Micro Focus Security ArcSight Connectors

SmartConnector for IBM eServer iSeries Audit Journal File

Configuration Guide

June, 2018

Configuration Guide

SmartConnector for IBM eServer iSeries Audit Journal File

June, 2018

Warranty

Restricted Rights Legend

Trademark Notices

Revision History

Date	Description
10/17/2017	Added encryption parameters to Global Parameters.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
05/15/2012	Added new installation procedure.
05/15/2011	Added information regarding log files requiring a .txt extension.
02/15/2011	Added information about how to delete logs after processing them.
11/15/2010	Updated Type 5 journal entry description table.
09/24/2010	Clarified additional data mappings.
06/25/2010	Added support for AS/400 V5R3, V5R4, and V6R1.

SmartConnector for IBM eServer iSeries Audit Journal File

This guide provides information for installing the SmartConnector for IBM eServer iSeries Audit Journal File (formerly IBM AS/400 Audit Journal File) and configuring the device for audit log event collection. IBM eServer iSeries V5R2, V5R3, V5R4, and V6R1 Type 1 and Type 5 audit journal logs are supported.

Product Overview

The IBM eServer iSeries Audit Journal system is a secure integrated business system designed to run thousands of business applications. The purpose of the Audit Journal system is to record instances of access by subjects to objects, as well as allowing detection of any repeated attempts to bypass the protection mechanism, including any misuses of privileges, thus acting as a deterrent against system abuses and exposing potential security weaknesses in the system.

Configuration

Exported AudJrn Log Files

The SmartConnector for IBM eServer iSeries Audit Journal can parse the information contained in Audit Journal exported files transferred from the iSeries system to the host running the SmartConnector. Typically, iSeries administrators will create a script that will export and transfer the AudJrn files periodically to the host running the SmartConnector. The log files required a .txt extension for the connector to process them.

The SmartConnector will monitor a configurable folder for new files transferred; once a new file is detected, the file is processed and the file name appended with 'processed.' If the parser encounters an unexpected error, the file is put into a 'bad' folder. For example, if the parser defines a token to be of TimeStamp type, but the processed string is not of that type, it results in a java exception and the file will be put in the 'bad' folder. If the processed line is not of the correct format, the file is not appended with 'bad,' but a warning is given in the connector log.

The exported AudJrn file should contain one or more lines (one line per event) with the fixed-size fields described in the tables that follow.

Type 5 Journal Entry Fields

Offset	Field		Format	Description
1	Lenth of Entry	JOENTL	Zoned(5,0)	Total length of the journal entry including the entry length field.
6	Sequence Number	JOSEQN	Char(20)	Applied to each journal entry.
26	Journal Code	JOCODE	Char(1)	Always T.
27	Entry Type	JOENTT	Char(2)	See Audit Journal (QAUDJRN) entry types for a list of entry types and descriptions.

Offset	Field		Format	Description
29	Timestamp of Entry	JOTSTP	Char(26)	Date and time that the entry was made in SAA timestamp format 'yyyy-MM-dd-HH.mm.ss.uuuuuu'
55	Name of Job	JOJOB	Char(10)	The name of the job that caused the entry to be generated.
65	User Name	JOUSER	Char(10)	The user profile name associated with the job.
75	Job Number	JONBR	Zoned(6,0)	The job number.
81	Program Name	JOPGM	Char(10)	The name of the program that made the journal entry.
91	Program Library	JOPGMLIB	Char(10)	Name of the library that contains the program that added the journal entry.
101	Program ASP Device	JOPGMDEV	Char(10)	Name of APS device that contains the program that added the journal entry.
111	Program ASP Number	JOPGMASP	Zoned(5,0)	Number of the ASP that contains the program that added the journal entry.
116	Name of Object	JOOBJ	Char(10)	Used for journaled objects. Not used for audit journal entries.
126	Objects Library	JOLIB	Char(10)	Used for journaled objects. Not used for audit journal entries.
136	Member Name	JOMBR	Char(10)	Used for journaled objects. Not used for audit journal entries.
146	Count/RRN	JOCTRR	Char(20)	Used for journaled objects. Not used for audit journal entries.
166	Flag	JOFLAG	Char(1)	Used for journaled objects. Not used for audit journal entries.
167	Commit Cycle Identifier	JOCCID	Char(20)	Used for journaled objects. Not used for audit journal entries.
187	User Profile	JOUSPF	Char(10)	The name of the current user profile.
197	System Name	JOSYNM	Char(8)	The name of the system.
205	Journal Identifier	JOJID	Char(10)	Used for journaled objects. Not used for audit journal entries.
215	Referential Constraint	JORCST	Char(1)	Used for journaled objects. Not used for audit journal entries.
216	Trigger	JOTGR	Char(1)	Used for journaled objects. Not used for audit journal entries.
217	Incomplete Data	JOINCDAT	Char(1)	Used for journaled objects. Not used for audit journal entries.
218	Ignored by APY/RMVJRNCHG	JOIGNAPY	Char(1)	Used for journaled objects. Not used for audit journal entries.
219	Minimized ESD	JOMINESD	Char(1)	Used for journaled objects. Not used for audit journal entries.
220	Object Indicator	JOOBJIND	Char(1)	Used for journaled objects. Not used for audit journal entries.
221	System Sequence	JOSYSSEQ	Char(20)	A number assigned by the system to each journal entry.
241	Receiver	JORCV	Char(10)	The name of the receiver holding the journal entry.

Offset	Field		Format	Description
251	Receiver Library	JORCVLIB	Char(10)	The name of the library containing the receiver that holds the journal entry.
261	Receiver ASP Device	JORCVDEV	CHAR(10)	Name of ASP device that contains the receiver.
271	Receiver ASP Number	JORCVASP	Zoned(5,0)	Number of the ASP that contains the receiver that holds the journal entry.
276	Arm Number	JOARM	Zoned(5,0)	The number of the disk arm that contains the journal entry.
281	Thread Identifier	JOTHDX	Hex(8)	Identifies the thread within the process that added the journal entry.
289	Thread Identifier Hex	JOTHD	Char(16)	Displayable hex version of the thread identifier.
305	Address Family	JOADF	Char(1)	The format of the remote address associated with the journal entry.
306	Remote Port	JORPORT	Zoned(5,0)	The port number of the remote address associated with the journal entry.
311	Remote Address	JORADR	Char(46)	The remote address associated with the journal entry.
357	Logical unit of work	JOLUW	Char(39)	Used for journaled objects. Not used for audit journal entries.
396	Transaction ID	JOXID	Char(140)	Used for journaled objects. Not used for audit journal entries.
536	Reserved	JORES	Char(20)	Used for journaled objects. Not used for audit journal entries.
556	Null Value Indicators	JONVI	Char(50)	Used for journaled objects. Not used for audit journal entries.
606	Entry Specific Data Length	ESDLEN	Binary(5)	Length of the entry specific data.
611	Entry Specific Data	JOESD	variable	Entry specific data.

An example of a TYPE 5 format event line is as follows (data is not real):

```
12345123456789012345678907CP2008-02-26-01.00.05.094400JOJOB     MARY
987654JOPGM     JOPGMLIB  JOPGMDEV  00001
0000000000000000000000000000000000000000000000MARY      JOSYNM
00000012345678901234567890JORCV     JORCVLIB  JORCVDEV  0000100002
00000000000000019000000


                                                 Ã€MARY HAD A LITTLE LAMB
```

Type 1 Journal Entry Field Descriptions for Fixed-Length Fields

Field	Format
Entry length (JOENTL)	Zoned (5,0)
Sequence number (JOSEQN)	Zoned (10,0)
Journal code (JOCODE)	Char (1)

Field	Format
Entry type (JOENTT)	Char (2)
Date stamp (JODATE)	Char (6)
Time stamp (JOTIME)	Zoned (6,0)
Job name (JOJOB)	Char (10)
User name (JOUSER)	Char (10)
Job number (JONBR)	Zoned (6,0)
Program name (JOPGM)	Char (10)
Object name (JOOBJ)	Char (10)
Library name (JOLIB)	Char (10)
Member name (JOMBR)	Char (10)
Count/relative record number (JOCTRR)	Zoned (10,0)
Indicator flag (JOFLAG)	Char (1)
Commit cycle identifier (JOCCID)	Zoned (10,0)
Incomplete Data (JOINCDAT)	Char (1)
Minimized entry specific data (JOMINESD)	Char (1)
Reserved field (JORES)	Char (6)

An example of a TYPE 1 format event line is as follows (data is not real):

```
111112222222222TPW102004025440ZZZZZZZZZZ WWWW
333333JOPGM                                OOOOOOOOOOOOOOOOOOOOOO      XXXXXXXX
YYYYYYYYY
```

Additional Documentation

The AudJrn export files must be sent in a specific format. See the following IBM documentation.

DSPJRN (Display Journal) Command Description

Version	Path
V5R2	http://publib.boulder.ibm.com/iseries/v5r2/ic2924/index.htm?info/cl/dspjrn.htm
V5R3	http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/cl/dspjrn.htm
V5R4	http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=/cl/dspjrn.htm
V6R1	http://publib.boulder.ibm.com/infocenter/iseries/v6r1m0/index.jsp?topic=/cl/dspjrn.htm

Layout of Audit Journal Entries

Version	Path
V5R2	https://publib.boulder.ibm.com/iseries/v5r2/ic2924/books/c4153026.pdf
V5R3	http://publib.boulder.ibm.com/infocenter/iseries/v5r3/topic/books/sc415302.pdf
V5R4	http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/books/sc415302.pdf
V6R1	http://publib.boulder.ibm.com/infocenter/iseries/v6r1m0/topic/rzarl/sc415302.pdf

Differing Primary Languages

Be aware of the following when using FTP in an environment with different primary languages.

When data is transferred using TYPE E (or EBCDIC), the data is stored as is and therefore will be in the EBCDIC code page of the file from which it came. This can result in the stored file being tagged with an inappropriate CCSID value when the primary language of the two servers is different.

For example, when data in code page 237 is sent using TYPE E to the QSYS.LIB file system on a machine where the file does not exist, the data is stored as is in a new file tagged with CCSID 65535. If the receiving file already exists, then the data will be received as is and tagged with the existing file CCSID which may not be 237.

To avoid incorrect CCSID tagging, you can use the TYPE C CCSID subcommand (for example, TYPE C 237) to specify the CCSID of the data being transferred. When a CCSID is specified on a transfer and the data is written to an existing file, the data is converted to the CCSID of the existing file. If no target file exists before the transfer, a file is created and tagged with the specified CCSID.

In the preceding example, if the target file does not exist, a file with a CCSID of 237 is created on the receiving system. When the target file already exists, the data is converted from CCSID 237 to the CCSID of the target file.

When starting the FTP client, message TCP3C14: Unable to convert data from CCSID &1 to CCSID &2, may be displayed. This occurs if no character conversion is available between the EBCDIC CCSID specified by your job and the ASCII CCSID specified for the this FTP session.

You can change the ASCII CCSID by specifying a value for the coded character set identifier parameter of the STRTCPFTP CL command. CCSID 850, which contains the IBM Personal Computer Latin-1 coded character set, is an ASCII CCSID for which character conversions are available to all valid job CCSID values.

Specify Mapping Tables in the FTP Command

For FTP client, the ASCII mapping tables are specified in the FTP command. For FTP server this is done in the Change FTP Attributes (CHGFTPA) command. To specify the FTP client mapping tables:

1. Enter the command FTP.
2. Press PF4. The **Start TCP/IP FTP** screen is displayed.
3. Press F10. The prompts for outgoing and incoming ASCII/EBCDIC tables are displayed.

```
                        Start TCP/IP File Transfer (FTP)

Type choices, press Enter.

Remote system  . . . . . .



Internet address . . . . . .
Coded character set identifier     *DFT          1-65533, *DFT

                           Additional Parameters

Outgoing EBCDIC/ASCII table  . .   *CCSID        Name, *CCSID, *DFT
  Library  . . . . . .             *CURLIB       Name, *LIBL, *CURLIB
Incoming ASCII/EBCDIC table  . .   *CCSID        Name, *CCSID, *DFT
  Library  . . . . . .             *CURLIB       Name, *LIBL, *CURLIB


                                                                    Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Specify the CCSID (and hence the mapping tables) to be used for the FTP client. When the *DFT value is not changed, the CCSID value 00819 (ISO 8859-1 8 bit ASCII) is used. You may also specify a specific CCSID for both inbound and outbound transfers. The use of CCSIDs is discussed in National Language Support considerations for FTP.

Double-byte character set (DBCS) CCSID values are not permitted for the CCSID parameter on the CHGFTPA command. The DBCS CCSID values can be specified using the TYPE (Specify File Transfer Type) subcommand.

IBM includes mapping support in FTP to ensure compatibility with releases prior to V3R1. Use of mapping tables for incoming TYPE A file transfers results in the loss of CCSID tagging if the target file must be created. IBM strongly recommends that you use CCSID support for normal operations.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the

device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

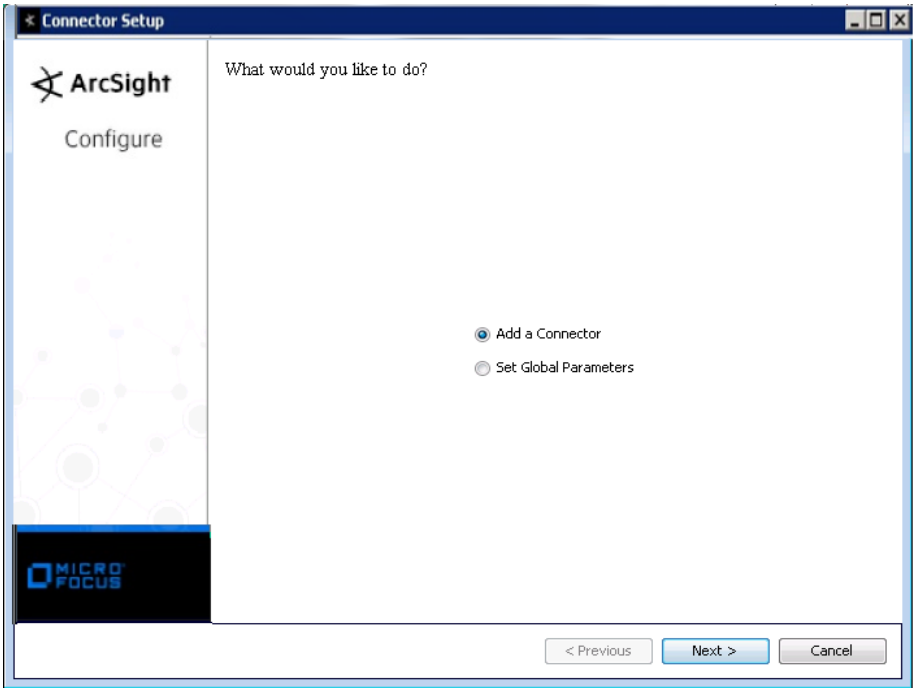
Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the Micro Focus SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

   Follow the wizard through the following folder selection tasks and installation of the core connector software:

   Introduction
   Choose Install Folder
   Choose Shortcut Folder
   Pre-Installation Summary
   Installing...
3. When the installation of SmartConnector core component software is finished, the following window is displayed:



Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using Micro Focus SecureData solutions to provide encryption. See the *Micro Focus SecureData Architecture Guide* for more information.

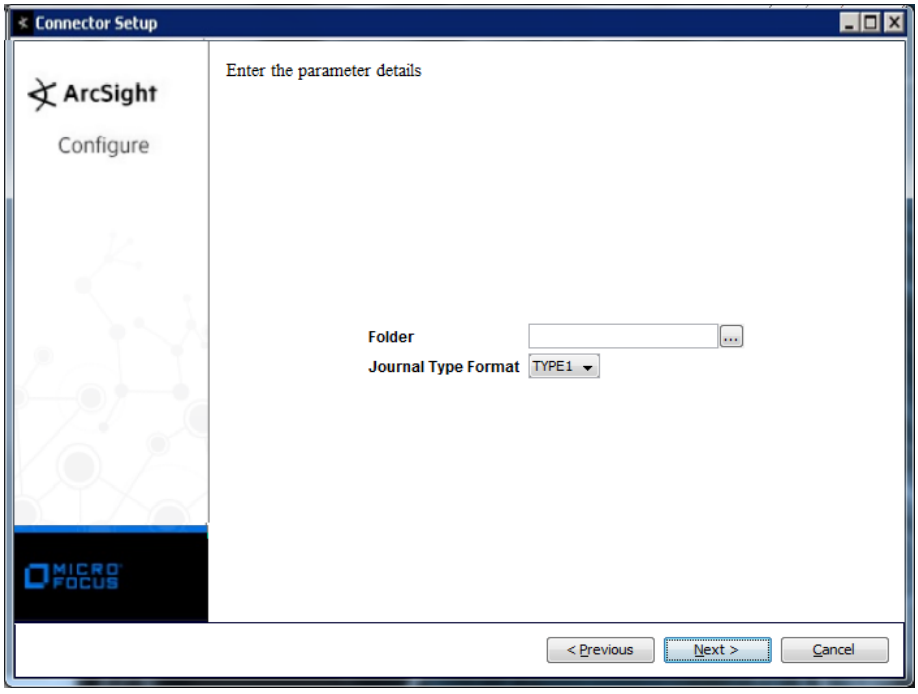
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the Micro Focus SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.

Parameter	Setting
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

1. Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
2. Select **IBM eServer iSeries Audit Journal File** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Folder Name	Absolute path to the directory containing the audit log files. Note that the connector expects log files to have a .txt extention.
Journal Type Format	Select Type 1 or Type 5 audit journal.

Select a Destination

1. The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.
2. Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.
3. Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
4. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1. Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
2. The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.
3. If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.
4. Click **Next** on the summary window.
5. To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to `$ARCSIGHT_HOME\current\bin` and run: `arcsight connectors`

To view the SmartConnector log, read the file `$ARCSIGHT_HOME\current\logs\agent.log`; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Delete Logs after Processing

After SmartConnector installation, you can access the connector's advanced parameters by editing the `agent.properties` file located at `$ARCSIGHT_HOME\user\agent`. directory in a DOS command window enter:

To delete log files after processing, change the value for the `mode` parameter from `RenameFileTheSameDirectory` to `DeleteFile`. Save the file and restart the connector for your changs to take effect.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Audit Journal TYPE 5 Mappings

ArcSight ESM Field	Device-Specific Field
Destination Host Name	JOSYNM
Destination Process Name	JOPGM
Device Custom Number 1	JONBR
Device Custom Number 2	JOCTRR
Device Custom Number 3	JOCCID
Device Custom String 1	JOESD
Device Custom String 2	JOLIB
Device Custom String 3	JOMBR
Device Custom String 4	JOINCDAT

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	JOMINESD
Device Event Category	JOENTT
Device Event Class ID	JOCODE plus JOENTT
Device Host Name	JOSYNM
Device Product	'AS/400'
Device Receipt Time	JOTSTP or JODATEJOTIME
Device Severity	JOCODE
Device Vendor	'IBM'
External ID	JOSEQN
File Name	JOOBJ
Name	JOJOB
Source Address	JORADR
Source Port	JORPORT
Source User Name	JOUSER or JOUSPF
Transport Protocol	JOADF

Audit Journal TYPE 1 Mappings

ArcSight ESM Field	Device-Specific Field
Destination Process Name	JOPGM
Device Custom Number 1	JONBR
Device Custom Number 2	JOCTRR
Device Custom Number 3	JOCCID
Device Custom String 1	JOENTT plus JOESD
Device Custom String 2	JOLIB
Device Custom String 3	JOMBR
Device Custom String 4	JOINCDAT
Device Custom String 5	JOMINESD
Device Event Category	JOENTT
Device Event Class Id	JOCODE
Device Product	'AS/400'
Device Receipt Time	JODATEJOTIME
Device Severity	JOCODE
Device Vendor	'IBM'
External ID	JOSEQN
File Name	JOOBJ
Name	JOJOB
Source User Name	JOUSER

Job Error Codes (Device Event Class ID/Message)

Code	Message
AD	A change was made to the auditing attribute.
AF	All authority failures.
AP	A change was made to program adopt.
AU	Attribute changes.CA,Changes to object authority (authorization list or object).
CA	Changes to object authority (authorization list or object).
CD	A change was made to a command string.
CO	Create object.
CV	Connection verification.
CP	Create, change, restore user profiles.
CQ	A change was made to a change request descriptor.
CU	Cluster operation
CY	Cryptographic configuration
DI	Directory services
DO	All delete operations on the system.
DS	DST security officer password reset.
EV	Environment variable
GR	General purpose audit record
GS	A descriptor was given.
IM	Intrusion monitor.
IP	Inter-process communication event.
IR	IP rules actions
IS	Internet security management
JD	Changes to the USER parameter of a job description.
JS	A change was made to job data.
KF	Key ring file name.
LD	A link, unlink, or lookup operation to a directory.
ML	A change was made to office services mail.
NA	Changes to network attributes.
ND	Directory search violations.
NE	End point violations.
OM	Object management change.
OR	Object restored.
OW	Changes to object ownership.
O1	Single optical object access.
O2	Dual optical object access.
O3	Optical volume access.
PA	Changes to programs (CHGPGM) that will now adopt the owner's authority.

Code	Message
PG	Changes to an object's primary group.
PO	A change was made to printed output.
PS	Profile swap.
PW	Passwords used that are not valid.
RA	Restore of objects when authority changes.
RJ	Restore of job descriptions that contain user profile names.
RO	Restore of objects when ownership information changes.
RP	Restore of programs that adopt their owner's authority.
RQ	A change request descriptor was restored.
RU	Restore of authority for user profiles.
RZ	The primary group for an object was changed during a restore operation.
SD	A change was made to the system directory.
SE	Changes to subsystem routing.
SF	A change was made to a spooled output file.
SG	Asynchronous signals
SK	Secure sockets connection
SM	A change was made by system management.
SO	A change was made by server security.
ST	A change was made by system tools.
SV	Changes to system values.
VA	Changes to access control list.
VC	Connection started or ended.
VF	Server files were closed.
VL	An account limit was exceeded.
VN	A logon or logoff operation on the network.
VO	Actions on validation lists.
VP	A network password error.
VR	A network resources was accessed.
VS	A server session started or ended.
VU	A network profile was changed.
VV	Service status was changed.
X0	Network authentication.
X1	Reserved for future audit entry.
X2	Reserved for future audit entry.
X3	Reserved for future audit entry.
X4	Reserved for future audit entry.
X5	Reserved for future audit entry.
X6	Reserved for future audit entry.
X7	Reserved for future audit entry.
X8	Reserved for future audit entry.
X9	Reserved for future audit entry.
XD	Directory server extension.
YC	A change was made to DLO change access.

Code	Message
YR	A change was made to DLO read access.
ZC	9 A change was made to object change access.
ZM	An object was accessed using a method.
ZR	A change was made to Object read access.
AA	User-specified.
XP	Internal entry.
RD	Delete receiver.
RS	Receiver saved.