Townsend SECURITY

Alliance LogAgent Quick Start Guide

Software version: 2.00

Documentation version: 2.00.002

Alliance LogAgent
Quick Start Guide

Townsend Security, Inc.
724 Columbia St. NW, Suite 400
Olympia, WA 98501 USA
Voice: (360) 359-4400
Fax: (360) 357-9047
Website: www.townsendsecurity.com
E-Mail: info@townsendsecurity.com

Table of Contents

Chapter 1: Introduction

Alliance LogAgent provides real-time security event collection on an IBM i platform. It extracts events from the security audit journal QAUDJRN, the system history file QHST, and the system operator message queue QSYSOPR. The events are converted to a standard log format, and then communicated to a Security Information and Event Manager (SIEM) solution, or a log collection server such as syslog-ng. The events are managed in real-time and sequenced to ensure that no events are lost in the process.

This guide is designed to help the system administrator quickly install and use the Alliance LogAgent product. It supplements, but does not replace, the Alliance LogAgent Reference Manual which covers these topics in more detail.

Chapter 2: Pre-requisites

Hardware

Alliance LogAgent will run on any IBM i RISC system running a supported version of OS/400, i5/OS, or i/OS.

Software

Alliance LogAgent will run on any version of OS/400, i5/OS or i/OS from V5R3 or later.

If you plan to use SSL/TLS communications to send log events to your SIEM solution or log server, you must install and configure the free IBM Digital Certificate Manager (DCM) licensed product. DCM gives you the ability to create certificates that are used for the SSL/TLS session.

Security configuration

In order to capture IBM i security events you must create the journal QAUDJRN and related journal receives, and set the appropriate auditing system security values. Please consult the IBM Security Reference Manual for information on how to do this.

Communications

In order to use Alliance LogAgent you must have a SIEM solution or a log collection server. Discuss this requirement with your security administrator. The security administrator should give you the IP address and port number (usually 514) of the log collection server. You will need this to configure Alliance LogAgent.

Chapter 3: Documentation

The following documentation may be helpful to you in installing and using the Alliance LogAgent application:

- Alliance LogAgent Reference Manual
- Alliance LogAgent Digital Certificate Management Guide
- IBM Security Reference Manual

Chapter 4: Installing the Product

Installing from CD

New for Alliance LogAgent Version 2.00 and later

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(*SIGNOFF) TEXT('Alliance LGA Ownership Profile') OWNER(*USRPRF)
AUT(*EXCLUDE)

CRTAUTL AUTL(ALLLGAOWN) TEXT('Alliance AUTL for Ownership of LGA
Product') AUT(*EXCLUDE)
```

Next, you can add Users to the Authorization List that you want to be able to use the product using the following commands:

```
CRTUSRPRF USRPRF(somebody) PASSWORD() AUT(*EXCLUDE)

ADDAUTLE AUTL(ALLLGAOWN) USER(somebody) AUT(ALL)
```

Insert the Alliance LogAgent product CD into your IBM i CD reader and enter the Load and Run (LODRUN) command to install the application:

```
LODRUN DEV(OPT01) DIR('/')
```

Enter the appropriate name of your CD optical device.

Follow the prompts to install the Alliance LogAgent library ALLSYL100 to your IBM i.

Installing from a Web download

New for Alliance LogAgent Version 2.00 and later

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(*SIGNOFF) TEXT('Alliance LGA Ownership Profile') OWNER(*USRPRF)
AUT(*EXCLUDE)

CRTAUTL AUTL(ALLLGAOWN) TEXT('Alliance AUTL for Ownership of LGA
Product') AUT(*EXCLUDE)
```

Next, you can add users to the Authorization List who will use the product by using the following commands:

```
CRTUSRPRF USRPRF(somebody) PASSWORD() AUT(*EXCLUDE)

ADDAUTLE AUTL(ALLLGAOWN) USER(somebody) AUT(ALL)
```

Unzip the web download and provide a password if prompted.

On the IBM i create a save file to receive the downloaded save file information:

```
CRTSAVF SAVF(QGPL/ALLSYL)
```

Use FTP in binary mode to transfer the file to your IBM i:

```
Start, Run, FTP
Open 1.1.1.1      // use your IBM i IP address
User username     // use your IBM i user profile
Pass password     // use your IBM i password
Binary
Put c:\allsyl.savf qgpl/allsyl
Quit
```

You can now restore the product library:

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

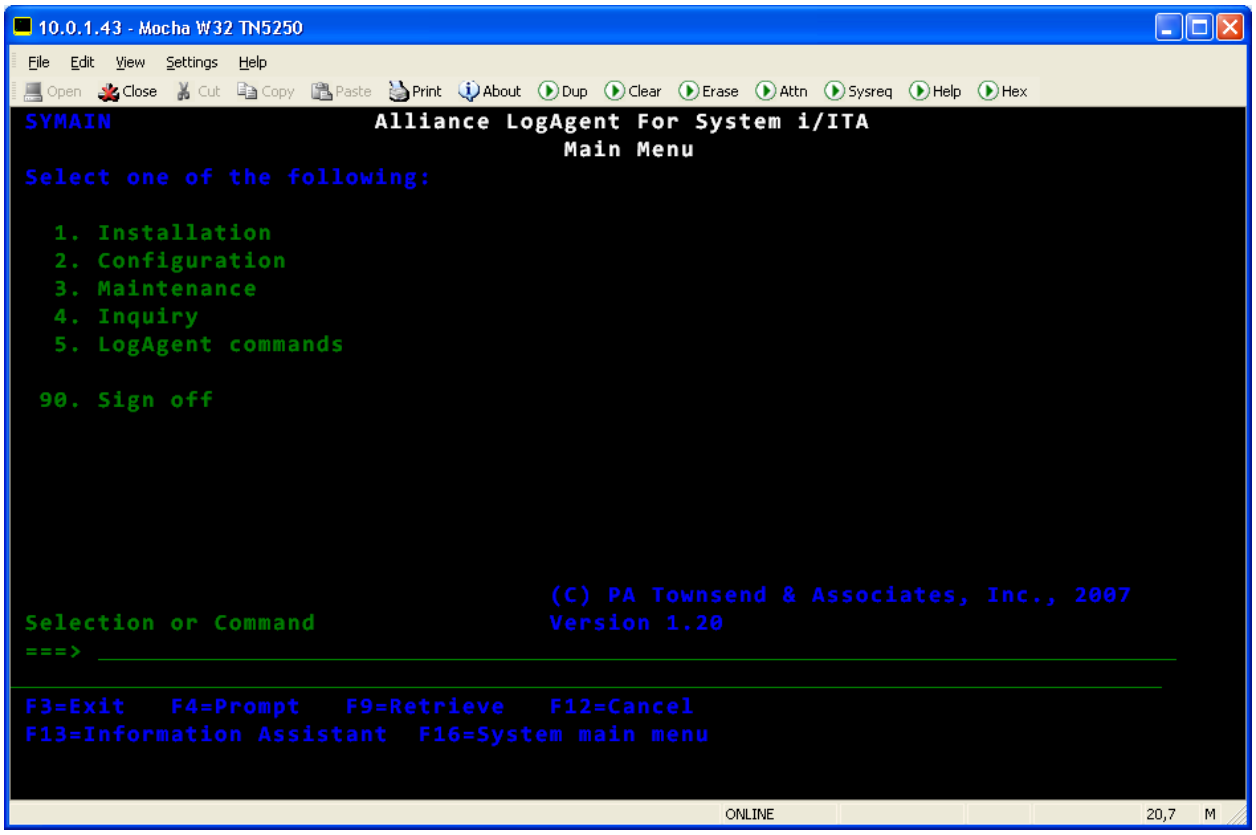

Chapter 5: Licensing the Product

Initial evaluation license

Use the product installation menu to install the first evaluation license. Add the library ALLSYL100 to your library list and display the main menu SYMAIN:

```
Addlible allsyl100

Go symain
```



Enter option 1 for Installation, then option 1 to enter a Trial Code. A new 30-day evaluation code is generated for you. Press ***Enter*** to update the code.

Alliance LogAgent is fully functional during the evaluation period.

Additional evaluation licenses

If your trial code expires before you finish your evaluation process, please contact your software supplier for an extension of your trial period.

Permanent licenses

After you pay for the software license you will receive a permanent license code. On the Installation menu select option 2 to Enter Permanent Code. Paste or type the code you received into this field and press ***Enter***. Your application is now permanently licensed.

Chapter 6: System Values That Affect Security Events

Several system values affect the collection and reporting of security events. These include:

- QAUDCTL – Auditing Control
- QAUDLVL – Security Auditing Level
- QAUDLVL2 – Security Auditing Level Extensions

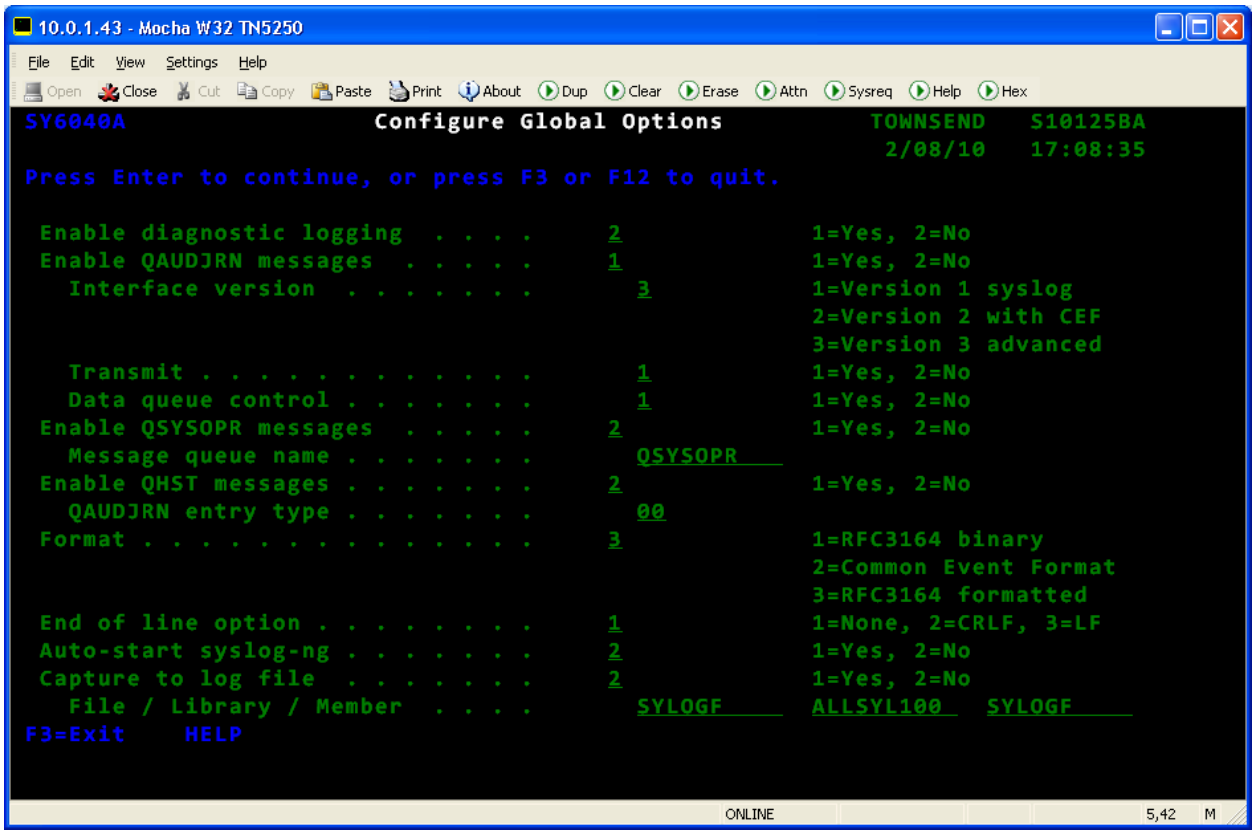
In addition to these system values, the Change User Audit (CHGUSRAUD) and Change Object Audit (CHGOBJAUD) commands can be used to gather important security information.

Please see the IBM Security Reference Manual for more information.

Chapter 7: Configuring LogAgent

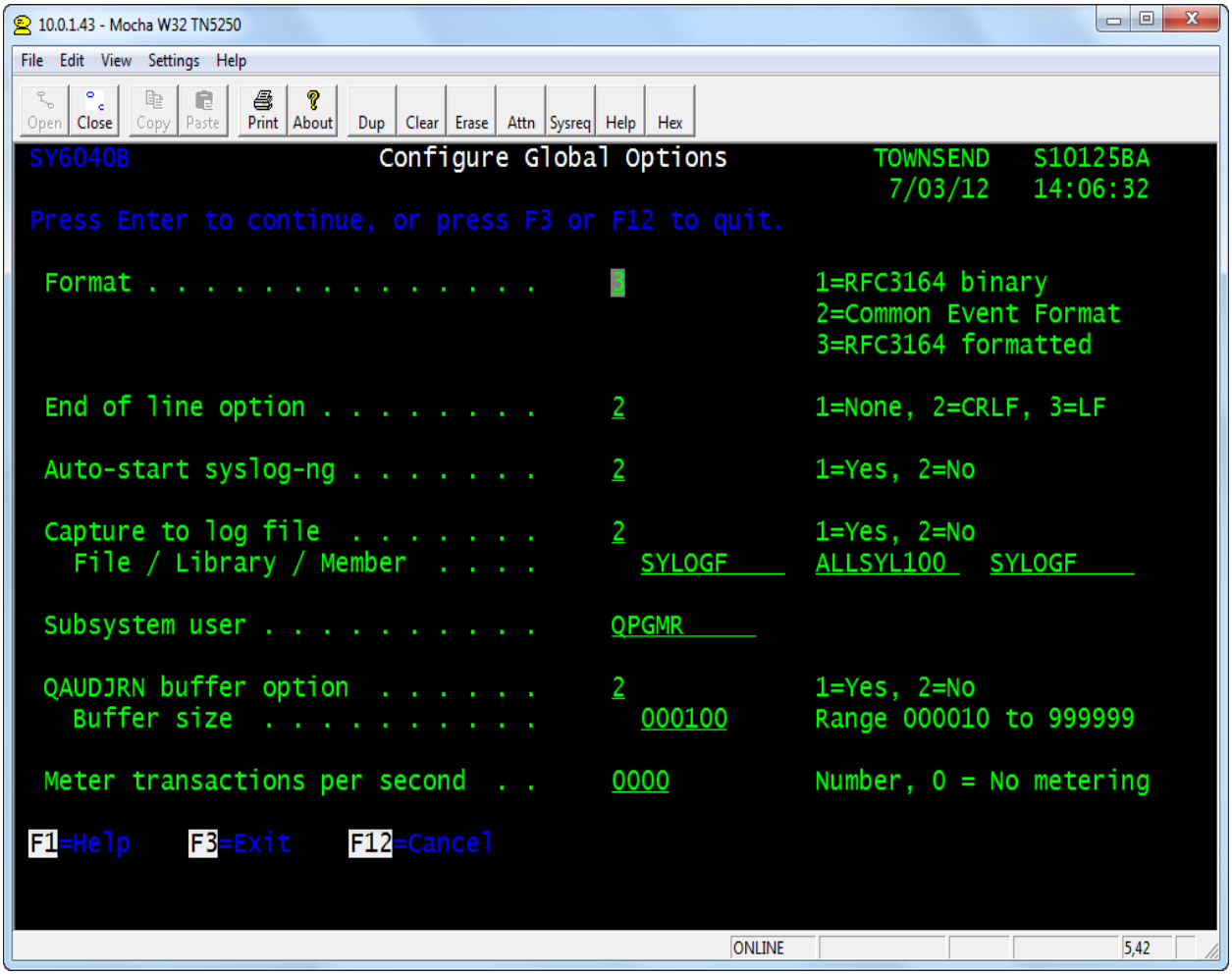
Global settings

You should now set the global options for Alliance LogAgent. From the main menu SYMAIN enter option 2 for Configuration, then option 1 to Configure Alliance LogAgent. The following panel is displayed:



You can use these settings as a starting point. These settings will collect information from the security audit journal QAUDJRN, but not from the QHST message file or from the system operator message queue QSYSOPR.

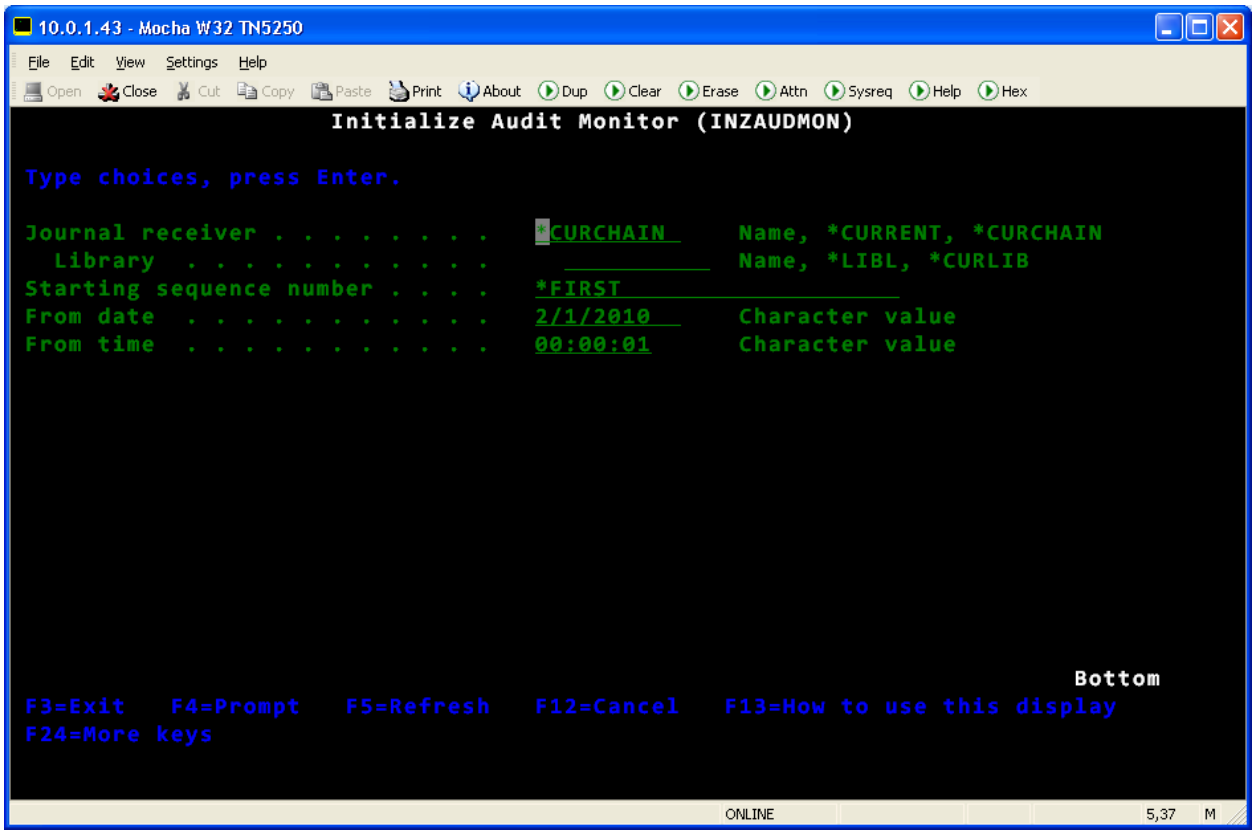
Press ***Enter*** to display the second configuration panel:



Press ***Enter*** to complete configuration.

Establishing the QAUDJRN starting point

Enter option 7 on the Configuration menu to set the starting point for the collection of security audit journal QAUDJRN. You can start the collection at a specific journal receiver and sequence number or at a specific start date and time:



In this example the starting date and time for security audit events is February 1, 2010 at 00:00:01 hours.

Chapter 8: Configuring Communications

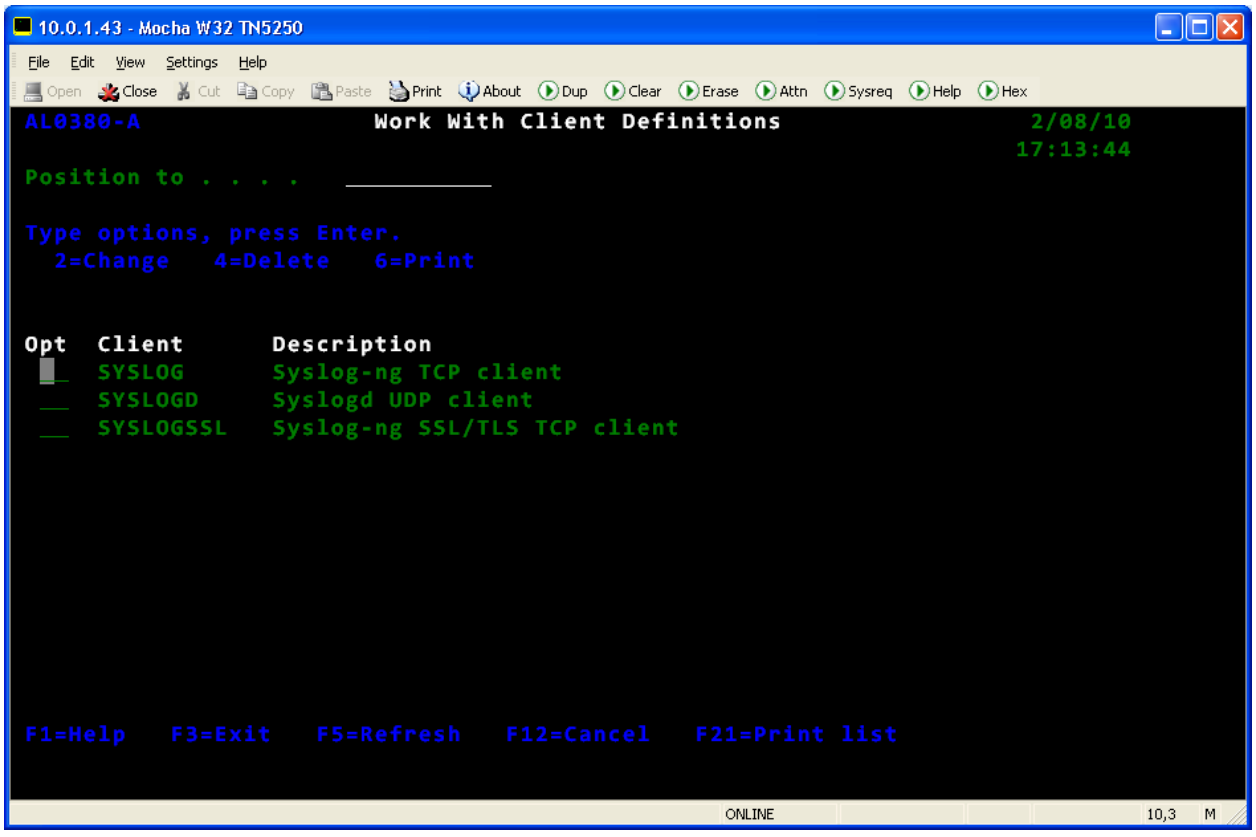
TCP communications for SIEM or log servers

Alliance LogAgent supports three methods of sending security events to a SIEM solution or log collection server:

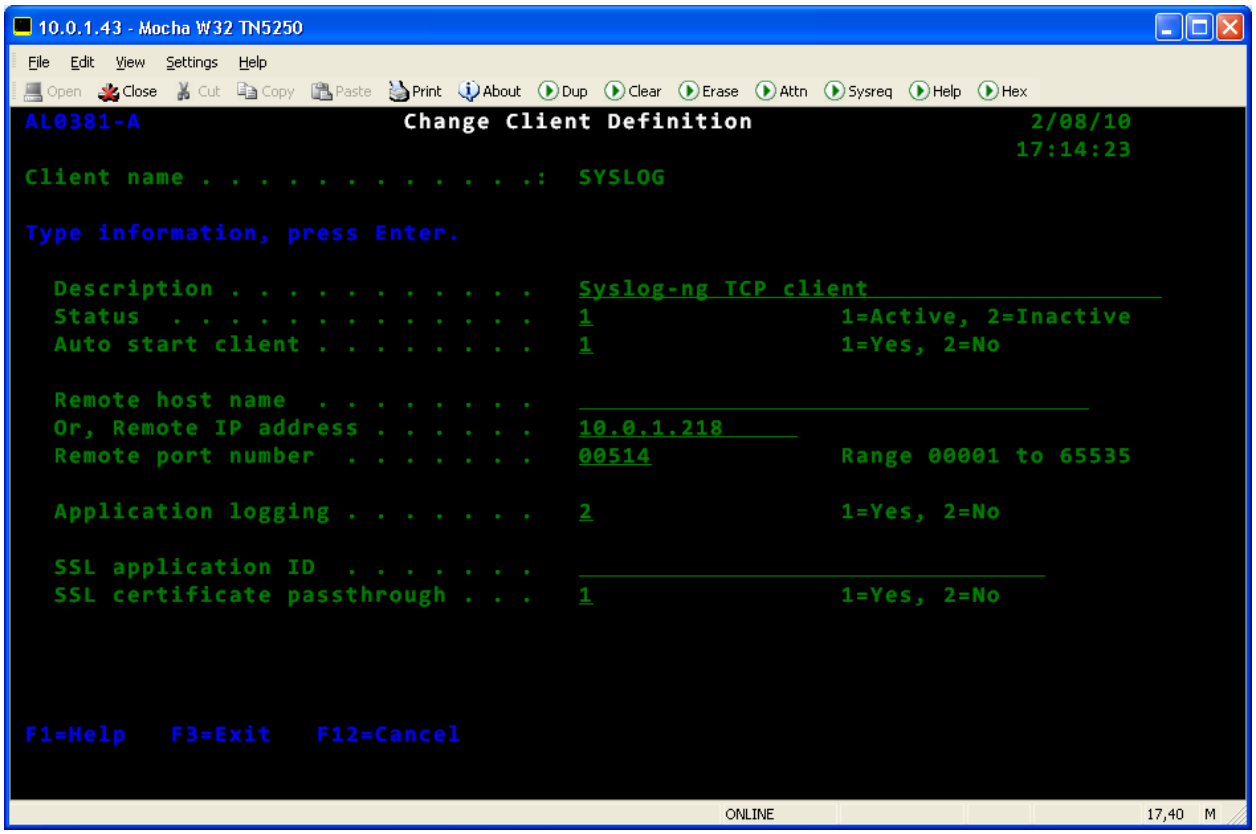
- UDP syslog communications
- TCP syslog communications
- SSL/TLS TCP syslog communications

Please consult with your network administrator to determine which communications protocol to use. Most IBM i customers use standard TCP communications.

From the main menu enter option 2 for configuration, then option 2 to Work With TCP Clients. The following panel is displayed:



To Change Client Definition, enter option 2 next to the SYSLOG parameter and press ***Enter***. The following panel is displayed:



Enter option 1 (Active) for Status, and option 1 (Yes) for Auto start client. When these options are enabled, communications will start automatically when the subsystem is started.

Be sure to specify the IP address of the SIEM or log collection server. The port number is normally 514, which is the default for log servers. However, you can enter any port number your network administrator specifies.

SSL TCP communications for SIEM or log servers

An option is provided for secure SSL/TLS TCP communications to your SIEM or log collection server. You must configure IBM Digital Certificate Manager (DCM) with certificates and an SSL Application ID, and your log server must be configured to accept secure SSL connections. Enter the SSL Application ID that you created in DCM in the appropriate field on this panel.

Chapter 9: Starting the ALLSYL100 Subsystem

Start the subsystem

You can enter option 10 on the Alliance LogAgent Configuration menu to start the ALLSYL100 subsystem, or you can use the Start Subsystem (STRSBS) command.

Active jobs

Depending on your configuration options, the following jobs may start in your subsystem:

- QAUDJRN – the security audit journal event collector
- QHST – the QHST message file collector
- QSYSOPR – the system operator message collector
  SYSLOG (2) – The pair of jobs that transmit information to the SIEM or log collection server

Performance

Alliance LogAgent runs in a batch subsystem at a low priority. It does not perform any special functions to use more CPU or disk resources than any other batch application.

When you first start Alliance LogAgent you may notice that it uses a fair about of CPU as it tries to process historical transactions.

> ***NOTE:*** Alliance LogAgent is running at a low priority and should not have a negative impact on interactive response times.

Automating the startup process

Alliance LogAgent jobs are designed to start automatically when the subsystem ALLSYL100 starts. You can automatically start this subsystem in your IPL start up job. View the system value QSTRUPPGM to determine which program runs at IPL. You can then modify this program to start the ALLSYL100 subsystem.

Chapter 10: Special Topics

Diagnosing communications problems

When you first start Alliance LogAgent you may encounter problems with the transmission of security events to your SIEM solution or log collection server. Use the Configuration menu option to Work With TCP Clients. Edit the configuration and enter option 1 (Yes) in the Application Logging parameter. Restart the subsystem and collect some error entries in the log.

You can now view the file ALLOGA to view the possible causes of the problem. Some common causes are:

- There is no TCP route to the log collection server (use CFGTCP to create a TCP route).
- The port number is configured incorrectly. Receive the correct port number and edit your TCP configuration.
- An SSL connection does not have a correct IBM DCM configuration. Use DCM to create a certificate and Application ID for this connection.

Diagnosing subsystem job problems

If jobs are not starting correctly, you can change the job logging level to collect detailed job logs. Use the program SYLOGON to enable detailed job logs:

```
CALL PGM(SYLOGON)
```

Restart the subsystem. Any failed jobs will now have a detailed job log.
You can disable detailed job logs with the SYLOGOFF program:

```
CALL PGM(SYLOGOFF)
```

Capturing events to a file

Alliance LogAgent has the ability to collect events to a file on the IBM i. This can help you diagnose problems with security events. Enter option 1 on the Configuration menu to enable logging to a file:

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

Alliance provides the file SYSLOGF in the product library for this purpose. You can also specify your own application file.

Chapter 11: Support

Contact your software supplier for any technical support you may need. You can also contact Townsend Security, Inc. on the web at:

http://www.townsendsecurity.com

Index

S

T

U

