Alliance LGA Reference Manual

Page Information

Last updated: 11.22.2017

Table of Contents

Chapter 1: Introduction

Alliance LogAgent for IBM i provides extended support for sending security, operator, server, and user log information to a Security Information and Event Management (SIEM) server, or any Syslogd or Syslog-ng compatible server. Alliance LogAgent for IBM i can help you bring your IBM i into your Security Information and Event Management (SIEM) strategy to meet regulatory compliance requirements and to properly monitor for potential security breaches.

The Syslog data standard

UNIX and Linux systems have long supported the collection of system and application logs under the general name of “syslogs”. Many system logs in these environments are text files that are created by various applications and services. System logs collect important information about the health of the server, and about the security environment. They are important sources of information about potential or real security threats. The format of system logs can be very informal and can include just informational text. However, there is a formal standard for system logs in RFC 3164. When logs are collected by the Alliance LogAgent application they are automatically placed in the RFC 3164 syslog format.

The Common Event Format (CEF) standard

Some Security Information and Event Management (SIEM) products use a special log format called the Common Event Format (CEF). Alliance LogAgent for IBM i supports the CEF format for customers who want to send information directly to log monitoring systems in CEF format.

The Log Event Extended Format (LEEF)

The IBM Security QRadar log collection server and SIEM solution works best with information in the LEEF format. Alliance LogAgent for IBM QRadar fully supports the LEEF standard. When sending security event information to QRadar you should select this option. Please note that the Alliance LogAgent QRadar support is a separately licensed option of Alliance LogAgent. Additionally you may need to update the QRadar DSM in order to receive support for Alliance LogAgent events.

IBM i security audit journal QAUDJRN

The system audit journal `QAUDJRN` can be configured to capture a large number of security and system management events. The Alliance LogAgent solution can capture the entries in the `QAUDJRN` journal in real time, format them for the Syslog, IBM LEEF, or CEF format, and send them to a syslogd or Syslog-ng server. The syslog server can be running on the IBM i or any remote server. The IBM i Security Reference Manual provides information on how to change system values, user profiles, and objects to capture various system change and security events.

IBM i QHST history log

The IBM i QHST message log collects important job, user, and security information. Alliance LogAgent can be configured to capture QHST entries and convert them to the security audit journal (`QAUDJRN`) for a permanent record of system activity.

IBM i operator messages

On the IBM i platform, the message queues `QSYSOPR` and `QSYSMSG` receive important application and system security messages. The Alliance LogAgent software can capture the messages in these message queues, format them to the syslog or CEF standard, and send them to a syslog server on the same IBM i or to a syslog server on a remote system.

IBM i exit point monitors

IBM provides many exit points for operating system, database, and applications. Many of these applications involve the exposing of sensitive security operations include user authentication, database access, data transfer, and other functions. Alliance LogAgent provides the ability to monitor and log activities available on selected number of IBM i exit points. When active, Alliance LogAgent exit point monitors capture information which is recorded to the IBM i security audit journal `QAUDJRN` .

IBM system statistics

Alliance LogAgent can collect basic system utilization information and send the information to your SIEM solution or log collection server. The system information collected includes CPU utilization, auxiliary storage utilization, number of jobs in the system, and similar statistics. When CPU or storage utilization rises about 95% the severity of the event is raised and can be monitor.

Database Monitor

Another feature of LogAgent is the Database Monitor application for File Integrity Monitoring (FIM). This requires an additional license code. Check with your software provider on how to get that. With Database Monitor you can capture change activity in database files and send these events to a log collection server or SIEM solution. Database Monitor lets you set user and application access lists, and report on unauthorized access at the column (field) level. See the Alliance LogAgent Database Monitor User Guide for more information.

User auditing

Alliance LogAgent provides an easy way to view user profile authorities and change user auditing. In addition to viewing a user's explicit authorities on the user profile, Alliance LogAgent will inspect any group profile or supplemental group profile to determine any authorities that are inherited from these users. You can then view the authorities and change the audit setting for each user. Alliance LogAgent recommends an audit level for each user and you can change the audit setting.

Administrative user logging

When configured for this feature, Alliance LogAgent will identify events in QAUDJRN with a field that identifies the effective user as an administrative user. Configuration options allow the system administrator to define which special authorities will be considered for tagging as an administrative user. To determine the cumulative level of privilege the Group Profile and all of the Supplemental Group User profiles are inspected. The cumulative and real level of authority is then used for administrative user reporting to the log collection server or SIEM solution. The format for administrative user reporting is:

Syslog: “admin_user=yes” QRadar LEEF: “adminUser=yes” CEF: “admin_user=”yes””

User audit reporting

Alliance LogAgent provides a user audit report which will report users with administrative rights that mirrors the administrator logging information sent to the log collection server or the SIEM solution. The Print User Audit Report (PRTAUTRPT) command runs the user audit report and provides options for selecting which users to include in the report, which special authorities to include in the privilege definition, and options for including or excluding disabled user profiles and profiles with no password. This report can help the IBM i security administrator easily determine which users have a high level of privilege, and how that privilege is derived from their user profile, group profile and supplemental group profiles.

User-generated logs

Alliance provides command and API interfaces to allow a user program to create Syslog or CEF event records. User applications can provide simple text values for messages and specify the priority and facility ID for the message. Any user application can be enabled for Syslog or

CEF application messages.

Filtering log entries by Event Type

Alliance LogAgent gives you the ability to filter the system audit journal (**QAUDJRN**) entries that you want to send to a central log server. This can reduce the amount of network traffic and the type of events you transmit to the server. Alliance provides a complete list of log system security audit journal event types and the security administrator can edit the events to suppress transmission to the central log server.

Filtering log entries by System Value

Alliance LogAgent gives you the ability to filter the system audit journal (**QAUDJRN**) entries for selected system value changes. Some system values such as the time are changed automatically by the operating system and such changes do not constitute potential security issues. A list of potential system values to exclude is provided by Alliance LogAgent but are not enabled by default. You can enable the system value filters if you wish.

Filtering log entries by user

Alliance LogAgent gives you the ability to filter the system audit journal (**QAUDJRN**) entries by user name. This can reduce the amount of network traffic and the type of events you transmit to the server. To filter event entries by user profile name you create a list of excluded users. This option is available from the configuration menu. Common IBM-provided users are included in the list, but are not active by default. To exclude these users, and any other users you define, you can make the excluded users active.

Filtering log entries by library object

Alliance LogAgent gives you the ability to filter the system audit journal (**QAUDJRN**) entries by object name and library. This can reduce the amount of network traffic and the type of events you transmit to the log collection server. To filter event entries by object name you create a list of excluded objects, and then define a list of objects you want to include. You can exclude all objects in a library, selected objects, or object types. These options are available from the configuration menu.

Filtering log entries by IFS directory and file

Alliance LogAgent gives you the ability to filter the system audit journal (**QAUDJRN**) entries by IFS directory and file name. This can reduce the amount of network traffic and the type of events you transmit to the log collection server. To filter event entries by IFS name you create a list of excluded IFS directories and files, and then define a list of IFS directories and files you want to include. You can exclude and include all files in an IFS directory or selected IFS files. These options are available from the configuration menu.

Apache, OpenSSH, PHP, Perl, and MySQL server logs

Many IBM i customers use open source solutions such as the Apache web server, OpenSSH, Perl, or MySQL on the IBM i. These open source applications support normal logging functions. When enabled these applications send logs to the IFS directory **`/var/log`**. You can automatically send these logs to a Syslogd or Syslog-ng server using the Balabit Syslog-ng Open Source Edition or Premium Edition product. See the separate documentation on the Syslog-ng product.

Syslog-ng server for IBM i

Townsend Security has partnered with Balabit IT Security to bring the Syslog-ng product to the IBM i platform. This application can be installed and run as a service directly on the IBM i platform. The application runs in the Portable Application Solutions Environment (PASE). When installed on the IBM i the Syslog-ng server can be configured to send any logs in the IFS file system.

Syslog-ng – the new standard for syslog processing

Syslog-ng is the next generation of server processing for system log management. Syslog-ng is available in an open source version and in a premium edition that provides additional security and management functions (see http://www.balabit.com). Syslog-ng is shipped with most Linux distributions and is available for a wide variety of platforms. Syslog-ng can act in one of three roles:

- As a client to collect and forward log information
- As a relay to receive and forward log information
- As a consolidation server to receive logs and save to a database

By consolidating logs on a central server Syslog-ng enables intelligent evaluation of IBM i information in one location. See the separate documentation on the Syslog-ng software solutions.

Security information and event management

Security information management systems attempt to monitor the health and security of all of the significant server systems in an Enterprise. Typically this means consolidating syslog and other information from servers in one repository, and then performing real-time analysis, reporting, and alerts of potential problems. A number of vendors provide software and appliance solutions for log analysis. These solutions include IBM Security QRadar, HP ArcSight, LogLogic, Alert Logic, Splunk, and many others. Alliance LogAgent for IBM i provides the solution needed to bring the IBM i platform into a common information management strategy.

Change log

The following change log documents additions, corrections and changes to this manual.

VERSION	DATE	DESCRIPTION
2.00.001	8/19/2012	Complete revision of the manual and release for version 2.00 of Alliance LogAgent.
2.00.002	12/29/2012	Corrected the RSTLIB command to include the Authorization List.
2.10.001	2/18/2013	Added new security event type profile definitions, excluded user filters, and enhanced configuration for Database Monitor and File Integrity Monitoring (FIM).
2.20.001	1/7/2014	Added new exit point monitors.
2.60.001	4/22/2015	Added new support for the IBM QRadar LEEF format for security events.
2.70.001	2/15/2016	Added enhancements, new features, and minor bug fixes.
2.71.000	2/23/2016	Minor bug fixes
2.80.000	5/6/2016	Added LPAR reporting on all QAUDJRN event types. Add support for monitoring both the QSYSOPR and QSYSMSG message queues.
2.90.000	6/27/2016	New features for the QAUDJRN user exit point programs and minor fixes.
2.91.000	6/28/2016	Minor fixes.
3.00.000	8/29/2016	Updates to support V7R3 security events and new fields. Updates to application controls when ending the ALLSYL100 subsystem so that jobs quiesce in a more controlled fashion. Enhance the install and upgrade processes to ensure that the Authorization List is correct. The End ALLSYL100 Subsystem (ENDSYLSBS) command has been added to the product. Minor bug fixes.
3.10.000	10/30/2016	New support for identifying administrative users on events has been added to the product to meet compliance regulations (see more below). A new assessment report has been added to help identify administrative users. Minor bug fixes.

Chapter 2: Installation

Pre-requisites

The Alliance LogAgent for IBM i product runs on any version of IBM i operating system or i5/OS from V6R1 and later.

Installing from an Internet download

> ***NOTE:*** Starting with version 2.00 of Alliance LogAgent, you must create an application user profile and authorization list for the product. Use the following steps to create the user profile and related objects before installing the product.

You will need to sign on as `QSECOFR` and create an Authorization List called `ALLLGAOWN` and a User Profile called `ALLLGAOWN` to secure the product using the following commands:

```
CRTUSRPRF USRPRF(ALLLGAOWN) PASSWORD(*NONE) USRCLS(*SECOFR) INLMNU(

CRTAUTL AUTL(ALLLGAOWN) TEXT('Alliance AUTL for Ownership of LGA Pr
```

Next, you can add Users to the Authorization List by using the following commands:

```
ADDAUTLE AUTL(ALLLGAOWN) USER(user-profile) AUT(*ALL)
```

You can also add group profiles to the Authorization List.

When you download the Alliance product from the website, you must unzip the product. Your software provider will supply a pass phrase for extracting the files. See the `Readme.txt` file in the download for instructions on how to copy the software to the IBM i using FTP. Once you transfer the Save file to the IBM i you will restore the library `ALLSYL100` :

```
RSTLIB SAVLIB(ALLSYL100) DEV(*SAVF) SAVF(QGPL/ALLSYL) MBROPT(*ALL) .
```

Press ***Enter*** and then follow the prompts. Observe that all objects are restored.

Upgrading Alliance LogAgent for IBM i

To upgrade the Alliance product you must first end the **`ALLSYL100`** subsystem and rename the library:

```
Endsbs sbs(allsyl100) option(*immed)

Rnmobj obj(allsyl100) objtype(*lib) newobj(allsylold)
```

After renaming the library you can install the new version using the Internet download instructions above.

After installing the new version use the **`Apply Release Upgrade`** option on the **`Installation`** menu to copy your configuration information from the old library to the new version.

Reverting to a previous version after an upgrade

You can revert to a previous version of the product by renaming the new library to a save name, and then renaming the old version to the library **`ALLSYL100`**. This will restore the previous version.

License codes

Before you can configure and use Alliance LogAgent you must enter a temporary or permanent license code. Follow the instructions in the readme file to step through entering the trial license. Please contact your software supplier to receive permanent license codes. Please note that there are separate license codes for LogAgent, Database Monitor, and IBM Security QRadar support. The Open Source Edition of the syslog-ng client application does not require a license code to operate.

Historical QAUDJRN messages

If you will be sending system audit journal information to a log collection server or SIEM solution you may wish to set the starting position of the QAUDJRN journal to the current journal receiver. By default Alliance LogAgent collects journal entries from the beginning of the current chain of journal receivers. The date of all log entries is the date of the actual journal entry, but there may be a lot of historical information that you do not want to process. If you decide to delete QAUDJRN journal receivers before starting log collection you should consider making a permanent backup of system audit journals before deleting them. Use the Work With Journal Attributes (**`WRKJRNA`**) command to view the journal receivers for the **`QAUDJRN`** journal. Use option 6 on the configuration menu to set the starting position for QAUDJRN journal entries.

QAUDJRN exit points

Alliance LogAgent provides **`QAUDJRN`** exit point programs that will prevent the deletion of a journal receiver before it has been fully processed. The journal receivers can be deleted by security administrators, and some mirroring products will attempt to delete journal receivers. It is important that journal receivers are not deleted before they are read by LogAgent. You can prevent their deletion using the `QAUDJRN` journal exit points. The options to install or uninstall the exit points are on the LogAgent Installation menu.

The user running the job needs to be added to the Authorization List ALLLGAOWN. If you are running a version prior to 2.00, the user needs to be added to the ALLLGAUSE Authorization List.

Chapter 3: Configuring IBM i Security Audit Journaling

You must create the IBM i security audit journal `QAUDJRN`, related journal receivers, and turn on security auditing before attempting to send security information to a log collection server or SIEM solution. The full documentation is provided in the IBM publication "iSeries Security Reference". Please refer to this document at the IBM Information Center. The following section provides a summary of the steps needed to activate security auditing.

Create the security journal receiver

Create the first journal receiver in a user library that is backed up on a regular basis. You can use an existing library, or you can create a library to contain the journals. The library can have public authority, but the journal receivers should exclude public authority. Use a name with a 4 or 5 digit number at the end of the name, and start with sequence number 1. The operating system will automatically increment the sequence number by 1 when creating a new journal receiver.

```
CRTJRNRCV
    JRNRCV(MYLIB/AUDRCV0001)
    THRESHOLD(100000)
  AUT(*EXCLUDE)
  TEXT('Auditing Journal Receiver')
```

Create the QAUDJRN journal

Create the `QAUDJRN` journal in the `QSYS` library. You must have authority to the `QSYS` library and `*AUDIT` special authority. Use the following parameters for this journal:

```
CRTJRN
  JRN(QSYS/QAUDJRN)
  JRNRCV(MYLIB/AUDRCV0001)
  MNGRCV(*SYSTEM)
  DLTRCV(*NO)
      RCVSIZOPT(*RMVINTENT *MAXOPT3)
  AUT(*EXCLUDE)
  TEXT('Auditing Journal')
```

Change an existing QAUDJRN journal

If you have an existing **QAUDJRN** journal, you should change the Receiver Size Options (**RCVSIZOPT**) to specify ***RMVINTENT** and ***MAXOPT3** . This provides a much larger journal sequence number and will prevent sequence number resets of the journal which can interrupt transfer of events to a log collection server. You can use the following command to change the journal:

```
CHGJRN
  JRN(QSYS/QAUDJRN)
  JRNRCV(*GEN)
      RCVSIZOPT(*RMVINTENT *MAXOPT3)
```

Change the system values for auditing

You specify which types of events are collected in the **QAUDJRN** journal by specifying the system values for **QAUDLVL** and **QAUDLVL2** . You can view a list of all of the auditing values by prompting the values when using the **WRKSYSVAL** command.

To collect basic security information you can use the ***SECURITY** group value like this:

```
CHGSYSVAL
  SYSVAL(QAUDLVL)
  VALUE('*SECURITY')
```

An alternative to using the ***SECURITY** group is to use the Change Security Audit (**CHGSECAUD**) command to set the basic security values and start auditing.

> ***NOTE:*** This command will create the journal and journal receiver, change the audit levels, and start audit collection. It is recommended that you specify the actual values with the Change System Value command rather than the Change Security Audit command.

If you want to collect more extensive security information you can add the values **PGMFAIL** , **AUTFAIL** , **PGMADP** , **SAVRST** , **OFCSVR** , and **SERVICE** :

```
WRKSYSVAL
  SYSVAL(QAUDLVL)
```

Once this command is run, enter option **2** to edit the system values and type in the following values:

```
*SECURITY
  *PGMFAIL
  *AUTFAIL
  *PGMADP
  *SAVRST
  *OFCSRFV
  *SERVICE
```

Certain data security regulations require that you monitor for system changes. To collect events for system changes you can add the values `CREATE` , `DELETE` , `OBJMGT` , `OPTICAL` , and `SAVRST` :

```
WRKSYSVAL
  SYSVAL(QAUDLVL)
```

Once this command is run, take option `2` to edit the system values and type in the following values:

```
*AUTFAIL
*NETCMN
*SAVRST
*OFCSRFV
*SERVICE
*CREATE
*DELETE
*OBJMGT
*OPTICAL
*SAVRST
*SECURITY
```

There is a limit to the number of values you can specify in the `QAUDLVL` system value. Use the `*AUDLVL2` special value to indicate that additional values are to be found in the `QAUDLVL` system value.

Auditing privileged user profiles

You should consider auditing the activities of any user with security administrator, all object, or service authority. You can use the Alliance LogAgent configuration option to review user auditing and make changes. Or, you can turn on user auditing with the Change User Audit (`CHGUSRAUD`) command. Use this command to enable the highest level of monitoring for any IBM provided profile and any profile that you create with special authorities such as `*SECADM` , `*SERVICE` , or `*ALLOBJ` :

```
CHGUSRAUD
  USRPRF(QSECOFR)
  AUDLVL(*ALL)
```

Repeat this process for all privileged users.

Auditing database file access

To audit access to any file containing sensitive data such as credit card numbers, social security numbers, etc., use the Change Object Audit command (`CHGOBJAUD`). You may also want to audit access to files that contain configuration information. For IFS files use the Change Audit (`CHGAUD`) command. For QDLS files use the Change DLO Audit (`CHGDLOAUD`) command.

```
CHGOBJAUD
  OBJ(MYLIB/MYFILE)
  OBJAUD(*ALL)

CHGAUD
  OBJ('/mydirectory/*')
  OBJAUD(*ALL)

CHGDLOAUD
  FOLDER(MYFOLDER)
  OBJAUD(*all)
```

Note that you must specify the value `*OBJAUD` in the `QAUDCTL` system value to perform object auditing.

Auditing program access

You may have programs that adopt special authority or which perform sensitive functions. A program that adopts the `QSECOFR` profile authority, or which maintains salary data are examples of this type of program. You can make a list of programs that adopt authority by using the Display Program Adopt (`DSPPGMADP`) command. Use the `CHGOBJAUD` command to start auditing:

```
CHGOBJAUD
  OBJ(MYLIB/MYPROGRAM)
  OBJAUD(*ALL)
```

Note that you must specify the value `*OBJAUD` in the `QAUDLVL` or `QAUDLVL` system value to perform object auditing.

Establish the audit end action system value

Use the `Work With System Values` command to establish the action to take if the system cannot write to the security audit journal. It is unlikely that this will occur, but you should set a value for this event.

```
WRKSYSVAL
  SYSVAL(QAUDENDACN)
```

Once the command is run, take option `2` to edit and insert the following values to the list:

```
*NOTIFY
```

Forcing journal entries to auxiliary storage

Use the `WRKSYSVAL` command to establish how often journal records are written to disk, but the more impact journaling has on system performance. The smaller the value, the less likely the loss of journal entries. For most users the value of `*SYS` will provide a balance between performance and log collection reliability. For maximum security set the value to `1` .

```
CHGSYSVAL
  SYSVAL(QAUDFRCLVL)
  VALUE (*SYS)

CHGSYSVAL
  SYSVAL(QAUDFRCLVL)
  VALUE(1)
```

Start security journal auditing

The system value `QAUDCTL` controls the actual collection of system events to the `QAUDJRN` security journal. You must change this system value to indicate that event collection should start. Use the `CHGSYSVAL` command to enable security auditing:

```
CHGSYSVAL
  SYSVAL(QAUDCTL)
  VALUE('*AUDLVL' '*OBJAUD')
```

Chapter 4: Configuring Alliance LogAgent

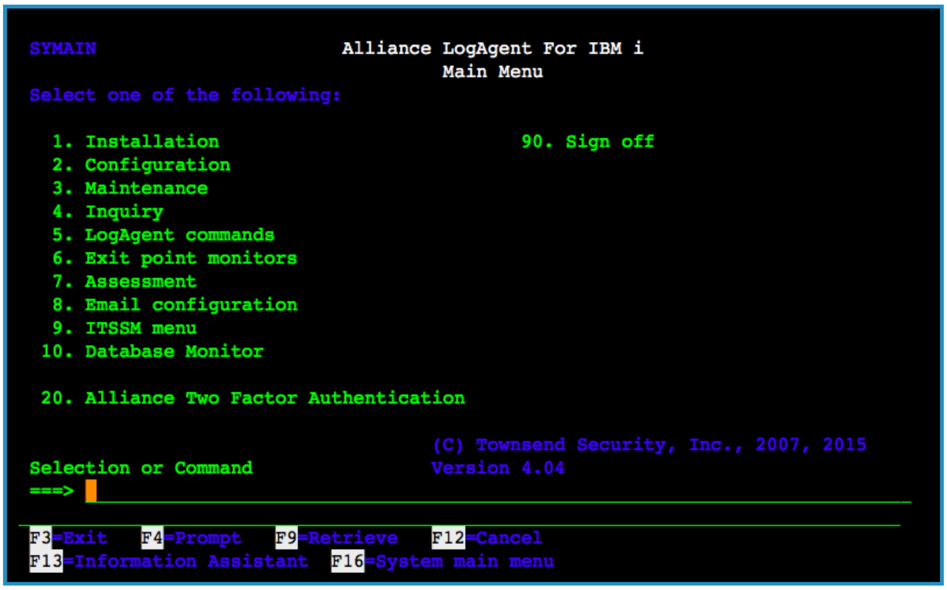
Configuring the Alliance LogAgent application involves configuring the global options for collecting and sending syslog messages, and configuring the communications client application to talk to the syslog server. Use the following options to configure global options and the communications client.

Displaying the main menu SYMAIN

After installing the Alliance LogAgent for IBM i product and entering a license code, you can configure the agent applications. You can display the main menu by adding the **`ALLSYL100`** library to your library list and displaying the main menu **`SYMAIN`** :

```
Addlible allsyl100
Go symain
```

The following menu panel is displayed:



From here you can start configuration (option 2), access logs (option 4), work with Database Monitor (option 10) etc.

Configuring Alliance LogAgent for IBM i

Take option 2 for **`Configuration`** , then option 1 to **`Configure Alliance LogAgent`** .

The following panel is displayed:

```
SY6040A                Configure Global Options           ROBBN      S214505V
                                                          11/09/17   05:49:59
Press Enter to continue, or press F3 or F12 to quit.

 Enable diagnostic logging  . . . .      2            1=Yes, 2=No
 Enable QAUDJRN messages  . . . . .      1            1=Yes, 2=No
   Interface version  . . . . . . .        3          1=Syslog, 2=CEF
                                                      3=Version 3 syslog

   Transmit . . . . . . . . . . . .        1          1=Yes, 2=No
   Restart on error . . . . . . . .        2          1=Yes, 2=No
 Data queue control . . . . . . . .      1            1=Yes, 2=No
 Enable QSYSOPR messages  . . . . .      2            1=Yes, 2=No
 Enable QSYSMSG messages  . . . . .      2            1=Yes, 2=No
 Enable QHST messages . . . . . . .      2            1=Yes, 2=No
   Message routing  . . . . . . . .      2            1=QAUDJRN, 2=Direct
   Filter option  . . . . . . . . .      1            1=All, 2=All logon/logoff
                                                      3=Sec Admin logon/logoff
                                                      4=QSECOFR logon/logoff
   QAUDJRN entry type . . . . . . .      00           Range 00 to 99
   Force QHST messages  . . . . . .      2            1=Yes, 2=No
                                                                    More...
F1=Help    F3=Exit    F12=Cancel
```

> ***NOTE:*** Any changes made in the configuration panels require you to end and restart the subsystem to take effect.

Enable diagnostic logging

The diagnostic logging option can help with troubleshooting. Enter option `1` (Yes) to `Enable diagnostic logging`. When diagnostic logging is enabled the job descriptions are set for maximum job logs. Enter option `2` (No) to disable application logging. These logs fill up fast so we recommend not using logging until needed, or managing the log file (allsyl100/allloga) to conserve resources.

Enable QAUDJRN messages

Enter option `1` (Yes) to enable sending `QAUDJRN` messages to a syslog server. When enabled the system security audit journal reader job will be started in the Alliance subsystem `ALLSYL100`. Enter option `2` (No) to not send audit journal entries to the syslog server. The default is `1` (Yes).

Interface version

Enter option `1` for the older first version of Alliance LogAgent interface. Enter option `2` to use the Common Event Format (CEF) for the interface. Enter option `3` for the advanced version of the interface which provides messages in RFC3164 format. Option `3` is recommended and is set as the default. For users of the IBM QRadar solution enter the value of `4` for the LEEF format.

Transmit

Enter option `1` (Yes) to transmit the log events to a log collection server or SIEM product. Enter option `2` (No) to not transmit logs. The default is set at `1` (Yes).

Restart on error

Enter option `1` (Yes) to restart the `QAUDJRN` event processing after an error. Enter option `2` (No) to terminate the `QAUDJRN` event processing when an error occurs.

Data queue control

Enter option `1` (Yes) to use **`Data queue control`**. Enter option `2` (No) to not use data queue control. Option `1` for data queue control is recommended if you are transmitting log entries to a log collection server using TCP.

Enable QSYSOPR messages

Enter option `1` (Yes) to enable sending **`QSYSOPR`** messages to a syslog server. Enter option `2` (No) to not send **`QSYSOPR`** messages to the syslog server.

Enable QSYSMSG messages

Enter `1` (Yes) if you want to capture system messages. Enter `2` (No) if you do not want to capture system messages. The default message queue for system messages is QSYSMSG.

Enable QHST messages

Enter option `1` to enable collection of **`QHST`** messages to the system security audit journal **`QAUDJRN`**. Enter option `2` to not collect **`QHST`** messages to the security audit journal. You must restart the **`ALLSYL100`** subsystem to start collecting messages. When enabled the job **`QHST`** will start as a subsystem job.

Message routing

Enter option `1` to send **`QHST`** messages to the security audit journal **`QAUDJRN`**. Enter option `2` to send messages directly to the log collection server. Sending messages directly to the log collection server is the recommended setting.

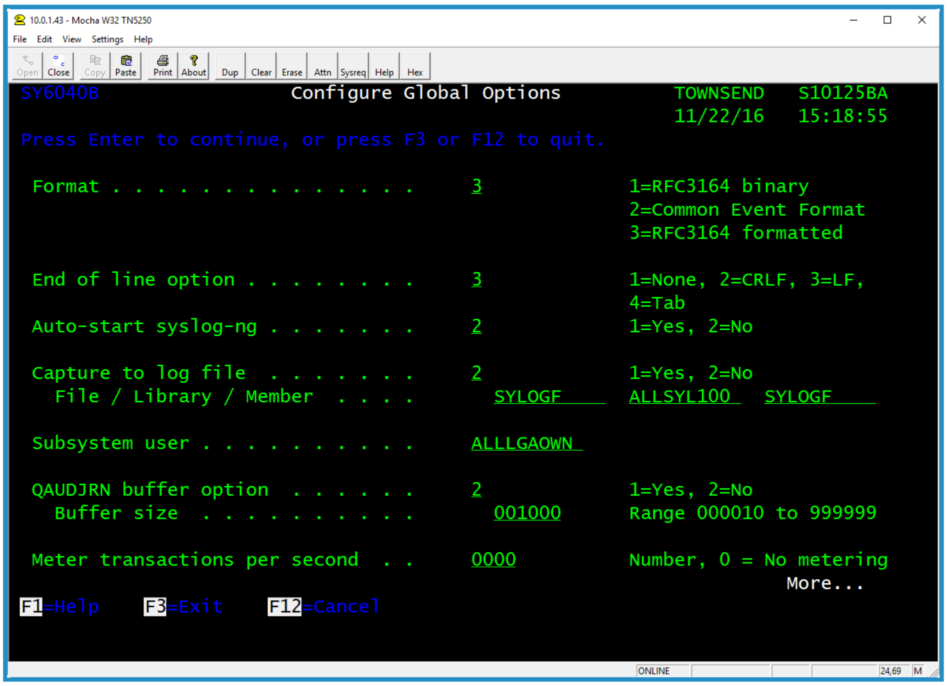
Filter option

Enter `1` to send all **`QHST`** messages to the log collection server. This is the default. Enter option `2` to send only log on and log off messages to the log collection server. This option will send log on and log off messages for all users. Enter option `3` to send log on and log off messages only for security administrators. Enter option `4` to send log on and log off messages for the **`QSECOFR`** user to the log collection server.

QAUDJRN entry type

If you enable writing **`QHST`** messages to the **`QAUDJRN`** security journal you must define an entry type to identify them. Enter the user defined entry type in this field. This is a numeric value from `00` to `99`. Generally it is better to send QHST events directly to the SIEM rather than through QAUDJRN because the information arrives on the SIEM faster.

Press ***Enter*** to display the second panel:



Format

Enter option **1** to create log messages in the Syslog format (RFC 3164). Enter option **2** to create log messages in Common Event Format (CEF). Enter option **3** for Advanced RFC 3164 format. Option 3 is the recommended option. For IBM QRadar users select option **4** for the LEEF format.

End of line option

Enter option **1** to not add any end of line characters. Enter option **2** to use carriage return and line feed characters at the end of each line. Enter option **3** to use a line feed character at the end of each line. Enter option **4** to use the tab character at the end of each line.

Auto-start syslog-ng

Enter option **1** (Yes) to automatically start the syslog-ng Premium Edition application in the Alliance subsystem environment. Enter option **2** (No) to not start the syslog-ng application. Note that you must first install the syslog-ng application from the **Alliance Configuration** menu, and you must configure it to collect logs. Contact your software provider for more information.

Capture to log file

Enter option **1** (Yes) to capture log events to a physical file. Enter option **2** (No) to not capture to a physical file. Option **2** is the default value. This will write everything we are sending to the SIEM into a file. This file can get full quickly so you must clear it or manage it when you are using it. We recommend keeping it **2** (No) when not using it.

Log file / Library / Member

If you entered the option to log to a physical file, enter the file name, library name, and member name in this field. You can use SYLOGF in ALLSYL100 or define your own.

Subsystem user

The Subsystem user name has to be ALLLGAOWN in releases 2.0 and after. This user and associated authorization list has to have been created before installing or upgrading Alliance LogAgent.

QUADJRN buffer option

Use this parameter to enable buffering of data communicated to a log collection or SIEM server. Most SIEM servers today have no problem taking in the events we send. Buffered transmission can add significant performance advantages. However, there is some risk that transactions may be lost if there is an abnormal termination of the `QAUDJRN` collector or communications job. If you enable buffering and need to check on the last event transmitted, review the log collection server and note the last journal sequence number. You can then set the starting point for the `QAUDJRN` to that sequence number.

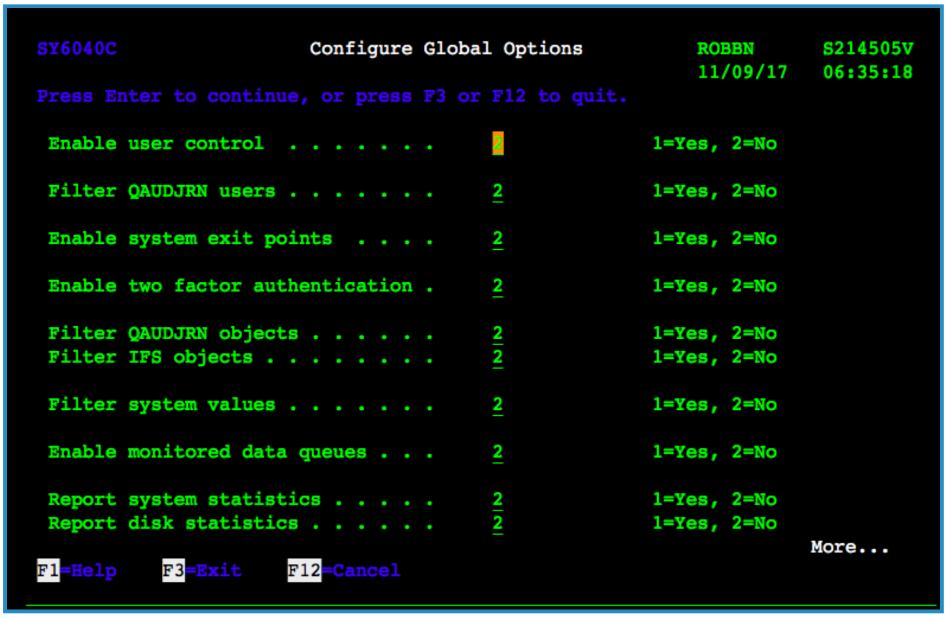
Buffer size

Enter a buffer size for transmission buffering. It is recommended that you start at `500` and increase this value if needed.

Meter transactions per second

Use this parameter to meter transactions being sent to your log collection or SIEM server. A value of zero (`0`) indicates no metering. Any other value will restrict the transmission to this number of transactions per second. Again, most SIEM servers today handle our transmissions with no issue.

Press ***Enter*** to display the third panel.



Enable User Control

If you take option 17 `Work with authorized users` on the configuration menu to create a list of users authorized to make changes with the LogAgent application you must enable it here for it to take affect. Enter `1` to enable user control. Enter `2` to disable user control.

Filter QAUDJRN users

Use this parameter to enable filtering of `QAUDJRN` users. You must first define a list of excluded users in option 7 `Work with QAUDJRN excluded users` on the configuration menu

Enable system exit points

Enter `1` (Yes) to enable Alliance LogAgent exit point monitoring. Enter `2` (No) to not enable exit point monitoring. If you have enabled exit points you can disable all exit point monitors by changing this option to `2` for No.
In addition to enabling exit point monitoring here, you must take option 3 on the main menu to **`Work with security types`** and by putting a 2 to change by the type you want to activate, enable the user exit point and define the program and library. You must also take option 13 from the configuration menu to **`Work with Exit point monitors`** and make the status active. Then back on the main menu take option 6 and enable the exit point monitor. On the iSeries end the host servers with the **`ENDHOSTSVR`** command with the option for *SIGNON, and then restart the host servers. End and restart the subsystem for all these changes to take effect.

Enable two factor authentication

Enter `1` (Yes) to enable Alliance Two Factor Authentication. You must have the Alliance Two Factor Authentication solution installed and licensed in order to activate this option. When enabled you will be required to authenticate via 2FA before you can make any configuration changes. Enter `2` (No) to not enable Two Factor Authentication.

Filter QAUDJRN objects

Use this parameter to enable filtering of **`QAUDJRN`** objects. Objects will be filtered based on the object filter definitions you create using options 8 and 9 on the configuration menu. Option 8 **`Work with QAUDJRN excluded objects`** allows you to exclude objects and option 9 **`Work with QAUDJRN included objects`** allows you to define object to include in monitoring.

Filter IFS objects

Enter `1` (Yes) if you wish to enable filtering of IFS objects. Enter `2` (No) if you do not want to filter IFS objects. When you enable this option you can define IFS directories and files to exclude and include. You must also define exclusion and inclusion rules using options 10 and 11 on the configuration menu to ` Work with QAUDJRN excluded IFS **`and`** Work with QAUDJRN included IFS`.

Filter system values

Enter `1` (Yes) to enable filtering system values. Enter `2` (No) to not enable system value filtering. If you enable this option you must define the system values you want to filter using option 12 in configuration menu to **`Work with excluded system values`**. A set of system values are provided by Alliance LogAgent but are inactive. You can review and activate the system values as appropriate for your security implementation.

Enable monitored data queues

Enter `1` (Yes) if you want to enable the monitoring and reporting of event information in user data queues. Enter `2` (No) to not enable user data queue monitoring. User data queue monitoring provides a way for your applications to write security and informational events to a data queue which is monitored by Alliance LogAgent. Alliance LogAgent will read the data queue entries and format them to syslog, LEEF, or CEF format and transmit them to a SIEM solution or log collection server.
If you choose to monitor data queues you must do a controlled shut down of the subsystem. Use the ENDSYLSBS command. The susbsystem will not end if the data queue jobs have not

ended.
Use option 14 ` Work with monitored data queues` on the configuration menu to define your data queues.

Report system statistics

Enter 1 (Yes) to report system statistics. Enter 2 (No) to not report system statistics. System statistics includes information such as percent CPU utilization, percent storage utilization, number of jobs in the system, temporary storage utilization, and other basic information about system health.

Report administrative users

Enter 1 (Yes) to report administrative users. Enter 2 (No) to not report administrative users through the additional event field. When you enable this option Alliance LogAgent will inspect the special authorities of the user, of the group profile, and of all supplemental group profiles to determine if this user is an administrative level user. Administrative level users are reported through the event fields:

Syslog: admin_user=yes LEEF: adminUser=yes CEF: admin_user="yes"

The special authorities used to determine the administrative level of the user can be defined on the following fields.

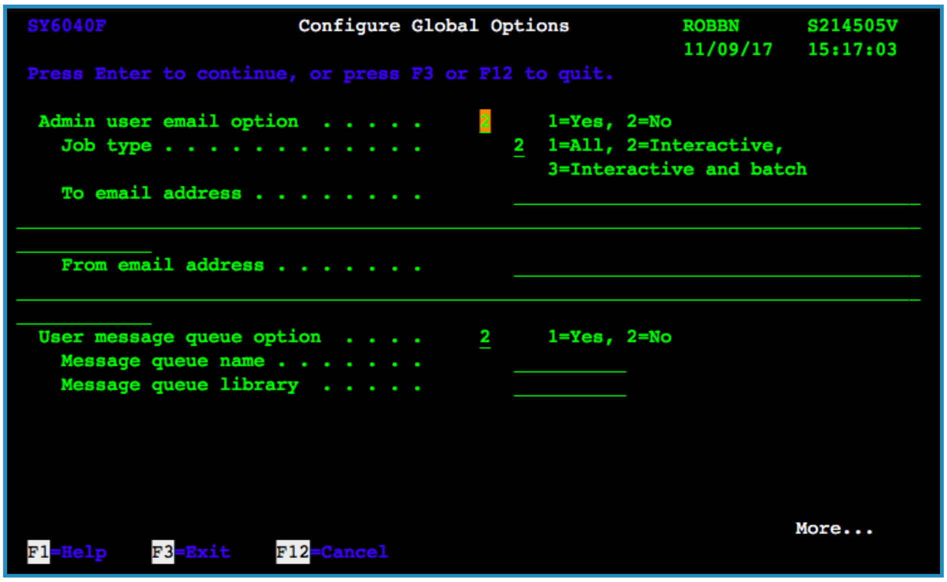
****ALLOBJ through *SPLCTL***

Enter 1 (Yes) for each special authority that you wish to include to identify an administrative user. Enter 2 (No) to exclude the special authority value from determining the administrative level of the user.

Exclude admin users

Many IBM-supplied user profiles do not have passwords enabled for system signon. You can exclude these user profiles by entering 1 (Yes) next to the specific IBM user profile. Enter 2 (No) to not exclude these user profiles. If you select the option to exclude these user profiles you should view the user profile to insure that they are not enabled for signon.

Press ***Enter*** to display the next panel.



```
SY6040F                 Configure Global Options           ROBBN     S214505V
                                                           11/09/17  15:17:03
Press Enter to continue, or press F3 or F12 to quit.

 Admin user email option  . . . . .        2      1=Yes, 2=No
   Job type . . . . . . . . . . . .          2    1=All, 2=Interactive,
                                                  3=Interactive and batch
   To email address . . . . . . . .

   From email address . . . . . . .

 User message queue option  . . . .        2      1=Yes, 2=No
   Message queue name . . . . . . .
   Message queue library  . . . . .

                                                                   More...
 F1=Help     F3=Exit     F12=Cancel
```

Admin user email option

Enter `1` (Yes) to enable email notification for administrative users. Enter `2` (No) to not enable email notification of administrative users. If you choose to enable email notifications here you must enter an email address.

NOTE:
Using the email notification option requires that you configure email services in Alliance LogAgent. On the main menu `SYMAIN` take option 8 `Email configuration`. Option 10 `Application settings allows you to configure LogAgent to communicate with your email server.

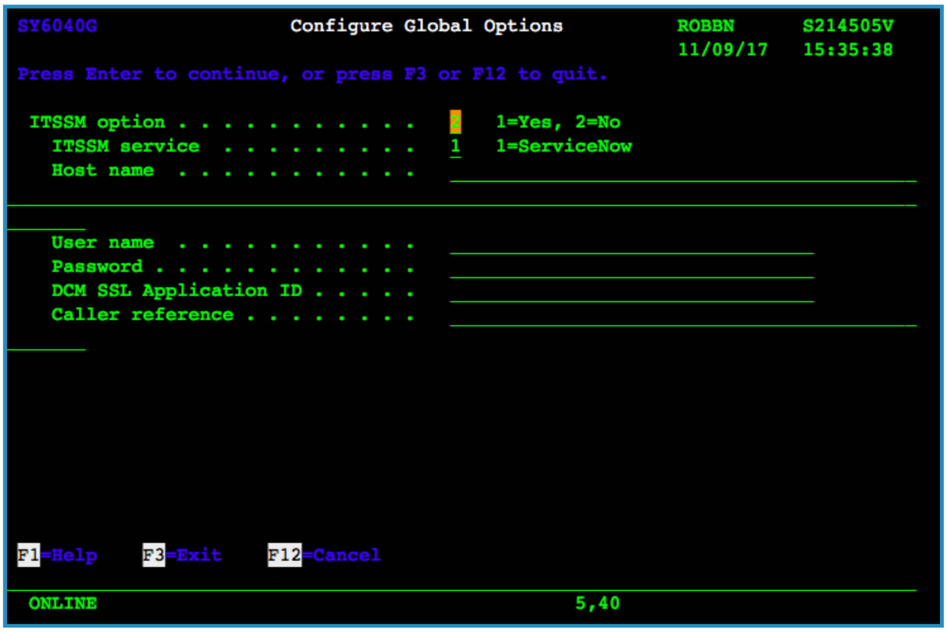
User message queue option

Enter `1` (Yes) to enable monitoring a user message queue. Enter `2` (No) to not enable the monitoring of a user message queue.

User message queue name and library

If the User message queues option is enabled enter the name of the message queue and the library name.

Press ***Enter*** to display the next panel.



ITSSM option

This option is used to activate integration and reporting to ServiceNow. If you do not use ServiceNow or do not want LogAgent to start tickets on specific events, leave the option as `2` (NO). If you want to activate it, make the option `1` (YES).

ITSSM service

Choose `1` for ServiceNow

Host Name

Enter your ServiceNow host name.

User name

Enter your user name for ServiceNow

Password

Enter your password for ServiceNow

DCM SSL Applictaion ID

Enter your Application ID from DCM. This is required for the SSL connection.

Caller reference

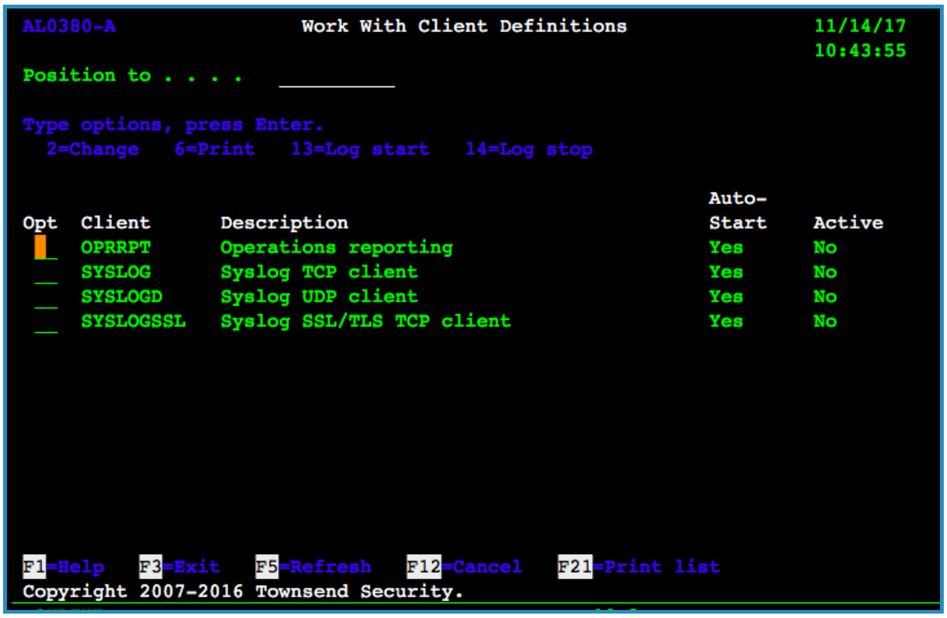
Enter your caller reference.

Press ***Enter*** to complete configuration and accept any changes made.

Configuring TCP client communications

In order to send syslog entries to a syslog server you must configure the Alliance TCP client communications. From the `Configuration` menu enter the option to `Work With TCP Clients`.

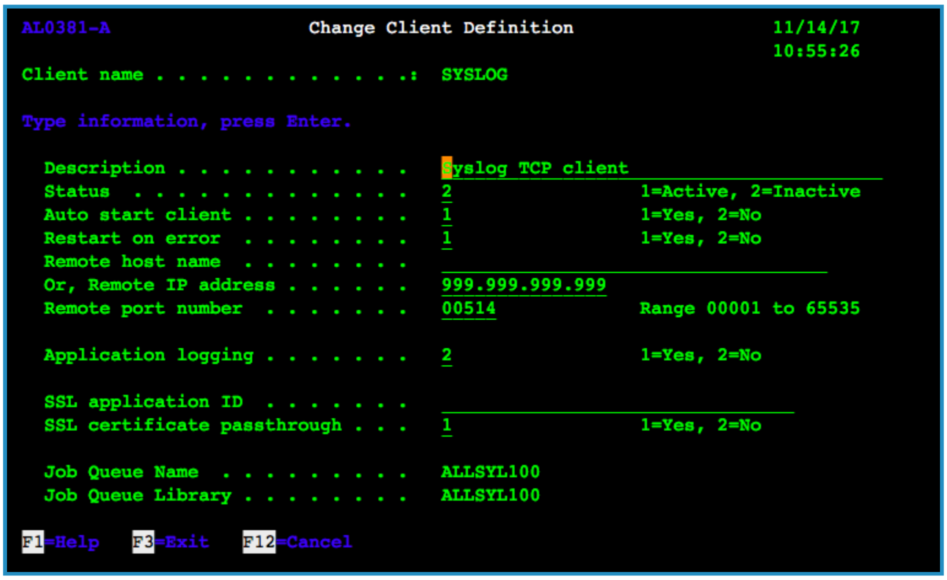
The following panel is displayed:



Four sample configurations are displayed. The first sample OPRRPT is used when Operational reporting is turned on in Database Monitor. SYSLOG uses standard TCP sockets to send syslog records to a Syslog-ng server. The second sample SYSLOGD sends log records to a Syslogd server using standard UDP communications. The third sample uses TLS TCP sockets to send syslog records to a Syslog-ng server using secure SSL communications. Your SIEM vendor or network administrator will be able to tell you what format to use. You have to use one of these existing configurations and you can only enable 1 unless using OPRRPT. OPRRPT can be enabled with any other client.

Enter option `2` to change a configuration.

When you enter option `2` to change the TCP client configuration the following panel is displayed:



Client name

The name of this configuration.

Description

Enter a description for this configuration.

Status

Enter `1` (Active) or `2` (Inactive). When the status is inactive the TCP client application will not be enabled.

Auto start client

Enter `1` (Yes) to automatically start the TCP client communications when the **`ALLSYL100`** subsystem starts. Enter `2` (No) to not automatically start the TCP client. Normally you will want to automatically start the TCP client application when the subsystem starts.

Restart on error

Enter `1` (Yes) to restart event processing after an error occurs. Enter `2` (No) to not start after an error.

Remote host name

Enter the DNS name for the syslog server. You can use the next field for the IP address if you do not have a DNS name for the server. But you must use EITHER the DNS OR the IP, not both.

Or, Remote IP address

Enter the IP address of the syslog server if you do not have a DNS name.

Remote port number

Enter the port number for the syslog server. Consult with your network administrator for the port number. This will be the port number for the source syslog TCP service.

Application logging

Enter `1` (Yes) to enable application logging. Enter `2` (No) to not enable application logging. When this option is enabled detailed log records are written to the file `ALLOGA`. These log entries are not sent to the syslog server.

> ***NOTE:*** We recommend keeping this turned off as the file grows very quickly.

SSL Application ID

If this client application chosen is SYSLOGSSL, it will use secure TLS communications. Enter an Application ID created in Digital Certificate Manager.. You can use the IBM DCM to create certificates and associated Application IDs.

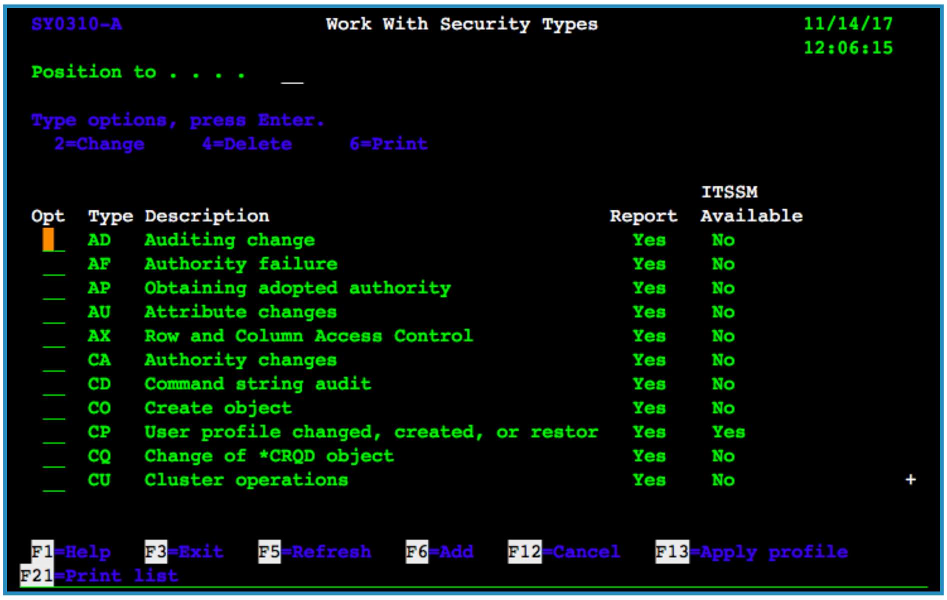
SSL certification passthrough

Enter `1` (Yes) to enable certificate passthrough. Enter `2` (No) to not allow certificate passthrough. Enabling certificate passthrough will disable certificate validity checking, but will not allow un-secure connections.

Press ***Enter*** to add the client and save the configuration.

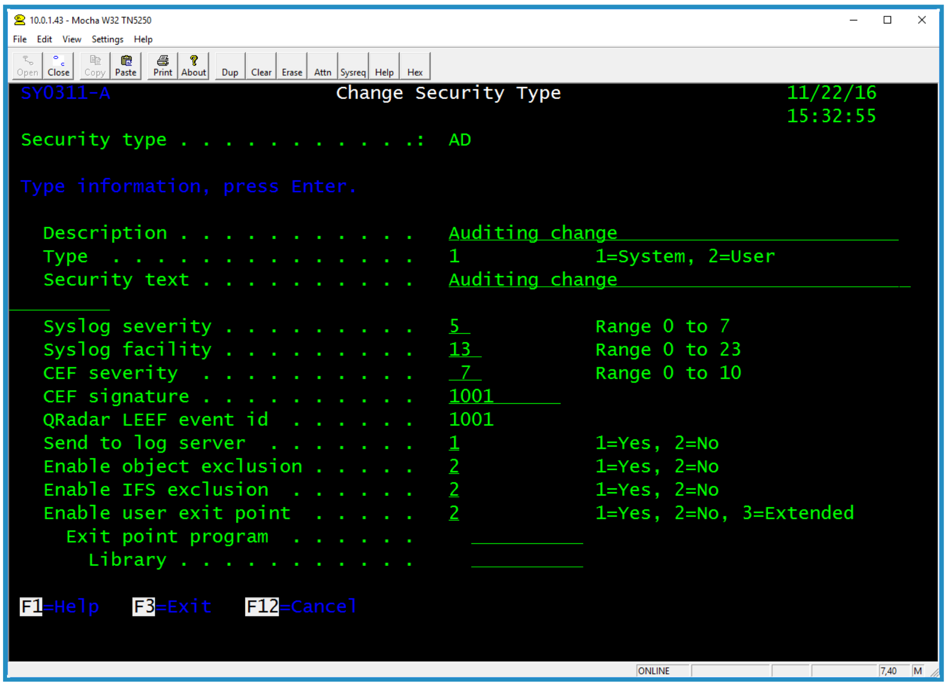
Work with security types

From the `Configuration` menu, enter the option to `Work with Security Types`. Use this option to define user-created `QAUDJRN` journal entries.



When a user application sends an entry to the security journal `QAUDJRN` a user-defined journal entry type is used. This is a two-character value and is different than the journal entry types that are created by i5/OS. In order to report these events you need to define them with this option and provide text and severity values. You must have `QSECOFR` authority to access this option.

When you enter option `2` to change a security type, the following panel is displayed:



Description

Enter a **`Description`** for this journal entry type, or use the default description.

Type

The **`Type`** indicates whether the event is a system provided event or a user defined event. This is an output field only.

Security text

Enter the text to be used with the log message. This text should be a brief description of the event type. You can use the default text.

Syslog severity

Enter a value for the severity of this event type. The lower the value, the higher the severity level of the message.

Syslog facility

Enter a facility ID for this event type. See the documentation in RFC 3164 for information on facility IDs. Since the priority of an event is the result of adding the severity by the facility, the lower the facility number the higher the severity of the message.

CEF severity

If you are reporting log events in the Common Event Format (CEF) enter the severity level. The higher the severity number the more severe the event.

CEF signature

If you are reporting events using CEF as defined in the previous field, enter a signature number for this event type. Alliance uses signature values from **`1000`** to **`1999`** so you should avoid signature values in this range.

QRadar Event ID

This is an output only field and displays the value of the QRadar Event ID.

Send to log server

Enter option **1** (Yes) to send this type of event to a log server. Enter option **2** (No) to suppress sending this event type to the log server. The default is option **1** (Yes).

From the event type list you can use function key ***F13*** to display a list of profile options. Profile options include the ability to turn off all IBM and user event types, and to define common IBM security types. When you press ***F13*** the following panel is displayed:

Enable object exclusion

Enter option **1** (Yes) to enable the exclusion of objects for this event. Enter option **2** (No) to not enable object exclusion. The default is option **2** (No). You must also define object exclusion rules on the Configuration Menu (options 8,9) for this option to take effect.

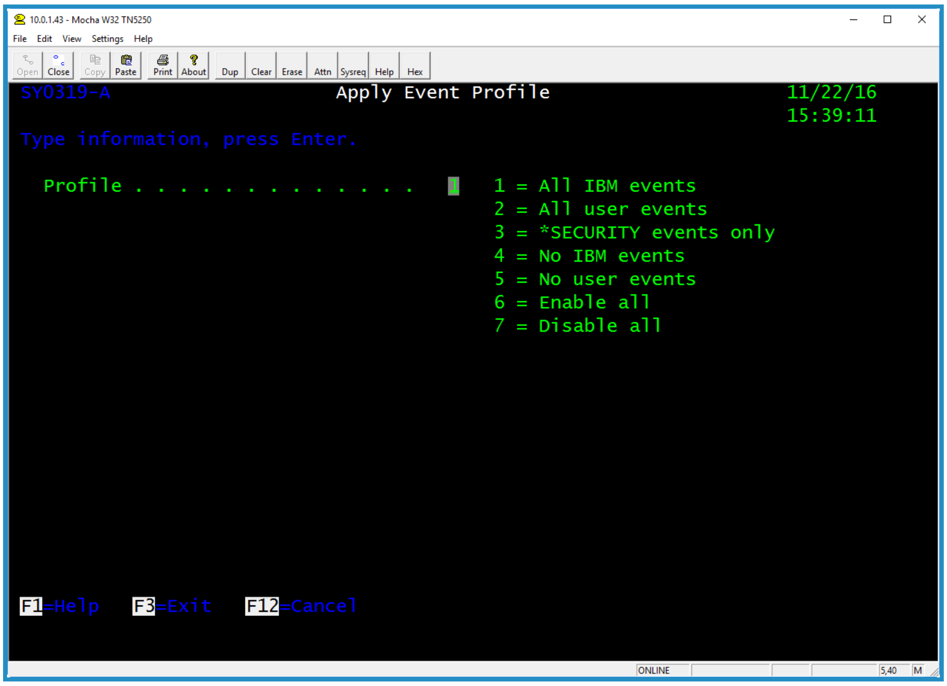
Enable IFS exclusion

Enter option **1** (Yes) to enable the exclusion of IFS objects for this event. Enter option **2** (No) to not enable IFS object exclusion. The default is option **2** (No). You must also define IFS object exclusion rules on the Configuration Menu (options 10, 11) for this option to take effect.

Enable user exit point

Enter option **1** (Yes) to enable a user exit point for this event. Enter option **2** (No) to not enable a user exit point. The default is option **2** (No). Enter **3** (Extended) for processing. If you enable user exit points for security events you must specify a program name. See the source file QCLSRC in the product library for examples of the user exit point parameters and formats. The Extended format allows for the exit point program to return a flag indicating that the event should or should not be processed. This gives LogAgent users the ability to filter events based on their own application logic and security policies.

Press F13 to apply a profile to selected security events.

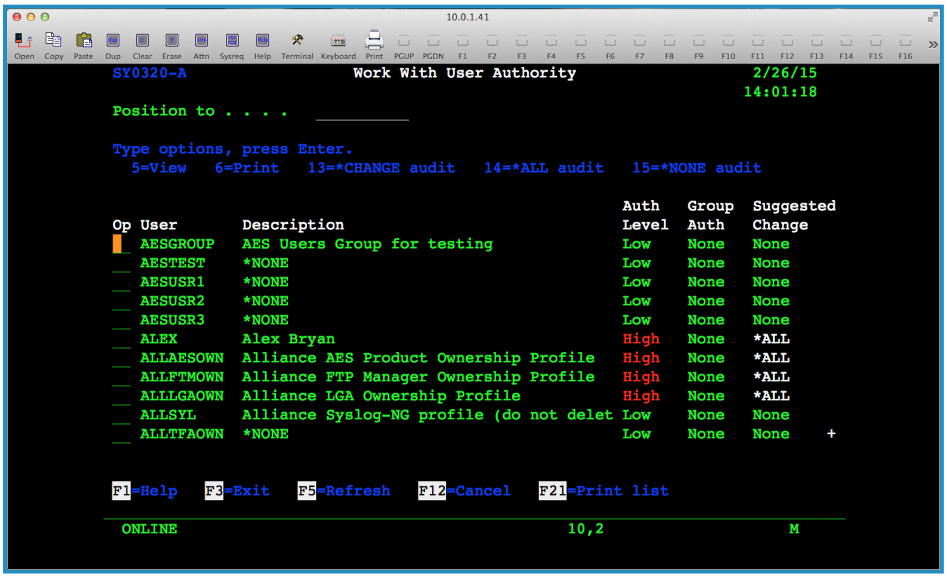


Use option **1** to enable reporting of all IBM event types. Use option **2** to enable reporting of all user types. Use option **3** to enable reporting of all security types as defined by IBM. Use option **4** to turn off reporting of all IBM events. Use option **5** to turn off reporting of all user event types. Use option `6` to enable reporting of all event types. Use option `7` to disable reporting of all event types.

Work with user audit

From the `Configuration` menu, use this option to view user profile security and audit settings, and to make changes to use audit options. This option will build a list of user profiles, resolve the group profile and supplemental group profile authorities, and recommend changes to user auditing settings. All users with a high level of security and object privileges should have user auditing enabled. Alliance LogAgent will recommend that users with security administration and all object authorities have the maximum level of user auditing enabled. Users with programmer or system operator privileges will be recommended for a medium amount of user auditing.

The following panel is displayed:



Op (Option)

Use this field to view, print, or change the audit level for a user profile.

User

The user profile name.

Description

The description of the user from the user profile. Only the first 40 bytes of the description are displayed.

Authority Level

The authority level assigned by LogAgent for this user. Any user with security officer, security administrator, system configuration, service, or all object authority will be classified as having a high level of authority. Programmers, system operators, and any user with job control authority will be classified as having a medium level of authority. All other uses will be classified as having a low level of authority.

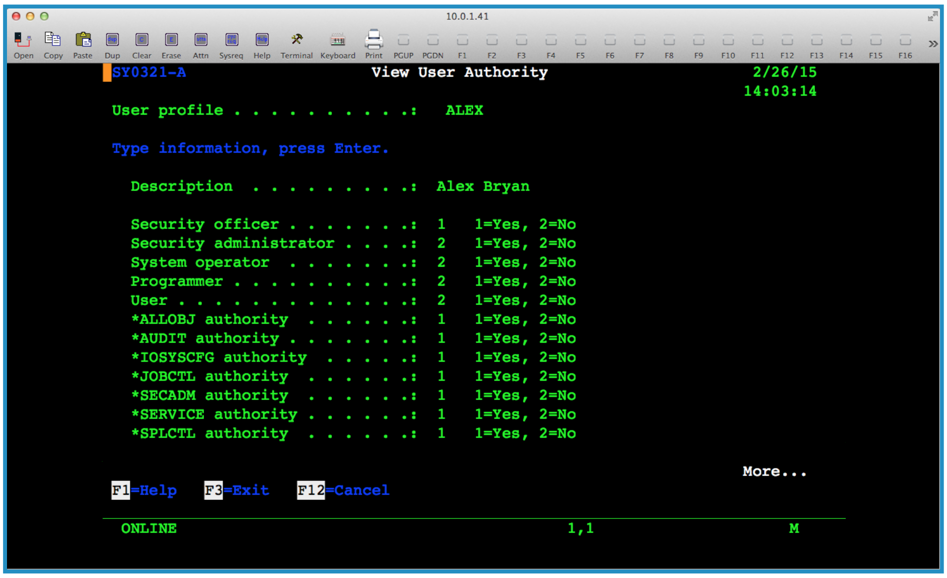
Group Authority

The parameter Group indicates that some of this user's authority is received from a Group Profile on their user profile. The parameter Supp indicates that some of this user's authority was inherited from a profile in the supplemental group for this user. The parameter Both indicates that some of this user's authority was inherited from both the group profile and profiles in the supplemental group.

Suggested Change

Alliance will suggest changes to user auditing if auditing is not already enabled. The value `*ALL` will be assigned to users with a high level of authority. The value of `*CHANGE` will be assigned to users with a medium level of authority. You can use options `13`, `14`, and `15` to change a user's authority to the value you think appropriate.

When you enter option `5` to view a user, the following panel is displayed:



Description

This is the description from the user profile.

Security officer, Security administrator, System operator, Programmer, User

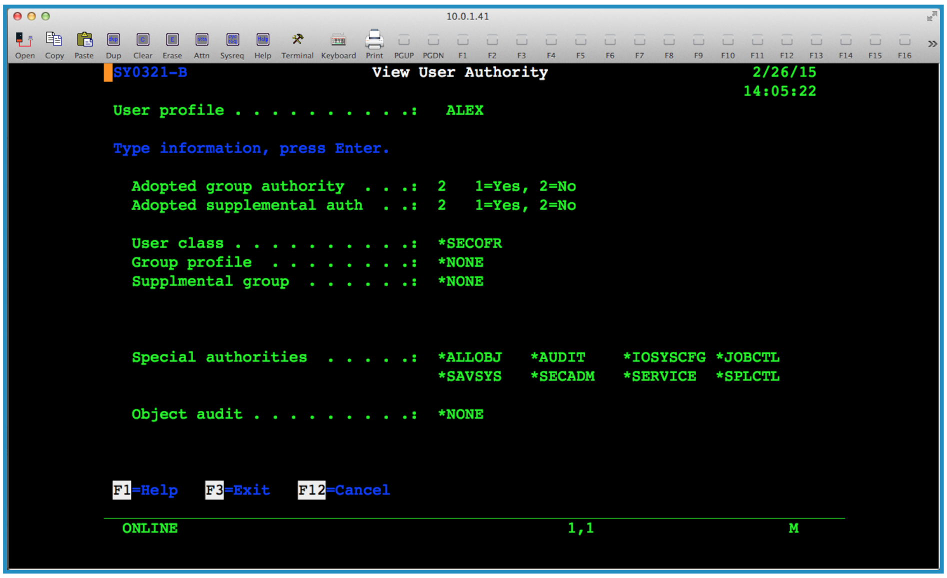
These values indicate the class of the user profile. Note that the values may be inherited from a group profile or a profile in the supplemental group for this user.

**ALLOBJ, *AUDIT, *IOSYSCFG, *JOBCTL, *SECADM, *SERVICE, *SPLCTL autho*

These values indicate the special authorities of the user. Note that the values may be inherited from a group profile or a profile in the supplemental group for this user.

Press ***Enter*** to continue.

The following panel is displayed:



Adopted group authority

This value is `1` if some of this user's authority is adopted from the group profile.

Adopted supplemental auth(ority)

This value is `1` if some of this user's authority is adopted from a supplemental group profile.

User class

This value indicates the class of this user. This value is not affected by the group profile or profiles in a supplemental group.

Group profile

The group profile for this user.

Supplemental group

The user profiles in the supplemental group for this user.

Special authorities

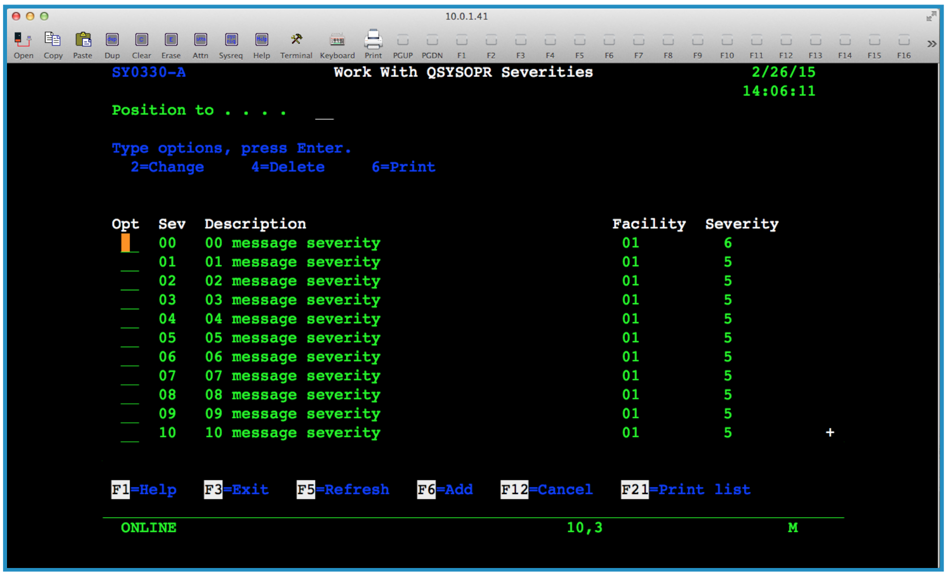
A list of special authorities for this user.

Object audit

The current setting for user auditing for this user.

Work with QSYSOPR severities

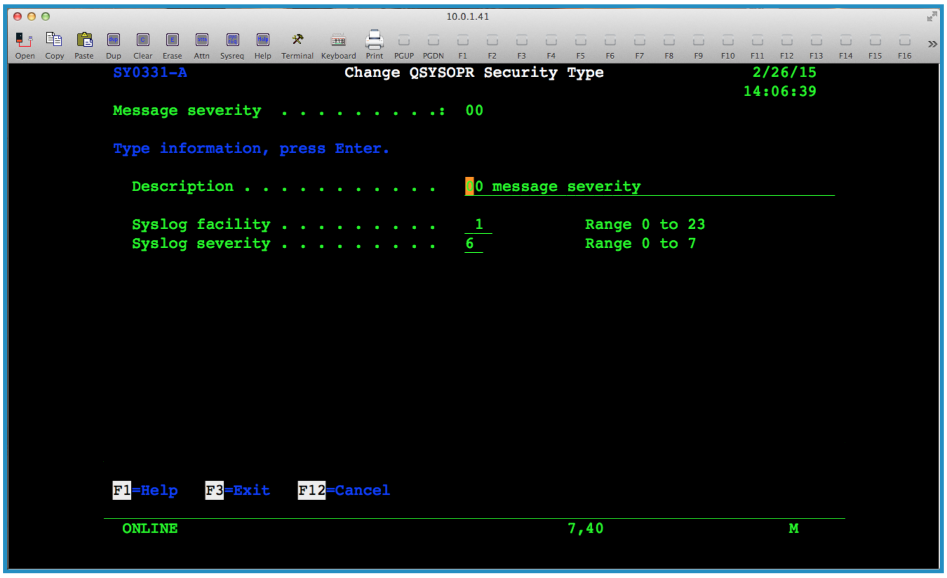
From the `Configuration` menu, use this option to associate the message severities in the `QSYSOPR` message queue with syslog severity values. Alliance LogAgent provides a default set of mappinsg between the severity of a message in `QSYSOPR` to the severity of the event reported to the syslog server. You can use this option to change these default mappings.



Opt(ion)

Enter option **2** to change, option **4** to delete, or option **6** to print the severity mapping. It is recommended that you do not delete entries in this table.

Use this panel to add or change a mapping between **QSYSOPR** message severity to syslog facility and severity.



Description

Enter a description for this mapping.

Syslog facility

Enter a syslog facility value for this mapping. Refer to the open standard document RFC 3164 for a definition of facility values.

Syslog severity

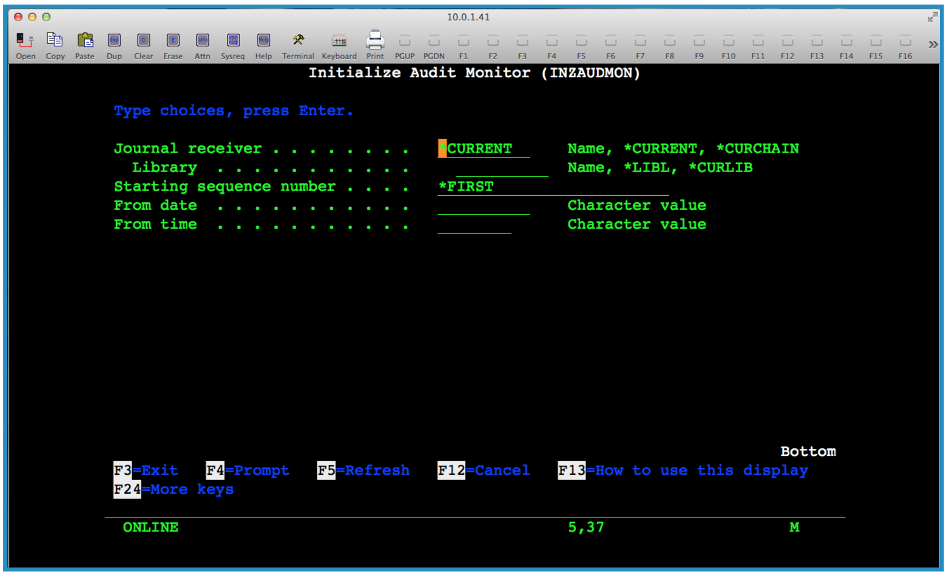
Enter a value for the severity of this message. Refer to the open standard document RFC 3164 for a definition of severity values.

Change QAUDJRN Starting Point

Use this option to define the starting point for the `QAUDJRN` extraction and reporting process. After installation Alliance LogAgent will start with the first entry in the first `QAUDJRN` journal receiver. You may wish to skip some of the older events. You can do this by specifying a starting journal sequence number and journal receiver.

To determine the name of the `QAUDJRN` journal receiver, use the Work With Journal Attributes (`WRKJRNA`) command for the journal `QAUDJRN` . This command will show you the name of the currently attached journal receiver.

The following panel is displayed:



Journal receiver and library

Enter the starting journal receiver and library. If you leave this field blank Alliance will use the first available journal receiver. If you specify a journal receiver name, Alliance will start with this journal receiver. The special value `*CURCHAIN` starts event processing with the first available journal receiver. The value `*CURRENT` starts event processing with the most recent journal receiver. If you have a large number of journal receivers on your system, it is recommended that you use the `*CURRENT` value for this parameter.

Starting sequence number

Enter the starting sequence number. This is a 20 digit sequence number, or a special value such as `*FIRST` . You set this value to `1` to start at the beginning of a journal receiver. Alliance will detect that the starting sequence number of a specific journal is larger and will start at the actual first entry in the journal receiver. You can use the Display Journal Receiver Attribute (`DSPJRNRCVA`) command to view the first sequence number in the journal.

From date

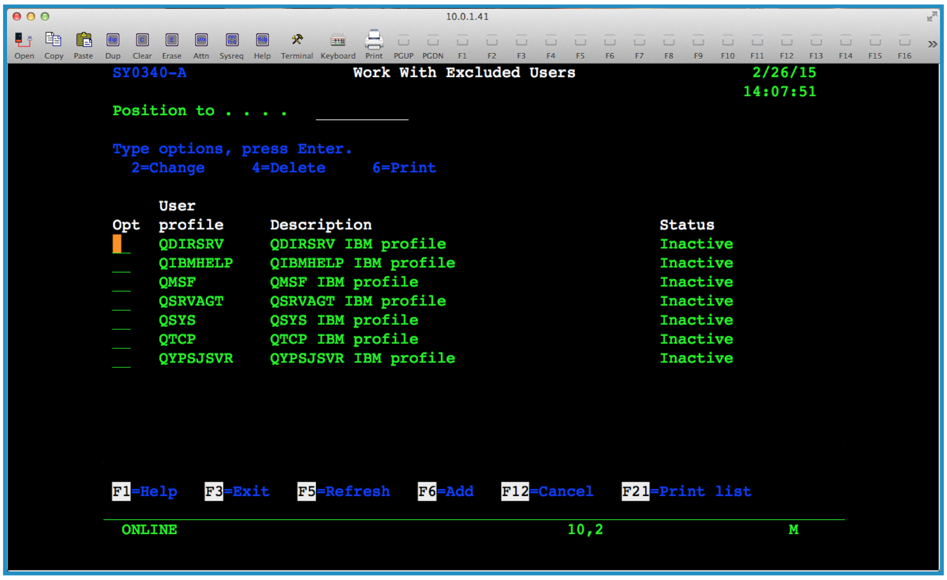
You can enter a starting date for the journal entries. This field is optional. Enter the date in mmddyyyy format. For example: `02052010` .

From time

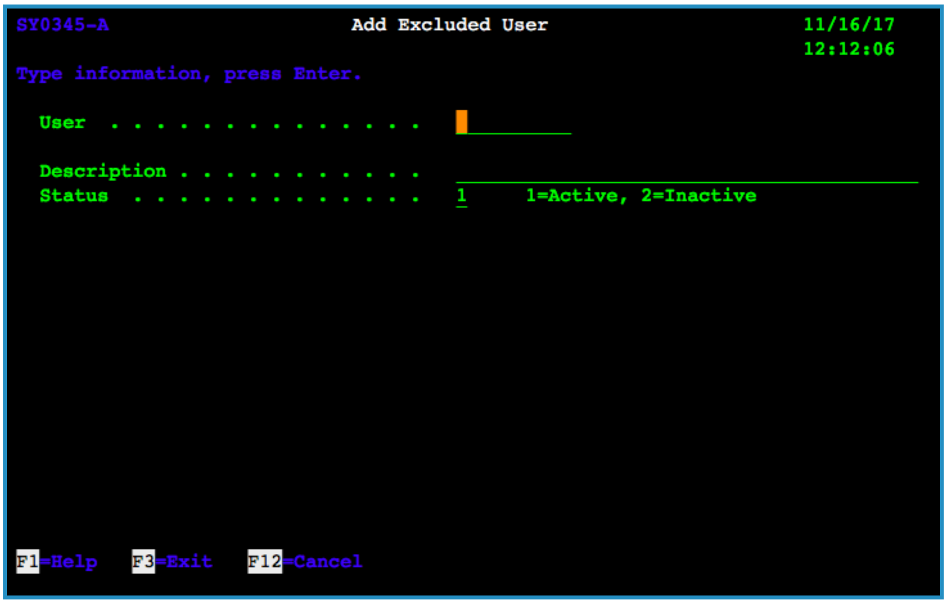
You can enter a starting time for the journal entries. This field is optional, but you must enter a date if you wish to specify a starting time. Enter the time in hhmmss format. For example: `120000` .

Work with QAUDJRN excluded users

If you wish to exclude certain users from reporting, you can add them to the excluded user list and enable the global configuration option for `QAUDJRN` excluded users. When you select option `7` from the configuration menu, the following panel is displayed:



Use option `2` to change the status of a user. Use option `4` to remove a user from the list. Use function key ***F6*** to add a new user. When you press function key ***F6*** the following panel is displayed:



Description

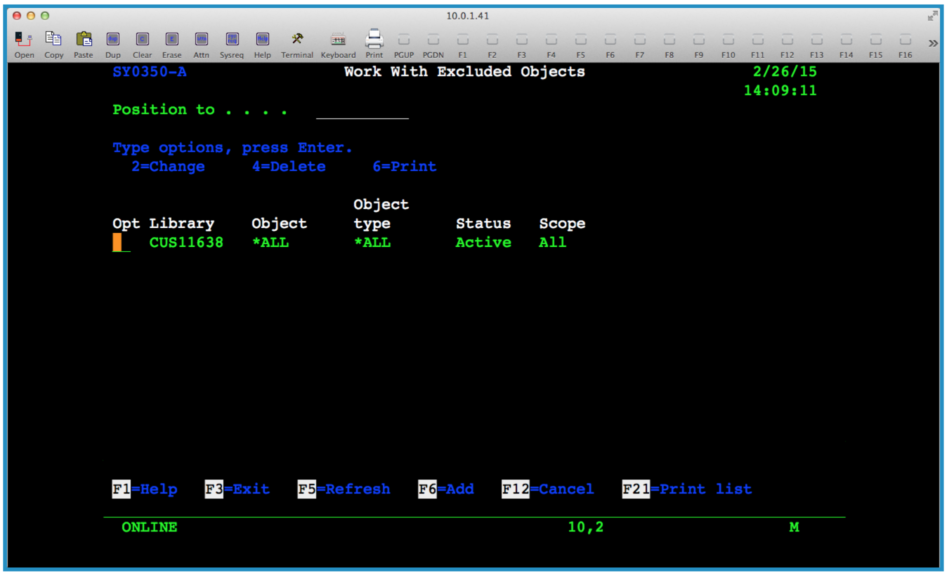
Enter a description for this user.

Status

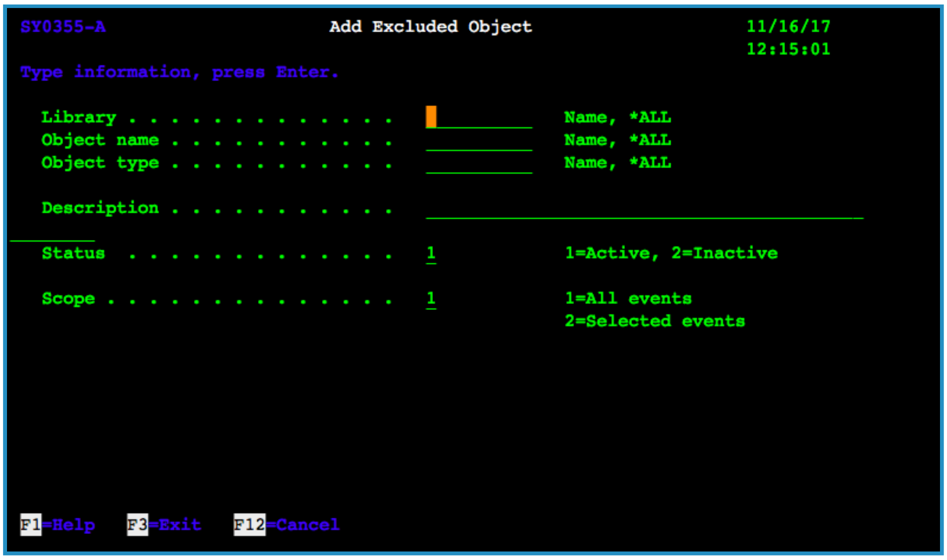
Enter option **`1`** (Active) to exclude this user from event processing. Enter option **`2`** (Inactive) to process this user's entries in the **`QAUDJRN`** event journal.

Work with QAUDJRN excluded objects

From the **`Configuration`** menu, enter the option to **`Work With QAUDJRN excluded objects`**. Use this option to exclude selected objects, or all objects in a library.



Use option **`2`** to change the status of an excluded object. Use option **`4`** to remove an excluded object from the list. Use function key ***F6*** to add a new object. When you press function key ***F6*** the following panel is displayed.



Library

Enter the library name for the excluded object.

Object name

Enter the object name to be excluded. You can use the special value of **`*ALL`** to exclude all objects from the library.

Object type

Enter the type of object to be excluded (for example, `*FILE` or `*PGM`). You can use the special value of `*ALL` to exclude all object types.

> ***Note:*** Specifying `*ALL` for both the `Object Name` and the `Object Type` will exclude all objects from the specified library.

Description

Enter a description for this excluded object definition.

Status

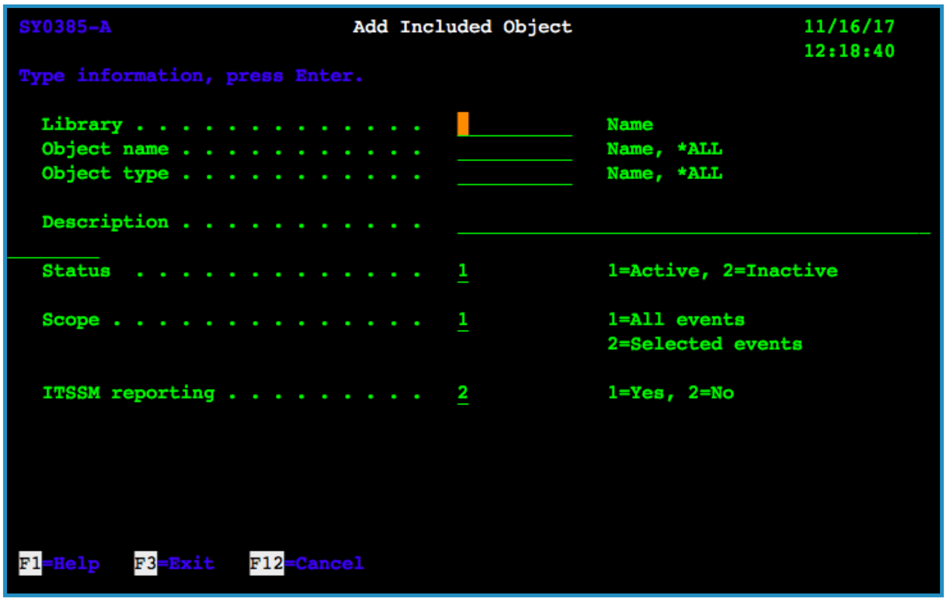
Enter option `1` (Active) to exclude this object from event processing. Enter option `2` (Inactive) to process this object's entries in the `QAUDJRN` event journal.

Scope

Enter `1` to process this excluded object definition for all events. Enter `2` to process this excluded object for selected events.

Work with QAUDJRN included objects

From the `Configuration` menu, enter the option to `Work With QAUDJRN included objects`. Use this option to include selected objects, or all objects in a library.



Library

Enter the `Library` name for the included objects.

Object name

Enter the `Object name` to be included. You can specify the special value of `*ALL` to include all objects in the library.

Object Type

Enter the `Object type` to be included. Use the standard object type special values provided by IBM. For example, to include programs you can use the value of `*PGM`. Specify the special value of `*ALL` to include all object types in the library.

Description

Enter a description for this included object definition.

Status

Enter `1` for Active or `2` for Inactive.

Scope

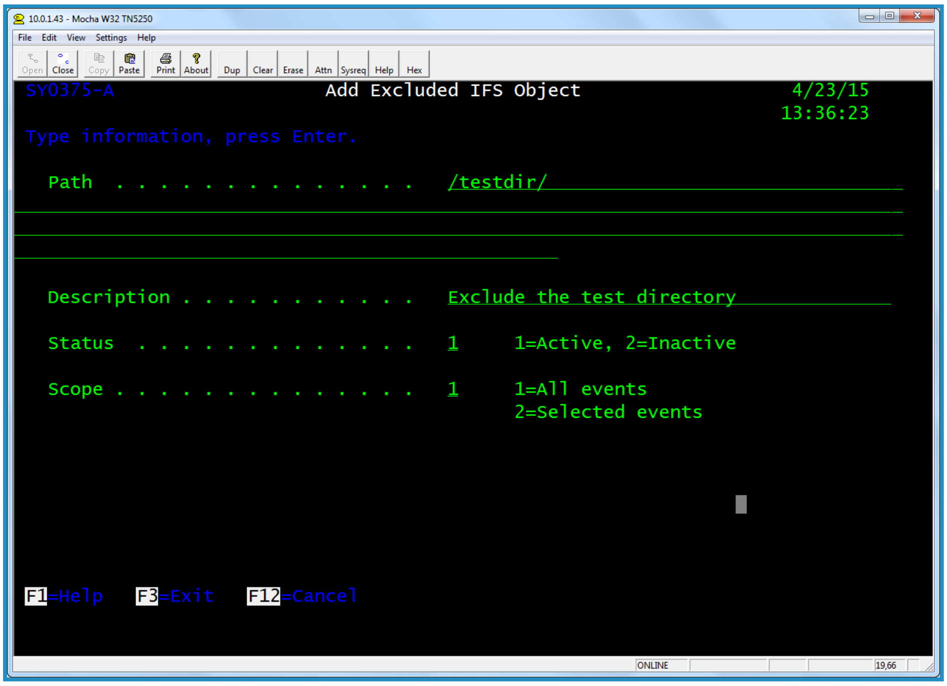
Enter `1` to process this included object definition for all events. Enter `2` to process this included object for selected events.

ITSSM reporting

Enter `1` (Yes) to report to ServiceNow or `2` (No) to not report to ServiceNow.
You must first define the ITSSM interface in the global configuration option, and specifically enable QAUDJRN object filtering.

Work with QAUDJRN excluded IFS

From the `Configuration` menu, enter the option to `Work With QAUDJRN excluded IFS`. Use this option to exclude IFS directories or specific files.



Path

Enter the full `Path` for the excluded IFS object. You can enter a directory name or a fully qualified file name. To exclude a directory specify the full path to the directory and the terminating slash (`/`) character. Do not use any special characters such as asterisk (`*`) or question mark (`?`) after the final slash for the directory. To exclude specific files use the fully qualified file name. IFS file names are not case sensitive.

Description

Enter a `Description` for this IFS exclusion definition.

Status

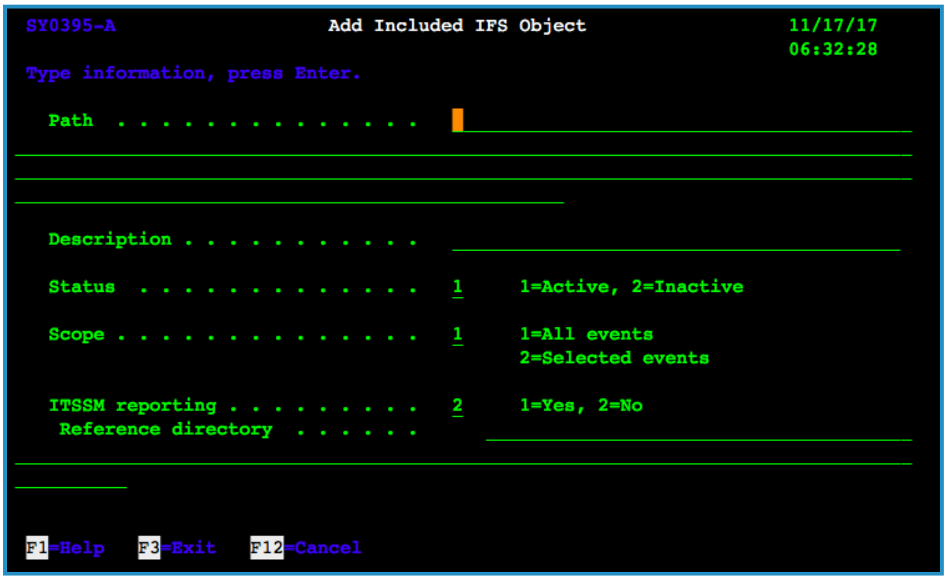
Enter `1` for Active or `2` for Inactive.

Scope

Enter `1` to process this excluded IFS definition for All events. Enter `2` to process this excluded IFS directory or file for Selected events.

Work with QAUDJRN included IFS

From the `Configuration` menu, enter the option to `Work With QAUDJRN included IFS`. Use this option to include selected directories, or all objects in a directory.



Path

Enter the full `Path` for the included IFS object. You can enter a directory name or a fully qualified file name. To include a directory specify the full path to the directory and the terminating slash (`/`) character. Do not use any special characters such as asterisk (`*`) or question mark (`?`) after the final slash for the directory. To include specific files use the fully qualified file name. IFS file names are not case sensitive.

Description

Enter a `Description` for this IFS inclusion definition.

Status

Enter `1` for Active or `2` for Inactive.

Scope

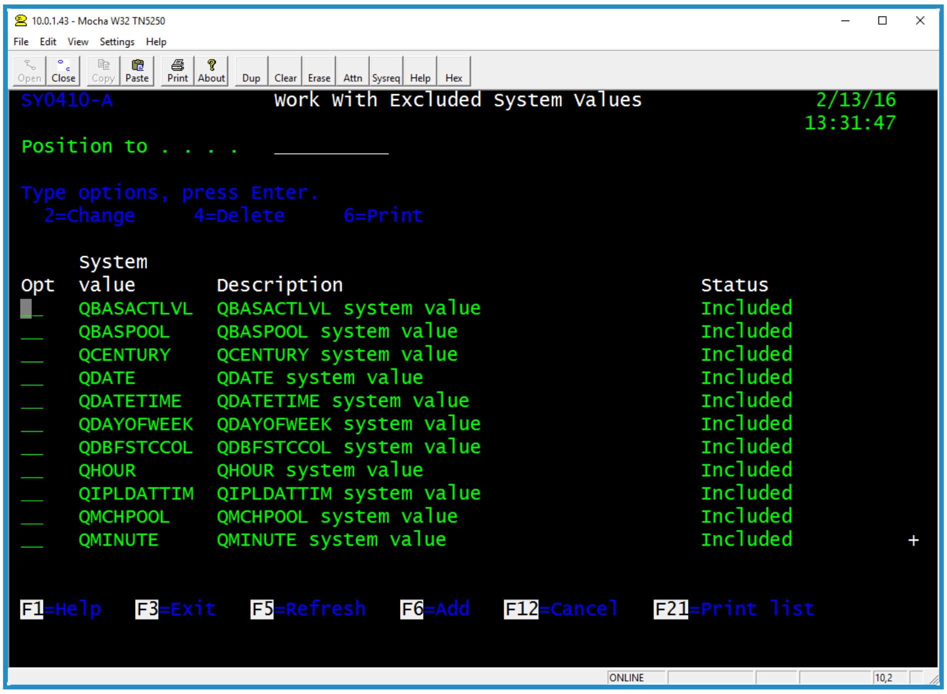
Enter `1` to process this included IFS definition for all events. Enter `2` to process this included IFS directory or file for selected events.

ITSSM reporting

Enter **1** (Yes) to report to ServiceNow or **2** (No) to not report to ServiceNow.
You must first define the ITSSM interface in the global configuration option, and specifically enable QAUDJRN object filtering.

Work with excluded system values

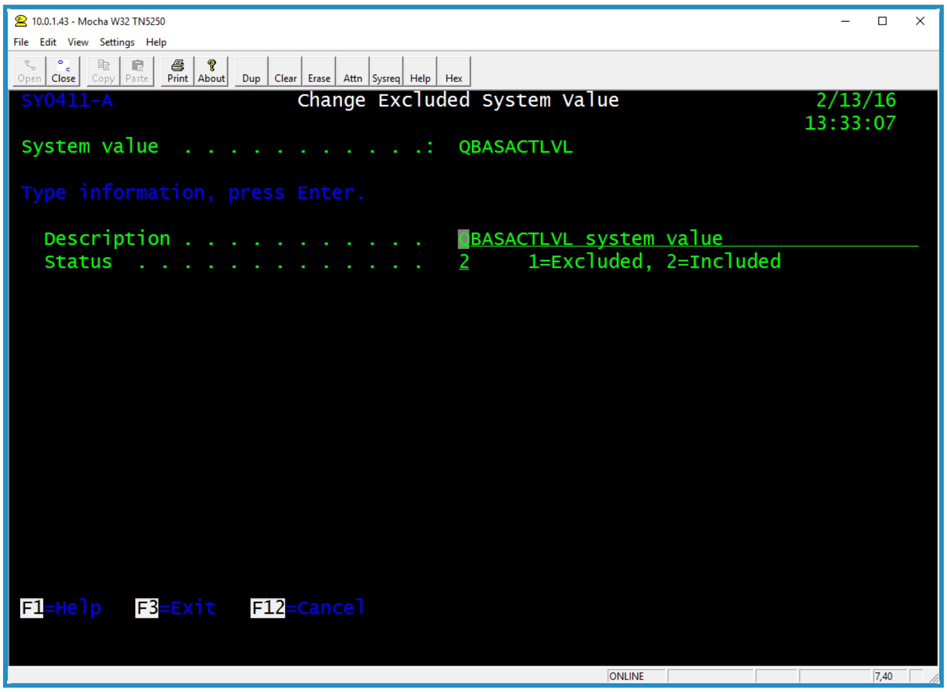
From the Configuration menu, enter the option to Work with excluded system values. Use this option to exclude reporting changes to selected system values.



Opt(ion)

Enter **2** to change a reporting for a system value change. Enter **4** to delete the system value from the list. This will not change the system value nor the reporting of the system value to the QAUDJRN journal. Enter **6** to print the value. Take **F6** to add a new system value.

The following panel is displayed when adding or changing a QAUDJRN system value to exclude from reporting.



Description

Enter the description for this system value.

System value

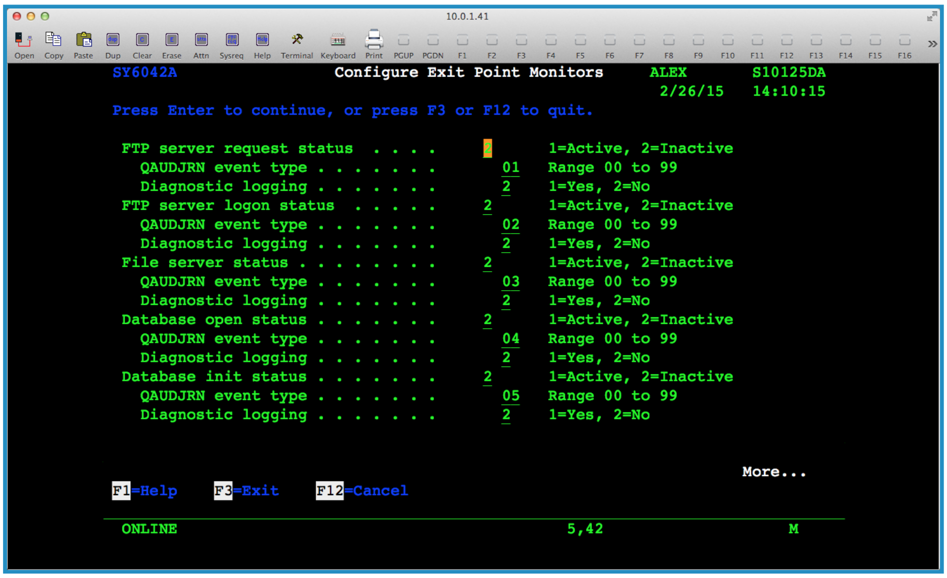
If adding a new system value, enter the name here.

Status_

Enter **`1`** to exclude this system value from reporting to your SIEM or log collection server. Enter **`1`** to include this system value in reporting. Certain system values are changed automatically by the OS/400 operating system and you may wish to exclude these events from reporting.

Work with exit point monitors

From the **`Configuration`** menu, enter the option to **`Work With Exit Point Monitors`**. Use this option to configure the operation of Alliance LogAgent exit point monitoring programs.



Exit point monitor status

Enter `1` for Active or `2` for Inactive. This option does not install the actual exit point monitor. If the exit point is installed and this field is set to Inactive, the exit point program will be called, but it will not perform security logging. To enable the exit point monitors you will have to go to option 6 on the main menu and start it there.

QAUDJRN event type

Enter the 2-digit event type you wish to use for this exit point.

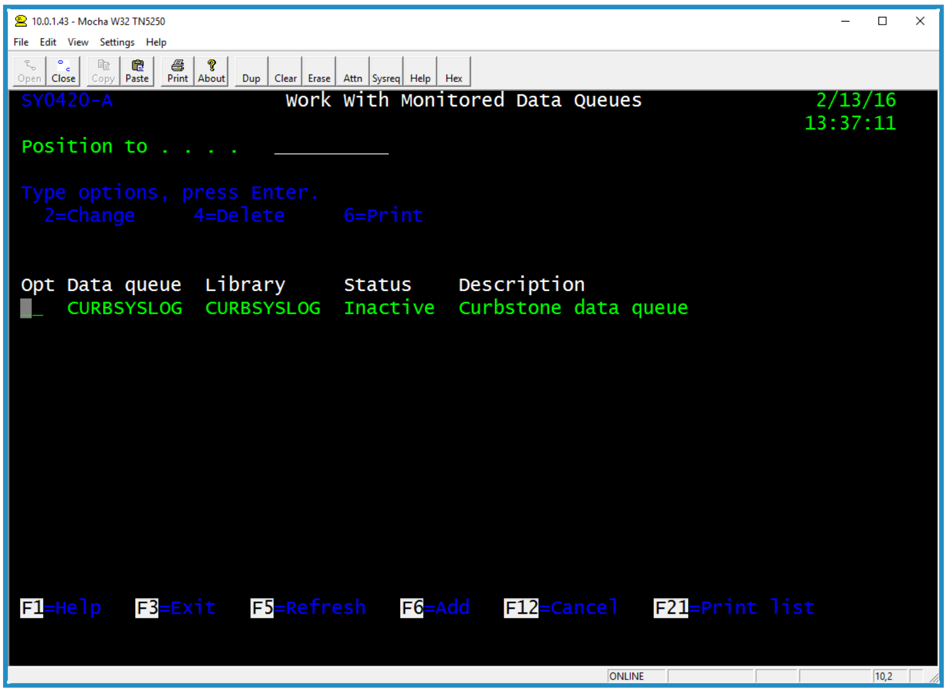
Diagnostic logging

Enter `1` for Yes to perform diagnostic logging. Enter `2` for No to not capture a diagnostic log.

> ***Note:*** Additional exit points are displayed on the following panels.

Work With Monitored Data Queues

From the Configuration menu, enter the option to Work with monitored data queues. Use this option to enable monitoring of one or more user data queues. When a user data queue is monitored by Alliance LogAgent any information your application writes to the data queue will be formatted to the syslog standard and transmitted to your SIEM solution or log collection server.

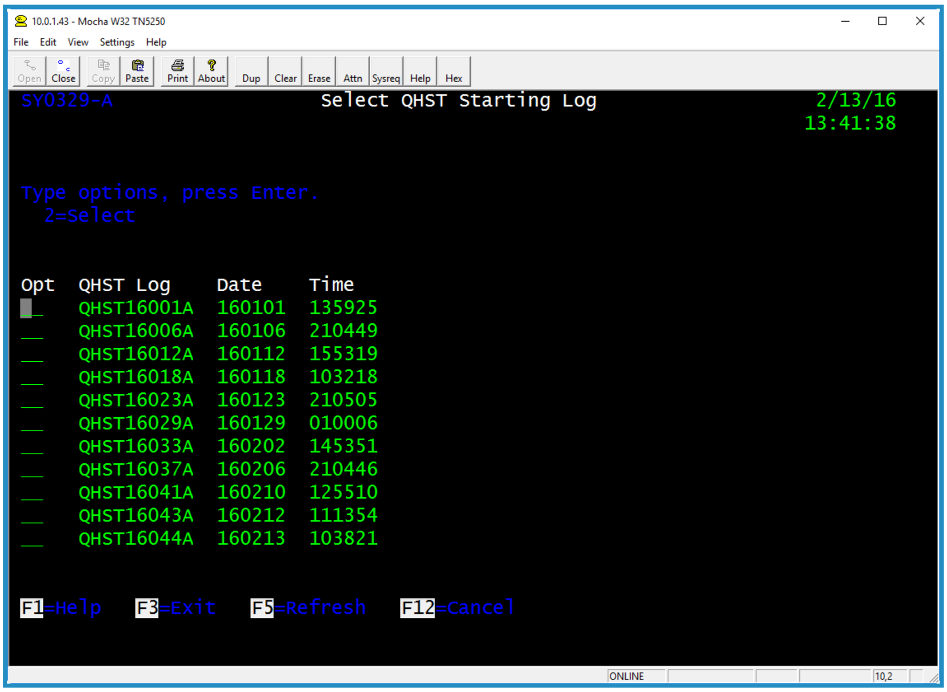


You can use option `2` to change the monitored status of the data queue.

If you are monitoring dataqueus and need to end the subsystem, we recommend using the **`ENDSYLSBS`** command in order to end the ALLSYL100 subsystem while gracefully ending all data queue monitoring jobs first. This will prevent damage to data queues. The subsystem will not end if the data queue monitoring jobs do not end. The command allows for retries and timing between retries.

Change QHST starting point

From the Configuration menu, select the option to Change **`QHST`** starting point. Use this option to select which **`QHST`** file to start processing. For IBM I customers with a large number of historical **`QHST`** files on their system, you can minimize the number of files that are processed when first installing and using Alliance LogAgent. Note that this option will build a list of all of the current **`QHST`** files and will synchronize an existing list.



Note that using option `2` will immediately set that `QHST` file as the starting point.

Synchronize QHST files

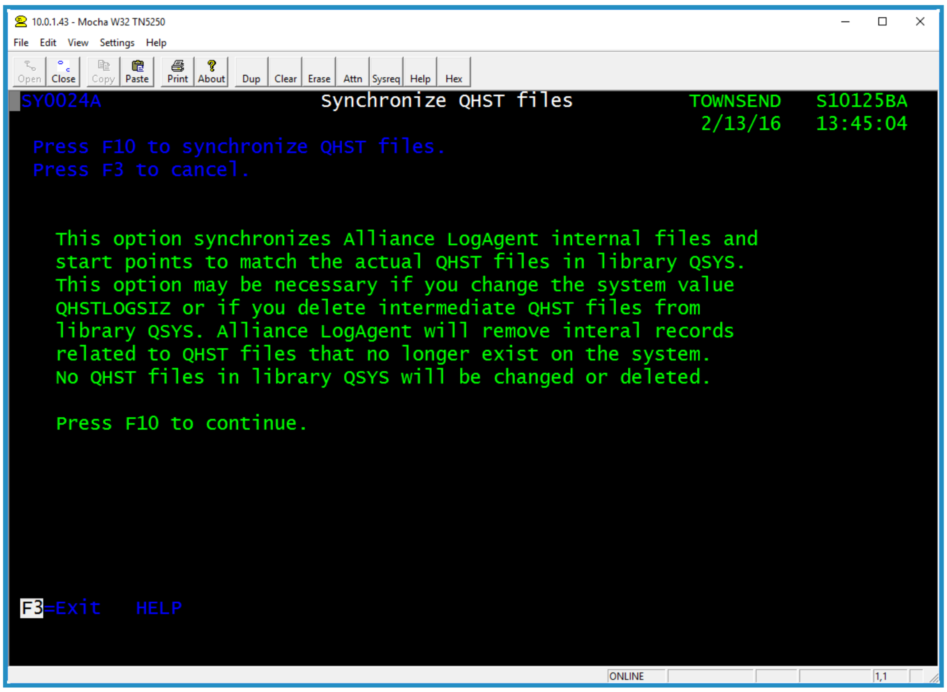
From the Configuration menu, select the option to Synchronize `QHST` files. If you delete intermediate `QHST` files from library `QHST` or take configuration options that affect the size of `QHST` files or the naming of QHST

```
files, Alliance LogAgent may become out of synchronization with the
```

QHST

```
files. This option will re-establish synchronization, removing any ir
```

QHST` files have been processed by which are no longer on the system.



Press ***F10*** to synchronize `QHST` files. Press ***F3*** to cancel this operation.

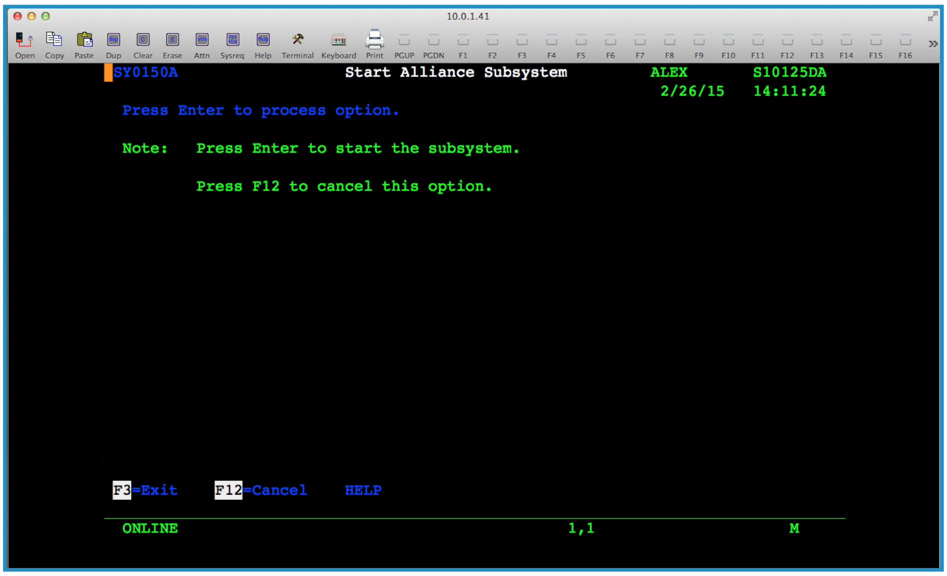
Work with Authorized Users

This option allows you to build and manage a list of user profiles who can access and make changes within Alliance LogAGent and Database Monitor. This option is activated in the configuration menu when **`Enable user control`** is set to 1 for yes. To enforce these changes you must end and restart the subsystem.

Press F6 to add a user, enter a description, then choose 1 for Yes to authorize the user to specific options. We ship with QAUDJRN enabled and you can change this once you have added another user.

Start LogAgent subsystem

After configuring the global options and a TCP communications client, you must start the Alliance subsystem **`ALLSYL100`** to start collecting logs. On the **`Configuration`** menu enter the option to **`Start LogAgent Subsystem`**. The following panel is displayed:



Press ***Enter*** to start the subsystem. When you first start the subsystem you may see and AUTO_START job. That will be replaced by any or all of the following jobs, depending on the configuration options you have entered:

- OPER_MESG – extracts messages from QSYSOPR and sends to the internal Syslog queue.
- QAUDJRN – extracts audit journal entries and sends to the internal Syslog queue.
- SYSLOG (2 instances) – receives Syslog messages from the Syslog queue and uses TCP, UDP, or TLS TCP to send to a local or remote instance of Syslog-ng server.

You can enter options on the **`Configuration`** Menu to view active jobs in the Alliance **`ALLSYL100`** subsystem, and to end the subsystem. You can also end the subsystem **`ALLSYL100`** manually using the End Subsystem (**`ENDSBS`**) command with the **`*IMMED`** option.

> ***NOTE:*** The first time you start the Alliance subsystem the audit journal and operator message queue processes will begin collecting information starting from the earliest message. If there is a substantial amount of history in the journal or message queue it may take time for these messages to be sent to the Syslog-ng server.

Automating the start of the Alliance subsystem ALLSYL100

Once you have the configuration the way you want you can automate the start of the **`ALLSYL100`** subsystem by modifying the IPL start up program. The name of the IPL start up program is stored in system value **`QSTRUPPGM`**. The program is usually **`QSTRUP`** in library **`QGPL`**. You can modify this program to add the following statements to start the **`ALLSYL100`** subsystem:

```
QSYS/STRSBS SBSD(ALLSYL100/ALLSYL100)
MONMSG MSGID(CPF0000)
```

You should place these statements after any commands that start the TCP/IP network services.

If you do not have the source for the **`QSTRUP`** program you can retrieve the source using the Retrieve CL Source (**`RTVCLSRC`**) command.

End QAUDJRN collector

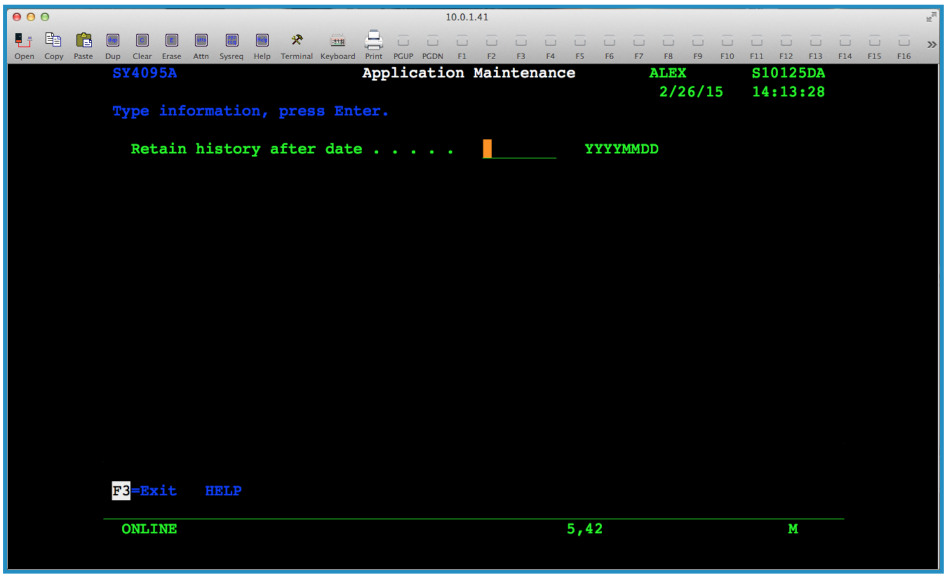
Use this option to end the QAUDJRN collector. The QUADJRN collector will stop after the current event is fully processed. After the QAUDJRN collector is ended you can end the ALLSYL100 subsystem.

Work with Auth List

Use this option to work with the authorization list ALLLGAOWN. This authorization list controls access to the Alliance LogAgent solution.

Application maintenance

The application maintenance option can be used to purge information from the internal diagnostic logs, historical information, and to reorganize any physical files used by the Alliance application. From the main menu enter the option for Application Maintenance, then enter option `1` to run maintenance. The following panel is displayed:



Retain history after date

Enter the date in YYYYMMDD format to indicate the retention date. Log and historical information more recent than this date will be retained. All physical files will be reorganized. Note that you should run this option when the Alliance subsystem **`ALLSYL100`** is not active.

Manually clearing Alliance log information

You can manually clear Alliance diagnostic log information with the following command from a command line:

```
clrpfm file(allsyl100/alloga)
```

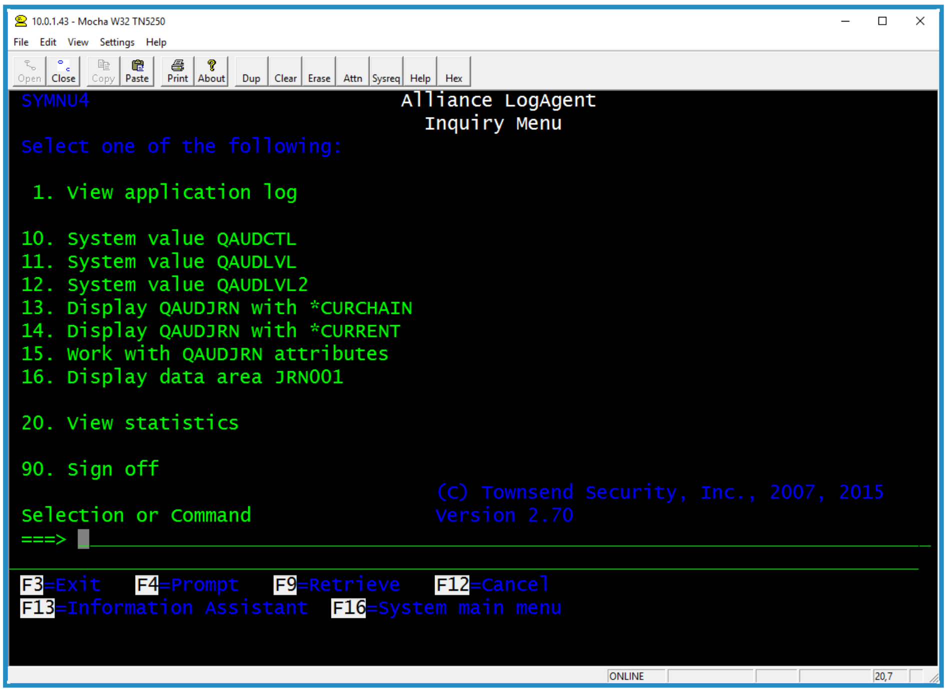
This command only clears the internal Alliance logs and does not delete any Syslog information.

Clear ALLOGA file

The ALLOGA file is used to collect diagnostic information when it is enabled. The file can become quite large. Use this option to clear the file.

Inquiry Menu

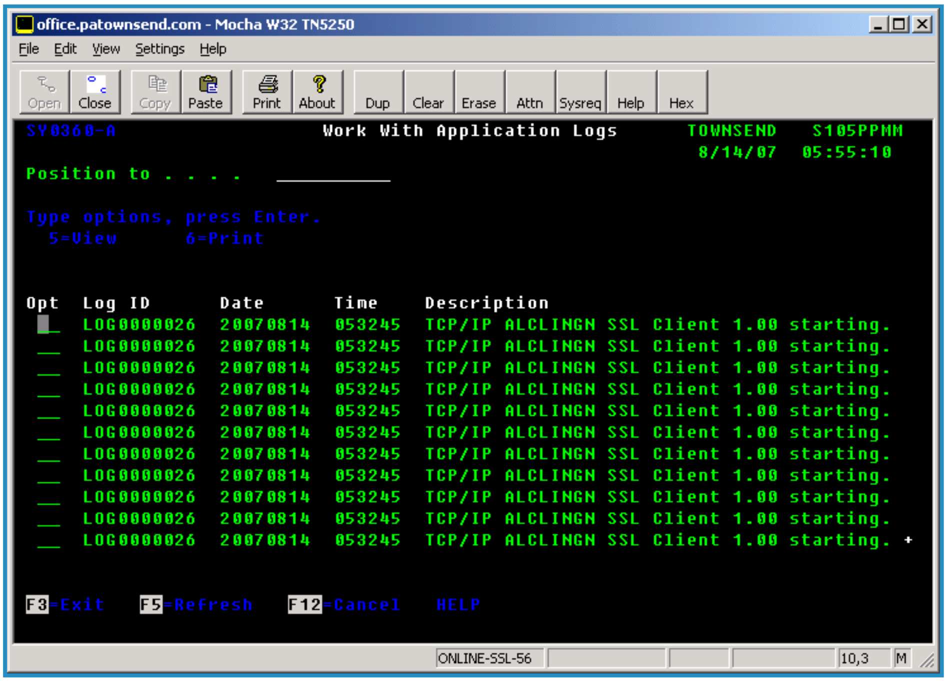
Use the Inquiry menu to view the application logs, system values, and other system and application information.



Select an option to start work.

View application logs

The View Application Logs option can be used to view internal Alliance application logs such as the TCP or TLS TCP application log. From the main menu enter the option for Inquiry, then option `1` to view the log. The following panel is displayed:



Enter option `5` to view the log or option `6` to print the log. For large logs it is recommended that you enter option `6` to print the log and then use the Work With Spooled Files (**WRKSPLF**) command to view the report.

Note that the application logs only contain internal Alliance diagnostic information and do not contain Syslog information that has been collected.

View System Values

Use options `10`, `11`, and `12` on the Inquiry menu to view the current system values that affect `QAUDJRN` event collection.

View QAUDJRN journal entries

Use options `13` and `14` on the `Inquiry` Menu to view the security audit journal `QAUDJRN`. Option `13` displays all of the available entries in the `QAUDJRN` journal. Option `14` displays only the entries in the most current `QAUDJRN` journal receiver.

Work with QAUDJRN attributes

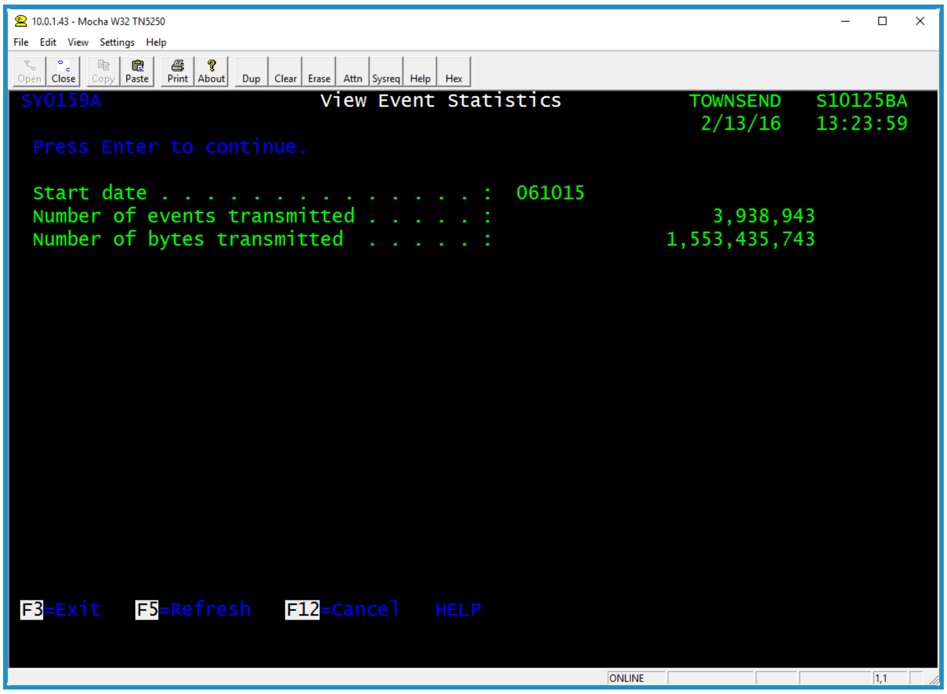
Use option `15` on the `Inquiry` menu to work with the journal attributes of journal `QAUDJRN`.

Display data area JRN001

Use option `16` to display the Alliance LogAgent control data area `JRN001`. This data area shows the current journal receiver and sequence number for `QAUDJRN` event reporting.

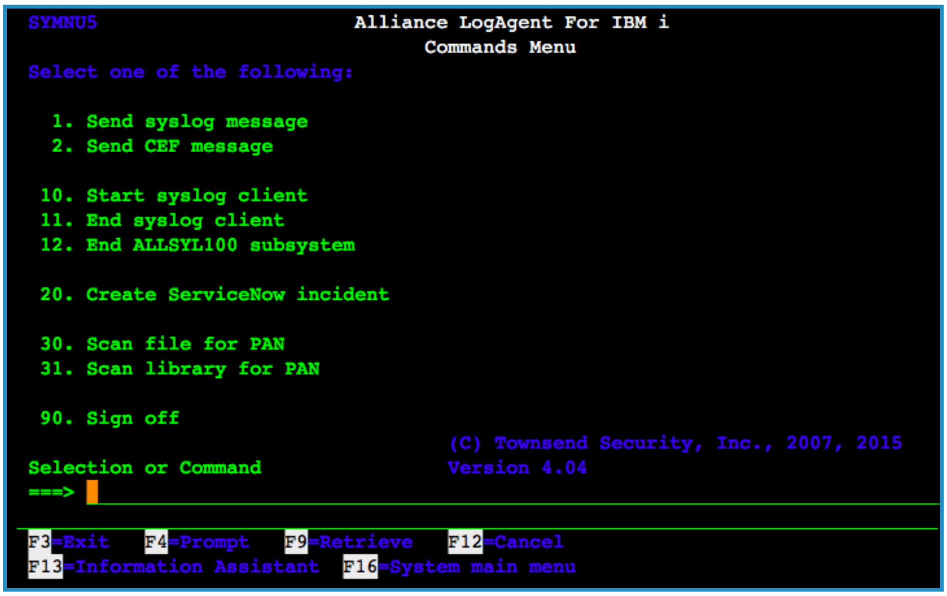
View statistics

Use option 20 to view information about the number of events processed by LogAgent.



LogAgent commands menu

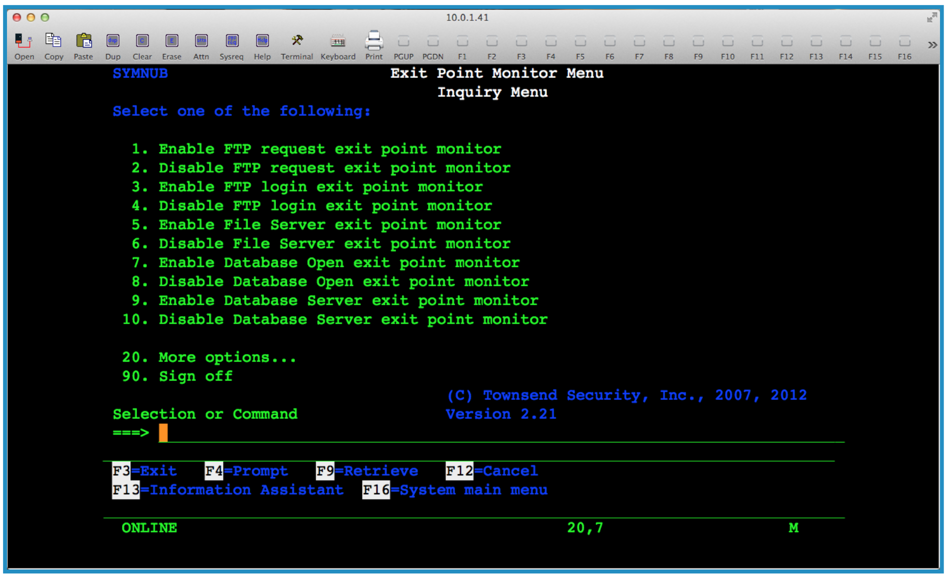
From the main menu **SYMAIN** select option **5** for **LogAgent commands** . The following menu is displayed:



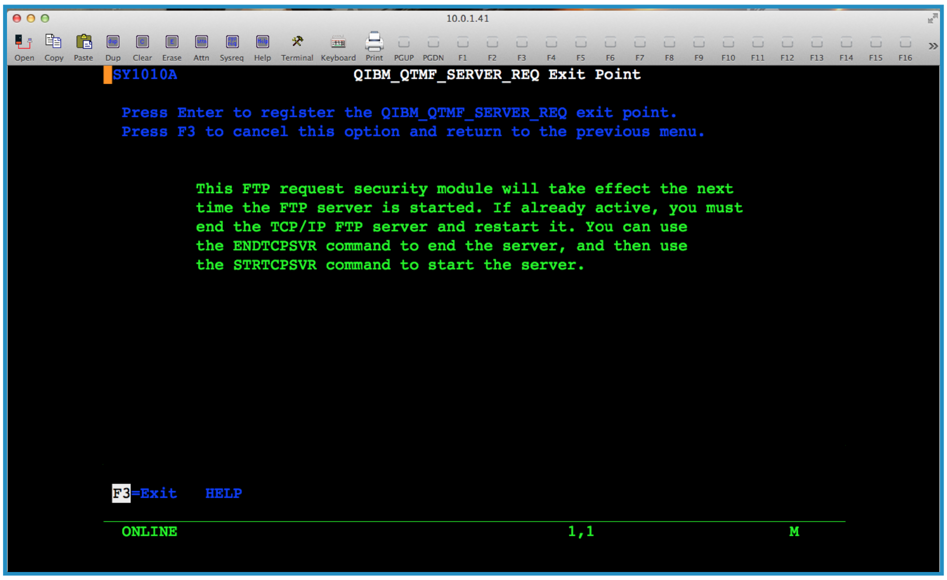
Use this menu to view a list of commands available in Alliance LogAgent. You can use the Send Syslog Message command in your applications to send an event to QAUDJRN in the syslog format. You can use the Send CEF Message command to in your applications to send an event to QAUDJRN in the Common Event Format. You can also use commands to start and stop a Syslog communications client, or to gracefully end the ALLSYL100 subsystem. You can also dynamically create an incident ticket with your ServiceNow account and scan files and libraries for PANs.

Exit point monitor menu

From the main menu **SYMAIN** select option **6** for **Exit Point Monitors** . The following menu is displayed:

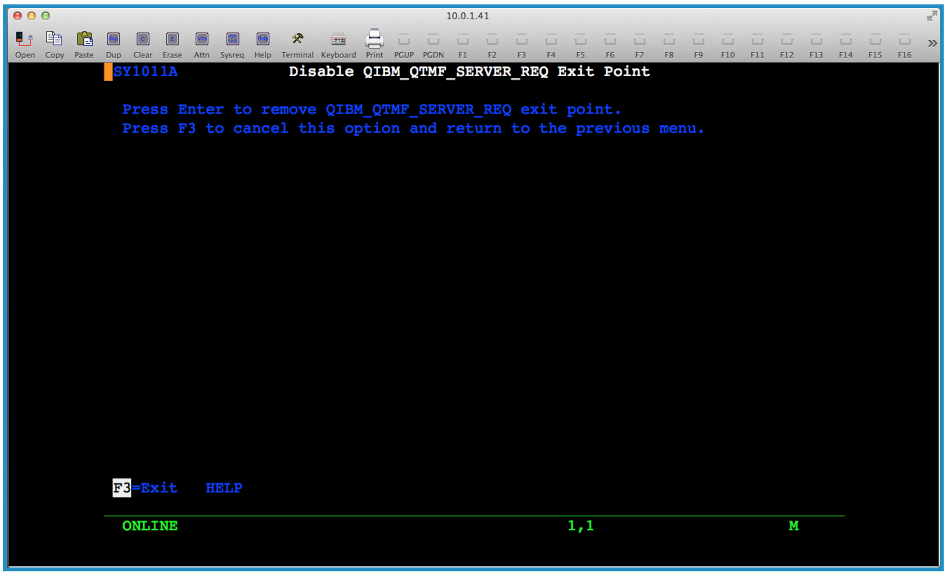


Select an option to enable or disable an exit point.



There are no input fields for this panel. Press ***Enter*** to install the Alliance LogAgent exit point program for this exit point.

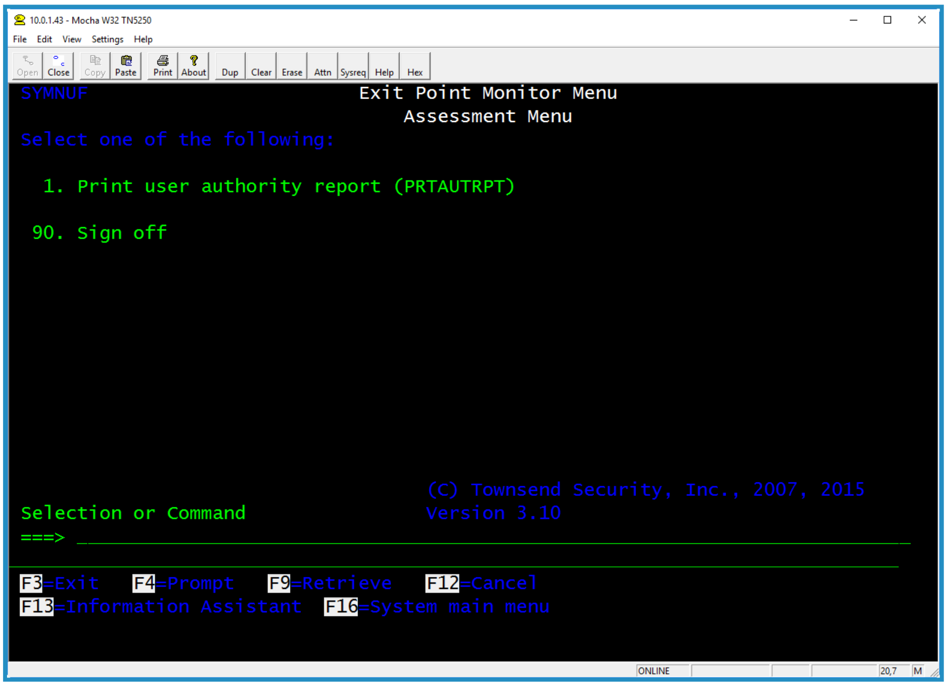
> ***Note:*** You may need to restart the specific server to activate the exit point.



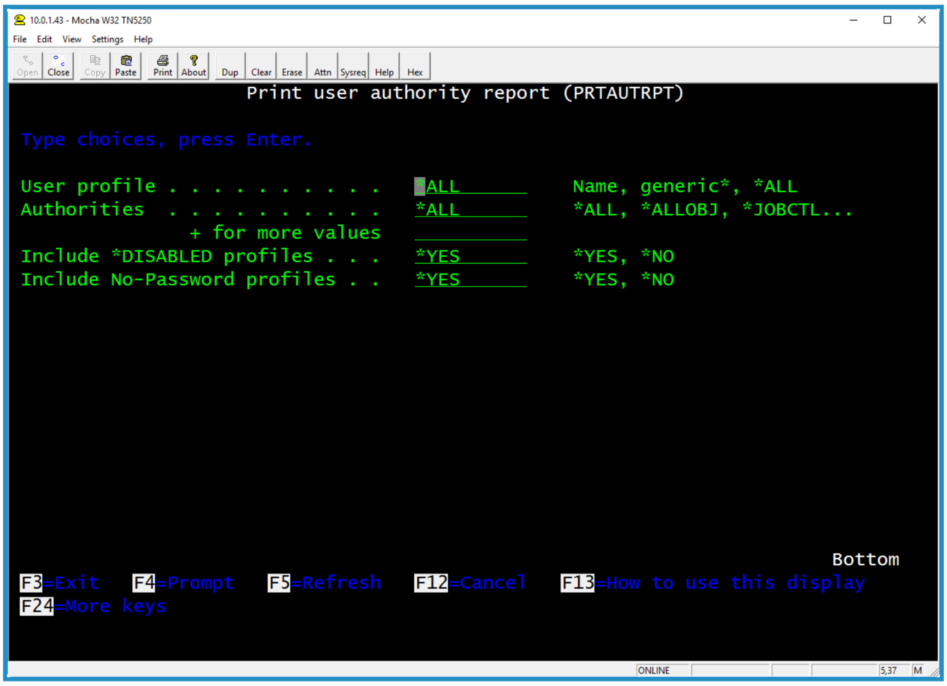
There are no input fields for this panel. Press ***Enter*** to remove the Alliance LogAgent exit point program from this exit point.

Assessment

From the main menu `SYMAIN` select option `7` for `Assessment`. The following menu is displayed:



Select option 1 to prompt the Print User Authority Report. The following command prompt is displayed:



User profile

Enter the user profile name for authority reporting. You can use the special value *ALL to report on all users. You can also use a generic name to report all users that begin with the generic value. Note that you can only report the authorities on user profiles for which you have authority.

Authorities

Enter up to eight special authorities to be included for determining the administrative level of the user. You can use the special value *ALL to include all of the possible special authorities.

*Include *DISABLED profiles*

Enter `*YES` to include disabled user profiles in this report. Enter `*NO` to not include disabled user profiles.

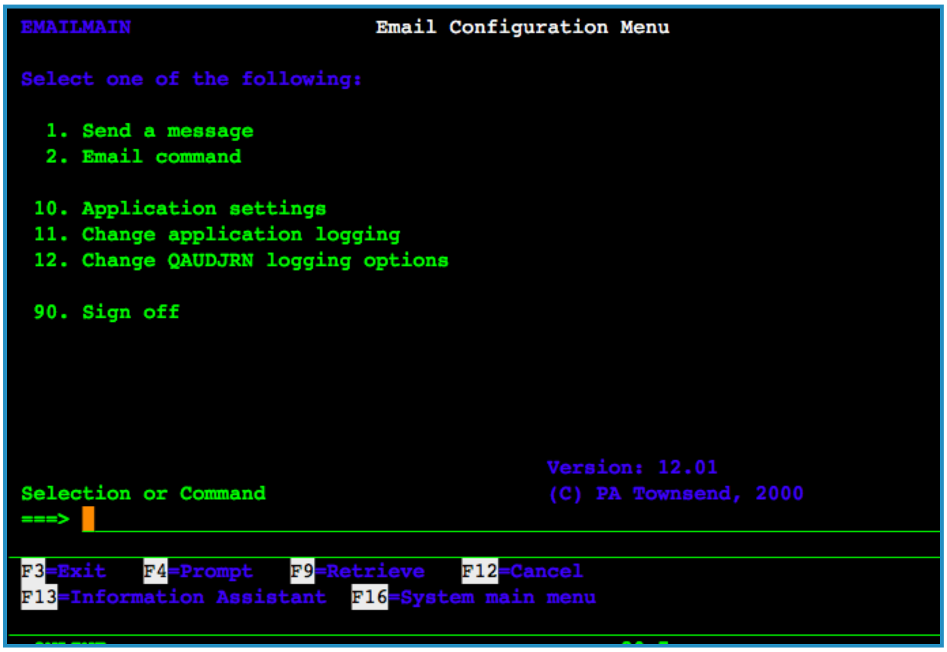
Include No-Password profiles

Enter `*YES` to include user profiles without a password in this report. Enter `*NO` to not include user profiles without a password.

Email configuration

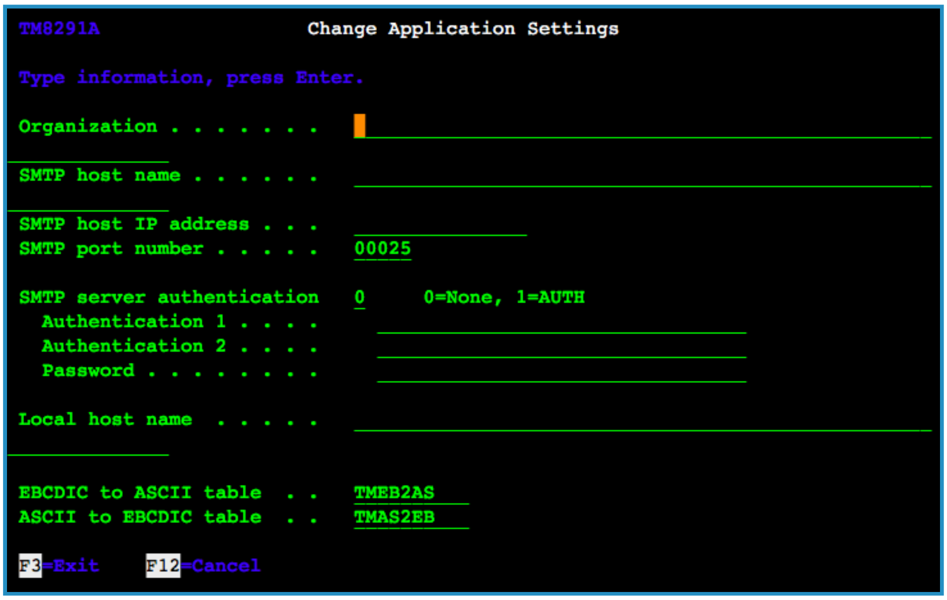
Alliance LogAgent contains a full SMTP client application for sending email messages to LAN or Internet recipients. You can even use Alliance to send messages to pagers or PCS devices.

From the main menu select the option for the Email menu.



Application settings

Use this option to define the application settings for the Alliance FTP Manager email client. You will define the address of the mail server, port number of the SMTP server, local host name, etc. You should consult your mail administrator before attempting to use the email notification facilities of Alliance. Many mail servers will prevent unauthorized access and you may have to provide the mail administrator with the IP address of the IBM i and the local host name you are using.



Organization

Enter the name of your company or organization. This can be any text description you like.

SMTP host name

You must enter either an SMTP host name or an SMTP host IP address. The domain name is in Internet format, for example: acme.com

SMTP host IP address

If you do not enter an SMTP host name you must enter an SMTP IP address. This is the IP address of your mail server.

SMTP port number

Enter the port number of your mail server for the SMTP service. This is usually port 25, but may be different. Consult your mail administrator for the correct port number.

SMTP server authentication

Choose `0` for none or `1` for AUTH If you choose to authenticate you must enter at least 1 form of authentication that is accepted. That can be a code or a password.

Local host name

Enter the name of your IBM i as it will identify itself to the mail server. This is usually the full domain name of the IBM i, for example: “S1015872.ACME.COM”. Give this information to you mail administrator.

EBCDIC to ASCII table

Enter the name of the table to use for EBCDIC to ASCII translation. The table TMEB2AS is provided. You may create your own translation tables and register them here. The file QTBLSRC in the product library has sample code for creating translation tables.

ASCII to EBCDIC table: Enter the name of the table to use for ASCII to EBCDIC translation. The table TMAS2EB is provided. You may create your own translation tables and register them here. The file QTBLSRC in the product library has sample code for creating translation tables.

ITSSM menu

If you have a ServiceNow account you can create an incident on the fly. Enter a description and comment and prioritize the options at the bottom of the screen. Press enter to create a ticket in ServiceNow.

Database Monitor

This option will take you to the DataBase Monitor main menu. Please refer to the DataBase Monitor manual for instructions and examples to set up reporting on specific files.

Alliance Two Factor Authentication menu

Use option 20 on the main menu SYMAIN to display the Alliance Two Factor Authentication product main menu. To use this option you must first install and license the optional Alliance Two Factor Authentication solution from Townsend Security. See the separate user documentation for more information about this solution.

Chapter 5: Performance Considerations

Many things can affect the performance of the Alliance LogAgent application. This section provides some guidance and suggestions on how you can get the best performance in your environment.

System audit event configuration

System values

The primary cause of performance problems with security event collection arises when the IBM i is configured to collect the maximum number of security events in the `QAUDJRN` security journal. The type of events that the system will collect in this journal is controlled by the system values `QAUDLVL` and `QAUDLVL2`. There are many settings available through these system values. IBM provides some general values like `*SECURITY`, but you can add to this basic set by using the other system value options.

Enabling all of the auditing options will result in a very large number of events generated in the `QAUDJRN` journal. It is not uncommon to find several million events generated on a daily basis when all of these options are enabled. By default, Alliance LogAgent will process all of these events and transmit them to your log collection server.

Use the Work With System Values (`WRKSYSVAL`) command and review the settings in `QAUDLVL` and `QAUDLVL2`. Enable only the events you need for security event reporting. Consider turning off print management events and object access event logging. These can produce a very large number of events.

> ***SECURITY NOTE:*** Be sure to check with your security administrator before changing any system values related to event collection to ensure that you are meeting compliance regulations related to log collection.

Object auditing

In addition to the system values that affect the types of events that are collected, you can also enable object level auditing using the Change Object Auditing (`CHGOBJAUD`) command. This command is used to enable or disable object level access auditing for programs, files, and almost any other type of object in your user libraries. If you enable object level auditing for an entire library, you may create a very large number of events in the `QAUDJRN` journal.

Consider using object level auditing on only the files and programs that are sensitive in nature. This can reduce the number of events and the amount of work that Alliance LogAgent needs to do for event reporting.

Filtering events

Alliance LogAgent has the ability to filter events based on the security event type. You may be collecting a large number of events, but may not need to report all of these events to your log collection server. You can turn off the processing and transmission of selected events. From the main menu `SYMAIN` enter option `2` for `Configuration,` then option `3` to `Work With Security Types` . Enter a `2` next to a security type to change it. You will find the option to report the event on the first panel:

```
Send to log server  . . . . . . .   1            1=Yes, 2=No
```

You can change this option to `2` (No) to suppress processing this security event. This action takes effect immediately. This option does not change any system values or security options. Events will still be collected in the `QAUDJRN` journal, but will not be processed by Alliance LogAgent.

Diagnostic logging

Alliance LogAgent provides for diagnostic logging to help you and the software support team quickly analyze potential problems. These diagnostic logging options cause the LogAgent to write data to log files in the product library. Application logging can have a negative impact on performance, and should only be enabled when you are trying to diagnose problems.

Communications logging

The communications applications have an option for application logging. From the main menu `SYMAIN` enter option `2` for `Configuration` , then option `2` to `Work With TCP Clients` . Enter a `2` next to your communications configuration. On the first panel you will find this option:

```
Application logging . . . . . . .    2                  1=Yes, 2=No
```

Be sure this option is set to `2` (No). If it is set to `1` (Yes), change it to `2` and update the configuration. Stop the `ALLSYL100` subsystem and restart it. You can now clear the logging file `ALLOGA`:

```
clrpfm file(allsyl100/alloga)
```

Application logging

The various collectors for the `QAUDJRN` security journal, `QHST` system message file, and `QSYSOPR` message queue can produce diagnostic information. From the main menu `SYMAIN` enter option `2` for `Configuration`, then option `1` to `Configure Alliance LogAgent`. On the first panel you will find this option:

```
Enable diagnostic logging . . . .    2                  1=Yes, 2=No
```

Make sure this option is set to `2` (No). If it is set to `1` (Yes), change it to `2` and update the configuration. End the `ALLSYL100` subsystem and restart it.

Job logging

If the Alliance LogAgent application is producing large job logs, you can reset the application to create basic job logs with the `SYLOGOFF` program:

```
call pgm(allsyl100/sylogoff)
```

This application will change all Alliance LogAgent job descriptions to use minimal logging.

Solution architecture

Application architecture

Alliance LogAgent is designed to work the way any normal IBM i application would work. The application does not make any changes to the system to allocate CPU or disk resources, and does not make system API calls to manipulate resources. It is designed to behave in the way any user application would work on the IBM i. This means that you can easily manage the resources used by Alliance LogAgent.

Journal event processing

To maximize performance and minimize the impact on your system, Alliance LogAgent retrieves a large block of security events each time it accesses the **QAUDJRN** journal entries. The process of reading events from the journal is expensive on CPU resources, so Alliance LogAgent attempts to minimize this impact by reading many events at one time. This also improves the ability of Alliance LogAgent to handle many events per second.

While Alliance LogAgent retrieves many entries from the journal at a time, it only processes one event at a time. An event is converted to syslog format, queued for transmission, and sent to your log collection server before the next event is processed. This means that the application will naturally give up resources to other active applications, and will not "capture" CPU resources through intensive CPU activity.

Subsystem architecture

The Alliance LogAgent jobs run in a subsystem named **ALLSYL100** . All of the jobs run at a priority of 50 or 60 which is a batch priority level. You can change the job execution priority by changing the class definition **ALLSYL100** in the application library. Even when Alliance LogAgent is processing a large volume of events it will not affect interactive performance. Of course, if your IBM i is already over-committed on CPU or disk resources, Alliance LogAgent may affect overall system performance. This would be true for any new application you installed on your system.

Job priorities and time slice

Because Alliance LogAgent runs at a batch priority of 50 or 60, it may affect the performance of other batch jobs running at the same priority. The i5/OS operating system will attempt to balance resources between multiple jobs running at this priority. You can lower the priority of the Alliance LogAgent jobs by changing the class **ALLSYL100** . For example, you can change the priority to 70 using this command:

```
chgcls cls(allsyl100/allsyl100) runpty(70)
```

Note that changing the priority to a very low level may cause the application to report events some time after they occur. Managing the priority of the Alliance LogAgent involves balancing your needs for timely information and your need for system performance.

The Alliance LogAgent application is configured to use a timeslice of 2000 in the batch environment. This should ensure that Alliance LogAgent shares resources with other applications on the system. However, in some environments you may have better performance by increasing or decreasing this value. Discuss this value with your system administrator. You can change the value using the Change Class (**CHGCLS**) command:

```
chgcls cls(allsyl100/allsyl100) timeslice(5000)
```

> ***IMPORTANT:*** If you change the subsystem or class provided in the Alliance LogAgent library, you must remember to re-apply these changes after you upgrade the product.

CPU utilization

High CPU utilization on a new installation

If you just installed Alliance LogAgent and you observe that it runs continually and registers high CPU utilization, it may be because Alliance LogAgent is processing historical events. By default, Alliance LogAgent will begin processing the oldest available events in the **`QAUDJRN`** security journal. If you have several weeks or months of data in the **`QAUDJRN`** it may take some time for Alliance LogAgent to process all of these events. Eventually Alliance LogAgent will finish processing the historical data and reduce its use of system resources. High CPU could also indicate that logging is turned on. Check both the client configuration and the global configuration to make sure logging is turned off. If you change the setting to 2 for No end and restart the subsystem. Be sure to clear the file **`ALLOGA`**

> ***NOTE:*** You can set the starting point for log collection using option `7` (Change QAUDJRN Starting Point) on the `Configuration` Menu. You can set the starting point to a specific journal receiver, or to a specific date and time. This can greatly reduce the amount of processing needed for a new installation.

High CPU utilization during Normal Operation

During normal processing you may see high CPU utilization rates by the Alliance LogAgent jobs. It is not uncommon to observe CPU utilization rates of 25 percent or higher. While the Alliance LogAgent jobs run at a low priority, the i5/OS operating system will give the application CPU resources if they are available. This is a normal condition and you should not observe a negative impact on interactive user jobs.

Temporary high CPU utilization may indicate that Alliance LogAgent is “catching up” by processing past events, or system activity generated a lot of events to process (see the section above about configuring system values).

Spikes in utilization

If you notice spikes in CPU utilization it almost always due to a spike in the number of **`QAUDJRN`** events that are being generated by the i5/OS operating system. This could be caused by a nightly backup or other activity that affects a large number of objects in user libraries. Review your system logs to determine what types of events are being collected during the time you observe the spike in activity. Look especially for ZR (object access) events and AD (authority adoption) events. You may want to adjust your security values to better manage the types of events that are being generated and processed by Alliance LogAgent.

Disk utilization

Capturing events to a physical file

Alliance LogAgent does not collect events in disk files even when processing a high volume of security events. This means that normal use of Alliance LogAgent should not have a significant impact on disk utilization. However, Alliance LogAgent gives you the ability to capture events to a user-defined file on your IBM i. Because event information can be quite large, and because there can be a very large number of events, this file can become quite large. Use option `1` (Configure Alliance LogAgent) to view the file collection option:

```
Capture to log file  . . . . . . .      2             1=Yes, 2=No
    File / Library / Member  . . . .     SYLOGF        ALLSYL100    SY
```

If the option is enabled you may want to turn it off and clear any captured events.

Application logging

As mentioned above, Alliance LogAgent provides options for collecting application events for diagnostic logging. If you observe the file `ALLOGA` in the `ALLSYL100` library becoming large, you should turn off the communications logging option (see above). You can then clear the file:

```
clrpfm file(allsyl100/alloga)
```

QAUDJRN buffering

Alliance LogAgent keeps track of all messages sent to a log collection or SIEM server. The delivery of each message is confirmed before another message is sent. While this provides the best security implementation to prevent lost events, it imposes a significant performance penalty. You can enable `QAUDJRN` event buffering to improve performance. If there is an unexpected system failure, you may need to reset the `QAUDJRN` starting point to pick up with the last message received by the log collection server. Buffering will provide much better performance for log transmission.

Chapter 6: Send To Syslog (SNDSYSLOG) Command

You can use the Send To Syslog (`SNDSYSLOG`) command to generate your own entries to Syslog-ng. The command can be run from a command line (CL), but you will probably want to use it in your application programs. The command can be added to any CL program to enable your applications to write to the Syslog-ng server. Note that the library `ALLSYL100` must be in your library list in order to use the `SNDSYSLOG` command.

Command parameters

```
SNDSYSLOG PRIORITY( priority-number )
    FACILITY( facility-number )
    DATE( date )
    TIME( time )
    HOST( host-name | blank )
    TAG ( tag-name )
    MSG( application-message )
    JOB( job-name )
    USER( user-name )
    JOBNO( job-number )
```

Priority

This is the Syslog priority number in the range of `0` to `7`. See the documentation in RFC 3164 for information on the meanings of the priority number.

Facility

This is the Syslog facility number in the range of `0` to `23`. See the documentation in RFC 3164 for information on the meanings of the facility number.

Date

Provide the date in the format CCYYMMDD where CC is the Century, YY is the year, MM is the month, and DD is the day. This is a character field.

Time

Provide the time in the format HHMMSS using 24-hour time notation.

Host

Provide the host name or the IP address of the host. If you leave this field blank Alliance will use system name from the Network Attributes. Use the Display Network Attributes (**DSPNETA**) command to view the system name.

Tag

Enter the application name or tag name you want to use for this Syslog entry.

MSG

Enter a message to be included in the Syslog entry. The message can be up to 1024 bytes in length. Please note that the maximum length of a Syslog entry, including the priority, date, host, tag, and message fields is 1024 bytes. If the resulting message is longer than 1024 bytes it will be truncated to this length and no error message will be sent.

Job

Enter the job name for this Syslog entry. This is an optional field.

User

Enter the user name for this Syslog entry. This is an optional field.

Job number

Enter the job number for this Syslog entry. This is an optional field.

Chapter 7: Send To CEF Log (SNDCEFLOG) Command

You can use the Send To CEF (**`SNDCEFLOG`**) command to generate your own entries to ArcSight ESM or compatible server. The command can be run from a command line (CL), but you will probably want to use it in your application programs. The command can be added to any CL program to enable your applications to write to the ArcSight ESM server. Note that the library **`ALLSYL100`** must be in your library list in order to use the **`SNDCEFLOG`** command.

Command parameters

```
SNDCEFLOG HOST( Host-name or IP address )
    DATE( date )
    TIME( time )
    VENDOR( vendor-name )
    PRODUCT( product-name )
    VERSION( product-version )
    SIGNATURE( signature-number )
    MSG( application-message )
    SEVERITY ( event-severity )
    EXTENSION( extended-message )
    JOB( job-name )
    USER( user-name )
    JOBNO( job-number )
```

Host

Provide the host name or the IP address of the host. If you leave this field blank Alliance will use system name from the Network Attributes. Use the Display Network Attributes (**`DSPNETA`**) command to view the system name.

Date

Provide the date in the format CCYYMMDD where CC is the Century, YY is the year, MM is the month, and DD is the day. This is a character field.

Time

Provide the time in the format HHMMSS using 24-hour time notation.

Vendor

Enter the vendor name for this event. The vendor name should be your company name for any user applications, or the name of your software provider if the message is for a vendor software solution.

Product

Enter the name of the software product for this event.

Version

Enter the version number for the software product.

Signature

Enter a unique signature value for this event. This value should be unique for this type of event. You should use signature values in the range of `1000` to `1999`.

MSG

Enter a message to be included in the log entry. The message can be up to 512 bytes in length. Please note that the maximum length of a log entry, including all fields is 1024 bytes. If the resulting message is longer than 1024 bytes it will be truncated to this length and no error message will be sent.

Severity

Enter a severity value from `0` to `10` with `0` being the lowest severity and `10` being the highest severity.

Extension

Enter additional text for this message. This is an optional field.

Job

Enter the job name for this Syslog entry. This is an optional field.

User

Enter the user name for this Syslog entry. This is an optional field.

Job number

Enter the job number for this Syslog entry. This is an optional field.

Chapter 8: Procedure ALLSysLog

You can use the Alliance procedure `ALLSysLog` in any ILE application to create entries for Syslog-ng. The service program `ALLSYSLOG` in library `ALLSYL100` can be bound to your application to provide an interface to this procedure.

ILE C definition

```
ALLSysLog(ULONG* pulPriority,
          ULONG* pulFacility,
          UCHAR* pcaTimestamp,
          UCHAR* pcaHost,
          UCHAR* pcaTag,
          UCHAR* pcaContent,
          ULONG* pulConvertOpt,
          UCHAR* pcaConvertTable,
          UCHAR* pcaMessage,
          ULONG* pulMessageLen,
          ULONG* pulReturn);
```

ILE RPG definition

```
d Priority            s           8b 0 inz(0)
d Facility            s           8b 0 inz(0)
d Timestamp           s           32a
d Host                s           64a
d Tag                 s           64a
d Content             s           2048a
d ConvertOpt          s           8b 0 inz(0)
d ConvertTbl          s           32a    inz('ANEB2AS   *LIBL')
d Message             s           2048a
d MessageLen          s           8b 0 inz(0)
d ReplyCode           s           8b 0 inz(0)


Callb(d)  'ALLFmtLog'
Parm                    Priority
Parm                    Facility
Parm                    Timestamp
Parm                    Host
Parm                    Tag
Parm                    Content
Parm                    ConvertOpt
Parm                    ConvertTbl
Parm                    Message
Parm                    MessageLen
Parm                    ReplyCode
```

See the previous documentation for the **SNDSYSLOG** command for information on the values of the parameters for this procedure.

Chapter 9: Procedure ALLCefLog

You can use the Alliance procedure **ALLCefLog** in any ILE application to create log entries for ArcSight ESM. The service program **ALLCEF** in library **ALLSYL100** can be bound to your application to provide an interface to this procedure.

ILE C definition

```
ALLCefLog(ULONG* pcaHost,
          UCHAR* pcaTimestamp,
          UCHAR* pcaDeviceVendor,
          UCHAR* pcaDeviceProduct,
          UCHAR* pcaDeviceVersion,
          UCHAR* pcaSignature,
          UCHAR* pcaContent,
          ULONG* pulSeverity,
          UCHAR* pcaExtension,
          ULONG* pulConvertOpt,
          UCHAR* pcaConvertTable,
          UCHAR* pcaMessage,
          ULONG* pulMessageLen,
          ULONG* pulReturn)
```

ILE RPG definition

```
d Host            s              65a
d Timestamp       s              32a
d Vendor          s              33a
d Product         s              33a
d Version         s              33a
d Signature       s              33a
d Content         s            2048a
d Severity        s               8b 0 inz(0)
d Extension       s            1024a
d ConvertOpt      s               8b 0 inz(0)
d ConvertTbl      s              32a   inz('ANEB2AS   *LIBL')
d Message         s            2048a
d MessageLen      s               8b 0 inz(0)
d ReplyCode       s               8b 0 inz(0)

Callb(d)  'ALLFmtCef'
Parm                    Host
Parm                    Timestamp
Parm                    Vendor
Parm                    Product
Parm                    Version
Parm                    Signature


Parm                    Content
Parm                    Severity
Parm                    Extension
Parm                    ConvertOpt
Parm                    ConvertTbl
Parm                    Message
Parm                    MessageLen
Parm                    ReplyCode
```

See the previous documentation for the **SNDSYSLOG** command for information on the values of the parameters for this procedure.

Chapter 10: Configuring IBM i Servers

Configuring Apache server logs

To enable logging in the Apache server, use the Work With Links (**WRKLNK**) command to edit the **httpd_conf** file in the **/www/(server-name)/conf** directory. You will need to add a **LogCycle** directive in order to force the Apache server to create one file. Without this directive the log files will have an appended time stamp and the syslog-ng application will not be able to process them. After updating the configuration file stop and restart the Apache web server instance with the Start TCP Server (**STRTCPSVR**) command.

```
LogCycle Off
CustomLog logs/access_log combined
```

You must now configure a source to read the file in syslog-ng. Apache logs will generally be placed in the **/www/(server-name)/logs** directory. Consult the syslog-ng documentation for instructions on how to configure syslog-ng to read the log file.

OpenSSH server logs

To enable logging in the OpenSSH server, use the Work With Links (**WRKLNK**) command to edit the **sshd_conf** file in the **/QopenSys/QIBM/ /ProdData/SC1/OpenSSH/openssh-3.5p1/etc** directory like this:

```
SyslogFacility AUTH
LogLevel INFO
```

Consult the documentation on the OpenSSH web site (http://www.openssh.org) for other syslog options.

After changing the sshd_config file you must create an empty log file. Sign on as **QSECOFR** , use the **STRQSH** shell, and use the following commands:

```
mkdir /var/adm
touch /var/adm/sshlog
```

You must now configure a source to read the file in syslog-ng. Consult the syslog-ng documentation for instructions on how to configure syslog-ng to read the log file.

Other server logs

A number of other open systems and proprietary applications can be deployed on the IBM i including MySQL, PHP, Perl, and others. Most of these types of applications can be enabled to collect system logs. Please consult the documentation for these servers on the steps to take to start collecting logs. Once logging is active you can configure a “source” statement in Syslog-ng to capture the logs.

Chapter 11: Problem Determination

In the event you have difficulties with an Alliance LogAgent application, the following procedures may be helpful.

System operator messages

When Alliance encounters a problem processing a Syslog transaction it may send a message to the system operator message queue. Use the `DSPMSG` command to view these messages. Many of the messages have second level text. You can press ***F1*** or the ***HELP*** key to view this text.

Application logging

The Alliance TCP client applications will create extra diagnostic information when the option for application logging is enabled. You should restart the subsystem when changing the logging option. When application logging is enabled there will be additional information written to the job log and to output spooled files in the job.

Appendix A – QAUDJRN Entry Type Mappings for CEF

The following table describes the default system security audit journal (`QAUDJRN`) mappings for the severity of messages assigned to Common Event Format (CEF) messages. You can use the `Work With Security Types` option on the configuration menu to change these values.

SEV	DESCRIPTION
7	Auditing change
9	Authority failure
6	Obtaining adopted authority

SEV	DESCRIPTION
4	Attribute changes
7	Authority changes
3	Command string audit
4	Create object
10	User profile changed, created, or restored
3	Change of *CRQD object
3	Cluster operations
3	Connection verification
10	Cryptographic configuration
2	Directory server
5	Delete object
10	DST security password set
7	System environment variables
3	Generic record
2	Socket description given to another job
2	Interprocess communication
7	IP rules action
3	Internet security management
9	Change to user parameter of job description
3	Actions that affect jobs
9	Key ring file
3	Link, unlink, or look up directory entry
3	Office services mail action
8	Network attribute changed
8	APPN directory search filter violation

SEV	DESCRIPTION
8	APPN end point filter violation
3	Object move or rename
7	Object restore
7	Object ownership changed
5	(Optical access) Single file or directory
5	(Optical access) Dual file or directory
5	(Optical access) Volume
8	Program changed to adopt authority
7	Change of an object's primary group
2	Printed output
7	Profile swap
10	Invalid user or password
7	Authority change during restore
8	Restoring job description with user profile specified
8	Change of object owner during restore
8	Restoring adopted authority program
8	Restoring a *CRQD object
8	Restoring user profile authority
8	Changing a primary group during restore
7	Changes to system distribution directory
7	Subsystem routing entry changed
3	Actions to spool files
3	Asynchronous signals
2	Secure sockets connections
5	Systems management changes

SEV	DESCRIPTION
7	Server security user information actions
10	Use of service tools
9	System value changed
8	Changing an access control list
3	Starting or ending a connection
3	Closing server files
5	Account limit exceeded
2	Logging on and off the network
5	Validation list actions
10	Network password error
8	Network resource access
2	Starting or ending a server session
7	Changing a network profile
9	Changing service status
5	Network authentication
1	DLO object accessed (change)
1	DLO object accessed (read)
1	Object accessed (change)
1	SOM access method
1	Object accessed (read)

Appendix B – Reducing the Number of Events

If you are looking to cut down on the number of `QAUDJRN` events that are sent to your log collection server, but still wish to remain compliant, below is a list of security events that can be turned off. Turning these off will reduce the traffic sent to your server. Note that the events will still be collected in the QAUDJRN journal.

> ***SECURITY NOTE:*** You should check with your auditor to ensure you are not turning off a `QAUDJRN` event that they are requiring.

`QAUDJRN` security types to turn OFF to reduce the events sent to server:

EVENT TYPE	DESCRIPTION
AP	OBTAINING ADOPTED AUTHORITY
CD	COMMAND STRING AUDIT
CV	CONNECTION VERIFICATION
GS	SOCKET DESCRIPTION GIVEN TO ANOTHER JOB
IP	INTERPROCESS COMMUNICATION
JS	ACTIONS THAT AFFECT JOBS
LD	LINK, UNLINK, OR LOOK UP DIR. ENTRY
O1	(OPTICAL ACCESS) SINGLE FILE OR DIR.
O2	(OPTICAL ACCESS) DUAL FILE OR DIR.
O3	(OPTICAL ACCESS) VOLUME
PO	PRINTED OUTPUT
SF	ACTIONS TO SPOOL FILES
SG	ASYNCHRONOUS SIGNALS
SK	SECURE SOCKETS CONNECTIONS
VC	STARTING OR ENDING A CONNECTION
VF	CLOSING SERVER FILES
VN	LOGGING ON AND OFF THE NETWORK
VS	STARTING OR ENDING A SERVER SESSION
YC	DLO OBJECT ACCESSED (CHANGE)
YR	DLO OBJECT ACCESSED (READ)
ZC	OBJECT ACCESSED (CHANGE)
ZM	SOM ACCESS METHOD

EVENT TYPE	DESCRIPTION
ZR	OBJECT ACCESSED (READ)