IBM Security zSecure V2.4.0

Enhancements for compliance automation and usability IBM Security zSecure Alert User Reference Manual

Chapter 1. About this document

This document describes the documentation updates as a result of the zSecure enhancements for compliance automation and usability (for APAR numbers OA60419, OA60420, and OA60459 - December 2020).

The following enhancements were made:

- More control automation for RACF, and some for ACF2 and Top Secret.
- Upgrade to STIG Version 6 Release 47 (6.47).
- New library: SCKACUST
  In previous zSecure versions, following a PTF, customers had to run job CKAZCUST to create new CKACUST members in the customer's Site and User CKACUST data sets.
  Starting with this SSE, the new SCKACUST library is added to the concatenation for DDname CKACUST. New CKACUST members that are introduced in compliance controls are now automatically provided in SCKACUST. Following specification of the relevant zSecure configuration information, these new members are automatically copied from SCKACUST to the customer's Site or User CKACUST data sets.
- New library: SCKACUSV
  The CKACUST data set has records that are limited to 80 characters. The CKACUSV data set allows specifying longer values. The issuer name of a digital certificate is an example of a value that can be much longer. Your zSecure configuration (by default, C2R$PARM) must define which data set is to be used as the CKACUSV data set, or it must be set up manually through option Setup Command files (SE.8).
- Additional VM events for SIEM.
- Background run capabilities for RA.3.2, AM.8, and AM.9.
- Support for SMF relocate section 443 and ID token extensions.
- New report types:

  CERTIFICATE
  A record in the TYPE=CERTIFICATE report type describes a digital certificate as it is present on a particular system.

  IOAENV
  The IOAENV report type shows the security settings of active BMC INCONTROL IOA environments, and it includes information on the IOA, Control-D, Control-M, and Control-O products.

  IP_INETD
  The IP_INETD report type shows configuration of network services that the inetd daemon manages.

  JES_DEVICE
  The JES_DEVICE report shows the available JES2 devices and the information that is used to secure them.

  JES_REMOTE
  The JES_REMOTE report shows the available remote JES2 workstations, and the information that is used to secure them.

  SSH_DAEMON
  The SSH_DAEMON report shows the configuration of the z/OS OpenSSH SSH daemons that run in the UNIX address spaces in the system.

  SUPSESS_REGION_CP
  The SUPSESS_REGION_CP newlist type can be used to report about IBM CL/SuperSession. Each record in the TYPE=SUPSESS_REGION_CP report describes a Network Access Manager Control Point.

  For details, see the documentation updates for the *zSecure CARLa Command Reference*.

- New ACF2_SENSDSN_ACCESS fields link logonids with started task to better determine their authorization.
- Enhancements for parsing parameter members.
- zSecure Alert enhancements:
  - zSecure Alert provides an option to exploit a CKRCARLA internal restart to refresh environment information while retaining job information.
  - Batch jobs are now provided to ease upgrade, maintenance, test, and roll-out of zSecure Alert configuration changes.
- The ability to run CKXLOGID authorized.

The documentation updates apply to V2.4.0 zSecure Admin, zSecure Audit, and zSecure Alert. The following publications were updated:

- *zSecure CARLA-Driven Components Installation and Deployment Guide*
- *zSecure Messages Guide*
- *zSecure Admin and Audit for RACF User Reference Manual*
- *zSecure Audit for ACF2 User Reference Manual*
- *zSecure Audit for Top Secret User Reference Manual*
- *zSecure CARLa Command Reference*
- *zSecure Alert User Reference Manual*

The following product name and terminology changes were applied throughout the zSecure documentation:

- "CA Roscoe Interactive Environment" to "Advantage CA-Roscoe"
- "Tivoli NetView" to "Z NetView"
- "Whitelist" to "allowlist".

Note:

- Referenced topics that have not changed are not included in this document. You can find them in the publication that the chapter applies to.
- The *zSecure (Admin and) Audit User Reference Manuals* and the *zSecure CARLa Command Reference* are available to licensed clients only. To access the zSecure V2.4.0 licensed documentation, you must sign in to the IBM Security zSecure Suite Library with your IBM ID and password. If you do not see the licensed documentation, your IBM ID is probably not yet registered. Send a mail to zDoc@nl.ibm.com to register your IBM ID.

Installation requirement

HOLD data in SMPE

APAR OA60419 is fixed by UJ04501, which includes a pre-installation job (in cover letter and ++HOLD(ACTION)). Change this job to meet your site's installation standards and then run it prior to installation.

Migration considerations

New SCKACUST and SCKACUSV libraries

- New SCKACUST and SCKACUSV libraries are distributed as part of the PTF package.
- CKACUST and CKACUSV data sets can be created through new job SCKRSAMP(CKAZSITE) for usage by a particular user. This new construction eliminates the need for maintaining Site (or customized) CKACUST instances through the CKAZCUST job for every PTF.
- For this update (only), a Site CKACUSV data set must be created and a reference to it must be added to the zSecure configuration (C2R$PARM).
- For a new installation, Site (or customized), CKACUST and CKACUSV data sets are created by using CKRZPOST; the zSecure configuration (C2R$PARM) includes provisions for both.

Chapter 3, “Maintenance and reporting,” on page 5 was added, and has the following sections:

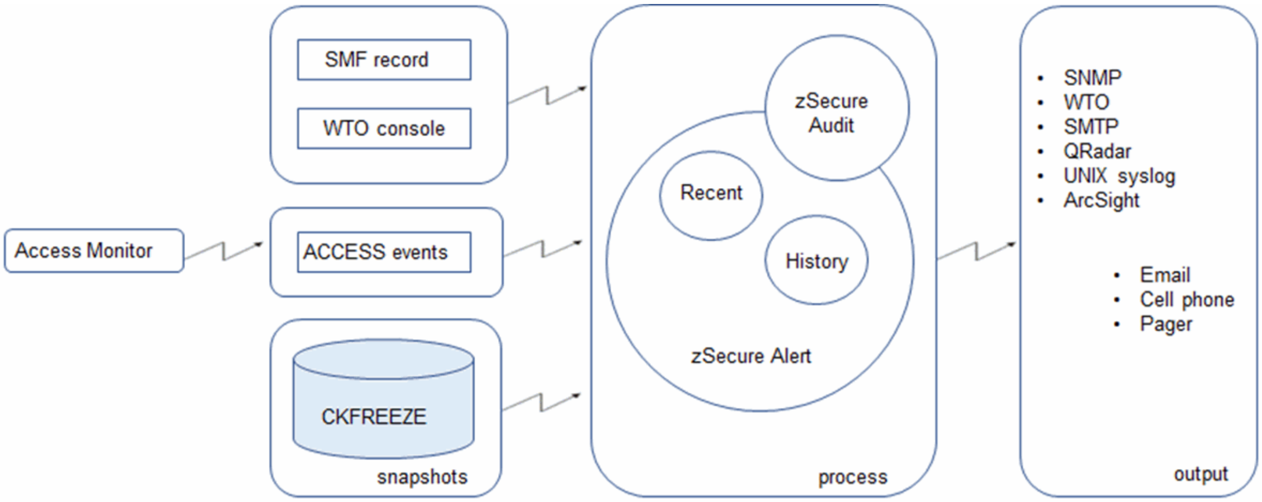
- “Subscription overview for recipients” on page 5
- “Test an alert configuration” on page 5
- “Upgrade an Alert configuration” on page 6
- “Refresh the Production set” on page 7
- “Export an Alert configuration” on page 8
- “Import an Alert configuration” on page 9
- “Compare C2PCUST data sets” on page 10
- “Select or unselect alerts or ranges of alerts” on page 12

The following sections were updated:

- “Chapter. Introduction” on page 3
- “Intervals” on page 3
- “Alert configuration: specify general settings” on page 4

Chapter. Introduction

The figure and following paragraph were updated:



Although zSecure Alert can be configured, maintained, and activated by using the ISPF interface, batch jobs are available to execute select tasks. See Chapter 3, “Maintenance and reporting,” on page 5.

"Intervals"

The following paragraphs were updated:

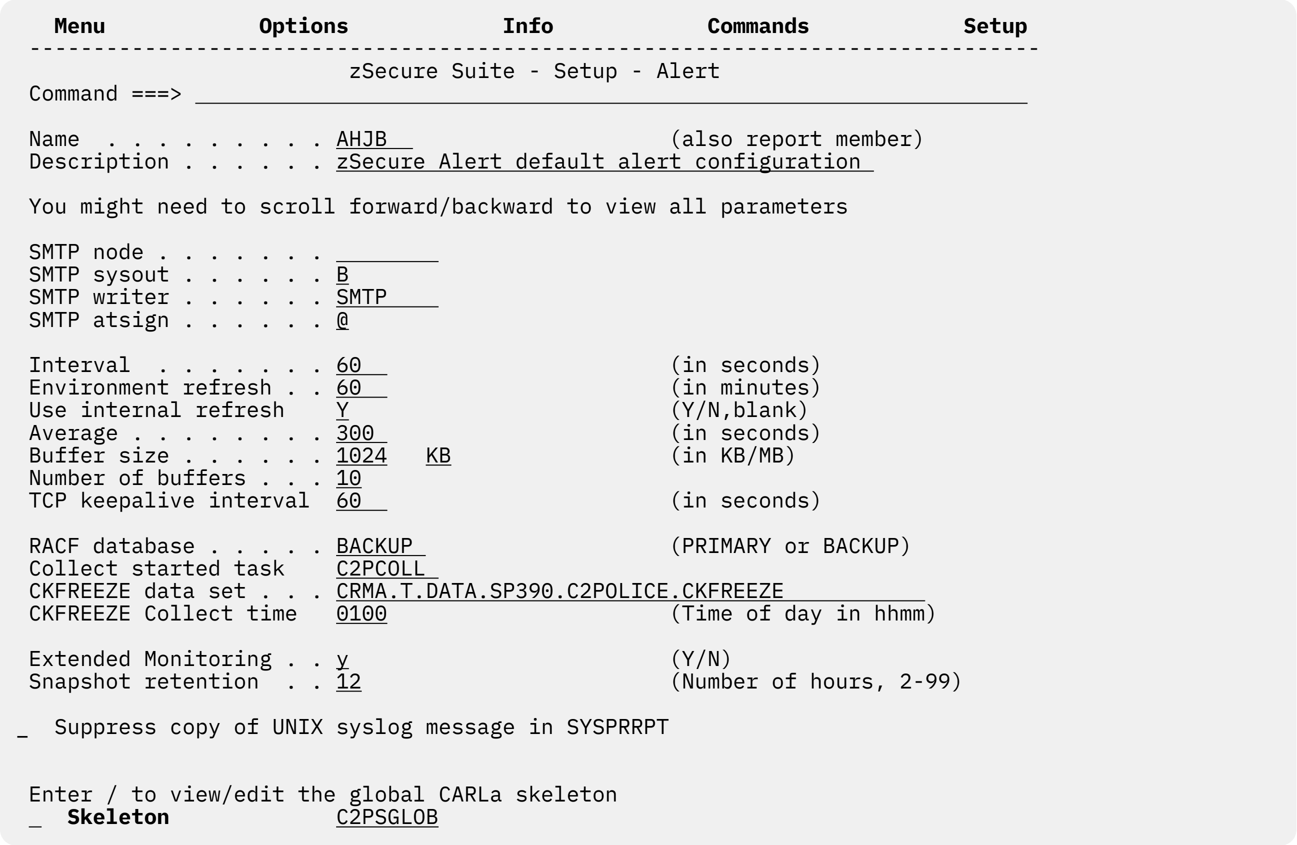
> The preprocessing subtask (also known as stage-1) obtains current information about the system environment and user attributes. This task is carried out hourly by default. If you require current information, you must process the security database and the CKFREEZE file more frequently. Processing the security database is relatively quick, but obtaining a new I/O configuration image is a costly process. zSecure Collect is typically scheduled to run once a day at a particular time to refresh the full CKFREEZE file. However, it is also possible to have zSecure Alert dispatch this task by using the operator command MODIFY C2POLICE,COLLECT. At the preprocessing interval, zSecure Alert can also create a small CKFREEZE snapshot of a subset of the system environment. This small CKFREEZE

snapshot is taken and processed only if extended monitoring is active. The small CKFREEZE is not intended for any other process.

As part of SMF processing, the CKRCARLA program retains certain SMF data to complete other SMF records that lack this data. An example of such SMF data is the user ID for SMF record type 15. By default, the refresh of the environment information involves stopping and starting the CKRCARLA subtask. As a result, the retained information is lost, and must be re-established. This often results in the fields being reported as "missing". It is possible to retain the information for a longer period through specification of the REFRESHMODE(INTERNAL) option. The necessary SMF information will be retained until the C2POLICE started task is restarted or stopped.

"Alert configuration: specify general settings"

The following panel was updated and a description was added:



```
  Menu            Options           Info            Commands          Setup
-------------------------------------------------------------------------------
                         zSecure Suite - Setup - Alert
Command ===> _________________________________________________________________

Name  . . . . . . . . . AHJB                          (also report member)
Description . . . . . . zSecure Alert default alert configuration

You might need to scroll forward/backward to view all parameters

SMTP node . . . . . . . ________
SMTP sysout . . . . . . B
SMTP writer . . . . . . SMTP
SMTP atsign . . . . . . @

Interval  . . . . . . . 60                            (in seconds)
Environment refresh . . 60                            (in minutes)
Use internal refresh    Y                             (Y/N,blank)
Average . . . . . . . . 300                           (in seconds)
Buffer size . . . . . . 1024   KB                     (in KB/MB)
Number of buffers . . . 10
TCP keepalive interval  60                            (in seconds)

RACF database . . . . . BACKUP                        (PRIMARY or BACKUP)
Collect started task    C2PCOLL
CKFREEZE data set . . . CRMA.T.DATA.SP390.C2POLICE.CKFREEZE
CKFREEZE Collect time   0100                          (Time of day in hhmm)

Extended Monitoring . . y                             (Y/N)
Snapshot retention  . . 12                            (Number of hours, 2-99)

_  Suppress copy of UNIX syslog message in SYSPRRPT


Enter / to view/edit the global CARLa skeleton
_  Skeleton             C2PSGLOB
```

Figure 1. Setup Alert panel: Copying the default Alert Configuration

Use internal refresh

Select this option to use an internal restart of CKRCARLA to refresh environment information while retaining job information. Using this option enables completion of SMF records with additional data from other SMF records for a longer period of time. If this option is not selected, completion of job data is available only if those other SMF records are written during the current environment refresh interval.

Use of this option requires additional storage to retain job information. Ensure that sufficient storage above the 2GB boundary is available; one gigabyte of storage is sufficient to retain data for approximately 8 million jobs.

Chapter 3. Maintenance and reporting

zSecure Alert can be configured, maintained, and activated by the ISPF interface, under option SE.A. However, when a zSecure Alert configuration is distributed to many LPARs, it might be more efficient to automate some functions by using batch jobs.

The batch jobs for automating some functions can be found as members in CKRJOBS and in SCKRSAMP, or as procedures in SCKRPROC. For general instructions for customizing zSecure-supplied jobs, see *zSecure Admin and Audit for RACF User Reference Manual*.

Subscription overview for recipients

Generally, recipients of alert messages do not have access to the zSecure Alert configuration option SE.A. However, many do require some kind of assurance that their IDs are not quietly removed from the Alert configuration. An overview can be sent through email to recipients of alert emails, as a reminder and possibly as a check on correct or modified settings. For this purpose, job C2PJRECI and procedure C2PCRECI are supplied.

You must copy job C2PJRECI from SCKRSAMP or CKRJOBS to a data set that your job scheduling software uses and adapt it to your needs. Specify your Alert configuration in parameter ACONF, and you can specify the CKRPARM member name with the Security zSecure Alert-enabled zSecure configuration in parameter CONFIG.

Test an alert configuration

You can generate a "Verify set" and a "Production set" of members to test your alert configuration in a batch job.

The ISPF interface option **SE.A.A** provides the V line command. It builds CARLa members that end in a V, and tests that the generated CARLa contains no syntax errors ("Verify set" of members). Similarly, the F line command copies these members to a named member, without the V, which the Alert STC uses ("Production set" of members).

You can test either of these sets in a batch job that uses procedure member C2PCTEST. The job relies on having the input data set names that are defined in your CKRPARM configuration member &CONFIG, or specified with explicit JCL SET commands after the INCLUDE MEMBER=&CONFIG. Parameter CONFIG=C2R$VOID on the procedure ensures that these overrides are not wiped out within the procedure. Use the VERIFY parameter to select the set of members: V for the "Verify set" and blank for the "Production set".

```
//JCLLIB   JCLLIB ORDER=(your.prefix.CKRPARM,
//         #thlq.SCKRPROC)
//         SET CONFIG=C2R$PARM
//         INCLUDE MEMBER=&CONFIG.
//*
//* Optionally override names from C2R$PARM
//*
//         SET C2PCUST=your.prefix.C2PCUST
//         SET ACONF=C2PDFL
//*
//         SET UNLOAD=&DPREF..&SYS..UNLOAD
//         SET CKFREEZE=&DPREF..&SYS..CKFREEZE
//         SET SMF=&DPREF..&SYS..SMF
//         SET ACCESS=NULLFILE   If there is no ACCESS data set
//         SET ACCESS=&DPREF..&SYS..DATA.C2PACMON.DYYMMDD
//*
//* Verify the CARLa scripts (ending in V)
//*
//TESTCONF EXEC C2PCTEST,CONFIG=C2R$VOID,
//         ACONF=&ACONF,VERIFY=V
```

The batch job generates alert messages to SYSOUT data sets based on records from the input data sets UNLOAD, CKFREEZE, SMF, and, optionally, ACCESS. If your installation does not use alert 1120 (or other alerts that use Access Monitor records), specify ACCESS=NULLFILE; otherwise, specify a consolidated ACCESS data set name. Currently, zSecure Alert does not support testing WTO-based alerts.

Note: This job uses an UNLOAD data set instead of the Active or Backup security database as the C2POLICE started task would. The CARLa commands that are supported on these data sets are slightly different.

Upgrade an Alert configuration

You can automate some steps that are required to update an Alert configuration.

The ISPF interface SE.A.A uses ISPF skeletons in the SCKRSLIB data set to build the CARLa programs. If these skeletons were updated by maintenance (PTFs) or changes to the installation defined alerts, the Verify (V) line command and the Refresh (F) line command must be used for each configuration that is used in every C2PCUST data set. In installations where the C2PCUST data set is distributed to each LPAR, verifying or refreshing the configurations is a laborious task.

The C2PJUPGR job was built to automate these steps. It performs the following tasks:

- Takes a single configuration from an existing C2PCUST data set.
- Rebuilds the "Verify set" of members from the skeletons.
- Runs CARLa in these members with events from the input data sets (as explained in "Test an alert configuration" on page 5).
- When there were no syntax failures in this verification, it refreshes the "Production set" with the "Verified set".

In other words, the C2PJUPGR job replaces the production members in the C2PCUST data set with the V members.

```
//JCLLIB   JCLLIB ORDER=(your.prefix.CKRPARM,
//         #thlq.SCKRPROC)
//         SET CONFIG=C2R$PARM
//         INCLUDE MEMBER=&CONFIG.
//*
//* Optionally override names from C2R$PARM
//*
//         SET C2PCUST=your.prefix.C2PCUST
//         SET ACONF=C2PDFL
//*
//         SET UNLOAD=&DPREF..&SYS..UNLOAD
//         SET CKFREEZE=&DPREF..&SYS..CKFREEZE
//         SET SMF=&DPREF..&SYS..SMF
//         SET ACCESS=NULLFILE   If there is no ACCESS data set
//         SET ACCESS=&DPREF..&SYS..DATA.C2PACMON.DYYMMDD
//*
//* Build the configuration for Verify (ending in V)
//*
//BUILD    EXEC C2PCBLD,CONFIG=C2R$VOID,ACONF=&ACONF
//*
//         IF (BUILD.C2PCBLD.RC<=8) THEN
//*
//* Verify the CARLa scripts (ending in V)
//*
//TESTCONF EXEC C2PCTEST,CONFIG=C2R$VOID,
//         ACONF=&ACONF,VERIFY=V
//*
//         IF (TESTCONF.STAGE1.RC<=8 AND TESTCONF.REPORT.RC<=8) THEN
//*
//* If successful, copy the Verified set to Production set
//*
//UPGRADE  EXEC C2PCREF,CONFIG=C2R$VOID,ACONF=&ACONF
//*
//         ENDIF
//         ENDIF
//*
//         IF (NOT UPGRADE.C2PCREF.RUN) THEN
//*
//* Something failed, start recovery actions
//*
//FAILMSG  EXEC PGM=IKJEFT1B,
// PARM='send ''Batch upgrade of alert configuration &ACONF failed'''
//SYSTSPRT  DD SYSOUT=*
```

```
//SYSTSIN   DD DUMMY
/*
//         ENDIF
//
```

The C2POLICE started task uses this new "Production set" after the operator issues an F C2POLICE,REFRESH (or RESTART, when new options were introduced), or upon completion of the environment interval (typically after 1 hour).

Specify the alert configuration name by using the ACONF symbol in the beginning of the job. When more configurations from the same C2PCUST data set are used, upgrade each configuration separately.

Extra parameters

C2PCBLD supports only a few parameters due to limitations of the JCL PARM field. Extra parameters can be passed as a full TSO command in a DD name, by modifying the call to C2PCBLD in the sample JCL like so:

```
//*
//* Build the configuration for Verify (ending in V)
//*
//BUILD    EXEC C2PCBLD,CONFIG=C2R$VOID,ACONF=&ACONF,
//         PARM.C2PCBLD=''
//C2PCBLD.SYSTSIN DD *
ISPSTART CMD(%C2PESETP BUILD SET(aconf) +
ALERT(alerts) +
PCIPARM(parmdsn) +
SENSPARM(parmdsn) +
SIMESM(simesm) +
)
//*
```

The parameter value must contain the following keywords:

SET
The member name prefix of the alert configuration, also referenced as ACONF.

ALERT
A list of alert numbers to be included in the Alert configuration. When *alerts* is omitted, the alerts that are selected though ISPF option SE.A.A are built. By specifying ALERT(ALL), all available alerts are included, even when some are not (fully) specified; this can result in syntactically incorrect alerts.

PCIPARM
The data set that contains CLASSIFY, PCIAUTH, PCIPAN, and other members that are customized through option SE.A.P. When *parmdsn* is missing, these members are expected to be included in C2PCUST.

SENSPARM
The data set that contains SENSAPFU, SENSMEMB, and other members that are customized through option SE.A.S. When *parmdsn* is missing, these members are expected to be included in C2PCUST.

SIMESM
Supports building an Alert configuration for an ACF2 system while it runs on a RACF-protected system, and the other way around. When this parameter is missing, the current security system is used.

Refresh the "Production set"

In some installations, the security operations team is not authorized to change production started tasks, even the input (configuration) members used by C2POLICE. In such a situation, the security operations team can limit themselves to selecting and modifying the Alert configuration by using SE.A.A, and verifying the result by using the V line command.

Another team (or an overnight batch job) might refresh the "Production set" by using the full C2PJUPGR job, or just the procedure C2PCREF. C2POLICE uses this new "Production set", as described in "Upgrade an Alert configuration" on page 6.

```
//JCLLIB   JCLLIB ORDER=(your.prefix.CKRPARM,
//         #thlq.SCKRPROC)
//         SET CONFIG=C2R$PARM
//         INCLUDE MEMBER=&CONFIG.
//*
//* Optionally override names from C2R$PARM
//*
//         SET C2PCUST=your.prefix.C2PCUST
//         SET ACONF=C2PDFL
//*
//* Copy the Verified set to Production set
//*
//UPGRADE  EXEC C2PCREF,CONFIG=C2R$VOID,ACONF=&ACONF
```

Export an Alert configuration

Procedure C2PCUTIL provides an EXPORT function.

The C2PCUTIL EXPORT function writes selected entries from the site alert table and the recipients table in C2PCUST to a "transport file"; this includes members from C2PCUST that those alerts need. The transport file contains as much information as is needed to copy "sets" and "installation-defined alerts" to another C2PCUST (in the same LPAR, or in another LPAR).
The C2PCUTIL IMPORT function reads the transport file and updates the destination C2PCUST data set.

The syntax of the EXPORT command is as follows:

```
EXPORT SET( set ) ALERT( alert ) MEMBER( member ) DD( dd ) WORKFILE( workfile )
       PCI SENS EXIT LIST EMPTY
```

set
Pattern or list of patterns to match the set name. Default is *.

alert
Pattern or list of patterns to match alert ID numbers. Default is *. For the selected alert ID numbers, the alert parameters and destinations are exported. For selected installation-defined alerts, the alert entry in the site alert table and the skeleton member are also exported.

member
Pattern or list of patterns for additional members that must be exported. For example, installation-defined control members, similar to SENSREAD.

dd
Output (transport) file: RECFM=FB,LRECL=80. Default is SYSUT2.

workfile
Temporary file that is required to export members: RECFM=FB,LRECL=80. Default is SYSWORK. C2PCUTIL JCL provides a SYSWORK DD statement.

PCI
Requests export of the PCI/DSS related control members in C2PCUST, as managed in SE.A.P.

SENS
Requests export of the SENSITIVE RESOURCE-related control members in C2PCUST, as managed in SE.A.S.

EXIT
Requests export of the C2PX members in C2PCUST.

LIST
Exports the email list definition as defined in SE.A.E, but not the actual email data sets.

EMPTY

Generates output lines for all ISPF dialog variables in the entries, even when uninitialized. By default, only initialized fields are copied.

A "pattern" in the SET, ALERT, and MEMBER keywords consists of a fixed part that is followed by an asterisk. Patterns and member names can be mixed in the "list of patterns". For example:

```
*
PROD SYS*
1* 2* 51* 52*
```

The following JCL can be used to print the contents of the transport data set (with output dd SYSUT2), or to create a transport data set in SYSUT3. The transport data set must be copied to the destination system and processed with the IMPORT function.

```
// SET  C2PCUST=C2POLICE.C2PCUST
//*
// EXEC C2PCUTIL,CONFIG=C2R$VOID
//SYSTSIN DD *
ISPSTART CMD(%C2PESETP EXPORT set(t*) alert(4*) +
pci dd(sysut3) +
)
//SYSUT2 DD SYSOUT=*
//SYSUT3  DD DISP=(NEW,CATLG),DSN=MYID.C2POLICE.EXPORT,
// UNIT=SYSDA,SPACE=(TRK,(10,10)),LRECL=80,RECFM=FB,DSORG=PS
```

Figure 2. Sample JCL to export sets that start with T, and from these (only) the RACF-specific installation-defined alerts, and the PCI-DSS control members.

Import an Alert configuration

Procedure C2PCUTIL provides an IMPORT function.

The C2PCUTIL IMPORT function reads selected entries from a previously constructed transport data set and updates an existing C2PCUST data set. If C2PCUST is empty, the necessary ISPF tables are created. If the existing ISPF tables were maintained by an older zSecure version, the tables are first upgraded.

Entries in the import data set are compared with entries in C2PCUST and flagged as either new or `existing`, depending on matching names. Existing entries are compared, resulting in an `identical` or `different` status. SYSTSPRT lists the status is for entries in the transport data set.

The syntax of the IMPORT command is as follows:

```
IMPORT SET( set ) ALERT( alert ) MEMBER( member ) DD( dd ) WORKFILE( workfile )
   ADD( add ) REPLACE( replace ) COMPARE( compare )
```

set

Pattern or list of patterns to match the set name. Default is *. Sets are added or replaced in C2PCUST under control of the ADD and REPLACE options.

alert

Pattern or list of patterns to match alert ID numbers. Default is *. For the selected alert ID numbers, the alert parameters and destinations are imported. For selected installation-defined alerts, the alert entry in the site alert table and the skeleton member are also imported (under control of the ADD and REPLACE options).

member

Pattern or list of patterns for additional members that must be imported. For example, installation-defined control members, similar to SENSREAD.

dd

Input file: RECFM=FB,LRECL=80. Default is SYSUT2.

workfile

Temporary file that is required to copy members: RECFM=FB,LRECL=80. Default is SYSWORK. C2PCUTIL JCL provides a SYSWORK DD statement.

add

Selects the entry types to be added, when no matching entry is found in C2PCUST. By default, no entries are added. Possible values:

SET

Alert sets and set parameters are imported, as entered with the E line command in the initial display from SE.A.A. In addition, the set parameters include the `Selected` versus `Not selected` state of all alerts.

ALERT

Custom alert entries and parameters are copied, as well as alert parameters for (IBM) standard alerts as modified by using the E line command on the alert selection lists. New alerts are not`Selected`, unless alert sets are also copied; manual selection of alerts is required.

DEST

Alert destinations for selected sets and selected alert IDs are copied, as entered with the W line command. By selecting SET and/or ALERT and omitting DEST, alerts are copied without recipient information.

LIST

Specifications of the email destination lists are copied, without affecting reference to these lists IDs.

MEMBER

Members that are included in the transport data set are copied, possibly under control of MEMBER(*member*) selection. This includes alert skeletons, PCI, and SENS value lists and other members that are selected with the EXPORT command.

replace

Selects the entry types that are to be replaced in C2PCUST. Values are SET, ALERT, DEST, LIST, MEMBER, or * (see "add" on page 10). By default, no entries are overwritten.

compare

Requests additional, line by line comparison of entries. Values are SET, ALERT, DEST, LIST, or * (see "add" on page 10). By default, no details are printed.

See "Export an Alert configuration" on page 8 for valid patterns.

The following JCL adds or replaces all sets, alerts, alert parameters, and destinations and corresponding members from the transport data set.

```
// SET  C2PCUST=C2POLICE.C2PCUST.NEW
//*
// EXEC C2PCUTIL,CONFIG=C2R$VOID
//SYSTSIN DD *
ISPSTART CMD(%C2PESETP IMPORT SET(*) alert(*) +
add(*) replace(*) +
dd(sysut1) +
)
//SYSUT1  DD DISP=OLD,DSN=MYID.C2POLICE.EXPORT
```

Figure 3. Sample JCL to import all entries from a transport data set.

Note: After the IMPORT function, before using the V line command to build the alert members, use SE.A.A to inspect the alert set and newly imported alerts that are selected in their respective sets.

Compare C2PCUST data sets

The C2PCUTIL EXPORT function followed by an IMPORT to another C2PCUST data set can be used as a rudimentary compare utility. SYSTSPRT lists the entry names in the transport data set, and the status of entries with the same name in C2PCUST. The COMPARE keyword can be used to list fields in the table entries with differences, showing the 8-byte field name and the first 32 bytes of the values. By default, only the entry key is shown. Differences in members are not illustrated.

The following job first exports all configurations and all alerts from C2POLICE.C2PCUST.OLD, including related skeletons and PCI-DSS control members. The second step compares these entries with the corresponding entries in C2POLICE.C2PCUST.NEW, prints the status of each entry, and shows non-identical values of the table entries. Identical entry values are suppressed.

```
// SET  C2PCUST=C2POLICE.C2PCUST.OLD
//*
// EXEC C2PCUTIL,CONFIG=C2R$VOID
//SYSTSIN DD *
ISPSTART CMD(%C2PESETP EXPORT set(*) alert(*) +
pci dd(sysut3) workfile(syswork) +
)
//SYSUT3  DD DISP=(,PASS),UNIT=SYSDA,LRECL=80,RECFM=FB,DSORG=PS,DSN=&&A
//SYSWORK DD DISP=(,PASS),UNIT=SYSDA,LRECL=80,RECFM=FB,DSORG=PS,DSN=&&B
//*
// SET  C2PCUST=C2POLICE.C2PCUST.NEW
//*
// EXEC C2PCUTIL,CONFIG=C2R$VOID
//SYSTSIN DD *
ISPSTART CMD(%C2PESETP IMPORT set(*) alert(*) +
compare(*) +
dd(sysut3) workfile(syswork) +
)
//SYSUT3  DD DISP=OLD,UNIT=SYSDA,LRECL=80,RECFM=FB,DSORG=PS,DSN=&&A
//SYSWORK DD DISP=OLD,UNIT=SYSDA,LRECL=80,RECFM=FB,DSORG=PS,DSN=&&B
```

Figure 4. Sample JCL to compare entries in C2POLICE.C2PCUST.OLD with the corresponding entries in C2POLICE.C2PCUST.NEW

The following figure shows sample compare output:

```
ISPSTART CMD(%C2PESETP IMPORT SET(*) alert(*) compare(*) dd(sysut3) workfile(syswork))
zSecure Alert batch interface
Input parms IMPORT SET(*) ALERT(*) COMPARE(*) DD(SYSUT3) WORKFILE(SYSWORK)
Import alert configuration to C2POLICE.C2PCUST.NEW from SYSUT3.
Identical Configuration C2PDFL
Different Configuration ACF2
Field    C2POLICE.C2PCUST.NEW             Import
C2PESELR 2212 2213 2214 2301              2102 2104 2105 2106 2111 2112 21
C2PEMON  N                                Y

Different Configuration TEST
Field    C2POLICE.C2PCUST.NEW             Import
C2PEINTV i:60;t:300;b:1024;n:10;c:0100;s: i:60;t:301;b:1024;n:10;c:0100;s:
C2PESELR 1207 1208 1212 1213 1503 1504    1101 1102 1122 1214 1602 4042
C2PENPAR LOCAL;C;SMTP;;@;                 LOCAL;B;XMTP;F;¢;
C2PESELA                                  1111 1122

Unmatched Configuration NEW
Unmatched Custom Alert 4301
Unmatched Custom Alert 4801
Unmatched Custom Alert 4002
Unmatched Mailing List DESTIES
Different Destination ACF2
Field    C2POLICE.C2PCUST.NEW             Import
C2PESDSN WF;                              SF;
C2PESNMP                                  127.0.0.1
C2PESLUX                                  127.0.0.1
C2PECEFU                                  127.0.0.1
C2PEFROM &jobname at &system <mbox@domain &jobname at &system <mboy@domain
C2PEMATO                                  mboy@domain.old
C2PECELT                                  a@phone.com
C2PECELF &jobname at &system <mbox@domain &jobname at &system <mbox@domain
```

Figure 5. Sample compare output

```
Identical Destination C2PDFL
Different Destination TEST
Field    C2POLICE.C2PCUST.NEW             Import
C2PESDSN W;                               EF;CF;SF;WF;U;A;
C2PESNMP                                  127.0.0.1
C2PESLUX                                  127.0.0.1
C2PECEFU                                  127.0.0.1
C2PEFROM &jobname at &system <mbox@domain &jobname at &system <mbox1¢domai
C2PEMATO                                  user11¢domain.null
C2PECELT                                  0¢domain.null
C2PECELF &jobname at &system <mbox@domain &jobname at &system <mbox1¢domai
C2PECELR                                  9¢domain.null

Unmatched Destination NEW
Unmatched Alert Parms TEST
Unmatched Alert Parms TEST 1101
Unmatched Alert Parms NEW 1806
Unmatched Alert Parms NEW 1805
Unmatched Alert Parms NEW 1804
Unmatched Alert Parms NEW 1304
Unmatched Alert Parms NEW 1701
Unmatched Alert Parms NEW 1122
Unmatched Alert Parms NEW 1120
Unmatched Alert Parms NEW 1102
Unmatched Alert Parms NEW 1115
Unmatched Alert Parms TEST 1806
Unmatched Alert Parms TEST 1805
Unmatched Alert Parms TEST 1804
Unmatched Alert Parms TEST 1304
Unmatched Alert Parms TEST 1701
Unmatched Alert Parms TEST 1122
Unmatched Alert Parms TEST 1120
Unmatched Alert Parms TEST 1115
Identical Alert Parms TEST 1102
Unmatched Alert Parms ACF2 2806
Unmatched Alert Parms ACF2 2805
Unmatched Alert Parms ACF2 2804
Unmatched Alert Parms ACF2 2120
Unmatched Alert Parms ACF2 2115
Unmatched Alert Parms ACF2 2102
Skip identical Member CLASSIFY
Skip identical Member PCIAUTH
Skip identical Member PCIPAN
Skip identical Member PCIPANCL
Skip different Member PC2AUTH
Skip different Member PC2PAN
Skip identical Member PC2PANCL
Skip new Member PGMS4301
Skip new Member ROBS4002
Skip new Member SMFS4801

Import summary
No table entries changed
No members changed
Batch utility complete, return code 0
```

Figure 6. Sample compare output (continued)

Select or unselect alerts or ranges of alerts

Procedure C2PCUTIL provides mutually exclusive SELECT and UNSELECT functions.

The C2PCUTIL EDIT command provides a SELECT option to activate one or more alerts in one or more sets, and an UNSELECT option to deactivate alerts. The SELECT and UNSELECT options are mutually exclusive.

When you have modified the list of selected alerts, the set must be (V) verified and (R) refreshed before the alerts are changed.

The syntax of the EDIT command is as follows:

```
EDIT SET( set ) ALERT( alert ) {SELECT|UNSELECT}
```

set
Pattern or list of patterns to match the set name. Default is *.

alert

Pattern or list of patterns to match alert ID numbers. Default is *.

SELECT

Adds the matching alert IDs to the list of selected IDs, in the selected alert sets.

UNSELECT

Removes the matching IDs from the selected alert sets.

See “Export an Alert configuration” on page 8 for valid patterns.

The following JCL unselects all User category alerts and next selects three of the alerts.

```
// SET  C2PCUST=C2POLICE.C2PCUST.NEW
//*
// EXEC C2PCUTIL,CONFIG=C2R$VOID
//SYSTSIN DD *
ISPSTART CMD(%C2PESETP EDIT SET(C2PDFL) ALERT(11*) UNSELECT)
ISPSTART CMD(%C2PESETP EDIT SET(C2PDFL) ALERT(1120 1121 1122) SELECT)
//
```

Figure 7. Sample JCL to manage alert selections.