



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for IBM eServer iSeries Audit Journal File

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for IBM eServer iSeries Audit Journal File	4
Product Overview	5
Configuration	6
Exported AudJrn Log Files	6
Additional Documentation	10
DSPJRN (Display Journal) Command Description	10
Layout of Audit Journal Entries	10
Differing Primary Languages	10
Specify Mapping Tables in the FTP Command	11
Installing the SmartConnector	13
Preparing to Install the SmartConnector	13
Configuring and Installing the SmartConnector	13
Deleting Logs after Processing	15
Device Event Mapping to ArcSight Fields	16
Audit Journal TYPE 5 Mappings	16
Audit Journal TYPE 1 Mappings	17
Job Error Codes (Device Event Class ID/Message)	18
Send Documentation Feedback	22

Configuration Guide for IBM eServer iSeries Audit Journal File

This guide provides information for installing the SmartConnector for IBM eServer iSeries Audit Journal File (formerly known as, IBM AS/400 Audit Journal File) and configuring the device for audit log event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

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

This section includes the following topic:

Exported AudJrn Log Files

The SmartConnector for IBM eServer iSeries Audit Journal parses the information contained in Audit Journal exported files transferred from 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 monitors 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 will be put into the `'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 must contain one or more lines (one line per event) with the fixed-size fields described in the following tables:

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.
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.

Configuration Guide for IBM eServer iSeries Audit Journal File Configuration

Offset	Field		Format	Description
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.

Offset	Field		Format	Description
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.
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.

Offset	Field		Format	Description
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.

Example of a TYPE 5 format event line:

```
1234512345678901234567890TCP2008-02-26-01.00.05.094400JOJOB      MARY
987654JOPGM          JOPGMLIB  JOPGMDEV  00001
0000000000000000000000000000000000000000000000000MARY        JOSYNN
000000012345678901234567890JORCV      JORCVLIB  JORCVDEV  0000100002
000000000000000000000000000000000000000000000000
```

MEMARY 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)
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)

Field	Format
Incomplete Data (JOINCDAT)	Char (1)
Minimized entry specific data (JOMINESD)	Char (1)
Reserved field (JORES)	Char (6)

Example of a TYPE 1 format event line:

```
1111122222222222TPW102004025440222222222 WWW
333333JOPGM
YYYYYYYYY 00000000000000000000000000000000 XXXXXXXXX
```

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

Layout of Audit Journal Entries

Version	Path
V5R2	https://publib.boulder.ibm.com/series/v5r2/ic2924/books/c4153026.pdf
V5R3	http://publib.boulder.ibm.com/infocenter/series/v5r3/topic/books/sc415302.pdf
V5R4	http://publib.boulder.ibm.com/infocenter/series/v5r4/topic/books/sc415302.pdf
V6R1	http://publib.boulder.ibm.com/infocenter/series/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 (CHGFTP) command. To specify the FTP client mapping tables:

1. Enter the FTP command.
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 . . . . .                  Name, *LIBL, *CURLIB
Incoming ASCII/EBCDIC table . .   *CCSID      Name, *CCSID, *DFT
Library . . . . .                  Name, *LIBL, *CURLIB

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

4. 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 CHGFTP 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.

Installing 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.

Preparing to Install the SmartConnector

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

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

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

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

Configuring and Installing the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. From the **Type** drop-down menu, select **IBM eServer iSeries Audit Journal File** and click **Next**.

5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameters	Description
Folder Name	Absolute path to the directory containing the audit log files. Ensure that the log files have a .txt extension.
Journal Type Format	Select Type 1 or Type 5 audit journal.

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) 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 then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

Deleting Logs after Processing

1. Open the `agent.properties` file located at `$ARCSIGHT_HOME\user\agent`.
2. Go to advanced parameters.
3. Change the value for the mode parameter from **RenameFileTheSameDirectory** to **DeleteFile**.
4. Save the file and restart the connector to apply your changes.

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
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

ArcSight ESM Field	Device-Specific Field
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.

Code	Message
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.
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.

Code	Message
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.
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.

Code	Message
XP	Internal entry.
RD	Delete receiver.
RS	Receiver saved.

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to receive events.

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Configuration Guide for IBM eServer iSeries Audit Journal File (ArcSight Connectors 8.4.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!