CorreLog®

CorreLog Agent For SAP

SAP Audit Log Monitor Interface

This application note describes how to install configure the CorreLog to accept and format SAP audit files. The information herein supplements the CorreLog “Windows Tool Set Manual” and "File Transfer Queue Adapter User Manual", and describes how to install, configure, and test this SAP support function, which accepts and formats SAP security audit files for inclusion in the CorreLog message database.

Background Information

SAP Audit files consist of fixed length ASCII text records, which are continuously appended (without any new line separators) to an audit file. CorreLog can read and format these files two distinct ways:

1. **Agent Adapter.** The operator can add the “SAP-adapter.dll” software to a copy of the agent program, which permits the agent to read the SAP audit file as if it was a regular streaming log file.

2. **File Transfer Queue.** The operator can use the “File Transfer Queue” software to read and format files, where these files are transferred to the CorreLog server using a mechanism such as FTP.

Both of the above techniques are described in this application note.

Using the "SAP Adapter" software described here, a simple system can be constructed to permit a SAP audit log file to be handled in a fashion identical to other log files, permitting SAP messages to be threaded, alerted upon, or reported on like any other received message.

Using the SAP Agent Adapter

The user can configure the SAP monitor at a copy of the agent program using the following procedure:

1. Install the SAP extensions at a new or existing site. The SAP extensions are typically installed via a self-extracting WinZip file, such as:

   ```
   wt-sap-x-x-x.exe
   ```

   The above file can be obtained from CorreLog support.

2. After installing the agent, click down into the IP Address for the agent program, click “Edit Remote Config”, to display the remote agent configuration.

3. On the remote agent configuration screen, click the “Wizard” button to run the configuration wizard, and provide the following values in response to each screen:

Log File Monitor Type:	Adapter
Adapter Identifier:	SAP:
Adapter Module:	SAP-adapter.dll
Log File Monitor Path	(pathname to SAP audit file.)

   Use defaults for all other values. When the Wizard finishes, the SAP adapter has been added to the list of monitored logs.

Note that the pathname to the Log File Monitor (specified on the second screen of the Wizard) can contain wildcards or standard date and time notation to access the log file. For example, a typical path may be a value such as:

```
C:\SAP\Audit\%Y-%m-%d.aud
```

The above pathname will monitor a file in the SAP\Audit:” folder, where the file name is in “YYYY-MM-DD.aud” format.

After adding the above entry, SAP audit records that are appended to the specified file will automatically be sent to CorreLog. The operator can configure keyword overrides to filter messages or change the severities of the messages that are received.

More information on keywords and general usage of the agent can be found in the “Windows Tool Set User Manual”, available from the “Home” screen of CorreLog after installation.

Using the SAP Formatter and File Transfer Queue

As an alternative to the real-time monitoring available via the Windows Agent adapter, the SAP Log File Monitor can be included in the CorreLog File Transfer Queue Adapter software, version 5.1.2 (and greater.) Installation and usage of this adapter is documented in detail with the “File Transfer Queue” user manual. This feature permits batch process of existing SAP files.

Once the File transfer queue software is installed, a queue (and the external formatter) should be configured to accept SAP files. The operator first creates a formatter using the “SAP-util.exe” program, composing a simple batch file as follows, and placing this file in the “formatters” directory of the CorreLog Server.

```
REM: # File FQ_APP_SAP_LOG.bat
REM: # Requires the SAP-util.exe program, which is
REM: # installed as part of the SAP adapter software.

..\wintools\SAP-util.exe %FQ_PATHNAME%

REM: # File was transferred.
```

After creating the FQ_APP_SAP_LOG.bat external file as described above, the procedure to configure the SAP File queue is as follows:

1. On the CorreLog Server, create a directory folder that will receive the SAP audit files. This path is typically "C:\CorreLog\SAP-queue", but the operator can select any pathname.

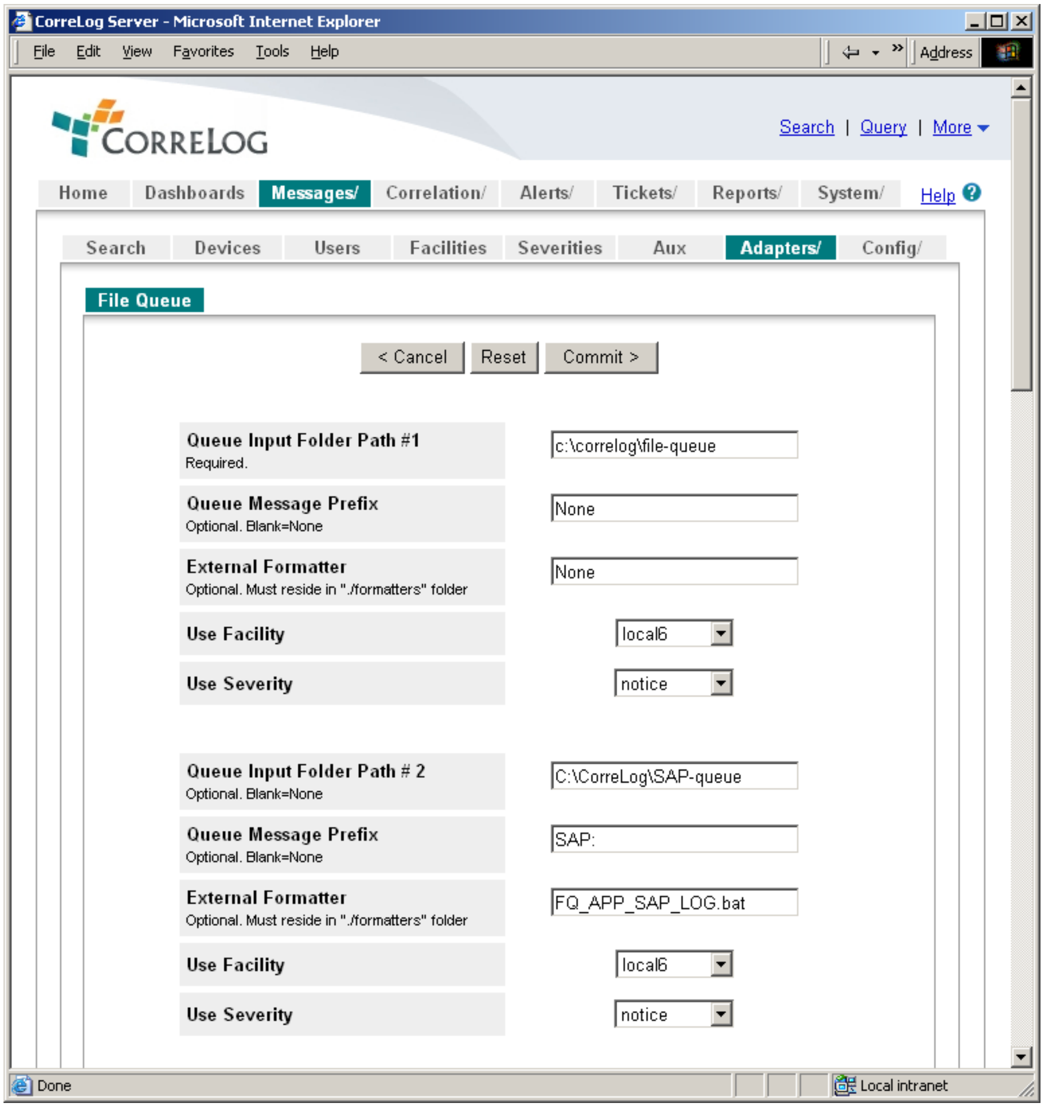
2. Log into the CorreLog Web Interface, and navigate to the "Messages > Adapters> File Queue" screen.

3. Click the "Edit" button on this screen to edit the various queues.

4. On the "Queue Edit" screen, add the following items to a spare slot (typically Slot #2 for a new installation.)

Queue Input Folder:	C:\CorreLog\SAP-queue
Queue Message Prefix:	SAP:
External Formatter:	FQ_APP_SAP_LOG.bat

5. When finished, the screen "Edit" screen should appear similar to that shown in the screenshot below:


CorreLog Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
CORRELOG
Search | Query | More
Home Dashboards Messages/ Correlation/ Alerts/ Tickets/ Reports/ System/ Help
Search Devices Users Facilities Severities Aux Adapters/ Config/
File Queue
< Cancel Reset Commit >
Done
Local intranet

Queue Input Folder Path #1 Required.	c:\correlog\file-queue
Queue Message Prefix Optional. Blank=None	None
External Formatter Optional. Must reside in "./formatters" folder	None
Use Facility	local6
Use Severity	notice
Queue Input Folder Path # 2 Optional. Blank=None	C:\CorreLog\SAP-queue
Queue Message Prefix Optional. Blank=None	SAP:
External Formatter Optional. Must reside in "./formatters" folder	FQ_APP_SAP_LOG.bat
Use Facility	local6
Use Severity	notice

6. Click "Commit" to save the new configuration. The "CorreLog\SAP-queue" entry created above will appear on the top level "Adapters > File Queue" screen.

No other steps are needed to configure the queue. After performing the above steps, any SAP audit file that is copied to the C:\CorreLog\SAP-queue folder will be read by the CO-queue.exe program, deleted from the queue, and transmitted to CorreLog.

Support for CEF Common Event Format

The SAP adapter and agent supports CEF format (for those SIEM devices that support this special format,) This feature is enabled by adding a "MessageFormat" directive to the agent configuration file, specifying CEF format.

To modify the agent configuration file, edit the CO-sysmsg.cnf file (located in the same folder as the CO-sysmsg.exe Windows agent program) and add the following directive somewhere after the "MessagePort" directive and prior to the first "EventLog" specification. (For example, add this after the "MessagePrefix" directive, or replace the "MessagePrefix" directive with the following):

```
MessageFormat CEF
```

After making the above change, stop and restart the "CorreLog Syslog Message" service for the change to take effect. The agent will then transmit all event logs and the SAP messages in CEF format. A typical SAP message in CEF format is as follows:

```
Oct 1 13:05:47 myhost CEF:0|CorreLog|SAP Agent|5-5-3|AU5|RFC/CPIC
logon successful|1|deviceFacility=audit cat=RFC/CPIC suser=MyUser
msg=AU5 - SAP Audit Time: 2015/10/01 13:05:47 - Data: 00000000D0 -
Terminal: 183.245. - SAP User: MyUser Report: SAPMSSY1 - Client Flag: 1 -
Client ID: 200 - Args: R&0 10.1.1.2 - Audit Class: RFC/CPIC Logon - Severity:
Info - Descr: RFC/CPIC logon successful.
```

Comment: If CEF is not required, then this step should generally be omitted since CEF has multiple limitations, and is not easily human readable. Use the standard SAP agent formatting where possible, since this is designed for maximum interoperability with programs and devices (with the exception of those SIEMS that actually require CEF for their normal operation.)

Note that when specifying a "MessageFormat", the SAP AND ALSO the Event Log messages will be in CEF format. The "MessagePrefix" directive is ignored when the "MessageFormat" is set to CEF.

Refer to the Windows Tool Set User Manual for more information on using CEF and MessagFormat directives.

Description of SAP-util.exe Program

As part of the SAP installation, a command line utility is provided that can be used to debug and inspect a raw SAP file. The “SAP-util.exe” program is placed in the “wintools” directory along with the “SAP-adapter.dll”.

Basic usage of the program can be displayed by launching the utility at a command prompt with no arguments: General usage of this utility program is as follows:

SAP-util.exe (auditfile)

> Executing the program with the pathname of a SAP audit file as the first and only argument will dump a textual listing of the file to standard output. This is the mode of operation used by the File Transfer Queue described above.

SAP-util.exe –tail (auditfile)

> Executing the program with the “-tail” option, followed by the pathname of a SAP audit file, will continuously tail the log file, displaying formatted records as new information is appended to the bottom of the file. The user enters CTRL+C to exit the program.

SAP-util.exe –raw (auditfile)

> Executing the program with the “-raw” option, followed by the pathname to a SAP audit file, will continuously tail the log file, displaying unformatted records as new information is appended to the bottom of the file. (This option is similar to the “-tail” option described above, except no formatting is applied.) The user enters CTRL+C to exit the program.

SAP-util.exe –sim (bytecount) (auditfile)

> This special option copies the specified audit file to standard output, pausing after the specified number of bytes is written. This mode of operation is generally use for test and demonstration.

SAP Adapter Licensing Instructions

The CorreLog Agent for SAP software is licensed software. On initial installation, the SAP adapter will create a 90-day evaluation license for itself, to permit easy evaluation of the product.

To execute the program for longer than 90 days, you must contact support@correlog.com or your CorreLog account manager, and send the "SAP Site Identifier" value to CorreLog support.

Specific steps to license the program are as follows:

- First, locate the "wintools\SAP-adapter.txt" file. This text file contains the site identifier for the agent installation. This file always resides in the same folder as the CO-sysmsg.exe" program, by default the file location "CorreLog\wintools\SAP-adapter.txt".

- Send the "SAP-adapter.txt" file to CorreLog support via e-mail. When this file is received, CorreLog will generate an "auth.txt" file for the SAP installation, and e-mail you this file. (The "auth.txt" file is a short text file containing encrypted license codes.)

- Once you have received the "auth.txt" file from CorreLog Support, save this file in the same location as the "CO-sysmsg.exe" and "CO-sysmsg.log" file, by default the location "CorreLog\wintools\auth.txt" (but possibly some other location at your site.)

- Stop and restart your agent, and verify that the SAP adapter is operating properly. You may check the "CO-sysmsg.log" file, located in the "wintools" folder, for SAP license and error message.

Note that if the CorreLog Agent for SAP is not licensed, it will generate periodic error messages and will stop sending SAP data. (The rest of the agent will continue to run uninterrupted, but no SAP messages will be sent.)

If the site identifier changes, because the agent is relocated to a new platform, you may request another version of the "auth.txt" file from CorreLog support.

Finally, note that other licensing options and methods may be available. You should contact CorreLog support or your account manager for more information on license methods and options.

Common SAP Adapter Messages And Codes

Event Class	Code	Severity	Description
Dialog Logon	AU2	Error	Logon failed.
Dialog Logon	AUM	Warning	User locked in client after erroneous password checks.
Dialog Logon	AUN	Info	User in client unlocked after being locked due to invalid password.
Dialog Logon	BUD	Error	WS: Delayed logon failed. Refer to Web service log.
Dialog Logon	AU1	Info	Logon successful.
Dialog Logon	AUO	Error	Logon failed.
Dialog Logon	CUA	Warning	Rejected assertion.
Dialog Logon	CUB	Notice	SAML 2.0 Logon.
Dialog Logon	CUC	Notice	SAML 2.0 Logon
Dialog Logon	CUD	Debug	Subject Name ID.
Dialog Logon	CUE	Debug	Attribute value.
Dialog Logon	CUF	Notice	Authentication assertion.
Dialog Logon	CUG	Error	Signed logout request rejected.
Dialog Logon	CUH	Error	Unsigned logout request rejected.
Dialog Logon	AUC	Info	User logoff.
Dialog Logon	BUE	Notice	WS: Delayed logon successful. Refer to Web service log.
Dialog Logon.	BUK	Debug	Assertion used.
Dialog Logon.	BUL	Notice	SAML 2.0 Logon.
Dialog Logon	BUM	Debug	Subject Name ID.
Dialog Logon	BUN	Debug	Attribute value.
Dialog Logon	BUO	Notice	Authentication assertion.
Dialog Logon	BUP	Notice	SAML 2.0 Logon
Dialog Logon	BUQ	Info	Signed logout request accepted.
Dialog Logon	BUR	Notice	Unsigned logout request accepted.
RFC/CPIC Logon	AU6	Error	RFC/CPIC logon failed.
RFC/CPIC Logon	AU5	Info	RFC/CPIC logon successful.
RFC Function Call	AUL	Error	Failed RFC call.
RFC Function Call	CUW	Error	Failed Web service call.
RFC Function Call	CUZ	Info	Generic table access by RFC with activity.
RFC Function Call	AUK	Info	Successful RFC call.
RFC Function Call	CUV	Info	Successful WS call.

Transaction	AU4	Error	Start of transaction failed.
Transaction	AUP	Warning	Transaction locked.
Transaction	AUQ	Notice	Transaction unlocked.
Transaction	AU3	Notice	Transaction started.
Report	AUX	Error	Start report failed.
Report	AUW	Notice	Report started.
Master Change	AU7	Warning	User created.
Master Change	AUU	Notice	Object activated.
Master Change	AU8	Warning	User deleted.
Master Change	AU9	Warning	User locked.
Master Change	AUA	Notice	User unlocked.
Master Change	AUB	Warning	Authorizations for user were changed.
Master Change	AUD	Critical	User master record was changed.
Master Change	AUR	Warning	Object created.
Master Change	AUS	Warning	Object deleted.
Master Change	AUT	Warning	Object changed.
Master Change	BU2	Notice	Password changed for user in client.
System	AUE	Critical	Audit configuration changed.
System	AUF	Debug	Audit event for user in client.
System	AUG	Info	Application server started.
System	AUH	Critical	Application server stopped.
System	AUI	Debug	Audit: slot inactive.
System	AUJ	Debug	Audit: Activity status changed.
Other Events	AUV	Error	Digital signature error.
Other Events	BU0	Debug	Security audit log event.
Other Events	BU1	Error	Password check failed for user in client.
Other Events	BU3	Critical	Change security check during export.
Other Events	BU4	Critical	Transport request contains security-critical source objects.
Other Events	BU8	Critical	Virus Scan Interface: Virus found by profile.
Other Events	BUG	Error	HTTP Security Session Management was deactivated for client.
Other Events	BUY	Critical	Field contents changed.
Other Events	BUZ	Critical	Audit event: program line and event.
Other Events	CU0	Debug	Security audit log event.
Other Events	CUK	Critical	C debugging activated.
Other Events	CUL	Critical	Field content changed.
Other Events	CUM	Debug	Jump to ABAP Debugger.

Other Events	CUN	Critical	A manually caught process was stopped from within the debugger.
Other Events	CUO	Critical	Explicit database commit or rollback from debugger.
Other Events	CUP	Debug	Non-exclusive debugging session started.
Other Events	CUY	Debug	Object operation.
Other Events	AUY	Notice	Download bytes to file.
Other Events	AUZ	Warning	Digital Signature.
Other Events	BU5	Warning	ICF Recorder entry executed for user.
Other Events	BU6	Warning	ICF Recorder entry executed by user.
Other Events	BU7	Warning	Administration setting was changed for ICF Recorder.
Other Events	BU9	Error	Virus Scan Interface: Error occurred in profile.
Other Events	BUA	Error	WS: Signature check error. Refer to Web service log.
Other Events	BUB	Warning	WS: Signature insufficient. Refer to Web service log.
Other Events	BUC	Warning	WS: Time stamp is invalid. Refer to Web service log.
Other Events	BUH	Warning	HTTP Security Session of user and client was hard exited.
Other Events	CUQ	Warning	Logical file name not configured. Physical file name not checked.
Other Events	CUR	Warning	Physical file name does not meet requirements set by logical file name.
Other Events	CUS	Warning	Logical file name is not a valid alias for logical file name.
Other Events	CUT	Warning	No validation is active for logical file name.
Other Events	AU0	Debug	Audit - Test.
Other Events	BUF	Notice	HTTP Security Session Management was activated.

For Additional Help And Information…

Detailed specifications regarding the CorreLog Server, add-on components, and resources are available from our corporate website. Test software may be downloaded for immediate evaluation. Additionally, CorreLog is pleased to support proof-of-concepts, and provide technology proposals and demonstrations on request.

CorreLog, Inc., a privately held corporation, has produced software and framework components used successfully by hundreds of government and private operations worldwide. We deliver security information and event management (SIEM) software, combined with deep correlation functions, and advanced security solutions. CorreLog markets its solutions directly and through partners.

We are committed to advancing and redefining the state-of-art of system management, using open and standards-based protocols and methods. Visit our website today for more information.

CorreLog, Inc.
http://www.CorreLog.com
mailto:support@CorreLog.com