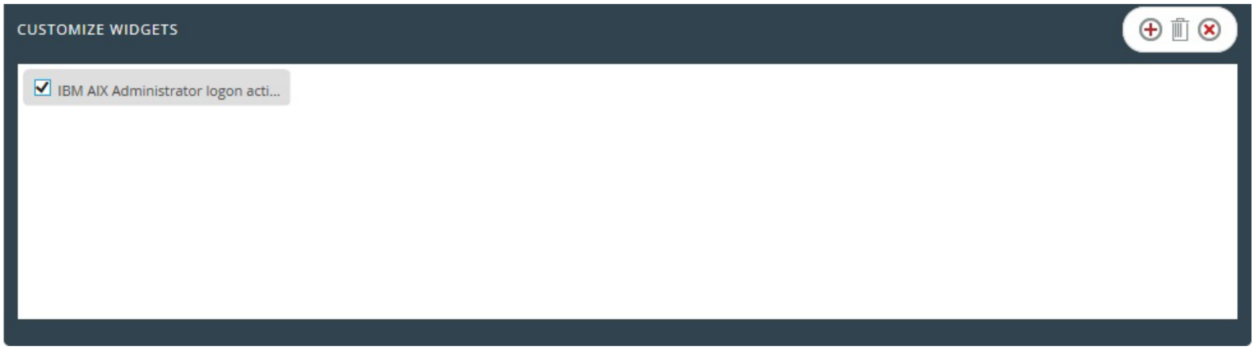
LABEL	COUNT
USER_Exit	4

user: su tty: /dev/pts/2

LABEL	COUNT
USER_Login	4

Figure 31

15. If satisfied, Click **Configure** button.



☑ IBM AIX Administrator logon acti...

Figure 32

16. Click 'customize' ⚙ to locate and choose created dashlet.
17. Click ⊕ to add dashlet to earlier created dashboard.

Sample Flex Dashboards

1. **IBM AIX-Administrator logon activity**

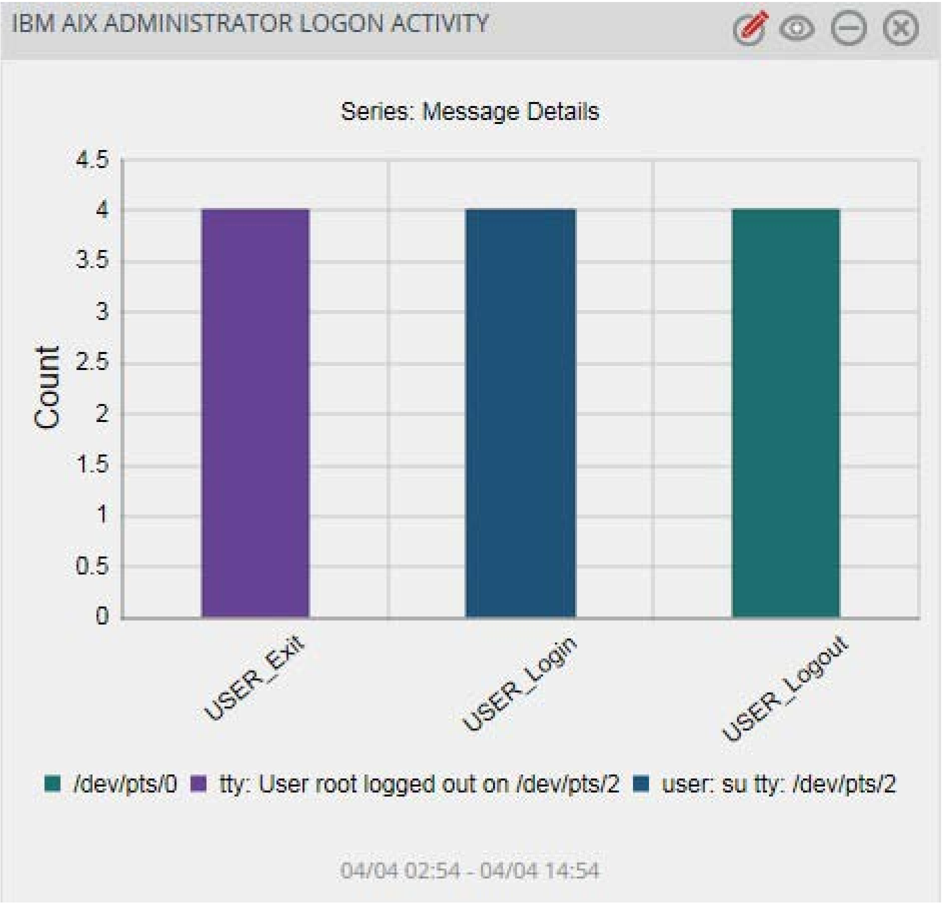


Figure 33

2. IBM AIX-User authentication failed

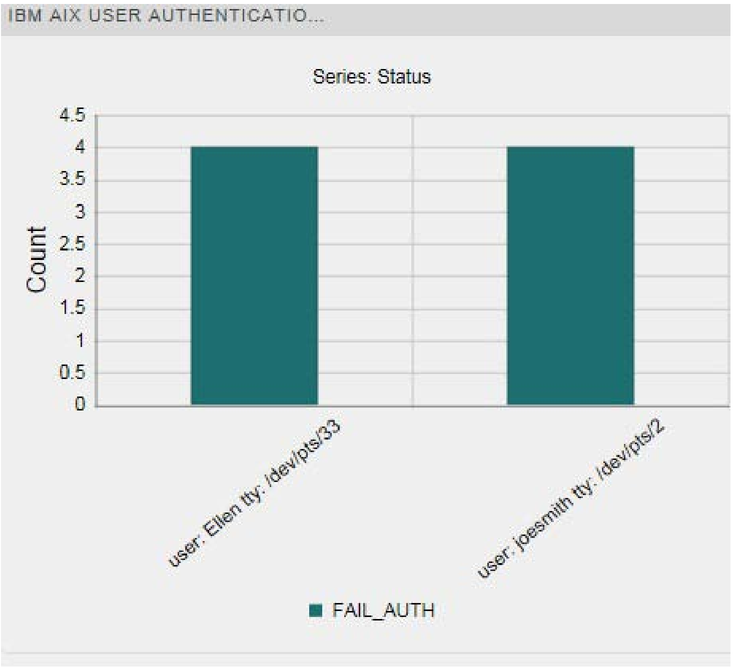


Figure 34

3. IBM AIX-Security objects audit

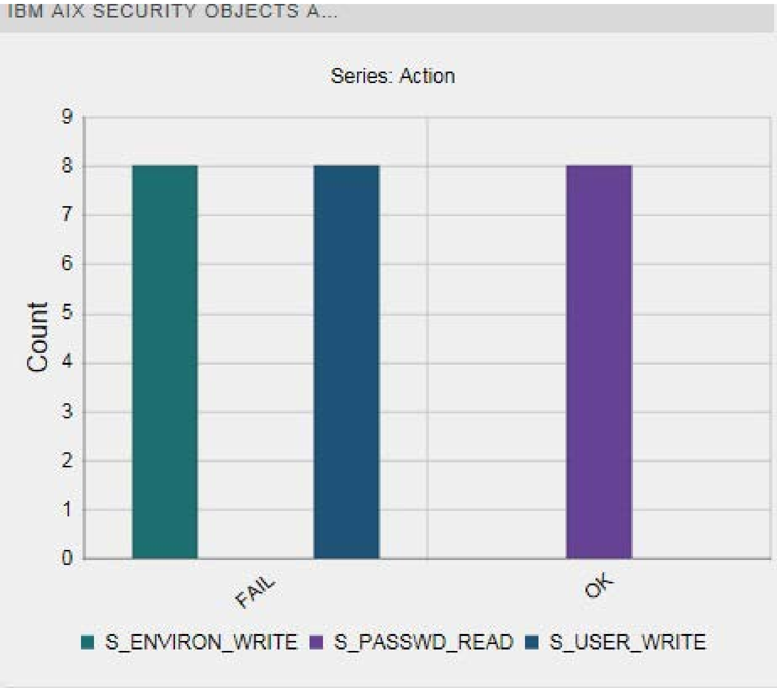


Figure 35