CA Chorus™ for Security and Compliance Management

Administration Guide

Version 04.0.00

CA Technologies Product References

This document references the following CA Technologies products:

- CA ACF2™ for z/OS (CA ACF2)
- CA Chorus™
- CA Chorus™ for DB2 Database Management
- CA Chorus™ for Security and Compliance Management
- CA Chorus™ Software Manager
- CA Datacom®/AD (CA Datacom/AD)
- CA Top Secret® for z/OS (CA Top Secret)
- CA Vantage™ Storage Resource Manager (CA Vantage)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Managing CA Chorus Components

How to Start CA Chorus

Before you start using the CA Chorus web service application, ensure that the started tasks required for the configuration of CA Chorus are active on all of your systems. You can start the CA Chorus and discipline-related components independently.

Start CA Chorus for Security and Compliance Management Components

Select the following procedures based on your configuration.

Start CA ACF2

After you configure CA ACF2, you can start the product.

Before starting CA ACF2, verify the following:

- CAIRIM is installed. (CAIRIM is part of the CA Common Services.)
- The TSO procedure IKJACCNT is available. This procedure is the default used for your initial signon with the default user ID and default GSO TSO options.

Follow these steps:

1. Start CA ACF2 using one of these methods:
   - If you want to start CA ACF2 automatically and you have edited the CAISECXX member of CAI.CAACF.PARMLIB as described in CA ACF2 System Initialization, do the following:
     - Copy CAISECXX from CAI.CAACF.PARMLIB into the CAISEC*xx* member of SYS1.PARMLIB.
     - Copy the CAIACFXX member from CAI.CAACF.PARMLIB into the CAIACF*xx* member of SYS1.PARMLIB. It contains the CA ACF2 startup parameters.

     You can proceed to item #3 at this point.
   - If you want to start CA ACF2 manually, add the S ACF2 command to the COMMND*xx* member of SYS1.PARMLIB. Because CA ACF2 runs as a subsystem, it should be fully initialized before you process any job with JES2 or JES3.

2. Construct the initial set of Global System Options (GSO) records.

   During the initial IPL, CA ACF2 attempts to locate GSO records. When CA ACF2 detects that no records are present, it prompts the operator for continuation options as shown in the following sample. Reply as indicated to construct the initial set of GSO records. Subsequent CA ACF2 startups do not require operator intervention.

   ```
   ACF79505 INITIAL START IN PROGRESS FOR SYSTEM: sysid
   ACF79510 WARNING: NO GSO RECORDS FOUND FOR SYSTEM: sysid
   *10 ACF79517 CONTINUE GSO PROCESSING WITH DEFAULT VALUES?
   reply 10,u
   ACF79530 NO GSO RECORD FOUND FOR: recid SYSID: sysid
   *11 ACF79534 CONFIRM USE OF DEFAULTS FOR: recid SYSID: sysid
   reply 11,u
   ACF79507 GSO PROCESSING COMPLETED WITHOUT ERROR
   ```

   If you are migrating from a prior version, changes or additions to GSO options can result in warning message ACF79600, which indicates that the record is outdated. This message is normal. Change the records flagged to set the new or changed option as appropriate for the site. Refresh the GSO record to put the option into effect.

   Note: When a new field is added to an existing GSO record, the value of the new field is not necessarily the default value specified in the documentation. This is because when a new field is added to an existing GSO record, the new field assumes the value that is in the area of the record that it now represents. To ensure the default values are used for new fields, the record must be inserted by the current version of CA ACF2.

3. Start JES.

   JES2 needs only a warm start. JES3 requires a hot start.

4. Start TSO and log on to the system as ACFUSER or the site-specified logonid supplied in job INITIAL.

5. Complete the following if you have a shared DASD environment.

   The CA ACF2 GSO BACKUP record should include the CPUID parameter to identify the single system responsible for backup processing. You can use the NOBACKUP parameter of the S ACF2 command to deactivate automatic backup processing on a given system. BACKUP is the default. For more information, see the chapter "Maintaining Global System Options Records" in the *Administrator Guide*.

You no longer need to identify the CA ACF2 subsystem name in IEFSSN*xx* in SYS1.PARMLIB. CA ACF2 intercepts the system security initialization module and dynamically installs its own subsystems by building subsystem control table (SSCT) entries.

Start CA Top Secret

CA Top Secret can be started:

- As a subsystem before JES. Specify SUB=MSTR on the O/S START command. TYPE=2 (or JES2) and LEVEL=SP n.n.n must be specified in the JES control option. Failure to do so displays the message TSS9112E-UNABLE TO DETERMINE JES LEVEL.
- During a system IPL after JES initialization. Start CA Top Secret *before* all of the CA Common Services except CAIRIM. CAIRIM must initialize before CA Top Secret.

If the TSS address space is up before JES, the $$$LOG$$ spool file is automatically allocated when JES starts. For CPF nodes that require sysout support, the nodes will need to be defined in the NDT and refreshed after JES is up. Spool files for those nodes will then be allocated without restarting the TSS address space. Because of this change, TSS must shut down before JES.

Note: If a subsystem with the same name as a started task exists, the MSTR subsystem is the default for the started task. If no MSTR subsystem exists, the primary JES subsystem is used. In CA Top Secret r15, we established a subsystem with the name TSS. Therefore, if the procname that starts CA Top Secret is TSS, it will start under the master subsystem. To avoid the procname running under MSTR, change the name of the proc.

How to Initialize CA Top Secret as a Subsystem

This section explains how to use CAISEC00 to start CA Top Secret and CA SAF SECTRACE subsystems automatically. You can initialize CA Top Secret from CAISEC00 or from the command table SYS1.PARMLIB(COMMNDxx).

Note: For first-time installations of CA Top Secret, put a START TSS entry in SYS1.PARMLIB(COMMNDxx) or a TSS(xx START) entry in CAISEC00; otherwise, you must start CA Top Secret manually from the operator console.

1. Create a member called CAISEC00 for your started tasks. In CAISEC00, list each subsystem name, whether it should start automatically, and which members of SYS1.PARMLIB contain additional operands for the START command. For example:

```
EDIT ---- SYS1.PARMLIB(CAISEC00) - 01.01 --------------- COLUMNS 001 072 COMMAND
===> SCROLL ===> CSR
************************ TOP OF DATA ************************ 00000001 TSS(xx
START)
00000003 TRCE(xx START)
00000004 PROMPT
************************ BOTTOM OF DATA ************************
```

   Note: To start some, but not all, of the subsystems listed in the CAISEC00 member, place an asterisk (*) to the left of the name of each subsystem that you do not want to start. Notice that the entry number matches the SYS1.PARMLIB member. For example, TSS(01 START) matches member CAITSS01.

2. Specify the following keyword in the CAISEC00 member. To do so, selecting the CAISECxx suffix by responding to the prompt message:

   PROMPT

   Indicates that the operator console should be prompted for specification of the CAISEC initialization parameters. During CA SAF initialization, a WTOR message CAS2070I is issued to allow the operator to specify the CA SAF initialization parameters.

3. Specify that CA SAF is to use the CAITSSxx parmlib member by using one of the following options:

   ```
   TSS(xx)
   TSS(xx START)
   TSS(xx NOSTART)
   ```

4. Specify the CAISECxx parmlib member suffix by using one of the following options:

   ```
   SEC=xx or SEC(xx)
   ```

   This step lets a site maintain multiple CAISECxx parmlib members. CAISEC00 is the initial parmlib member processed during CA SAF startup processing. Within the CAISEC00 member, you can specify any of the valid initialization parameters, including SEC=xx to indicate that an alternate parmlib member should be processed. The last value processed for any of the valid initialization keywords is the value selected for processing. To avoid initialization processing loops, a CAISEC member suffix can be specified only once for processing.

   Note the following behaviors:

   - To use the CAISEC00 parmlib member as it currently exists, use the U option to cause CA SAF. This value is the default, and it lets you continue processing.
   - The U option is available as a response to the prompt at the console only; you cannot use it as a keyword value in CAISEC00. You are unable to specify any other parameters after you specify U.
   - If you specify a single parameter or multiple parameters, such as TSS(xx), these replace their counterparts in CAISEC00 or any other CAISECxx member that you specify with the SEC(xx) parameter. All other parameters remain the same.

   Note: To use one or more of these options automatically at startup, put them in CAISEC00 and remove the PROMPT keyword.

Start the CA LDAP Server

At this point, the product is deployed and configured. You are ready to start up the CA LDAP Server.

1. Copy the LDAPR151 STC PROC from CDT9JCL into your proclib.
2. Start the STC using the LDAPR151 job.

CA LDAP is now started on your system.

Start the CA Compliance Manager Components (Manually)

The CA Compliance Manager components that you chose to implement must be started and active so that the security events from the external security manager (ESM) can be processed through the Router and received by the active components and updated.

The following started task procedures are used to start the CA Compliance Manager components:

- CMGRRTR - starts the Router component (required)
- CMGRLOGR - starts the Logger component
- CMGRWHSE - starts the Warehouse component
- CMGRMON - starts the Monitor component
- CMGRALRT - starts the Alert component

Important! The Router must be started and active before any of the other components can start receiving events.

Follow these steps:

1. Copy all the CA Compliance Manager started task procedures from the CAI.CEIQPROC library into the library from which the procedures will be executed (for example, SYS1.PROCLIB).
2. Modify and configure the started task procedures to conform to your installation standards. Specify the logstream name and the DB2 subsystem (ssid) or CA Datacom/AD MUF name (CMGRMUF). For more information, see the CA Compliance Manager *Implementation Guide*.
3. Start the Router by issuing the following console command:

   ```
   S CMGRRTR
   ```

4. Verify that the Router successfully started.
5. Start the Logger component, if you are implementing a Data Mart repository, by issuing the following console command. Otherwise, skip this step:

   ```
   S CMGRLOGR
   ```

6. Verify that the Logger component successfully started.

   If the Router is not active, CA Compliance Manager prompts you to start the Router. Retry component initialization by responding 'Y' to the following prompt:

   ```
   CMGR220I CMGR Retry Initialization <Y> or <N> ?
   ```

   Issue the following status operator command to view Logger component status:

   ```
   F CMGRLOGR,STATUS
   ```

7. Start the Warehouse component, if you are implementing a Warehouse, by issuing the following console command:

   ```
   S CMGRWHSE
   ```

8. Verify that the Warehouse component successfully started.

   If the Router is not active, CA Compliance Manager prompts you to start the Router. Retry component initialization by responding 'Y' to the following prompt:

   ```
   CMGR220I CMGR Retry Initialization <Y> or <N> ?
   ```

   Issue the following status operator command to view Warehouse component status:

   ```
   F CMGRWHSE,STATUS
   ```

9. Start the Monitor component, if you are implementing a Monitor repository, by issuing the following console command:

   ```
   S CMGRMON
   ```

10. Verify that the Monitor component successfully started.

    If the Router is not active, CA Compliance Manager prompts you to start the Router. Retry component initialization by responding 'Y' to the following prompt:

    ```
    CMGR220I CMGR Retry Initialization <Y> or <N> ?
    ```

    Issue the following status operator command to view Monitor component status:

    ```
    F CMGRMON,STATUS
    ```

11. Start the Alert component by issuing the following console command:

    ```
    S CMGRALRT
    ```

12. Verify that the Alert component successfully started.

    If the Router is not active, CA Compliance Manager prompts you to start the Router. Retry component initialization by responding 'Y' to the following prompt:

    ```
    CMGR220I CMGR Retry Initialization <Y> or <N> ?
    ```

    Issue the following status operator command to view Alert component status:

    ```
    F CMGRALRT,STATUS
    ```

Start the CA Compliance Manager Components (Automatically)

You can use the command table in SYS1.PARMLIB(COMMNDxx) instead of the console command to start CA Compliance Manager component address spaces as early as possible during the IPL process, preferably before JESx initialization.

Follow these steps:

1. Copy all the CA Compliance Manager started task procedures from the CAI.CEIQPROC library into the library from which the procedures will be executed (for example, SYS1.PROCLIB).

   - CMGRRTR - starts the Router component (required)
   - CMGRLOGR - starts the Logger component
   - CMGRWHSE - starts the Warehouse component
   - CMGRMON - starts the Monitor component
   - CMGRALRT - starts the Alert component

   Important! The Router must be started and active before any of the other components can start receiving events.

2. Edit the COMMNDxx member in SYS1.PARMLIB to add the following entries for any of the CA Compliance Manager components you chose to implement:

   ```
   COM='S CMGRRTR,SUB=MSTR'
   COM='S CMGRLOGR,SUB=MSTR'
   COM='S CMGRWHSE,SUB=MSTR'
   COM='S CMGRMON,SUB=MSTR'
   COM='S CMGRALRT,SUB=MSTR'
   ```

3. Verify that the CA Compliance Manager components you chose to implement successfully started during the IPL process.

   Issue any of the following status operator command to view component status:

   ```
   F CMGRRTR,STATUS
   F CMGRLOGR,STATUS
   F CMGRWHSE,STATUS
   F CMGRMON,STATUS
   F CMGRALRT,STATUS
   ```

Start the CIA Real-Time Component

After completing the configuration, security definitions, and control options steps, you can start and stop the CIA real-time component.

The following steps describe how to start and stop the CIA real-time component:

- Automatically start during initialization
- Start with a console command
- Stop the CIA real-time component

Note: We recommend that the CIA real-time component address spaces start as early as possible following security product initialization.

Automatically Start During Initialization

The CIA real-time component is automatically started if you defined the proper CIA security definitions and control options earlier in this Guide.

Start with a Console Command

If you did not yet start the CIA real-time component, use a console command to manually start the CIA real-time component.

To manually start the CIA real-time component, issue the following command at the console:

```
S CIARTUPD
```

Note: If you changed the name of the CIA real-time component procedure, specify that value in the command rather than CIARTUPD.

How to Stop CA Chorus

You can stop the CA Chorus components independent of the back-end products supporting each discipline. For example, CA Database Management for DB2 for z/OS products that are used with CA Chorus for DB2 Database Management. When the CA Chorus components are down, the back-end products continue to operate in your environment.

Stop CA Chorus for Security and Compliance Management Components

Select the following procedures based on your configuration.

Stop the CIA Real-Time Component

To stop the CIA real-time component address space, issue the following command at the console:

```
P CIARTUPD
```

Note: If you changed the name of the CIA real-time component procedure, specify that value in the command rather than CIARTUPD.

Stop the Router

You can stop the Router address space at any time.

To stop the Router component, issue the following command at the console:

```
P CMGRRTR
```

Note: CMGRRTR represents the active CA Compliance Manager procedure.

Important! Stopping the Router shuts down not only the Router but also any associated active component address spaces, including the following:

- Alert component (CMGRALRT started task procedure)
- Logger component (CMGRLOGR started task procedure)
- Monitor component (CMGRMON started task procedure)
- Warehouse component (CMGRWHSE started task procedure)

Stop the Alert Component

Use this procedure to stop the Alert component address space at any time.

To stop the Alert component, issue the following command at the console:

```
P CMGRALRT
```

Note: CMGRALRT represents the active CA Compliance Manager procedure.

Stop the Logger Component

Use this procedure to stop the Logger component address space at any time.

To stop the Logger component, issue the following command at the console:

```
P CMGRLOGR
```

Note: CMGRLOGR represents the active CA Compliance Manager procedure.

Stop the Warehouse Component

Use this procedure to stop the Warehouse component address space at any time.

To stop the Warehouse component, issue the following command at the console to shut down the Warehouse component address space:

```
P CMGRWHSE
```

Note: CMGRWHSE represents the active CA Compliance Manager procedure.

Stop the Monitor Component

You can stop the Monitor component address space at any time.

To stop the Monitor component, issue the following command at the console:

```
P CMGRMON
```

Note: CMGRMON represents the active CA Compliance Manager procedure.

Appendix A: Additional CA Chorus for Security and Compliance Management Configuration

Configure the Global Configuration

Configure the global configuration to specify CA Compliance Manager settings.

Follow these steps:

1. Add the CHORUS CETJPLD library to the steplib in the Compliance Manager Monitor and Alert PROCS.
2. Stop and re-start both address spaces.
3. Add the Quick Links module to a dashboard.
4. Click Administer Compliance Policy.

   The Policy Administrator UI opens.
5. Click the applicable instance from the Administration pane.

   The tree expands to show the folders.
6. Click Policy Administration, Configuration.

   The Configuration window opens.
7. Type the CA Unicenter web address, your CA Unicenter user ID, password, and then confirm your password under Service Desk.

   The service desk settings are set.
8. Type the DLL file name *libedb2* in the module field under Change Control.

   The change control setting is set.
9. Type the CA Chorus host, port, log location, and log level under Alerts.

   Note: Using SSL for alerts is optional. Your environment must be configured before you can use this option. For more information about enabling SSL, see the *CA Chorus for Security and Compliance Management Site Preparation Guide*.

   The Chorus Alerts are configured.
10. Select the Weekend/Weekday Designation from the drop-down list.

    Weekends and weekdays are defined.

11. (Optional) Specify the default WTO Route Code and Descriptor Code Designation.

    The default settings for WTO are specified.

12. Click Create Configuration.

    A confirmation message appears.

Global Configuration Pane

The Global Configuration pane lets you manage the global settings for the Service Desk account, change control, email servers, CA Chorus alerts, weekend/weekday designations, and WTO route code/descriptor code designation.

The Global Configuration pane contains the following fields:

Service Desk

Includes the fields to identify the service desk and the user.

URL

Defines the address of CA Unicenter where the CA Compliance Manager sends service desk notices.

Example: http://*yourserver.com*:*port*/axis/services/R11_USD_WebService

Userid, Password, Confirm

Defines your CA Unicenter ID and password. When service desk notices occur, the CA Compliance Manager associates the service desk ticket with this user ID.

Change Control

Includes change control options.

Module

Defines the data link library (DLL).

Email

Includes email options.

Primary Email Server

Defines the URL of the primary email server.

Primary Email Server Port

Defines the port of the primary email server.

Backup Email Server

Defines the URL of the backup email server.

Backup Email Server Port

Defines the port of the backup email server.

Alert

Includes the CA Chorus Alert options.

Machine Name for Alerts

Defines the server name that the CA Chorus alert is sent to. This value is defined under TEIID_MACHINE in the ENVETJ member in *chorus_runtime_hlq*.CETJOPTN.

Example: yourserver.com

Port for Alerts

Defines the port on the server where the CA Chorus alert is sent.

Example: 7070

The following definition details the CA Chorus port:

httpconnectorport

The port number that is used to access CA Chorus Application Server. Use the value of JBOSS_HTTP_PORT in CETJOPTN(ENVETJ). By default, this value is the TEIID_PORT value +4 for HTTP. For SSL, use the value of JBOSS_SSL_PORT in CETJOPTN(ENVETJ). By default, the value is the TEIID_PORT value + 10.

Host URL

Indicates the full URL that the CA Chorus alert is sent to. This noneditable field is displayed if you have specified machine name and port for alerts.

Example: http://yourserver.com:7070/Chorus/services/eventListener

Log Location

Defines the path to the file containing the log for the alert session.

Log Level

A numeric value indicating the level of logging.

Use SSL

(Optional) Lets you use SSL for alerts. Your environment must be configured before you can use this option. For more information about setting CA Compliance Manager components, see the *CA Chorus for Security and Compliance Management Site Preparation Guide*.

Weekend/Weekday Designation

Weekend

Specifies two days that are considered the weekend.

Weekdays

Indicates the nonweekend days that are considered weekdays.

Default WTO Route Code/Descriptor Code Designation

Includes the WTO message default options. The numerical values have different meanings and can be used differently across organizations. If you are unsure of the value to use, contact your System Programmer.

Default Descriptor Code

Specifies the descriptor code that is assigned to the WTO messages sent by the CA Compliance Manager.

Default Route Code

Specifies the default routing code that is used for the WTO messages sent by the CA Compliance Manager.

CA Chorus for Security and Compliance Management TSF Database Recommendations

The following chart uses the following TSFPARMS (member of CETJOPTN) metric management tier parameters:

- MMT1EXPIRY = 1D = 1 day
- MMT2EXPIRY = 14D = 14 days

The following chart is based on the statistics interval value taken from the security products parameter: CHORUSSTATI

If your security product collects statistical data for Command Propagation Facility (CPF) nodes, this chart also provides recommended values for up to five CPF nodes.

Number of Systems (LPARS)	Security Chorus Statistics Interval Value	Recommended TSF Database Cylinders for System	Recommended TSF Database Cylinders for CPF nodes	Recommended TSF Database Cylinders Total
1	30 seconds	5	1	6
	60 seconds	4	1	5
	15 minutes	3	1	4
	30 minutes	3	1	4
3	30 seconds	15	3	18
	60 seconds	8	2	10
	15 minutes	7	1	8
	30 minutes	7	1	8
5	30 seconds	24	5	29
	60 seconds	16	4	20
	15 minutes	11	2	13

Number of Systems (LPARS)	Security Chorus Statistics Interval Value	Recommended TSF Database Cylinders for System	Recommended TSF Database Cylinders for CPF nodes	Recommended TSF Database Cylinders Total
	30 minutes	11	1	12

The following chart uses the following TSFPARMS (member of CETJOPTN) metric management tier parameters:

- MMT1EXPIRY = 7D = 7 days
- MMT2EXPIRY = 8D = 8 days

The chart is based on the statistics interval value taken from the security products parameter: CHORUSSTATI

If your security product collects statistical data for Command Propagation Facility (CPF) nodes, this chart also provides recommended values for up to five CPF nodes.

Number of Systems (LPARS)	Security Chorus Statistics Interval Value	Recommended TSF Database Cylinders for System	Recommended TSF Database Cylinders for CPF nodes	Recommended TSF Database Cylinders Total
1	30 seconds	23	6	29
	60 seconds	13	3	16
	15 minutes	3	1	4
	30 minutes	3	1	3
3	30 seconds	69	16	85
	60 seconds	38	9	47
	15 minutes	8	2	10
	30 minutes	7	1	8
5	30 seconds	115	27	142
	60 seconds	63	15	78
	15 minutes	14	3	17
	30 minutes	11	2	13