CA Chorus™ Software Manager

Administration Guide

Version 06.0.00, Seventh Edition

This Documentation, which includes embedded help systems and electronically distributed materials (hereinafter referred to as the “Documentation”), is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Chorus™ Software Manager (CA CSM)
- CA ACF2™ for z/OS
- CA Allocate™ DASD Space and Placement (CA Allocate)
- CA Auditor for z/OS
- CA Chorus™
- CA Common Services for z/OS
- CA Database Management Solutions for DB2 for z/OS
- CA Datacom®/DB
- CA Datacom/MSM
- CA Disk Backup and Restore (CA Disk)
- CA Distributed Security Integration for z/OS (CA DSI Server)
- CA Easytrieve® Simplified Design System (CA Easytrieve)
- CA Panvalet® (CA Panvalet)
- CA PDSMAN® PDS Library Management (PDSMAN)
- CA SMF Director
- CA SYSVIEW
- CA Top Secret® for z/OS
- CA View®

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.

Documentation Changes

7th Edition (March 2015)

The following documentation updates have been made after the last release of this documentation:

- Maintaining CA CSM > Maintenance > Apply Maintenance to CA CSM (see page 59): updated step 1b to clarify the instruction and the menu option to select

6th Edition (February 2015)

The following documentation updates have been made after the last release of this documentation:

- CA CSM Implementation and Status > Implementation Checklist > Security Administrator (see page 102): added a required READ permission to BPX.CAHFS.CHANGE.FILE.TIME

5th Edition (November 2014)

The following documentation updates have been made after the last release of this documentation:

- Configuring CA CSM > Configure CA CSM to Use HTTPS > Enable HTTPS with Certificates Stored in USS Files (see page 46): updated the code sample in step 2b with the sslEnabledProtocols keyword
- Configuring CA CSM > Configure CA CSM to Use HTTPS > Enable HTTPS with Certificates Stored in an External Security Manager (see page 47): updated the code sample in step 2c with the sslEnabledProtocols keyword

4th Edition (October 2014)

The following documentation updates have been made after the last release of this documentation:

- Configuring CA CSM > Setting Up CA CSM User ID Without UID(0) > Set Up CA CSM User ID Without UID(0) for CA Top Secret for z/OS (see page 28): updated step 2
- Configuring CA CSM > Setting Up CA CSM User ID Without UID(0) > Set Up CA CSM User ID Without UID(0) for CA ACF2 for z/OS (see page 29): updated step 2
- Configuring CA CSM > Setting Up CA CSM User ID Without UID(0) > Set Up CA CSM User ID Without UID(0) for IBM RACF (see page 30): updated step 2

- Configuring CA CSM > Configure CA CSM to Use HTTPS > Allow CA CSM to Connect Through HTTPS in a Secured Environment (see page 50): added information about the length limit
- CA CSM Implementation and Status > Implementation Checklist > Security Administrator (see page 102): added permissions for the data sets that are referenced in particular option file keywords; added BPX.DAEMON to the list of FACILITY class profiles

3rd Edition (August 2014)

The following documentation updates have been made after the last release of this documentation:

- Configuring CA CSM > Configure CA CSM to Use HTTPS > Allow CA CSM to Connect Through HTTPS in a Secured Environment (see page 50): added the topic
- Troubleshooting: moved the section to the *Troubleshooting Guide*

2nd Edition (May 2014)

The following documentation updates have been made after the last release of this documentation:

- Troubleshooting > Product Installation in an Existing SMP/E Environment Fails: added the topic

1st Edition (April 2014)

The following documentation updates have been made after the last release of this documentation:

- Introduction (see page 13): restructured the chapter, removed out-of-date information, moved the Overview topic to the *Release Notes*
- Preparing for Installation: removed the chapter, moved information to the *Installation Guide* and *Site Preparation Guide*
- Installing and Setting Up CA CSM: removed the chapter, moved information to the *Installation Guide* and *Site Preparation Guide*
- Post-Installation Tasks: removed the chapter, moved information to the *Installation Guide* and *Site Preparation Guide*
- Setting Up CA CSM (see page 23): added a new chapter that inherits existing topics from the removed sections
- Configuring CA CSM (see page 27): added a new chapter that inherits existing topics from the removed sections
- Configuring CA CSM > Setting Up CA CSM User ID Without UID(0) (see page 27): added information about message EDC5129I to the topics related to different security systems

- Configuring CA CSM > Run CA CSM on Another LPAR (see page 32): added a new topic
- Configuring CA CSM > Configuring FTP and HTTP Connections > Configuring FTP Connections for a New Installation > Configuring HTTP Proxy Settings (see page 45, see page 44): restructured the section, splitting into several topics
- Configuring CA CSM > Configure CA CSM to Use HTTPS (see page 45): restructured the sections, added new topics on enabling HTTPS with certificates stored in an external security manager, and configuring CA CSM to override HTTP
- Configuring CA CSM > Enable IEC988I Message in MUF Startup: removed the topic as out-of-date
- Configuring CA CSM > Set Up a Secure FTP Connection for Deployment (see page 53): added a new topic
- Maintaining CA CSM (see page 57): added a new chapter that inherits existing topics from the removed sections
- Maintaining CA CSM > Stop CA CSM (see page 66): updated step 2 with information about commands for z/OS, CA SYSVIEW, and SDSF
- Database Administration: removed the chapter, moved information to the scenario *Administering the CA CSM Database*
- SCS Address Space Administration (see page 73): restructured and streamlined the chapter
- CA CSM Implementation and Status > Implementation Checklist > Security Administrator (see page 102): updated data sets for IBM RACF program control; added information about access in case of using CA SAF HFS security
- CAMSM> Implementation and Status > Implementation Checklist > Options File Keywords: removed the section, moved the content to the *Installation Guide*
- CA CSM Implementation and Status > CA CSM Software Deployment Spawn Procedure Entities (see page 106): updated the example for SMPJHOME
- CA CSM Implementation and Status > Security for CA CSM Functions > Resource Profiles (see page 116): added the SYSREG.@PROFILE.UPDATE.*systemname* profile
- CA CSM Implementation and Status > DBINIT and DBUPDATE Settings (see page 122): updated the description of PASAdvancedSettingsMember not to include HTTP
- External Interfaces (see page 143) > added a new appendix, previously found in the User Guide
- Troubleshooting > Microsoft Internet Explorer 8 Running Slowly: added a new topic
- Troubleshooting > SMP/E Environment Does Not Appear on the Tree: added a new topic

Contents

Appendix A: CA CSM Implementation and Status 101

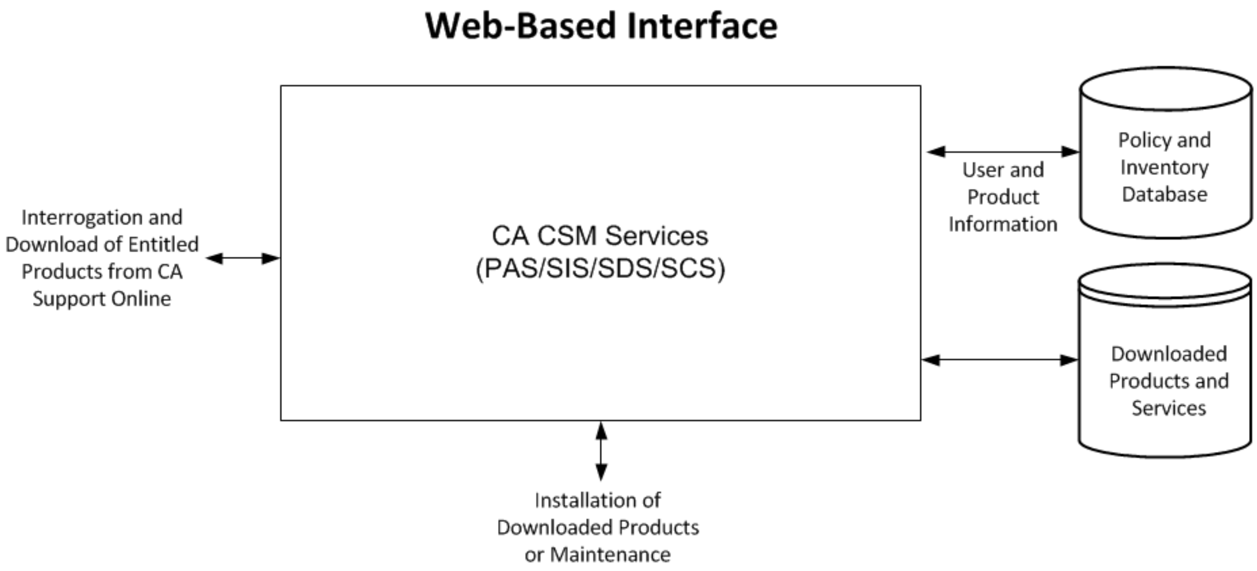
Chapter 1: Introduction

This section contains the following topics:

How CA CSM Works

CA CSM is a program that runs in the address space of an application server environment hosted on a z/OS system. Typically, this system is where you use SMP/E to install and maintain your products. The system is known as the SMP/E driving system. The CA CSM web-based interface enables you to perform SMP/E processing dynamically without having to code and submit the batch jobs manually.

The following illustration shows the main components and data flows:


Web-Based Interface
CA CSM Services
(PAS/SIS/SDS/SCS)
User and Product Information
Policy and Inventory Database
Downloaded Products and Services
Interrogation and Download of Entitled Products from CA Support Online
Installation of Downloaded Products or Maintenance

CA CSM has the following main components:

CA CSM Services

Provides the following services:

Product Acquisition Service (PAS)

Facilitates the acquisition of CA Technologies mainframe products and the service for those products, such as program temporary fixes (PTFs). The service retrieves information about the products to which your site is entitled and records these entitlements in a software inventory. The inventory is maintained on your driving system. The service can also download the LMP keys (licenses) for those products. The web-based interface enables you to browse the software inventory for available software and fixes, and makes them available within the driving system.

Software Installation Service (SIS)

Facilitates the installation and maintenance of CA Technologies mainframe products in the software inventory of the driving system. The web-based interface enables you to browse and manage the software inventory, and automate installation tasks. You can browse downloaded software packages, and can browse and manage SMP/E environments on the driving system.

Software Deployment Service (SDS)

Facilitates the deployment of CA Technologies mainframe products from the software inventory of the driving system. This service enables you to deploy installed products that are policy-driven with a set of appropriate transport mechanisms across a known topology. The enterprise system topology can include shared DASD environments, networked environments, and z/OS systems. Policies represent a combination of metadata input and user-supplied input. Metadata input identifies the component parts of a product. User-supplied input identifies the deployment criteria, such as where it goes and what it is named.

Software Configuration Service (SCS)

Facilitates the mainframe products configuration from the software inventory of the driving system to the targeted z/OS mainframe operating system. SCS guides you through the configuration creation process, and through the manual steps to implement the configuration. In addition, SCS includes an address space communications service running on each targeted z/OS system.

Database

Stores information for use by CA CSM.

Policy

Stores site and user information for downloading and processing CA Technologies mainframe products.

Inventory

Stores information about the CA Technologies mainframe products to which you are entitled.

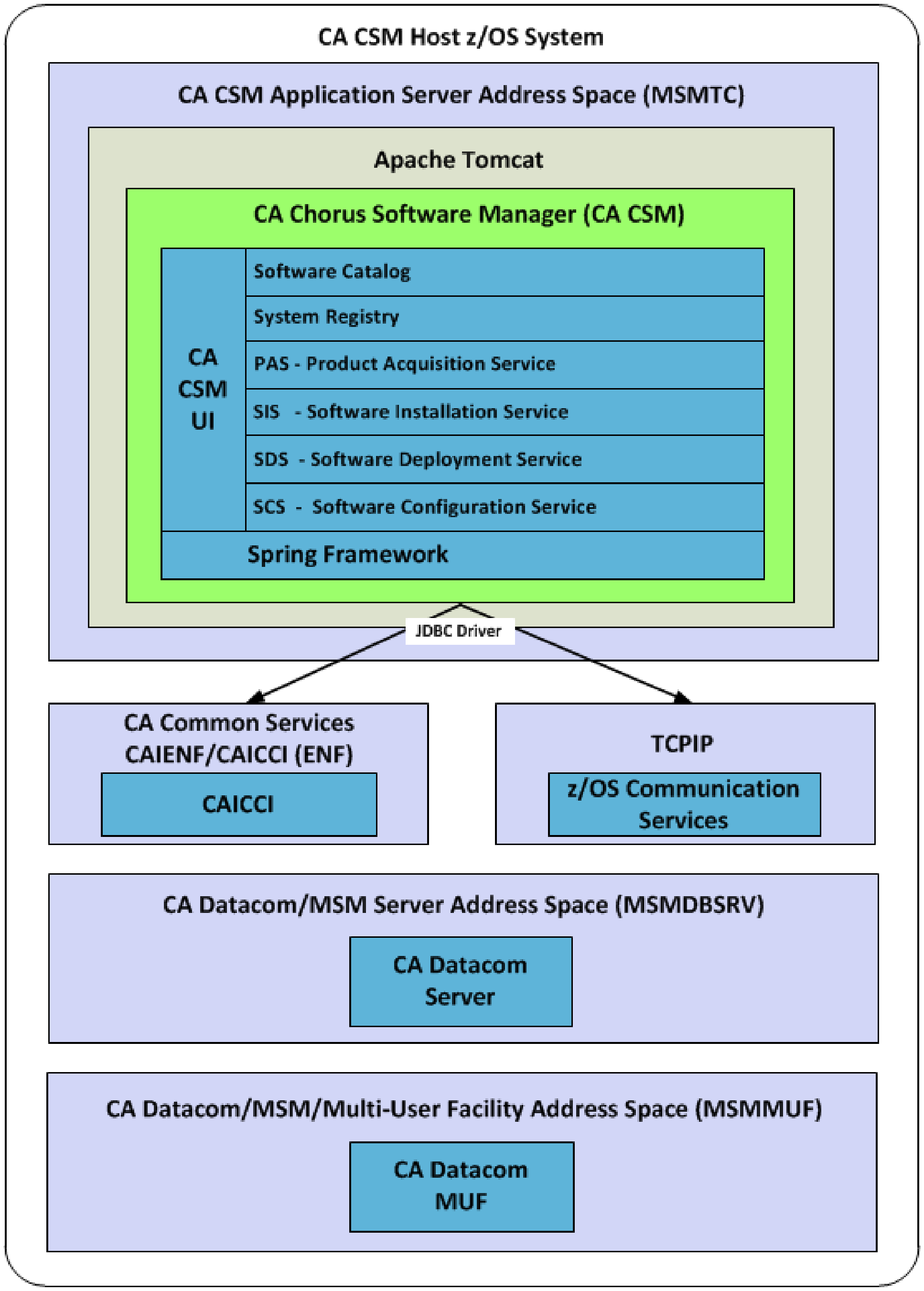
The web-based Interface

Enables you to acquire, install, maintain, deploy, and configure your CA Technologies mainframe products from the CA CSM catalog, and manage your SMP/E environments. The web-based interface includes online help that provides information about how to use CA CSM.

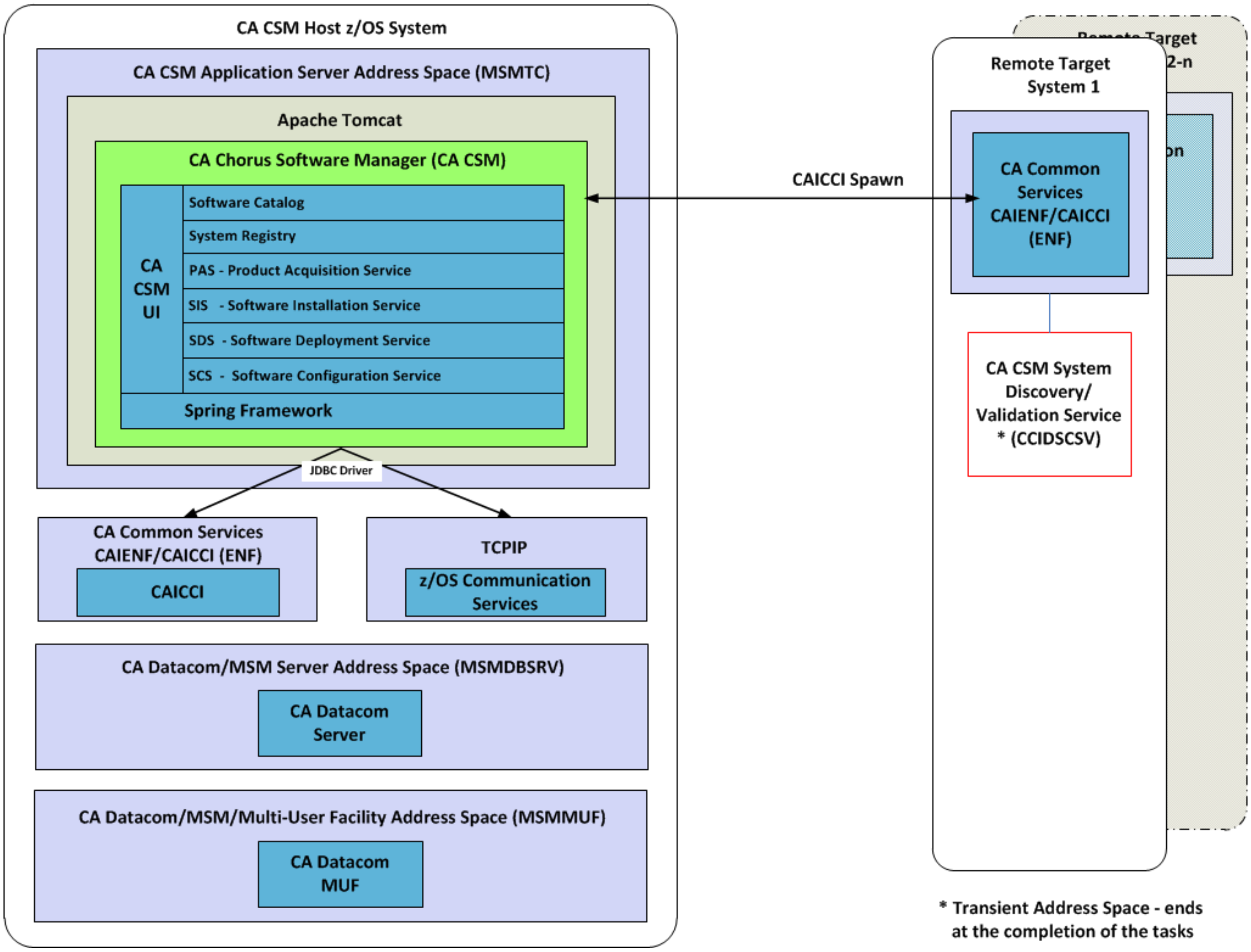
CA CSM Operational Architecture Diagrams

The following diagrams show configurations of CA CSM with CA Common Services for z/OS on remote and local systems.

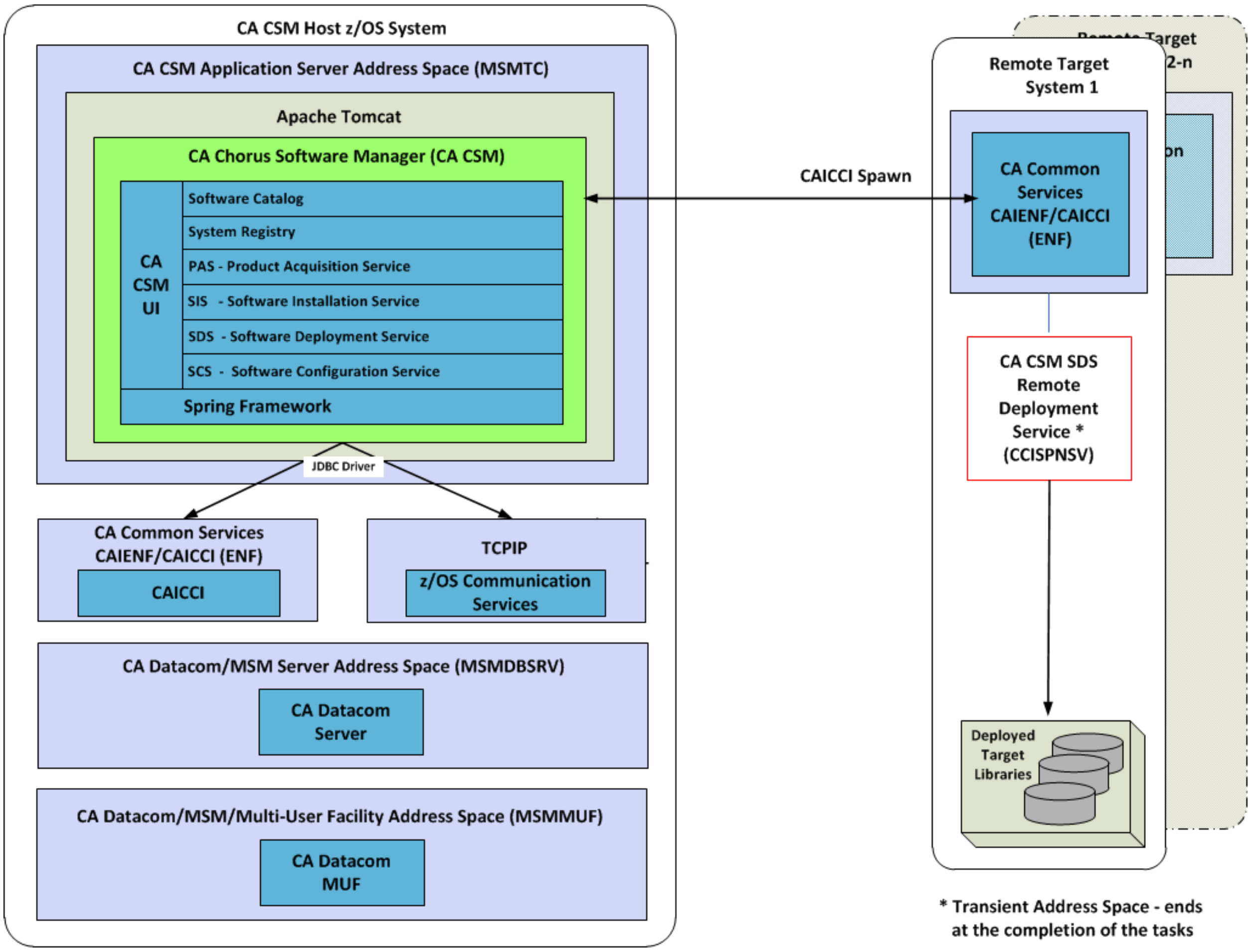
CA CSM on z/OS Host System


CA CSM Host z/OS System
CA CSM Application Server Address Space (MSMTC)
Apache Tomcat
CA Chorus Software Manager (CA CSM)
CA CSM UI
Software Catalog
System Registry
PAS - Product Acquisition Service
SIS - Software Installation Service
SDS - Software Deployment Service
SCS - Software Configuration Service
Spring Framework
JDBC Driver
CA Common Services CAIENF/CAICCI (ENF)
CAICCI
TCPIP
z/OS Communication Services
CA Datacom/MSM Server Address Space (MSMDBSRV)
CA Datacom Server
CA Datacom/MSM/Multi-User Facility Address Space (MSMMUF)
CA Datacom MUF

CA CSM on z/OS Host System with System Discovery/Validation Service on Remote Target System

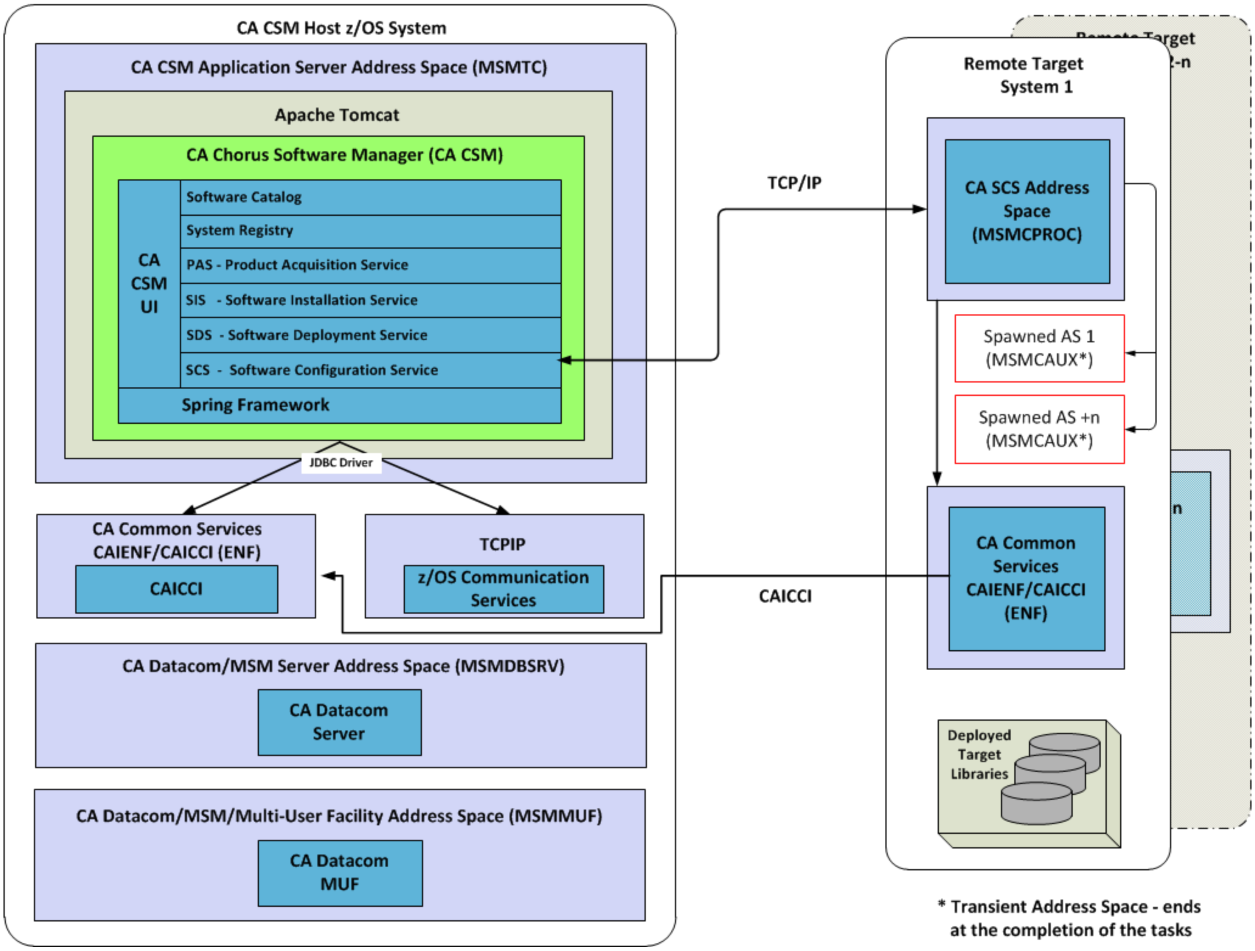

CA CSM Host z/OS System
CA CSM Application Server Address Space (MSMTC)
Apache Tomcat
CA Chorus Software Manager (CA CSM)
CA CSM UI
Software Catalog
System Registry
PAS - Product Acquisition Service
SIS - Software Installation Service
SDS - Software Deployment Service
SCS - Software Configuration Service
Spring Framework
JDBC Driver
CA Common Services CAIENF/CAICCI (ENF)
CAICCI
TCPIP
z/OS Communication Services
CA Datacom/MSM Server Address Space (MSMDBSRV)
CA Datacom Server
CA Datacom/MSM/Multi-User Facility Address Space (MSMMUF)
CA Datacom MUF
CAICCI Spawn
Remote Target 2-n
Remote Target System 1
CA Common Services CAIENF/CAICCI (ENF)
CA CSM System Discovery/ Validation Service * (CCIDSCSV)
* Transient Address Space - ends at the completion of the tasks

CA CSM on z/OS Host System with SDS Remote Deployment Service on Remote Target System

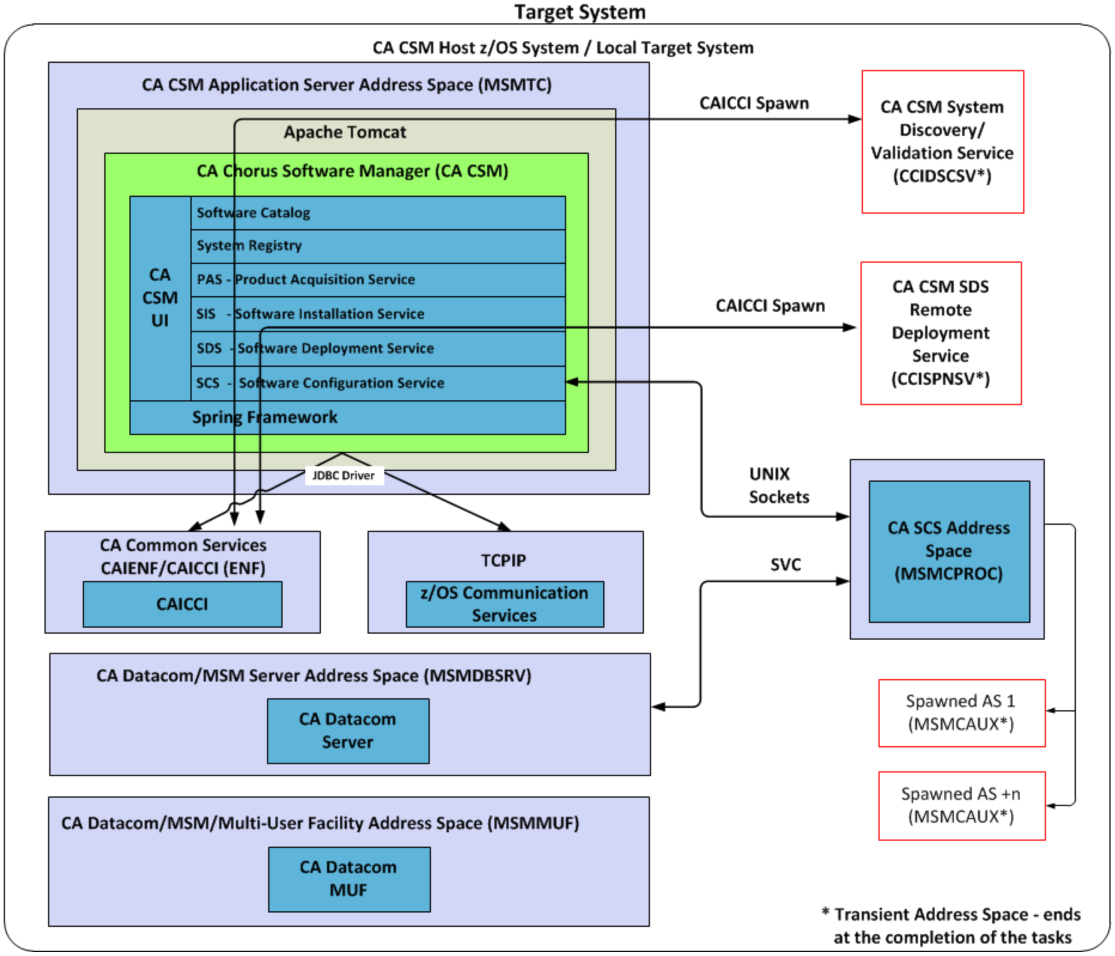

CA CSM Host z/OS System
CA CSM Application Server Address Space (MSMTC)
Apache Tomcat
CA Chorus Software Manager (CA CSM)
CA CSM UI
Software Catalog
System Registry
PAS - Product Acquisition Service
SIS - Software Installation Service
SDS - Software Deployment Service
SCS - Software Configuration Service
Spring Framework
JDBC Driver
CA Common Services CAIENF/CAICCI (ENF)
CAICCI
TCPIP
z/OS Communication Services
CA Datacom/MSM Server Address Space (MSMDBSRV)
CA Datacom Server
CA Datacom/MSM/Multi-User Facility Address Space (MSMMUF)
CA Datacom MUF
CAICCI Spawn
Remote Target System 2-n
on
Remote Target System 1
CA Common Services CAIENF/CAICCI (ENF)
CA CSM SDS Remote Deployment Service * (CCISPNSV)
Deployed Target Libraries

* Transient Address Space - ends at the completion of the tasks

CA CSM on z/OS Host System with SCS Address Space on Remote Target System


CA CSM Host z/OS System
CA CSM Application Server Address Space (MSMTC)
Apache Tomcat
CA Chorus Software Manager (CA CSM)
CA CSM UI
Software Catalog
System Registry
PAS - Product Acquisition Service
SIS - Software Installation Service
SDS - Software Deployment Service
SCS - Software Configuration Service
Spring Framework
JDBC Driver
CA Common Services CAIENF/CAICCI (ENF)
CAICCI
TCPIP
z/OS Communication Services
CA Datacom/MSM Server Address Space (MSMDBSRV)
CA Datacom Server
CA Datacom/MSM/Multi-User Facility Address Space (MSMMUF)
CA Datacom MUF
TCP/IP
CAICCI
Remote Target System 1
Remote Target
-n
CA SCS Address Space (MSMCPROC)
Spawned AS 1 (MSMCAUX*)
Spawned AS +n (MSMCAUX*)
CA Common Services CAIENF/CAICCI (ENF)
n
Deployed Target Libraries
* Transient Address Space - ends at the completion of the tasks

CA CSM on z/OS Host System with System Registry Validation Service + SDS Remote Deployment Service + SCS Address Space on Local Target System


CA CSM Host z/OS System / Local Target System
CA CSM Application Server Address Space (MSMTC)
Apache Tomcat
CA Chorus Software Manager (CA CSM)
CA CSM UI
Software Catalog
System Registry
PAS - Product Acquisition Service
SIS - Software Installation Service
SDS - Software Deployment Service
SCS - Software Configuration Service
Spring Framework
JDBC Driver
CAICCI Spawn
CA CSM System Discovery/ Validation Service (CCIDSCSV*)
CAICCI Spawn
CA CSM SDS Remote Deployment Service (CCISPNSV*)
UNIX Sockets
CA SCS Address Space (MSMCPROC)
SVC
CA Common Services CAIENF/CAICCI (ENF)
CAICCI
TCPIP
z/OS Communication Services
CA Datacom/MSM Server Address Space (MSMDBSRV)
CA Datacom Server
Spawned AS 1 (MSMCAUX*)
Spawned AS +n (MSMCAUX*)
CA Datacom/MSM/Multi-User Facility Address Space (MSMMUF)
CA Datacom MUF
* Transient Address Space - ends at the completion of the tasks

Network Flows

CA CSM uses the following process to connect you directly to the appropriate CA Technologies website, where they can manage your CA Technologies software:

1. You connect to CA CSM from within your corporate Intranet (locally connected or tunneled in through VPN) using the HTTP protocol such as http://*yourmainframe*:*yourport*/MSM).
   - Your systems programmers initiate all actions.
   - No port is exposed to the Internet.
   - No communication is initiated from outside your Intranet.

2. The CA CSM Product Acquisition Service communicates with CA Technologies using the same methods that you previously used when manually accessing the website, as follows:

   HTTPS

   Passes the credentials to, and obtains product information from the appropriate CA Technologies website.

   FTP

   Downloads software packages from CA FTP Services to your mainframe system using an anonymous FTP, with no credentials passed. CA CSM accesses one of the following locations:

   - ftp://scftpd.ca.com
   - ftp://ftp.ca.com
   - ftp://supportftp.ca.com

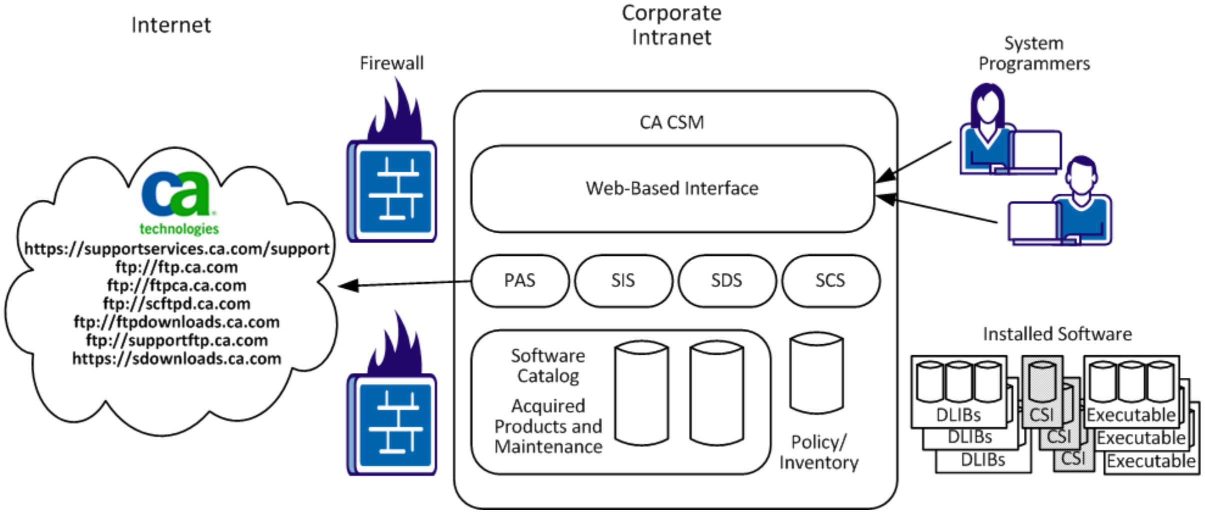
Note: The following information is the only unencrypted data sent to and from CA Technologies:

- Your email address for anonymous FTP (no password)
- The CA Technologies product information, either base install packages or solutions.

None of this data is part of any privacy or encryption standards.

This process is depicted in the following illustration:

CA CSM Network Flows



Chapter 2: Setting Up CA CSM

This section contains the following topics:

Security Setup for Users

This section contains the following topics:

Set Up USS Authorization for Users

CA CSM users require access to USS. Each user must have an OMVS segment. Your security administrator must set up these segments.

Follow these steps:

1. Select an OMVS UID number to associate with each user ID. Your security administrator can have a policy for assigning OMVS UID numbers. If not, use a unique number.

   Note: For more information about OMVS UID numbers, see the *IBM UNIX System Services Planning*.

2. Define the OMVS segment for the user. For a user ID *uuuuuuu*, UID number *nnn*, and home directory *path_name*, enter the following commands:

   - For CA ACF2 for z/OS systems, enter the following commands:

     ```
     SET PROFILE(USER) DIV(OMVS)
     INSERT uuuuuuu UID(nnn) HOME(path_name) OMVSPGM(/bin/sh)
     ```

   - For CA Top Secret for z/OS systems, enter the following commands:

     ```
     TSS ADD(uuuuuuu) HOME(path_name) OMVSPGM(/bin/sh) UID(nnn)
     GROUP(ggggggg)
     ```

   - For the IBM RACF systems, enter the following command:

     ```
     ALU uuuuuuu OMVS(UID(nnn) HOME(path_name) PROGRAM(/bin/sh))
     ```

   Note: The OMVS segment must contain the following components:

   - A home directory (HOME)
   - A login shell (PROGRAM or OMVSPGM)

3. Ensure that you have completed this process for each user ID that you want to authorize. To confirm the contents of the OMVS segment, enter the following commands:

   - For CA ACF2 for z/OS systems, enter the following commands:

     ```
     SET PROFILE(USER) DIV(OMVS)
     LIST uuuuuu
     ```

   - For CA Top Secret for z/OS systems, enter the following command:

     ```
     TSS LIST(uuuuuu) DATA(ALL)
     ```

   - For the IBM RACF systems, enter the following command:

     ```
     LISTUSER uuuuuu OMVS NORACF
     ```

4. Select a home directory to associate with each user ID. Ensure that it exists and that the UID has read/write access to it.

   You can use the UNIX directory (*path_name*), as shown in Step 2, or you can use a customized home directory name.

   For example, to set up a directory that is named /u/name for UID*nnn*, issue the following commands in the OMVS UNIX shell:

   ```
   mkdir /u/name
   chown nnn /u/name
   chmod 775 /u/name
   ```

5. Confirm the owner and access to the directory by using the following command:

   ```
   ls -ld /u/name
   ```

   The following result appears:

   ```
   drwxrwxr-x   2 user  group  8192 Sep  31 14:58 /u/name
   ```

Set Up User Security for CA CSM Functions

CA CSM uses resource profiles (see page 116) in the CAMSM resource class to grant access to resources on the web-based interface. You use these profiles to configure user security. If you plan to enable security checking for CA CSM functionality, your security administrator must configure the security before users access the web-based interface.

The default name of the SAF resource class is CAMSM. You can change the resource class name during CA CSM installation. To change the name, edit the safResourceClass keyword in the CA CSM options file.

If you want to change the setting after CA CSM is installed and set up, you can update the following statement in the SAMPLIB(MSMLIB) member:

```
IJO="$IJO-Dsaf.resource.class=saf_resource_class_name"
```

The safSecurity keyword in the CA CSM options file controls whether SAF resources are used to control access to CA CSM functions. If you want to change the setting after CA CSM is installed and set up, you can update the following statement in the SAMPLIB(MSMLIB) member. The value, false, disables security; and the value, true, enables security.

```
IJO="$IJO -Dactivate.saf.manager=false_or_true"
```

Important! If CA CSM fails to start with SAF security enabled, the following error is displayed in the CA CSM job log:

SafError - Error during DSI java open. RC=13

The resource profiles provide granular access to resources. However, for a start, configure security for two generic roles, administrator and general user.

Follow these steps:

1. Configure user security by using the resource profiles.

   The users are secured for various roles.

2. Recycle the CA CSM application server.

   The configured security takes effect.

Note: We recommend that you use the same credentials that are used for performing product management work before CA CSM. Using the same credentials ensures that you have the same access rights within CA CSM that you have through TSO, BATCH, ISPF, and SMP/E.

For a change to user security privileges to take effect, recycle the CA CSM application server.

More information:

Security for CA CSM Functions (see page 114)

CA CSM Associated Security IDs - OMVS Segment and Home Directory

If the msmserv USS directory path is unavailable, CA CSM does not operate. Assign a user ID to the application address spaces with this home directory path. This step prevents the possibility of CA CSM filling up a USS system or another application file system. This action ensures that CA CSM is isolated to the file systems allocated for its use.

A user ID with a valid OMVS segment defined must be assigned to the CA CSM address spaces. This OMVS segment requires that a valid home directory is defined. We recommend that the user IDs are assigned to a home directory of the USS path for the msmserv directory. If the default USS directory paths are used, this path is /u/users/msmserv.

Note: For more information, see user documentation for your security product.

Chapter 3: Configuring CA CSM

This section contains the following topics:

Setting Up CA CSM User ID Without UID(0)

After the CA CSM installation is complete, you can configure CA CSM not to use UID(0) when running.

This section contains the following topics:

Prerequisites

To run CA CSM without UID(0), ensure that the following requirements are met:

- The CA CSM user ID that is associated with the CA CSM application server must have a UID other than 0.
- The first user to log in to CA CSM must have a UID other than 0.

  Note: The LJWK directory and the mount point are created using the user ID of the first user instead of the CA CSM user ID (*CA_CSM_USER_ID*).

Set Up CA CSM User ID Without UID(0) for CA Top Secret for z/OS

Modify this procedure according to your security system settings.

The CA CSM user ID is the ID that is associated with the CA CSM application server.

Follow these steps:

1. Review the prerequisites (see page 27).
2. After the installation of CA CSM finishes, create a group, for example, CACSMGRP with a GID definition in your security system, and specify CACSMGRP to be the default group for the CA CSM user ID and each CA CSM user.
3. Change the owner and the group by issuing the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MSMPATH
   chgrp –R CACSMGRP MSMPATH
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   chown –R CA_CSM_USER_ID RunTimeUSSPath
   chgrp –R CACSMGRP RunTimeUSSPath
   ```

   where MSMPATH, MountPath, and RunTimeUSSPath are values that are referenced in the MSMSetupOptionsFile.properties file.

   Note: When you issue the commands for *RunTimeUSSPath*, the following message can appear:

   ```
   EDC5129I No such file or directory
   ```

   This message is issued against the ioeagfmt file and does not affect command completion in any way. You can ignore this message.

   Important! Also, issue these commands after you run the MSMDEPLY job.

4. If you plan to run the CA CSM application server as a started task, accomplish relevant configuration settings. For more information, see "Set Up Started Task Security" in the *Site Preparation Guide.*
5. Assign the following required IBMFAC class permissions to the CA CSM user ID:

   ```
   IBMFAC BPX.CONSOLE ACCESS(UPDATE)
   IBMFAC BPX.SERVER  ACCESS(UPDATE)
   IBMFAC BPX.FILEATTR.APF ACCESS(READ)
   IBMFAC BPX.FILEATTR.PROGCTL ACCESS(READ)
   IBMFAC BPX.FILEATTR.SHARELIB ACCESS(READ)
   ```

6. Assign the following required UNIXPRIV class permissions to the CA CSM user ID:

   ```
   UNIXPRIV SUPERUSER.FILESYS.CHANGEPERMS ACCESS(READ)
   UNIXPRIV SUPERUSER.FILESYS.MOUNT ACCESS(UPDATE)
   UNIXPRIV SUPERUSER.FILESYS.PFSCTL ACCESS(READ)
   ```

7. Assign the following optional SERVAUTH class permissions, to the CA CSM user ID:

   ```
   SERVAUTH EZB.FTP ACCESS(READ)
   SERVAUTH EZB.STACKACCESS ACCESS(READ)
   ```

8. After the first task within CA CSM finishes, issue the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   ```

   where MountPath is a value that is referenced in the MSMSetupOptionsFile.properties file.

Set Up CA CSM User ID Without UID(0) for CA ACF2 for z/OS

Modify this procedure according to your security system settings.

The CA CSM user ID is the ID that is associated with the CA CSM application server.

Follow these steps:

1. Review the prerequisites (see page 27).
2. After the installation of CA CSM finishes, create a group with a GID definition, for example, CACSMGRP, in your security system, and specify CACSMGRP to be a group for the CA CSM user ID and each CA CSM user.
3. Change the owner and the group by issuing the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MSMPATH
   chgrp –R CACSMGRP MSMPATH
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   chown –R CA_CSM_USER_ID RunTimeUSSPath
   chgrp –R CACSMGRP RunTimeUSSPath
   ```

   where MSMPATH, MountPath, and RunTimeUSSPath are values that are referenced in the MSMSetupOptionsFile.properties file.

   Note: When you issue the commands for *RunTimeUSSPath*, the following message can appear:

   ```
   EDC5129I No such file or directory
   ```

   This message is issued against the ioeagfmt file and does not affect command completion in any way. You can ignore this message.

   Important! Also, issue these commands after you run the MSMDEPLY job.

4. In the FACILITY resource class, define the following resource names with access rights to the CA CSM user ID:

   ```
   BPX.CONSOLE             UPDATE
   BPX.SERVER              UPDATE
   BPX.FILEATTR.APF        READ
   BPX.FILEATTR.PROGCTL    READ
   BPX.FILEATTR.SHARELIB   READ
   ```

5. In the UNIXPRIV resource class, define the following resource names with access rights to the CA CSM user ID:

   ```
   SUPERUSER.FILESYS.CHANGEPERMS   READ
   SUPERUSER.FILESYS.MOUNT         UPDATE
   SUPERUSER.FILESYS.PFSCTL        READ
   ```

6. In the SERVAUTH resource class, define the following resource names with access rights to the CA CSM user ID:

   ```
   EZB.FTP          READ
   EZB.STACKACCESS  READ
   ```

7. After the first task within CA CSM finishes, issue the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   ```

   where MountPath is a value that is referenced in the MSMSetupOptionsFile.properties file.

Set Up CA CSM User ID Without UID(0) for IBM RACF

Modify this procedure according to your security system settings.

The CA CSM user ID is the ID that is associated with the CA CSM application server.

Follow these steps:

1. Review the prerequisites (see page 27).
2. After the installation of CA CSM finishes, create a group with a GID definition, for example, CACSMGRP, in your security system, and specify CACSMGRP to be the default group for the CA CSM user ID and each CA CSM user.

3. Change the owner and the group by issuing the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MSMPATH
   chgrp –R CACSMGRP MSMPATH
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   chown –R CA_CSM_USER_ID RunTimeUSSPath
   chgrp –R CACSMGRP RunTimeUSSPath
   ```

   where MSMPATH, MountPath, and RunTimeUSSPath are values that are referenced in the MSMSetupOptionsFile.properties file.

   Note: When you issue the commands for *RunTimeUSSPath*, the following message can appear:

   ```
   EDC5129I No such file or directory
   ```

   This message is issued against the ioeagfmt file and does not affect command completion in any way. You can ignore this message.

   Important! Also, issue these commands after you run the MSMDEPLY job.

4. In the FACILITY resource class, define the following profiles with access rights to the CA CSM user ID:

   ```
   BPX.CONSOLE            UPDATE
   BPX.SERVER             UPDATE
   BPX.FILEATTR.APF       READ
   BPX.FILEATTR.PROGCTL   READ
   BPX.FILEATTR.SHARELIB  READ
   ```

5. In the UNIXPRIV resource class, define the following profiles with access rights to the CA CSM user ID:

   ```
   SUPERUSER.FILESYS.CHANGEPERMS   READ
   SUPERUSER.FILESYS.MOUNT         UPDATE
   SUPERUSER.FILESYS.PFSCTL        READ
   ```

6. In the SERVAUTH resource class, define the following profiles with access rights to the CA CSM user ID:

   ```
   EZB.FTP          READ
   EZB.STACKACCESS  READ
   ```

7. After the first task within CA CSM finishes, issue the following commands under SUPERUSER authority:

   ```
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   ```

   where MountPath is a value that is referenced in the MSMSetupOptionsFile.properties file.

Run CA CSM on Another LPAR

You can run CA CSM on another LPAR within a sysplex with a shared DASD. For example, you install CA CSM on LPAR1 and later you want to run it on LPAR2 without reinstalling.

Note: You can run CA CSM only on one LPAR at a time that is using the same USS file systems. You must have installed the correct level of CA Common Services for z/OS function CETN*xxx* on the new LPAR. The level of CA Common Services for z/OS function CETN*xxx* depends on your version of CA CSM and is the same version as on the first LPAR.

Important! CA CSM stores the USS paths that are used for the file systems in the CA Datacom database. The USS path names must be identically used on both LPAR systems.

For example, you have the following USS path on LPAR1:

```
/u/users/csmpt/PT51/mpm/scroot/DatabaseM/CA/CA_ACF2_-_MVS/
```

Use the same USS file system for the installation on LPAR2. When you restart CA CSM on LPAR2, Shared File System automatically creates the prefix before the USS path and mounts CA CSM to the correct system.

Follow these steps:

1. Log in to CA CSM running on LPAR1 and navigate to the Settings tab, System Settings, Mount Point Management. Select Unmount at Shutdown. Click Apply to save your changes.
2. Shut down CA CSM on LPAR1.
3. Unmount the CA CSM USS file system from LPAR1. This file system was mounted before executing the CA CSM application server started task or batch JCL. This file system is also referenced in the SAMPLIB(MSMLIB) member. For example:

   C_HOME=/*parent_path*/msmserv/*version_number*/msmruntime/tomcat

   The mountpoint in the previous case is for the following file system:

   /*parent_path*/msmserv/*version_number*/
4. (Optional) Verify the file system and the z/OS data set information that is required for the mountpoint by issuing the following command in OMVS:

   df –vkP | grep /*parent_path*/msmserv/*version_number*/
5. Mount the CA CSM USS file system on LPAR2.
6. Edit two XML files, context.xml and server.xml, that are at *parent_path*/msmserv/*version_number*/msmruntime/tomcat/conf using the Edit ASCII option. We recommend that you use the ISPF editor.

- In the context.xml file, specify the following parameters:
  - SystemID
  - HostName
- (Optional) If you need to change the port numbers that CA CSM uses in the URL for the new LPAR2 that CA CSM will now reside on, edit the server.xml file.
  - To edit the shutdown port, change the shutdown parameter in the following line:

  ```
  <Server port="25955" shutdown="MSMTCEND">
  ```

  - To edit the connection port and redirect port, change the port and redirectPort parameters in the following line:

  ```
  <Connector connectionTimeout="20000" port="25958" protocol="HTTP/1.1"
  redirectPort="25957"/>
  ```

Note: You can predefine these files for each LPAR on which you want CA CSM to run. For example, you have two CA CSM eligible LPARs, LPAR1 and LPAR2. Create the context and server files are as follows:

- For LPAR1: context.xml.LPAR1 and server.xml.LPAR1
- For LPAR2: context.xml.LPAR2 and server.xml. LPAR2

7. Stop the MUF and CA Datacom Server on the current LPAR1.
8. Duplicate the corresponding files for LPAR2 and rename them to their original names: context.xml and server.xml
9. Start the MUF and CA Datacom Server started tasks or batch JCL on LPAR2.
10. (Optional) Log in to CA CSM running on LPAR2 and navigate to the Settings tab, System Settings, Mount Point Management. Clear the check box Unmount at Shutdown. Click Apply to save your changes.

Enable the Notice and Consent Banner in CA CSM

After you set up and install CA CSM, you can configure it so that it displays the Notice and Consent banner every time a user logs in to CA CSM.

When CA CSM is started for the first time, the file that is named MSMBanner.html is created in the following directory:

```
tomcat/webapps/MSM/
```

The file contains the sample banner.

Follow these steps:

1. Copy the sample file MSMBanner.html to the following directory:

   ```
   tomcat/webapps/
   ```

2. (Optional) Modify the contents of the file so that it conforms to the requirements of your organization.

   The banner is available and appears the next time a user logs in to CA CSM.

   Note: Do not change the CA CSM access URL in the following string:

   ```
   <a href="MSMMain.html">
   ```

Binding the CA CSM Application Server to a TCP/IP Stack in a Multi-TCP/IP Stack Environment

When your LPAR with CA CSM has multiple TCP/IP stacks, establish a TCP/IP stack affinity to a desired stack. Establishing a stack affinity binds all socket communications to that stack.

To establish a stack affinity, select one of the following methods:

- Add a DD statement SYSTCPD DD to the CA CSM startup JCL (*RunTimeMVSHLQPrefix*.JCL(MSMTCSRV)) pointing to a specific TCPIP.DATA data set. For example:

  ```
  //SYSTCPD DD DSN=TCPIP.SEZAINST(TCPDATA),DISP=SHR
  ```

- Add the environment variable _BPXK_SETIBMOPT_TRANSPORT to the *RunTimeMVSHLQPrefix*.SAMPLIB(MSMLIB) member that is associated to the STDENV DD of the CA CSM application server. For example:

  ```
  export _BPXK_SETIBMOPT_TRANSPORT=stackname
  ```

- Add an extra step, AFFINITY, in the CA CSM startup JCL (*RunTimeMVSHLQPrefix*.JCL(MSMTCSRV)) before the MSMSRV step:

  ```
  //AFFINITY EXEC PGM=BPXTCAFF,PARM=stackname
  ```

Configuring FTP and HTTP Connections

This section describes how to configure FTP connections for both new and existing CA CSM installations, and how to configure HTTP connections.

Note: Before you start, verify that you have a CA Support Online account. You can verify it on the System Settings, Software Acquisition page.

Configuring FTP Connections for an Existing Installation

No FTP configuration changes are needed when upgrading from a previous version of CA CSM to CA CSM Version 6.0.

Configuring HTTP Connections for an Existing Installation

If you used an HTTP proxy server with NTLM authentication in a previous version of CA CSM, verify that all users have the NTLM domain in the user name. Do so from the Settings tab, the User Settings, Software Acquisition page (see page 45). For example:

```
mydomain\user1
```

Otherwise, no HTTP configuration changes are needed when upgrading from a previous version of CA CSM to CA CSM Version 6.0.

Configuring FTP Connections for a New Installation

FTP Session Options

CA CSM uses a Java-based FTP client. This FTP client has several options that control how the session operates. These options are not considered to be related to FTP proxies that provide authentication services when logging in to the FTP server.

FTP session options are specified in the installed CA CSM data set *RunTimeMVSHLQPrefix*.SAMPLIB(PASADVOP). This data set is an XML file and has an FTPOPTIONS section defining all the available FTP session options. Each option is set to the FTP client default.

The <FTPOPTIONS> XML tag is read for every FTP connection that CA CSM establishes. If the tag is not defined or empty, then the CA CSM FTP client uses the defaults as described in this section.

The following example is a code syntax sample for FTP session settings:

```
<FTPOPTIONS>key_1=value_1, key_2=value_2</FTPOPTIONS>
```

You can use the following keys:

firewall.friendly

The firewall.friendly FTP option is set to true by default:

```
<FTPOPTIONS>firewall.friendly=true</FTPOPTIONS>
```

You only specify this option if you want to override it.

The firewall.friendly option refers to FTP operating in passive mode. Passive mode causes the FTP server to open a listening port for the FTP data connection. If this option is set to false, then the FTP client opens the listening port for the server.

You can ask your network administrator if passive mode is supported. Alternatively, you can test if the default is acceptable by running a batch FTP program. After the statements that log you in to the FTP server as *anonymous*, insert QUOTE PASV.

The job output displays a message that contains the following text:

```
227 Entering Passive Mode (IP_address,FTP_server_code)
```

- If you see this message, you do not have to specify the firewall.friendly option.
- If you do not see this message, rerun the job with QUOTE PASV removed. The job output now displays a message that contains the following text:

  ```
  200 PORT command successful.
  ```

  If you see this message, set firewall.friendly to false.

verify.pasv.ip

The verify.pasv.ip FTP option is set to true by default:

```
<FTPOPTIONS>verify.pasv.ip=true</FTPOPTIONS>
```

You only specify this option if you want to override it.

Important! We recommend that you do not override this option unless your firewall support absolutely requires it.

Some firewall implementations may intercept and alter the IP address that is returned from the FTP server in response to the PASV command. In this case, you may see the following message in CA CSM application server (see page 151) logs:

```
Host attempting data connection ip_address_1 is not same as server ip_address_2
```

ip_address_1

Identifies the altered IP address from the firewall server.

ip_address_2

Identifies the IP address of the FTP server.

default.timeout

The default.timeout FTP option is set to zero (0) by default:

```
<FTPOPTIONS>default.timeout=0</FTPOPTIONS>
```

You only specify this option if you want to override it.

The value of this option represents time in milliseconds. The default value 0 is interpreted as an infinite timeout. Some environments can encounter timeout issues when downloading large files that are 200 MB or more.

For example, a large file is downloaded using an FTP command line session in OMVS. When the data transfer is complete, a subsequent FTP command, for example, **ls**, is entered. A timeout condition can result with a message, for example:

```
Connection to server interrupted or timed out. Waiting for reply.
```

In this case, a value of 10000 (representing 10 seconds) resolves this situation if CA CSM encounters it.

default.port

The default.port option is set to 21 by default. This port is the industry standard default port that FTP uses. There may be some firewall implementations that alter this default port, even if there are no FTP proxy authentication methods.

```
<FTPOPTIONS>default.port=21</FTPOPTIONS>
```

You can change the port number 21 to the required port number.

Note: This option has no affect if you enable FTP proxy settings.

control.keep.alive.timeout

Keepalive packets (no-operation packets) prevent routers from closing a control connection during large file transfers after a certain period of inactivity. The control.keep.alive.timeout option specifies how often (every *x* seconds) a keepalive packet is sent.

The control.keep.alive.timeout option is not specified by default (no keepalive packet is sent). You can set this option to the required frequency of sending keepalive packets (in seconds). For example, to force the file download methods to send a keepalive packet every five minutes (300 seconds), add the following statement in the *RunTimeMVSHLQPrefix*.SAMPLIB(PASADVOP) data set:

```
<FTPOPTIONS>control.keep.alive.timeout=300</FTPOPTIONS>
```

More information:

FTP Proxy Settings (see page 38)

FTP Proxy Settings

FTP Basic Proxy Settings

When you select only the Enable Proxy Settings check box in the FTP Proxy section on the System Settings, Software Acquisition page, CA CSM supports the following basic FTP proxy authentication methods:

- Without user credentials (see page 38)
- With user credentials (see page 38)

Configure without User Credentials

Follow these steps:

1. On the Settings tab, go to System Settings, Software Acquisition.
2. In the FTP Proxy section, select the Enable Proxy Settings check box, and provide the FTP proxy port and address.
3. Click Apply.

   The changes take effect.
4. Go to User Settings, Software Acquisition.
5. In the FTP Proxy section, verify that the user name and password are *not* provided. If they are provided, remove both of them, and click Apply.

   The changes take effect.

CA CSM sends the following commands:

- An FTP USER command with the anonymous@ftp.ca.com parameter
- An FTP PASS command with your ID for the CA Support Online website as the password

Configure with User Credentials

Follow these steps:

1. On the Settings tab, go to System Settings, Software Acquisition.
2. In the FTP Proxy section, select the Enable Proxy Settings check box, and provide the FTP proxy port and address.
3. Click Apply.

   The changes take effect.
4. Go to User Settings, Software Acquisition.

5. In the FTP Proxy section, provide a user name and password for the FTP proxy server.
6. Click Apply.

   The changes take effect.

CA CSM connects to the specified proxy server and sends the following sequence of FTP commands to authenticate and log in to the FTP server:

```
USER FTP_proxy_user_ID@ftp.ca.com
PASS proxy_password
USER anonymous
PASS Support_Online_user_ID
```

Note: The same scenarios are applied to all other CA FTP servers where ftp.ca.com is mentioned.

FTP Advanced Proxy Settings

If the FTP basic settings do not support your FTP proxy authentication methods, FTP advanced proxy settings allow you to customize the FTP authentication and logon as your FTP proxy requires. These advanced settings are stored in a PDS member named PASADVOP. When CA CSM is installed, PASADVOP is placed into the *RunTimeMVSHLQPrefix*.SAMPLIB data set. To see the current location of the PASADVOP, look in FTP Proxy, Advanced Settings Data Set, on the System Settings, Software Acquisition page. This member has a generic template containing advanced FTP settings. You can use the default values in the member or can modify them using ISPF editor to match your FTP and HTTP proxy authentication methods.

Example PASADVOP Member

All XML elements must be specified between the tags <ADVOPTIONS></ADVOPTIONS>.

```
<ADVOPTIONS>
  <FIREWALL>
    <FIRECMD>HOST;</FIRECMD>
    <FIRECMD>USER;@REMOTE_USER;@REMOTE_HOST;</FIRECMD>
    <FIRECMD>PW;@REMOTE_PW;</FIRECMD>
  <FIREWALL>
</ADVOPTIONS>
```

The following example is a code syntax sample for FTP proxy settings:

```
<FIREWALL>
  <FIRECMD>keyword;</FIRECMD>
<FIREWALL>
```

Use the following keywords for supporting various FTP proxy authentication schemes:

HOST

Defines the name of your FTP proxy server. When this keyword is encountered, CA CSM substitutes the value that is entered for the FTP Proxy Server name on the System Settings, Software Acquisition page. The FTP client uses this value to connect initially.

USER

Defines the user for authenticating to the enabled proxies. When this keyword is encountered, it is substituted with the value that is entered for the FTP Proxy User that is specified on the User Settings, Software Acquisition page.

PW

Defines the password for authenticating to the enabled proxies. When this keyword is encountered, it is substituted with the value that is entered for the FTP Proxy Password that is specified on the User Settings, Software Acquisition page.

REMOTE_HOST

Defines the FTP address of the remote server. When this keyword is encountered, it is substituted with the appropriate FTP URL.

REMOTE_USER

Defines the user for authenticating to the remote server. When this keyword is encountered, it is substituted with *anonymous*.

REMOTE_PW

Defines the password for authenticating to the remote server. When this keyword is encountered, it is substituted with your user ID for the CA Support Online website.

ACCT

Instructs the CA CSM FTP client to issue an ACCT command to the FTP server. This keyword allows an accompanying parameter. This parameter is typically the proxy password that the PW keyword represents.

Follow the keywords with a semicolon (;). Outline the proxy authentication using these keywords. CA CSM substitutes the actual values from the System Settings, Software Acquisition page.

More information:

Defining FTP Advanced Settings (see page 41)

Defining FTP Advanced Settings

We recommend that you set up the advanced settings by running a batch job in z/OS executing the IBM FTP program. You can transpose the FTP proxy authentication scheme to the data set containing advanced settings.

For example, the input to your FTP batch job is the following sample:

```
//INPUT DD *
proxy_host_URL_or_IP
anonymous@ftp.ca.com proxy_userid
Support_Online_user_id
ACCT proxy_password
/*
```

Notes:

- A space precedes *proxy_userid*.
- If your network administrators require quotes, quotes can surround the second input line.

In this case, you would edit the advanced settings data set as follows:

```
<ADVOPTIONS>
  <FIREWALL>
    <FIRECMD>HOST;</FIRECMD>
    <FIRECMD>REMOTE_USER;@REMOTE_HOST; USER;</FIRECMD>
    <FIRECMD>REMOTE_PW;</FIRECMD>
    <FIRECMD>ACCT; PW;</FIRECMD>
  </FIREWALL>
</ADVOPTIONS>
```

- The HOST keyword is substituted with the FTP proxy name specified for the FTP Proxy Server name on the System Settings, Software Acquisition page.
- The REMOTE_USER keyword is substituted with anonymous.
- The USER keyword is substituted with the value specified for the user in the FTP Proxy section on the User Settings, Software Acquisition page.
- The REMOTE_HOST keyword is substituted with the appropriate CA Technologies FTP server URL.
- The ACCT keyword instructs the CA CSM FTP client to issue an ACCT command to the FTP server. This keyword allows an accompanying parameter. The parameter is typically the proxy password that the keyword PW represents, depending on what network administrators require.

- CA CSM substitutes your user ID on the CA Support Online website as specified in the CA Support Online Accounts section on the System Settings, Software Acquisition page for the REMOTE_USER keyword. The PW keyword is substituted with the value specified for the password in the FTP Proxy section, on the User Settings, Software Acquisition page. All of these substitutions are concatenated in the order that the FIRECMD statement specifies. The *at* symbol (@) is inserted into the resolved string exactly as specified.

Sometimes, the FTP input does not easily translate into the FIRECMD elements. In that case, you can use the SYSOUT of the batch FTP job. Use the //INPUT DD * batch job that is described at the beginning of this section to look for specific FTP commands and note the specific sequence.

The following SYSOUT is an abbreviated listing. The listing highlights the relevant statements that are used to formulate the FIRECMD statements.

Note: Comments are indicated by ==>.

```
EZA1450I IBM FTP CS V1R9
EZA1772I FTP: EXIT has been set.
    ==> The EZA1554I message shows the IP address of the FTP proxy server, and
    message 220 typically, but not always, displays the URL of the FTP proxy.
    Either of these can be specified in the CA CSM FTP Proxy settings as
    an IP address or the FTP proxy server name. This would translate to
    <FIRECMD> HOST;</FIRECMD>.
EZA1554I Connecting to:   123.456.789.1 port: 21.
220 Secure FTP server running on ftpproxyserver
    ==> The EZA1701I message indicates that the FTP USER command accepts a
    concatenated string to provide the FTP proxy user ID, the FTP user ID, and
    the actual FTP site to connect after the authentication is completed. This
    concatenated string would be translated as
    <FIRECMD>REMOTE_USERID;@USER;@REMOTE_HOST;</FIRECMD>.
EZA1459I NAME (123.456.789.1:ZOSUSERID):
EZA1701I >>> USER anonymous@proxy_userid@ftp.ca.com
    ==> Message 331 is an FTP proxy reply that indicates that the PASS command
    will accept a concatenated string to provide the passwords for both
    the FTP proxy server and the FTP server. As it does not specify which should
    be first, check the //INPUT DD * sample to see that the FTP server password
    is first (anonymous). Typically, but not always, if the user IDs are
    concatenated, the passwords are concatenated in the same order. That means,
    as in this case, the FTP user ID is first, therefore the FTP password is
    first. This concatenated string would be translated to
    <FIRECMD>REMOTE_PW;@PW;</FIRECMD>.
331 password: use password@password
EZA1789I PASSWORD:
EZA1701I >>> PASS
```

```
    ==> The following replies indicate the FTP proxy has successfully
    authenticated your FTP proxy credentials, and is logging in to the
    FTP server. The FTP server is acknowledging you have successfully
    logged in.
230-User proxy_userid authenticated by Secure FTP authentication
230-Connected to server. Logging in...
230-220 ftp.ca.com NcFTPd Server (licensed copy) ready.
230-331 User anonymous okay, need password.
230-230-You are user #18 of 4000 simultaneous users allowed.
```

The following sample is an example of using the SITE command. The server uses this command to provide system-specific services that are essential to file transfer but not sufficiently universal to be included as commands in the protocol.

```
<ADVOPTIONS>
  <FIREWALL>
    <FIRECMD>HOST;</FIRECMD>
    <FIRECMD>USER;</FIRECMD>
    <FIRECMD>PW;</FIRECMD>
    <FIRECMD>SITE;REMOTE_HOST;</FIRECMD>
    <FIRECMD>REMOTE_USER;</FIRECMD>
    <FIRECMD>REMOTE_PW;</FIRECMD>
  </FIREWALL>
</ADVOPTIONS>
```

FTP Advanced Proxy Settings Restrictions

The following restrictions are applied:

- CA CSM does not support actual user IDs and passwords within the <FIRECMD> element.
- CA CSM supports concatenating proxy user IDs with FTP user IDs (*anonymous*), and concatenating proxy passwords with FTP passwords (ID for the CA Support Online website). However, concatenating a proxy user ID and proxy password, or *anonymous* with the ID for the CA Support Online website is *not* supported.

  For example, the following sample is supported:

  ```
  <FIRECMD>USER;@REMOTE_USER;</FIRECMD>
  <FIRECMD>PW;@REMOTE_PW;</FIRECMD>
  ```

  The following sample is *not* supported:

  ```
  <FIRECMD>USER;PW;</FIRECMD>
  <FIRECMD>REMOTE_USER;REMOTE_PW;</FIRECMD>
  ```

In this case, put the user ID and password on separate FIRECMD elements, for example:

```
<FIRECMD>USER;</FIRECMD>
<FIRECMD>PW;</FIRECMD>
<FIRECMD>REMOTE_USER;</FIRECMD>
<FIRECMD>REMOTE_PW;</FIRECMD>
```

Configuring HTTP Proxy Settings

The following scenarios are possible depending on your site configuration.

If you do not use an HTTP proxy server, your HTTP connection settings are complete.

HTTP Proxy Server without Authentication

Follow these steps:

1. On the Settings tab, go to System Settings, Software Acquisition.
2. In the HTTP Proxy section, select the Enable Proxy Settings check box, and provide the HTTP proxy port and address.
3. Click Apply.

   The changes take effect.
4. Go to User Settings, Software Acquisition.
5. In the HTTP Proxy section, verify that the user name and password are *not* provided. If they are provided, remove both of them, and click Apply.

   The changes take effect.

HTTP Proxy Server with Basic Authentication

Follow these steps:

1. On the Settings tab, go to System Settings, Software Acquisition.
2. In the HTTP Proxy section, select the Enable Proxy Settings check box, and provide the HTTP proxy port and address.
3. Click Apply.

   The changes take effect.
4. Go to User Settings, Software Acquisition.

5. In the HTTP Proxy section, provide a user name and password for the HTTP proxy server.

6. Click Apply.

   The changes take effect.

HTTP Proxy Server with NTLM Authentication

Follow these steps:

1. On the Settings tab, go to System Settings, Software Acquisition.

2. In the HTTP Proxy section, select the Enable Proxy Settings check box, and provide the HTTP proxy port and address.

3. Click Apply.

   The changes take effect.

4. Go to User Settings, Software Acquisition.

5. In the HTTP Proxy section, provide the NTML domain, user name and password for the HTTP proxy server. The following sample is an example of providing the NTML domain and user name:

   ```
   mydomain\user1
   ```

6. Click Apply.

   The changes take effect.

Configure CA CSM to Use HTTPS

This section describes how to configure CA CSM to enable HTTPS access using a digital certificate.

Enable HTTPS with Certificates Stored in USS Files

You can configure CA CSM to use HTTPS instead of HTTP for user access manually, using a USS file to store certificates.

Follow these steps:

1. Generate a keystore:

   a. Start an OMVS session and enter the following command:

   ```
   keytool -genkey -alias tomcat -keyalg RSA
   ```

   A prompt appears.

   Note: keytool is a Java command that resides in the Java libraries. These libraries have a name similar to /*Customer-Java-Prefix*/ java/J6.0.1/bin/, where *Customer-Java-Prefix* is the Java USS directory name at your site. You can add this directory name in your USS profile path variable for successful command execution.

   b. Follow the prompt, remember your keystore password, and press Enter when you are prompted if you want to keep the default password.

   A default keystore is created in your home directory with one self-signed certificate inside.

   c. (Optional) If you want a different location, enter the following command, replacing the /path/to/my/keystore portion with your site-specific information:

   ```
   keytool -genkey -alias tomcat -keyalg RSA \ -keystore /path/to/my/keystore
   ```

2. Configure Apache Tomcat:

   a. Go to tomcat/conf and open the server.xml file.

   b. Uncomment or replace the part with the SSL connector, as follows:

   ```
   <!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
      <Connector port="30308" maxHttpHeaderSize="8192"
                 maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
                 enableLookups="false" disableUploadTimeout="true"
                 SSLEnabled="true"
                 keystorePass="tomcat"
                 keystoreFile="/a/path/to/my/keystore/.keystoreFile"
                 algorithm="IbmX509"
                 acceptCount="100" scheme="https" secure="true"
                 clientAuth="false" sslProtocol="TLS"
                 sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1" />
   ```

   c. Change the port and keystoreFile parameters to fit your needs.

d. Ensure that keystorePass matches the password that you specified in the previous step.

e. In the standard HTTP connector, provide the redirectPort to match the one you specified in the SSL connector, as follows:

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
    <Connector port="30305" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" redirectPort="30308"
               acceptCount="100"
               connectionTimeout="20000" disableUploadTimeout="true" />
    <!-- Note : To disable connection timeouts, set connectionTimeout
     value to 0 -->
```

3. Start (or restart) Apache Tomcat.

4. Enable your browser to use TLS encryption, and restart the browser.

5. Access the HTTPS URL.

   Note: When you access the HTTPS URL from your browser for the first time, you may be prompted to confirm that you trust the certificate.

6. Click Yes to add this certificate to your trusted certificates.

Note: For more information, see documentation for the Apache Tomcat 7.0 Servlet/JSP Container.

Enable HTTPS with Certificates Stored in an External Security Manager

You can configure CA CSM to use HTTPS instead of HTTP for user access manually using an external security manager, for example, CA Top Secret for z/OS, CA ACF2 for z/OS, or IBM RACF to store digital certificates.

Follow these steps:

1. Generate a digital certificate for Apache Tomcat, and attach it to a SAF key ring using the appropriate procedure for your external security manager.

   We recommend you generate the certificate using the RSA algorithm. The recommended certificate alias is **tomcat**.

2. Configure Apache Tomcat:

   a. Stop the Apache Tomcat server.

   b. Go to tomcat/conf and open the server.xml file.

c. Uncomment or replace the part with the SSL connector, as follows:

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
   <Connector port="30308" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          SSLEnabled="true"
          algorithm="IbmX509"
          acceptCount="100" scheme="https" secure="true"
          clientAuth="false" sslProtocol="TLS"
          sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1"
          keystoreType="JCERACFKS"
          keystoreFile="safkeyring://KEY_RING_OWNER/KEY_RING_NAME"
          sslImplementationName="com.ca.sslsocket.CASSLImplementation" />
```

d. Change the port parameter to fit your needs.

e. Change the keystoreFile parameter so that it describes the SAF key ring containing the certificate:

   a. Replace *KEY_RING_OWNER* with the ID of the user that will run the Apache Tomcat server. The user must have READ authority for that key ring.

   b. Replace *KEY_RING_NAME* with the name of the key ring.

   Example: keystoreFile="safkeyring://MSMSERV/CSMKEYRING"

f. If your site uses the IBM Integrated Cryptographic Services Facility (ICSF) to manage digital certificates in the external security manager, change the keystoreType parameter to a value of JCECCARACFKS.

g. If you want to force Apache Tomcat to always use HTTPS for incoming connections, configure HTTPS to override HTTP (see page 49).

3. Start the Apache Tomcat server.

   Note: When the Apache Tomcat server is starting up, the following message may appear in the output:

   ```
   WARNING: configured file: ./path/safkeyring://KEY_RING_OWNER/KEY_RING_NAME.
   does not exist.
   ```

   You can ignore this message.

4. Enable your browser to use TLS encryption, and restart the browser.

5. Access the HTTPS URL.

   Note: When you access the HTTPS URL from your browser for the first time, you may be prompted to confirm that you trust the certificate.

6. Click Yes to add this certificate to your trusted certificates.

Note: For more information, see documentation for the Apache Tomcat 7.0 Servlet/JSP Container.

Configure HTTPS to Override HTTP

You can configure CA CSM to always use HTTPS instead of HTTP for user access manually.

Follow these steps:

1. Verify that you are able to access CA CSM using both HTTP (see page 45, see page 44) and HTTPS (see page 45).
2. Shut down Apache Tomcat.
3. Configure Apache Tomcat in the web.xml file:
   a. In the tomcat/conf directory, open the web.xml file.
   b. Add the following XML under the web-app tag:

```
<security-constraint>
     <web-resource-collection>
     <web-resource-name>Protected Context</web-resource-name>
        <url-pattern>/*</url-pattern>
     </web-resource-collection>
           <!-- auth-constraint goes here if you require authentication -->
      <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
      </user-data-constraint>
</security-constraint>
```

   c. Save and close the web.xml file.
4. Configure Apache Tomcat in the server.xml file.
   a. In the tomcat/conf directory, open the server.xml file.
   b. Locate the Connector XML definition that contains the HTTP port number that Apache Tomcat runs on.
   c. Change or add, if necessary, the redirectPort attribute to the Connector XML tag. Set its value as the port number of the HTTPS Connector. For example:

```
<!-- A "Connector" represents an endpoint by which requests
         and responses are returned. Documentation at :
         Java HTTP Connector: /docs/config/http.html (blocking &
         non-blocking)
     Java AJP  Connector: /docs/config/ajp.html
         APR (HTTP/AJP) Connector: /docs/apr.html
         Define a non-SSL HTTP/1.1 Connector on port 8080
    -->
    <Connector address="123.456.789.321" port="8080"
               protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="30308" />
```

   d. Save and close the server.xml file.

5. Start Apache Tomcat.
6. Restart your browser.
7. Access the HTTP URL, and verify that it redirects to the HTTPS URL instead.

Note: For more information, see documentation for the Apache Tomcat 7.0 Servlet/JSP Container.

Allow CA CSM to Connect Through HTTPS in a Secured Environment

In some strictly secured environments, only the selected applications are allowed to connect through HTTPS. These applications use predefined user-agent HTTP header.

By default, CA CSM has the HTTPS request header set to **CA CSM**. You can change it to the value that your network environment accepts to allow CA CSM to connect over HTTPS. For example, downloading product news, updating the complete product list, getting the latest maintenance, or using the CA RS maintenance wizard.

Metacharacters that are valid for USS may affect the way your customized header name is displayed. To interpret a metacharacter as a regular character, use a backslash.

If the length of your header name exceeds one line in your editor and needs to continue on the next line, precede the header name continuation with IJO=”${IJO}.

Examples:

- To set your header name to CA USER, define the header name as **CA\" \"USER**:
  ```
  IJO="$IJO -Dhttp.header.user.agent= CA\" \"USER"
  ```
- To set your header name to $USER, define the header name as **\$USER**:
  ```
  IJO="$IJO -Dhttp.header.user.agent= \$USER"
  ```
- To set your header name to a string that is longer than the editor line:
  ```
  IJO="$IJO -Dhttp.header.user.agent=
  The_customized_header_name_exceeds_one_line_and_conti"
  IJO=”${IJO}nues_on_the_next_line”
  ```

Follow these steps:

1. Stop the CA CSM application server.
2. Include the following parameter in the *RunTimeMVSHLQPrefix*.SAMPLIB(MSMLIB) data set member, and set it to the value that your environment accepts:

   IJO="$IJO -Dhttp.header.user.agent=*your_header_name*"
3. Start the CA CSM application server.

   The changes take effect.

Configure Mount Parameters for CA CSM File Systems

Depending on your site and environment requirements, you can configure mount parameters for CA CSM product, software catalog, temporary, and deployment file systems. For example, you can decide whether to perform security checks, or how to proceed when the system that owns a file system goes down.

Initially, CA CSM uses the default values of these parameters. You can override the defaults.

Follow these steps:

1. Perform one of the following steps:
   - Manually unmount all file systems.
   - In CA CSM, navigate to the Settings tab, the Mount Point Management page, and select the Unmount at Shutdown check box. Save the changes.
2. Stop the CA CSM application server.
3. Uncomment and update the following line in the *RunTimeMVSHLQPrefix*.SAMPLIB(MSMLIB) member:

   ```
   IJO="$IJO -DADD_MOUNT_DEFAULT_OPTIONS=SETUID|NOSETUID,SECURITY|NOSECURITY,
   AUTOMOVE|NOAUTOMOVE|UNMOUNT"
   ```

   SETUID|NOSETUID

   Specifies whether the setuid() and setgid() mode bit is supported.

   SETUID

   Supports the setuid() and setgid() mode bit on an executable file. This option is the default.

   NOSETUID

   Disables the setuid() and setgid() mode bit support on an executable file. When the program is executed, the UID or GID are not changed, and the APF and Program Control extended attributes are not honored. The entire HFS is uncontrolled.

   SECURITY|NOSECURITY

   Specifies whether to perform the UNIX permissions checks.

   SECURITY

   Enables the UNIX permissions checks. This option is the default.

   NOSECURITY

   Disables the UNIX permissions checks. Any new files or directories that are created are assigned an owner of UID(0), no matter what UID issued the request. A user can access or change any file or directory.

AUTOMOVE|NOAUTOMOVE|UNMOUNT

For a sysplex where systems participate in a shared file system, specifies how to proceed when the system that owns a file system goes down.

AUTOMOVE

Automatically changes ownership of the file system to another system that participates in a shared file system. This option is the default.

NOAUTOMOVE

Keeps ownership of the file system. As a result, the file system becomes inaccessible.

UNMOUNT

Unmounts the file system when the node leaves the sysplex.

Note: For more information about these options, see the following books:

- *IBM z/OS UNIX System Services Planning*
- *IBM z/OS UNIX System Services Command Reference*
- *IBM z/OS XL C/C++ Run-Time Library Reference*

4. Start the CA CSM application server.

   The mount parameters take effect.

5. If you enabled the Unmount at Shutdown feature in Step 1, navigate to the Settings tab, the Mount Point Management page, and clear the Unmount at Shutdown check box. Save the changes.

To restore the defaults, leave the parameters empty, or comment out the line in the *RunTimeMVSHLQPrefix*.SAMPLIB(MSMLIB) member.

Example

This example enables setuid() and setgid() mode bit on executable files, disables security checks, and does not allow file systems to change ownership:

```
IJO="$IJO -DADD_MOUNT_DEFAULT_OPTIONS=NOSECURITY,NOAUTOMOVE"
```

Configure MUF Message Printing

To help you distinguish between several MUF regions, the MUFMSG parameter in the (CUSMAC)MUFSTART member is used. This parameter is configured to specify the printing of the MUF job name, informational data, and MUF name. These properties precede the message number on messages that the MUF issued and some of the messages that concern communication with the MUF:

```
MUFMSG=YES,YES,YES
```

The prefixed message is displayed in the following format:

```
jobname:svc_number:subid:DB0xxxxI
```

If you run only one MUF region, you can change this parameter to disable the printing. To do so, set the MUFMSG parameter as follows:

```
MUFMSG=NO,NO,NO
```

Configuring Output Descriptors

To be able to select an Output Descriptor from the CA CSM Policy wizard, provide the output descriptor values in the CA CSM server startup JCL. The sample JCL provided in the CA CSM runtime JCL library is named MSMTCSRV. The sample JCL provided in the CA CSM runtime PROCLIB library is named MSMTC. You can use multiple output descriptors in the CA CSM startup JCL which gives you the ability to select one of them from the wizard. The selected output descriptor is used when the policy is executed for the processing of the CA CSM task output by the JES spool option. Output descriptors are only available through this wizard if they are specified in the CA CSM startup JCL.

The following examples show output descriptors using site-specific meaningful names:

```
//CAVIEW    OUTPUT  CLASS=9,FORMS=2UP
//CASPOOL   OUTPUT  CLASS=S
```

Note: For more information about output descriptors and the parameters for the OUTPUT JCL statement, see the *IBM z/OS MVS JCL Reference*.

Set Up a Secure FTP Connection for Deployment

You can set up CA CSM to support the ability to deploy products to remote systems using FTP over TLS (Transport Layer Security). This feature allows for data to be exchanged in a secure, encrypted manner.

This feature uses X.509 digital certificates.

Certificates can be read from a security manager (CA Top Secret for z/OS, CA ACF2 for z/OS, or IBM RACF) using SAF key rings, or from USS Java key stores. In addition, CA CSM provides support for sites that use the IBM Integrated Cryptographic Service Facility (ICSF) for hardware certificate management.

The following table summarizes the available key store types that CA CSM supports:

Storage	Certificate Management	Key Stores
Security Manager	Software	JCERACFKS
Security Manager	Hardware	JCECCARACFKS
USS	Software	JKS, JCEKS, PKCS12
USS	Hardware	JCECCAKS

Note: For more information about key store types available under Java, see the *Security Reference for IBM SDK, Java Technology Edition*.

Follow these steps:

1. Click the Settings tab, and click the Software Deployment link under System Settings in the Settings section on the left side.

   The Deployed Software page opens.

2. In the Key Store Settings section, select the type of the key store that you want to use.

   The fields in the section appear. The fields vary depending on the selected key store type.

3. Set up values for the fields, and click Apply.

   A dialog that shows the progress of the task opens. When the task completes, you can click Show Results on the Progress tab to close this dialog. The task output browser opens and you can view the action details. Click Close to close the task output browser.

   Note: While a task is in progress, you can perform other work. You can click Hide to exit the dialog and view the task status later on the Tasks tab.

   The FTP connection settings are saved.

4. Add an FTP location. When adding an FTP location, select the check box Enable Secure FTP Transmission.

   The FTP location with secured FTP transmission enabled is added.

   You can now deploy products using FTP over TLS.

Note: For more information about adding an FTP location, see the online help.

More information:

Export Certificates from the gskkyman Database (see page 55)

Export Certificates from the gskkyman Database

If your FTP server uses the gskkyman key database as the FTP key ring, export the certificate from the gskkyman database and import it to the Java JKS key store. Doing so allows CA CSM to use the same certificate as the FTP server uses.

Follow these steps:

1. Create a copy of the cacerts file at *JAVA_HOME*/lib/security/ to use for CA CSM key store.

   Note: The cacerts file is the default JKS certificates file that IBM Java ships with. The cacerts file contains several root Certificate Authority certificates and is typically used to prime any new JKS key store.

2. Use the gskkyman utility and export the appropriate Certificate Authority from the FTP key ring file using binary ASN.1 DER format.

   Note: For more information about the gskkyman utility, see the *z/OS Cryptographic Services System Secure Sockets Layer Programming*.

3. Use the Java keytool utility and import the Certificate Authority into the key store database that you created in Step 1. Use the following command:

   ```
   keytool –import –trustcacerts –file /path_to_exported_ca_certificate
   –keystore /path_to_copy_jks_cacerts/file_name
   ```

   The utility prompts you to make the imported CA trusted and enter the key store password. The initial password that the cacerts file that is shipped with Java is **changeit**.

4. Set up a secure FTP connection to deployment (see page 53).

Specify Unit Parameters for SYSUT3 and SYSUT4 of the Remote System in the SAMPLIB(MSMLIB) Member

In the IEBCOPY utility, you can specify particular UNIT parameters for the SYSUT3 and SYSUT4 DD statements by adding statements in the SAMPLIB(MSMLIB) member. Remote Deployment Service picks up and uses the UNIT parameters that are specified in this way when allocating SYSUT3 and SYSUT4 DD statements. If no statements are defined, Remote Deployment Service uses the default UNIT(SYSDA) when allocating SYSUT3 and SYSUT4 DD statements. To specify parameters, add the following statements:

```
IJO="$IJO -Dmsmdutil.sysut3.unit=SYSALLDA"
IJO="$IJO -Dmsmdutil.sysut4.unit=SYSALLDA"
```

Chapter 4: Maintaining CA CSM

This section contains the following topics:

Start CA CSM

The JCL members to start CA CSM are either in your JCL data set (*RunTimeMVSHLQPrefix*.JCL) or in your PROCLIB data set (*RunTimeMVSHLQPrefix*.PROCLIB). The member location is indicated in the summary report of the CA CSM installation and setup process. You can submit or start one of these members to run it as batch jobs or started tasks.

CA CSM allocates files on startup and during operation. If your site has products interfering with file allocation, verify that DD statements to exclude such processing are included in the MSMTCSRV JCL member that starts the CA CSM application server (see page 151).

Note: The CA CSM application server (see page 151) uses a default region size of 768 MB. If you want to change this value, update the REGSIZE parameter in the MSMTCSRV JCL member. Also, update the Xmx value in the following statement in the SAMPLIB(MSMLIB) member:

```
IJO="-Xms128m -Xmx768m -Xss768m"
```

Important! If you are upgrading, verify that your address spaces from the previous version of CA CSM are down. Also, unmount the APLROOT, SCROOT, and LJWK mount points from your previous version. Optionally, back up the start procedures of your previous version CA CSM, and copy the latest version procedures to your production library.

Follow these steps:

1. Submit the MSMMUFS JCL member or start the MSMMUF PROCLIB member.

   The CA Datacom/MSM Multi-User Facility (MUF) address space starts.

   Note: All data sets in STEPLIB must be APF-authorized.

If the MUF starts up successfully, messages similar to the following example appear:

```
DB00226I - MULTI-USER ACTIVATED XCF SUPPORT
DB00222I - MULTI-USER ACTIVATED CCI SUPPORT
DB00201I - MULTI-USER ENABLED, CXX=cxx_name  MUFNAME=muf_name   AD
```

2. Submit the MSMDBSVS JCL member or start the MSMDBSRV PROCLIB member.

   The CA Datacom/MSM server address space starts.

   If the server starts up successfully, messages similar to the following example appear:

   ```
   DSV00049I-CA Datacom Server Version 14.0 INITIALIZED –server_name
   ```

3. Submit the MSMTCSRV JCL member or start the MSMTC PROCLIB member.

   The CA CSM application server address space starts.

   If the server starts up successfully, the following message appears in STDOUT:

   ```
   MSM0009I - CA CSM startup complete.
   ```

   If the startup fails, the following message appears in STDOUT:

   ```
   MSM0010E - CA CSM startup failed.
   ```

   In addition, depending on the outcome of the startup, one of the following messages appears in the system console:

   ```
   MSM0009I CA CSM STARTUP COMPLETE
   MSM0010E CA CSM STARTUP FAILED
   ```

   Note: The startup JCL for the CA CSM application server (see page 151) region has a SYSMDUMP DD statement that is commented out. If your site standards and system support the capture of this dump to the spool system, you can uncomment the DD statement to provide for dump captures in the case of failures.

   After the successful startup of the CA CSM application server address space (see page 151), users can log in to CA CSM through a web browser.

4. (CA CSM upgrade only) Comment out the DBUPDATE DD card in the MSMTCSRV JCL member or MSMTC PROCLIB after you successfully bring up CA CSM for the first time.

Notes:

- Do not start the MSMTCSRV job (manually or with automation) until the MSMDBSRV job initialization completes and the BPXM023I message appears.
- After you successfully start up the CA CSM application server (see page 151), if the following message appears, ignore it:

  ```
  INFO: The APR based Apache Tomcat Native library which allows optimal performance
  in production environments was not found on the java library.path:
  ```

  CA CSM does not require the installation of this library.

- Do not change any CA CSM application server (see page 151) startup JCL parameters unless CA Support requested it. Doing so could make CA CSM inoperable.
- If you restart the CA Datacom/MSM server, restart the CA CSM application server.

More information:

Set Up User Security for CA CSM Functions (see page 25)
Stop CA CSM (see page 66)

Maintenance

After you set up and install CA CSM, you can use it to maintain itself.

Apply Maintenance to CA CSM

Important! To download maintenance, your CA CSM login user name must be associated with a registered user of the CA Support Online website on the Product Acquisition Settings page.

Follow these steps:

1. Update the Software Catalog with the CA CSM maintenance information from the CA Support Online website:

   a. Go to the Products tab and locate CA Chorus Software Manager in the Available Products panel on the left.

      Note: If you do not see CA Chorus Software Manager in the tree, use one of the products that are installable with CA CSM for this process. These products reflect CA CSM as a component so the maintenance is reflected there also. For more information, see CA Chorus Software Manager Enabled Products in the Recommended Reading section of the CA CSM page on the CA Support Online website.

   b. Expand the CA Chorus Software Manager entry in the tree. Right-click the version of CA CSM that you have installed, and select Update Product Release.

      The task takes some time to complete, and after it does, a message appears confirming that the software was successfully acquired.

   c. Click Hide.

      The message disappears.

   d. Locate the CA CSM maintenance in the right panel.

2. (Optional) Add test fixes using external maintenance.

   Note: For more information about applying test fixes and managing maintenance downloaded external to CA CSM, see the online help.

3. Review and apply the maintenance.

   The contents of the SMP/E target libraries and USS paths for CA CSM are updated. These libraries and paths are set up using the TargetHLQ and MSMPATH keywords in the MSMSetupOptionsFile.properties options file.

   Note: For more information about applying and managing maintenance, see the online help.

4. Stop CA CSM (see page 66).

   CA CSM stops operation.

5. Deploy the maintenance for CA CSM to the CA CSM run-time libraries and USS paths. The libraries and USS paths are set up using the RunTimeMVSHLQPrefix and RunTimeUSSPath keywords in the MSMSetupOptionsFile.properties options file.

   a. Customize the JCL(MSMDEPLY) job. Update the JOB statement, and specify **deploy** for arg1.

   b. Submit the job.

6. Start CA CSM.

   CA CSM becomes operational with the maintenance.

Important! Distinguish between the SMP/E target libraries and USS paths, and the runtime libraries and USS paths. CA CSM executes out of the runtime libraries and USS paths. When you apply maintenance, only the SMP/E target libraries and USS paths are updated. You must stop CA CSM and submit the MSMDEPLY job to update the runtime libraries and USS paths. Those updates take effect when you restart CA CSM.

SQL Plan Updates

You may need to apply updates that affect CA Datacom/MSM SQL plans. These SQL plans are delivered as CA Common Services for z/OS maintenance. CA Common Services for z/OS include the sample JCL member MSMCXPLN that you can use to update these SQL plans in the MUF environment.

Implement Latest SQL Plans

The member MSMCXPLN, located in your CA Common Services for z/OS SMP/E environment sample JCL library, is modeled JCL that can be used to update CA Datacom/MSM SQL plans. Execute this JCL whenever you apply PTFs that contain at least one module element and a related SQL plan element. You will be notified that sample JCL member MSMCXPLN requires modification and execution by a ++HOLD condition action occurring during the process of applying the PTF. Follow the instructions that are provided in the ++HOLD comments to modify and execute this member properly.

Note: If CETN600 (MSMCCS 6.0) exists in your CA Common Services for z/OS, verify that the SQL plans are synchronized in the CA Datacom/MSM database Version 6.0 and your running CA Common Services for z/OS libraries. Submit the MSMCXPLN job from the CA Common Services for z/OS JCL library for each MSMC*SQL member in the CA Common Services for z/OS library that DDDEF CAW0EXP represents.

Data Set Reference for Sample JCL

To locate the data set name for the appropriate sample JCL library, refer to the DDDEF element CAW0JCL.

Data Set Reference for SQL Plan

To locate the data set name for the appropriate SQL plan library, refer to the DDDEF element CAW0EXP.

Running CA CSM Version 6.0 with the SCS Address Spaces Containing Code from a Previous Version

CA CSM Version 6.0 does not contain the same version of SQL plans for previous versions of CETN400 and CETN500. This situation may cause you to receive an SQL -124 return code when connecting to a previous version SCS address space (CETN400 or CETN500).

After you upgrade to CA CSM Version 6.0, follow the instructions that are provided in this section to import SQL plans from the CETN400 or CETN500 library. In the instructions, replace CETN600 with CETN400 or CETN500. Do this if you plan to connect to one or more CA CSM address spaces that still contain code of a previous version (CETN400 or CETN500), and you cannot upgrade your CA Common Services for z/OS with CETN600.

Back Out Maintenance from CA CSM

You can back out applied (but not accepted) maintenance from CA CSM. When you back out CA CSM maintenance, you first use the CA CSM Restore action to update the SMP/E target libraries and USS paths. Then, stop CA CSM and submit the MSMDEPLY job to update the runtime libraries and USS paths. Those updates take effect when you restart CA CSM.

Follow these steps:

1. Back out the maintenance using the Restore action.

   The contents of the SMP/E target libraries and USS paths for CA CSM are updated. These libraries and paths are set up using the TargetHLQ and MSMPATH keywords in the MSMSetupOptionsFile.properties options file.

   Note: For more information about backing out maintenance, see the online help.

2. Stop CA CSM (see page 66).

   CA CSM stops operation.

3. Deploy the contents of the updated SMP/E target libraries and USS paths to the CA CSM runtime libraries and USS paths. The libraries and USS paths are set up using the RunTimeMVSHLQPrefix and RunTimeUSSPath keywords in the MSMSetupOptionsFile.properties options file.

   a. Customize the JCL(MSMDEPLY) job. Update the JOB statement, and specify *backout* for arg1.

   b. Submit the job.

4. Start CA CSM (see page 57).

   CA CSM becomes operational without the maintenance.

Fail-Safe Backout

Rarely, a bad test fix for CA CSM can render CA CSM itself inoperable. To correct the problem, you can use the MSMDEPLY job to restore the CA CSM runtime libraries and USS paths to an operable condition. Customize and submit the MSMDEPLY job with *backout* specified for arg1. After the job completes, restart CA CSM, and follow the normal procedure to use CA CSM to back out the bad test fix.

When the MSMDEPLY job is run with *deploy* specified, a copy of the current CA CSM runtime libraries and USS paths is saved before deployment. When the MSMDEPLY job is run with *backout* specified, that last saved copy of the CA CSM runtime libraries and USS paths is deployed.

Important! Only one saved copy of the CA CSM runtime libraries and USS paths is maintained. Each execution of the MSMDEPLY job with *deploy* specified replaces the last saved copy of the runtime libraries and USS paths with a new copy. You cannot back out multiple saved copies by running the MSMDEPLY job multiple times with *backout* specified.

Recovery If CA CSM Fails Because of Maintenance

Maintenance that has been applied to software that CA CSM depends on can sometimes cause CA CSM to fail. It is possible that you will not be able to use CA CSM to correct the problem.

- If the maintenance was applied to CA CSM itself, use the fail-safe backout method (see page 62) to return CA CSM to an operable condition.
- If the problem occurs because maintenance was applied to software belonging to another product that affects CA CSM, use SMP/E batch jobs to either apply new corrective maintenance or back out the maintenance. Then, restart CA CSM. This process could include applying new corrective maintenance to CA CSM itself. If you apply new corrective maintenance to CA CSM itself, you must deploy the maintenance before restarting CA CSM.

CA CSM Backup and Disaster Recovery

We recommend that you perform periodic backups of your CA CSM environment if there is a disaster.

Before you start the disaster recovery process, back up all SMP/E environments and data sets managed by CA CSM.

When you perform disaster recovery, you perform the following steps:

1. Recover all SMP/E environments that CA CSM manages.
2. Recover CA CSM itself.

CA CSM has to be recovered into an environment identical to the one that CA CSM was initially installed in. That is, the following configuration settings on the recovery system must be the same as on the original system:

- Operating system settings, such as TCP/IP ports, DASDs, and HLQs
- Settings of APF-authorized data sets required for CA CSM
- Java

  Note: The Java version must be supported by CA CSM.
- TCP/IP configuration, host names, IP addresses, and CAICCI SYSID of systems that are specified in deployment

Notes:

- The SAF settings for the recovery system must contain all changed SAF settings that were used when setting up CA CSM.
- Periodic backups of the CA Datacom/MSM database data areas, using the CA Datacom/DB utility function DBUTLTY, lets you safeguard your CA Datacom/MSM data during scheduled or unscheduled events that can impact accessibility to your product. For more information about how to reorganize your database, see the *Best Practices Guide*.

How You Back Up CA CSM

CA CSM backup is a several-step process.

Note: For backup, select and use a method that is appropriate for your site and environment. Managing the backup should be a part of your disaster backup routine.

Follow these steps:

1. Stop the CA CSM application server (see page 151).
2. Back up the following operating system settings:
   - Settings of the operating system such as ports, DASDs, HLQs
   - Java

     Note: The Java version must be supported by CA CSM.
   - TCP/IP
   - SAF

   Note: CA Datacom/MSM SVC is expected to be the same, and a list of APF-authorized data sets is preserved.
3. Obtain a list of data sets representing deployment file systems, software catalog file systems, and so on. The data sets are stored in the mountpoint table, the MP_DATASET column.

   Note: To obtain a list of the data set, you can submit JCL that runs a SQL statement (see page 65).
4. Stop the CA Datacom/MSM server and the MUF.
5. Back up the following CA CSM data sets:
   - Data sets representing mount points

     If you did not allocate individual file systems for these mount points, perform the following steps:

     a. Unmount all file systems that are mounted under the following file systems if they exist:

     ```
     /u/users/msmserv/msminstall
     /u/users/msmserv/msm
     /u/users/msmserv/msmruntime
     /u/users/msmserv/mpm
     ```

     b. Back up the directory structure corresponding to /u/users/msmserv.
   - All the data sets that you obtained from the mountpoint table.
   - All data sets under HLQs (CSIHLQ, TargetHLQ, DlibHLQ, DatabaseHLQ, and RunTimeMVSHLQPrefix) specified in the options file (MSMSetupOptionsFile.properties).

JCL for Executing SQL Statements

The following sample is an example of JCL that you can submit to run the SQL statement that discovers the content of the mountpoint table:

```
//*****************************************************************************
//*****************************************************************************
//*                                                                           *
//*JOBLIB DD DSN=HLQ.CUSLIB replace HLQ with HLQ of your CA CSM installation  *
//*          DSN=HLQ.CAAXLOAD replace HLQ with HLQ of your CA CSM installation*
//*                                                                           *
//*****************************************************************************
//*****************************************************************************
//B2UP     OUTPUT DEST=LOCAL,JESDS=ALL,DEFAULT=Y,
//         PAGEDEF=32D3,CHARS=GT20,FORMDEF=P2B111
//JOBLIB   DD DSN=HLQ.CUSLIB,
//         DISP=SHR
//         DD DSN=HLQ.CAAXLOAD,
//         DISP=SHR
//         DD DSN=SYSDEV.CCS.LINKLIB,
//         DISP=SHR
//         DD DSN=CEE.SCEERUN,DISP=SHR
//         DD DSN=CEE.AIGZMOD1,DISP=SHR
//*
//SQLEXEC  EXEC PGM=DBSQLPR,
//       PARM='prtWidth=1500,inputWidth=80'
//SYSUDUMP DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//STDERR   DD  SYSOUT=*
//STDOUT   DD  SYSOUT=*
//OPTIONS  DD  *
AUTHID=CASWMGT
/*
//SYSIN    DD  *
   SELECT MP_DATASET
   FROM MOUNTPOINT WHERE NOT MP_TYPE='PRODUCT' OR MP_TYPE IS NULL;
/*
```

The following sample is a fragment of output that you receive after submitting the JCL for discovering the content of the mountpoint table:

```
Command Line Options

____________________
INPUTWIDTH=80
PRTWIDTH=1500
Option File Options

___________________
AUTHID=CASWMGT
```

```
INPUT STATEMENT:
SELECT MP_DATASET
   FROM MOUNTPOINT WHERE NOT MP_TYPE='PRODUCT' OR MP_TYPE IS NULL;
MP_DATASET
VARCHAR(45)
_____________________________________________
OMVSUSR.CAMSM.APLROOT
OMVSUSR.CAMSM.LJWK
OMVSUSR.CAMSM.MSMT1
OMVSUSR.CAMSM.MSMT3
...
```

The data sets that are returned after the input statement are the data sets that you have to back up:

```
OMVSUSR.CAMSM.APLROOT
OMVSUSR.CAMSM.LJWK
OMVSUSR.CAMSM.MSMT1
OMVSUSR.CAMSM.MSMT3
```

How You Recover CA CSM from the Backup

To recover CA CSM from the backup, perform the following steps:

1. Recover operating system settings.
2. Recover CA CSM data sets.
3. Start CA CSM (see page 57).

Stop CA CSM

If you want to stop CA CSM (for example, during maintenance), you stop CA CSM in the reverse order as you start CA CSM (see page 57).

Follow these steps:

1. Enter the following z/OS system command:

   ```
   P MSMTC
   ```

   The CA CSM application server (see page 151) has successfully terminated, the following message appears in the system console:

   ```
   MSM0011I CA CSM HAS TERMINATED SUCCESSFULLY
   ```

   Note: If this message does not appear, CA CSM has failed to stop its operation. Force a shutdown using the following command:

   ```
   F MSMTC,APPL=FORCESHUTDOWN
   ```

After the forced shutdown has completed, the following message appears in the system console:

```
MSM0012W CA CSM TERMINATION WAS FORCED
```

Important! If you force a shutdown, some of your data may be lost. Therefore, use this method only if the standard stop method is not working.

The Tomcat job stops after CA CSM application server is terminated.

2. Submit the MSMDBSVP JCL member or start the MSMDBSRP PROCLIB member.

   The CA Datacom/MSM server stops.

   Note: Alternately, based on your security access, you can enter the following command. Replace *started_task_name* with the MUF database server job name and the MUF job name.

   - For z/OS:

     ```
     F started_task_name,EOJ
     ```

   - For CA SYSVIEW:

     ```
     MVS F started_task_name,EOJ
     ```

   - For System Display and Search Facility (SDSF):

     ```
     /F started_task_name,EOJ
     ```

3. Submit the MSMMUFP job or started task.

   The MUF stops, and CA CSM stops operation.

Chapter 5: Additional Administration Tasks

This section contains the following topics:

Send a Message to Current Users

You can use a z/OS modify command to send a message to a single user or all users who are logged in to the CA CSM web-based interface. For example, before you shut down CA CSM for maintenance, you can send a message to all CA CSM users that are logged in to the CA CSM application server to let them know that CA CSM is about to shut down.

To send a message to all CA CSM users currently logged in, enter the following command:

```
/F jobname,APPL=MSG,message text
```

Note: To send a message to a single user, add their TSO user ID, for example:

```
/F jobname,APPL=MSG,TSOuserID,message text
```

jobname

Specifies the name of the CA CSM application server on your system.

APPL=MSG

Specifies to the CA CSM address space to process this modify request as a messaging request.

TSOuserID

(Optional) Specifies the TSO user ID of the person you want to send the message to. If the TSO user ID is not included, the message is sent to all users who are currently logged in to the server.

message text

Specifies a body of a message. Enter free format message text to display to all users logged in to the CA CSM application server, or, if the TSO user ID is included, a single user.

Limitations: Do not include commas, even if you are using quotes for the message text itself.

Sample JCL to Send Message to Users

The following sample JCL shows how to send a message to all users logged in to CA CSM, and to a single CA CSM user with a TSO user ID of DOEJON01:

```
Proclib member INFORMSM below:

//***************************************************************************
//*****                                                                 *****
//*****  Send Message to CA CSM users                                  *****
//*****                                                                 *****
//*****  SERVER= is the number of the server to receive message.        *****
//*****  MSMMSG= is the message you want sent to the server user(s)     *****
//*****                                                                 *****
//*****  EXAMPLE JCL shown below how to send message to ALL users       *****
//*****                                                                 *****
//*****  /*JOBPARM SYSAFF=MACHINE31                                     *****
//*****  //          EXEC INFORMSM,SERVER=2,                            *****
//*****  // MSMMSG='CA CSM - IS SHUTTING DOWN - RESTART REQUESTED'     *****
//*****                                                                 *****
//*****  EXAMPLE JCL shown below how to send message to a CA CSM User  *****
//*****                                                                 *****
//*****  /*JOBPARM SYSAFF=MACHINE31                                     *****
//*****  //          EXEC INFORMSM,SERVER=2,                            *****
//*****  // MSMMSG='DOEJON01,TEST MESSAGE FROM JCL'                     *****
//*****                                                                 *****
//***************************************************************************
//*
//INFORMSM  PROC  MSMMSG=,
//             SERVER=
//*
//OPSCMD   EXEC PGM=OPSCMD,PARM='F MF2T&SERVER.SRV,APPL=MSG,&MSMMSG.'
//*
//OPS$OPSP DD DUMMY         Direct request to production subsystem OPSP
//*
//INFORMSM  PEND
//*
```

```
JCL to send message Below:

//INFORM5S  JOB (129300000),'Inform CA CSM user',
//        COND=(4,LT),
//        CLASS=A,
//        MSGCLASS=X,
//        NOTIFY=&SYSUID,
//        MSGLEVEL=(1,1)
//*
/*JOBPARM SYSAFF=MACHINE31
//*
// JCLLIB ORDER=(MF20.MSM.PROCLIB)
//*
//*********************************************************************
//*****                                                           *****
//*****  send message to CA CSM server user(s)                   *****
//*****                                                           *****
//*********************************************************************
//*
//          EXEC INFORMSM,SERVER=5,
// MSMMSG='CA CSM - Server is closing down in fifteen minutes       '
//          EXEC INFORMSM,SERVER=5,
// MSMMSG='CA CSM - Server will be restarted soon after             '
//
//*
// MSMMSG='DOEJON01, send a message to a user on a CA CSM server    '
//*
```

Check for Executing Tasks

Before you bring down CA CSM, be aware of executing tasks and the impact of ending them abruptly. The users that started those tasks may no longer be logged in to CA CSM.

Follow these steps:

1. Log in to the CA CSM web-based interface, click the Tasks tab, and ensure that the Current Tasks subtab is selected.

   The Tasks page appears showing only your tasks.

2. Select All tasks from the Show drop-down list.

   A list of all tasks appears.

3. Check the status of tasks, and if any have a status of Executing, consider contacting the owner of the task before you bring down CA CSM.

Reassign the Java Home Directory

You may want to reassign the Java home directory, for example, when you install a new minor version of Java into a different directory to preserve the old version. When you change the Java directory, correct the Java path in the following places:

- Change the value of the JAVA_HOME variable in the SAMPLIB(MSMLIB) member.

  Example: In the following sample SAMPLIB(MSMLIB) member, replace *original_path* with the new path.

  ```
  export JAVA_HOME=original_path
  ```

- Change the SMPJHOME DDDEF value in the CA CSM CSI that points to the Java home directory. The CA CSM CSI is located in CSIHLQ.SMPCSI.CSI. Change the SMPJHOME DDDEF value in the global (GLOBAL), target (CAIT0) and distribution (CAID0) zones. Use the UCLIN statement to change the SMPJHOME DDDEF value.

  Example: Use this UCLIN statement to change the SMPJHOME DDDEF value for all CA CSM CSI zones by replacing the zone variable with each zone name: CAID0, CAIT0, and GLOBAL.

  ```
  SET
  BOUNDARY(zone).
  UCLIN.
  REP  DDDEF(SMPJHOME)
       PATH('new_path').
  ENDUC.
  ```

Note: Once you start the MSMTC job, the JAVA_HOME path in the job log message has to match the path in the SMPJHOME DDDEF in the CA CSM CSI:

```
JVMJZBL1006I JAVA_HOME = new_path
```

- Change the JAVAPATH option in the MSMSetupOptionsFile.properties option file that is located in the *MSMPATH*/CEGPHFS directory.

  Example: In the following MSMSetupOptionsFile.properties option file sample, replace *original_path* with the new path.

  ```
  JAVAPATH=original_path
  ```

Chapter 6: SCS Address Space Administration

The *SCS address space* is a specially defined location where the system registry and commands for interrogating output and console traffic reside within the operating system. The SCS address space provides the services and processing necessary to implement configurations across your targeted z/OS systems. Each target system that is expected to support SCS processing must execute an SCS address space.

This section contains the following topics:

SCS Address Space Operation Considerations

This section contains the following topics:

Authorized Program Facility

Important! In SCS address space documentation, all references to the SYS1.PARMLIB data set indicate any data set that is defined in the logical PARMLIB concatenation.

Use the Authorized Program Facility (APF) to identify programs that use sensitive system functions. The SCS address space must be started as an APF-authorized job step. The SCS address space load library must be APF-authorized on each z/OS system where the SCS address space is started.

To ensure that the SCS address space is started as an APF-authorized job step, APF-authorize all libraries you include in the SCS address space STEPLIB concatenation. Putting a library in the concatenation that is not APF-authorized causes the entire library concatenation to lose its APF-authorization.

The APF lists are in the SYS1.PARMLIB member PROG*xx*. The lists contain the names of APF-authorized libraries. The order of the entries in the lists is not significant.

If you use the PROG*xx* members with dynamic format, you can issue the z/OS command SET PROG=*xx.* The changes take effect before the next IPL.

Note: For more information about APF lists, see the *IBM Initialization and Tuning Reference*.

Auxiliary Address Space

An initial auxiliary address space is created from a service request that the SCS address space makes. More auxiliary address spaces are created as needed.

The auxiliary address spaces are created and managed dynamically, depending on the level of concurrent configuration requests. They handle service requests on behalf of the SCS address space.

The SCS address space performs service requests on behalf of a user who is implementing a configuration. The SCS address space creates the auxiliary address spaces and schedules service requests to the auxiliary address spaces once they are active. The auxiliary address space executes the requests and the results are returned to the SCS address space.

Auxiliary Address Space Operation

The SCS address space automatically creates an auxiliary address space, when needed, to schedule a request. The auxiliary address space executes in a workload manager (WLM) dependent enclave that the SCS address space creates. If there are scheduled services, all SCS auxiliary address spaces remain active. When there are no more requests to run, the inactive auxiliary address spaces are stopped.

Note: The SCS address space creates and manages up to 20 auxiliary address spaces depending on the number of concurrent service requests processed.

You can specify SCS address space parameters to limit the maximum number of concurrently active auxiliary address spaces to a number less than 20.

You do not have to perform automated operations for the auxiliary address spaces; the SCS address space dynamically initiates them. In the unlikely event that the SCS address space fails, all auxiliary address spaces stop.

Encrypted Communications

To enable encrypted communications with the SCS address space, configure one of the following encryption methods:

- IBM System Secure Socket Layer (SSL)
- IBM Application Transparent Transport Layer Security (AT-TLS)

If a connection is made to the SCS address space from the web-based interface remote host, the address space detects the use of System SSL or IBM AT-TLS. If neither method is detected, the communication with the web-based interface is performed in clear text.

Implement Support for SSL Transmission

Set up the SCS Address Space to use *one* of the following:

- IBM System Secure Socket Layer (SSL) toolkit using a key store file that is located on a Hierarchical File System (HFS).

  Note: Execute the program *gskkyman* under OMVS at a shell prompt. Executing this program creates a key store file on the HFS, generates a self-signed certificate authority certificate, and generates a server certificate.

- External Security Manager (ESM)

  Note: Generate a server certificate by executing the commands of your ESM.

Create a Key Store File

You can create a key store file on zFS or HFS when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.
2. Select Create new database and enter the path and file name to the new key store file or database.

   Note: The path and file names must be writeable path/file names.

3. Enter a database password and enter the password expiration in days.

   Note: Press ENTER if the password never expires.

4. Enter **5000** for the database record length and enter **0** for the database mode.
5. Wait for acknowledgment that the key database is created.
6. Select Exit program.

   The key store file is created.

Create a Self-Signed Certificate Authority Certificate

You can create a self-signed certificate authority certificate when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.
2. Select Open database, enter the path to the database that you created, and enter the database password.

   The Key Management menu appears.
3. Select Create a self-signed certificate.
4. Select certificate authority certificate with 1024-bit RSA key and select SHA-512.

   Note: Selecting certificate authority certificate with 1024-bit RSA key creates the certificate authority.
5. Enter a label for the self-signed certificate authority certificate and enter a common name.

   Note: The common name can be the same as the label.
6. Provide data for the prompts regarding ownership of the certificate. Ownership includes the following data:
   - Organizational unit
   - Organization
   - Organization city, state, and country
7. Enter the number of days the certificate is valid and enter **0** to continue.
8. Wait until the certificate is created.
9. Select Exit program.

   The self-signed certificate authority certificate is created.

Create a Server Certificate

You can create a server certificate when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.
2. Select Open database, enter the path to the database that you created, and enter the database password.

   The Key Management menu appears.

3. Select Manage keys and certificates, and enter the number of the certificate authority certificate to use.

   Note: You can use the number that you previously created.

4. Select Create a Signed Certificate and Key, and select User or server certificate with 1024-bit RSA key.

5. Enter a label for the server certificate and enter a common name.

   Note: The common name can be the same as the label.

6. Provide data for the prompts regarding ownership of the certificate. Ownership includes the following data:

   - Organizational unit
   - Organization
   - Organization city, state, and country

7. Enter the number of days the certificate is valid and enter **0** to continue.

8. Wait until the certificate is created.

9. Select Exit program.

   The server certificate is created.

Set the Server Certificate as the Default Certificate

You can set the server certificate as the default certificate when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.

2. Select Open database and enter the path to the database you created.

3. Enter the database password.

   The Key Management menu appears.

4. Select Manage keys and certificates and enter the number of the label for the server certificate.

5. Select the option to set the key as default.

6. Select Exit program.

   The server certificate is set as the default certificate.

Export the Certificate Authority Certificate

You can export the certificate authority certificate when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.
2. Select Open database and enter the path to the database that you created.
3. Enter the database password.

   The Key Management menu appears.
4. Select Manage keys and certificates and enter the number of the label for the certificate authority certificate to export.
5. Select Export certificate to a file and select Binary ASN.1 DER.
6. Enter the path name and file to export the certificate to and press Enter.
7. Select Exit program.

   The certificate authority certificate is exported.

Store the Database or Key Store Password Into a Stash File

You can store the database or key store password into a stash file when setting up the SCS address space to use SSL.

Follow these steps:

1. From a mainframe console, execute *gskkyman*.
2. Select Open Database and enter the path to the database that you created.
3. Enter the database password and select Store Database Password.

   The file, database_*name*.sth, is stored where the database file is stored.
4. Select Exit program.

   The database or key store password is stored into a stash file.

Import the Certificate Authority Certificate Into a Java Key Database

You can import the certificate authority certificate into a Java key database when setting up the SCS address space to use SSL.

Follow these steps:

1. Execute the keytool program that came with your Java SDK installation in superuser mode.
2. Enter the keystore password.

   Default: changeit
3. Enter yes to trust the certificate.

   Note: If the certificate is added successfully, then the configuration is complete.

   The certificate authority certificate is imported into a Java key database.

Example: Execute the keytool program

The following sample is an example of how to execute the keytool program:

```
keytool –import –trustcacerts –file /path/to/exported/ca/certificate –keystore
$JAVA_HOME/lib/security/cacerts
```

Set Up to Use System SSL

For the SCS address space to use System SSL, the PDSE member GSKSSL must be accessible to the program by one of two methods:

- Adding the PDSE named *pdsename*.SIEALNKE to the dynamic LPA (PROG*xx* member).

  Note: For more information about setting up System SSL, see the IBM guide, *z/OS Cryptographic Service System Secure Sockets Layer Programming.*
- Modifying the PROCLIB member containing the JCL procedure that is used to start the SCS address space. The name is commonly MSMCPROC (see page 153). Include a reference to *pdsename*.SIEALNKE by adding a DD statement for STEPLIB.

Go to the SCS address space configuration XML and enable SSL in the address space.

Once you have created the certificate authority certificate and server certificate, modify the parameter file that is named *MSMCPARM* (see page 89) for the SCS address space.

Default: MSMCPARM

Locate the SSL tag in the XML document, and set the keyring attribute to the key store/database file. Set the stashfile attribute to the equivalent stash file.

Update the SCS address space configuration XML by setting the keyring and stashfile in the SSL element of the XML document to point to the keystore database and password stash file.

Implement Support for AT-TLS Transmission

Application Transparent Transport Layer Security (AT-TLS) is a component of z/OS that provides encryption services for applications that exchange sensitive data but have not been instrumented to include encryption. This service lets you encrypt data being sent to the application without adding the extra API calls to do encryption.

To use the AT-TLS with the SCS address space, you must have completed the following:

- Configuration of the Communications Policy Agent
- Configuration of AT-TLS policies
- Installation of Server Certificate and Certificate Authority Certificate

Note: For more information about IBM Policy Agent, see the *IBM z/OS V1R11 Communications Server TCP/IP Implementation Volume 4: Security and Policy-Based Networking*.

Operator Communications Interface

z/OS operator commands are used to control the operation of the SCS address space.

You can control the groups of users who can issue operator commands. Use CA ACF2 for z/OS, CA Top Secret for z/OS, or IBM RACF to authorize or restrict users from issuing some or all commands.

To control the use of operator commands, create profiles in the SAF OPERCMDS class.

The command descriptions describe the authorization requirements for the command. In most cases, more than one level of authority is required and the user issuing the command must have all indicated access privileges.

SCS Address Space Operator Commands

This section contains descriptions of the commands that the SCS address space supports.

START Command—Start the SCS Address Space

The START command starts the SCS address space. You can enter START or the S abbreviation. You must have UPDATE authority to the SAF OPERCMDS class resource named *MVS.START.STC.procname* to use this command.

Note: Do not start the MSMCAUX procedure manually. The MSMCAUX procedure is started by the SCS address space (MSMCPROC).

The START command guidelines are as follows:

- START command parameter values override the JCL EXEC statement PARM keyword parameter values.
- Separate the keywords with two or more parameters with a comma or a space.
- Separate the keywords with two or more subparameters with a comma or a space.
- Parameters are specified as keyword parameters. Subparameters of a keyword can be positional.
- Parameters can be specified in any order.
- Parameter strings can include comments any place there is a space. Begin a comment with the starting comment delimiter (/*). (Optional) End the comments with the ending comment delimiter (*/).
- Parameters that are specified incorrectly are ignored.

This command has the following format:

```
Start procname[,,,(start_parameters)][,REUSASID=YES][,PARMS='exec_parameters']
```

procname

Specifies the name of the system PROCLIB member containing the JCL procedure that is used to start the SCS address space. The name is commonly MSMCPROC (see page 153).

,,,(*start_parameters*)

(Optional) Specifies the START command parameters (see page 88) for the SCS address space. The START command parameter values override the JCL EXEC statement PARM parameter values.

,REUSASID=YES

(Optional) Specifies that z/OS assigns a reusable address space identifier (ASID) to the SCS address space.

,PARMS=’*exec_parameters*’

(Optional) Specifies overriding the JCL EXEC statement PARM parameters (see page 88) for the SCS address space with the parameters you specify. The exec_parameter values that you specify override the JCL EXEC statement PARM parameter values.

Examples: Start the SCS Address Space

These examples identify how to start the SCS address space using the START command.

```
S MSMCPROC,REUSASID=YES,PARMS='CONFIG(SCSPARMS)'
```

```
S MSMCPROC,,,(CONFIG(SCSPARMS)),REUSASID=YES
```

SCS Address Space Initialization

The SCS address space is initialized when the following message is received:

```
MSMC0002I SCS initialization complete. SYSNAME=system_name, CCINAME=CAICCI_name
```

The SCS address space is fully operational when the following messages are received:

```
MSMC0423I Task MSMCIENG database connection opened
MSMC0424I Task MSMCFCOM database connection opened
```

To verify that the SCS address space is listening for connections, look for the following messages:

```
MSMC0617I The SCS address space is now listening for connections on the UNIX socket
MSMC0618I The SCS address space is now listening for connections on the INET/INET6
socket, port nnnn
```

STOP Command—Stop the SCS Address Space

The STOP command initiates the normal termination of the SCS address space. You can enter STOP or the P abbreviation. Provide CONTROL authority to the SAF OPERCMDS class resource named CAMSMSCS.STOP to use this command.

To authorize, use one of the following methods, depending on how the SCS address space was started:

- If the SCS address space was started as a started task, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.STOP.STC.procname.
- If the SCS address space was started as an initiated job, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.STOP.JOB.jobname.

This command has the following format:

```
stoP jobname
```

jobname

Specifies the SCS address space started task or initiated job name. The common name is MSMCPROC (see page 153).

Example: Stop the SCS Address Space

This example identifies how to stop the SCS address space using the STOP command.

```
P MSMCPROC
```

MODIFY Command—Modify the SCS Address Space

The MODIFY commands are used to control the operation of the SCS address space. You can enter MODIFY or the F abbreviation.

To authorize, use one of the following methods, depending on how the SCS address space was started:

- If the SCS address space was started as a started task, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.STC.*procname*.
- If the SCS address space was started as an initiated job, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.JOB.*jobname*.

The MODIFY commands are:

- ABEND
- DUMP
- STOP

The MODIFY command specifications are as follows:

- Parameters are specified as keyword parameters. Subparameters of a keyword can be positional.
- Parameters can be specified in any order.
- Parameter strings can include comments anywhere a space could appear. Start a comment with the starting comment delimiter (/*). (Optional) End the comment with the ending delimiter (*/).
- Separate the keywords with two or more specified parameters (each keyword with optional value) with a comma or a space.
- Separate the keywords with two or more subparameters with a comma or a space.

  Note: Ending a comment delimiter is optional if the comment is at the end of the parameter string.

MODIFY ABEND Command—Initiate Abnormal Termination of the SCS Address Space

The MODIFY ABEND command is used to initiate the abnormal termination of the SCS address space. You can enter MODIFY or the F abbreviation. Provide CONTROL authority to the SAF OPERCMDS class resource named CAMSMSCS.ABEND to use this command.

To authorize, use one of the following methods, depending on how the SCS address space was started:

- If the SCS address space was started as a started task, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.STC.procname
- If the SCS address space was started as an initiated job, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.JOB.jobname

This command has the following format:

```
modiFy jobname,ABEND
```

jobname

Specifies the SCS address space started task or initiated job name. The name is commonly MSMCPROC (see page 153).

Example: Modify the SCS Address Space using MODIFY ABEND command

This example identifies how to modify the SCS address space using the MODIFY ABEND command.

```
F MSMCPROC,ABEND
```

MODIFY DUMP Command—Capture an SVC Dump of the SCS Address Space

The MODIFY DUMP Command is used to capture an SVC dump of the SCS address space. You can enter MODIFY or the F abbreviation. Provide CONTROL authority to the SAF OPERCMDS class resource named CAMSMSCS.DUMP to use this command.

To authorize, use one of the following methods, depending on how the SCS address space was started:

- If the SCS address space was started as a started task, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.STC.*procname*.
- If the SCS address space was started as an initiated job, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.JOB.*jobname*.

This command has the following format:

```
modiFy jobname,DUMP[ASID(asid_list)]JOBNAME(job_list)[DSPNAME(dsp_list)]
```

jobname

Specifies the SCS address space started task or initiated job name. The common name is MSMCPROC (see page 153).

Default: The SCS address space if the JOBNAME is not specified.

ASID (*asid_list*)

(Optional) Specifies the address space identifier operator input (see page 86) of one or more address spaces to include in the dump.

Limits: 1-32767 decimal range or 1-7FFF hexadecimal range

Default: The SCS address space if the ASID parameter is not specified.

JOBNAME (*job_list*)

Specifies the name of one or more address spaces to include in the dump.

Note: The *jobname* can include wildcard characters with a question mark (?), or an asterisk (*). A question mark indicates a single mask character. An asterisk indicates a 0 or more mask characters.

Limits: 1-8 characters that are expressed as a quoted, *'abc'*, or a nonquoted, *abc*, character string. A separator or delimiter indicates the end.

DSPNAME (*dsp_list*)

(Optional) Specifies the data space identifier (see page 87) of one or more data spaces to include in the dump.

Default: The data spaces that are owned by the SCS address space if the DSPNAME is not identified

Note: Wildcard characters that are used in the JOBNAME and DSPNAME parameters can result in multiple address spaces being selected for inclusion in the dump.

Example: Dump the SCS address space and the Auxiliary address spaces using MODIFY DUMP command

This example identifies how to dump the SCS and Auxiliary address spaces using the MODIFY DUMP command.

```
F MSMCPROC,DUMP JOBNAME(MSMCPROC,MSMCAUX)
```

MODIFY STOP Command—Initiate Normal Termination of the SCS Address Space

The MODIFY STOP command is used to initiate the normal termination of the SCS address space. You can enter MODIFY or the F abbreviation. Provide CONTROL authority to the SAF OPERCMDS class resource named CAMSMSCS.STOP to use this command.

Note: The results of the STOP command and the MODIFY STOP command are identical.

To authorize, use one of the following methods, depending on how the SCS address space was started:

- If the SCS address space was started as a started task, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.STC.*procname*.
- If the SCS address space was started as an initiated job, provide UPDATE authority to the SAF OPERCMDS class resource named MVS.MODIFY.JOB.*jobname*.

This command has the following format:

```
modiFy jobname,STOP
```

jobname

Specifies the SCS address space started task or initiated job name. The common name is MSMCPROC (see page 153).

Example: Modify the SCS Address Space using MODIFY STOP command

This example identifies how to modify the SCS address space using the MODIFY STOP command.

```
F MSMCPROC,STOP
```

SCS Address Space ASID Operator Input Examples

The following example shows the SCS address space ASID operator input value that is expressed as a hexadecimal digit (A-F, 0-9):

```
X'nnnn'
```

The following example shows the SCS address space ASID operator input value that is expressed as a decimal digit (0-9):

ddddd

If the following address spaces exceed 15 when combined, only the first 15 are included in the dump:

- SCS address space
- Address spaces that the ASID parameter specifies
- Address spaces that the JOBNAME parameter specifies
- Address spaces owning the data spaces that the DSPNAME parameter specifies

SCS Address Space Data Space Identifier Input

The accepted data space identifier input designators are as follows:

asid.name

Specifies the hexadecimal address space identifier (ASID) of the owning address space and the *data_space_name* of the data space to include in the dump.

Limits: 1-7FFF hexadecimal range (ASID)

Default: SCS address space ASID and data spaces

Note: The first character of the specified ASID value must be a decimal digit. If the first significant digit of the ASID of the owning address space is not a decimal digit, specify the ASID with a leading zero.

jobname.name

Specifies the *jobname* of the owning address space and the *data_space_name* to include in the dump. The *jobname* can include wildcard characters with a question mark (?), or an asterisk (*). A question mark indicates a single mask character. An asterisk indicates a 0 or more mask characters.

Limits: 1-8 nonquoted characters

Note: No more than 256 data spaces are included in the dump. The wildcard characters that are used in the parameters could result in multiple data spaces being selected for inclusion in the dump.

If a data space is owned by an address space that is not included in the dump, add the address space of the ASID to the list of included address spaces. A maximum of 15 address spaces are allowed. The address space limitation could prevent specifying as many as 256 data spaces.

JCL EXEC Statement PARM Keyword and START Command Parameters

The SCS address space parameters are specified in a parameter library member. Sometimes, the SCS address space parameters are specified with the following elements:

- The PARM keyword parameter of the JCL EXEC statement in the address space startup JCL
- The START command that is used to start the SCS address space

Parameters that can be specified with the PARM keyword parameter of the JCL EXEC statement and with the START command are identical.

If the SCS address space parameters are specified using one of these alternate methods, adhere to the following guidelines:

- START command parameter values override the JCL EXEC statement PARM keyword parameter values.
- Separate the keywords with two or more parameters with a comma or a space.
- Separate the keywords with two or more subparameters with a comma or a space.
- Parameters are specified as keyword parameters. Subparameters of a keyword can be positional.
- Parameters can be specified in any order.
- Parameter strings can include comments any place there is a space. Begin a comment with the starting comment delimiter (/*). Optionally, end the comments with the ending comment delimiter (*/).
- Parameters that are specified incorrectly are ignored.

The parameters that are used with the JCL EXEC Statement PARM keyword parameter and START command are as follows:

CONFIG(*name)*

Specifies the name of the parameter library member containing the SCS address space configuration parameters.

Limits: 1-8 characters that are expressed as a quoted, *'abc'*, or a nonquoted, *abc*, string. A separator or delimiter indicates the end.

Default: MSMCPARM when CONFIG is not specified.

ROUTCDE(*routing code list*)

Specifies a routing code or a range of routing codes that are assigned to WTO messages.

Two values that are separated by a dash (-) specify an inclusive range of routing codes.

Routing codes that are specified are in addition to the specific routing codes defined for each message.

Limits: 1-128

Example: *ddd* (where *d* is a valid decimal digit (0-9))

CASE(MIXED|UPPER)

Specifies if WTO messages are written using mixed or uppercase only characters.

MIXED

The WTO messages can be written in mixed uppercase and lowercase characters.

UPPER

The WTO messages can be written using uppercase characters.

Default: MIXED

DAE(YES|NO)

Specifies if DAE dump suppression is allowed or prevented.

YES

DAE dump suppression is allowed.

NO

DAE dump suppression is prevented.

Default: YES

Parameter Libraries

SCS address space parameters are specified as configuration parameters in a member of the parameter library.

The parameter library is the data set or data sets allocated to the MSMPARM DD statement in the SCS address space JCL procedure.

The parameter library must be a partitioned data set or a concatenation of partitioned data sets and each partitioned data set must have variable-length records. Each parameter library member contains an XML document that specifies the address space parameters and contains various elements.

To facilitate using common configuration parameters for multiple instances of the SCS address space, configuration parameters in a member of a parameter library can contain z/OS system symbols.

Note: CA CSM includes the MSMCPARM parameter library member, which contains the default SCS address space parameters.

MSMCPARM Member

You can include the following elements in the MSMCPARM member documents that specify the address space parameters:

Data Recovery Parameters

Sets the parameters that are related to the SCS address space use of disk storage for data recovery purposes. The parameters are used when allocating data sets created to save existing data for recovery purposes.

The Data Recovery Parameters are specified using the following attributes:

dsnhlq

Specifies the data set name high-level qualifier that is used when allocating data sets created for data recovery purposes.

Limits: 1-17 bytes. The value can include static and dynamic system symbols and installation defined static system symbols.

Note: See the IBM *z/OS MVS Initialization and Tuning Reference* guide for a list of system symbols.

(Optional) *&SYSUID*

Specifies the user ID of the CA CSM user that initiated the configuration request for which data sets are created for recovery purposes.

Limits: The ampersand character (&) cannot be specified as a literal in the attribute value of an XML document. The character must be used to convert subsequent characters to a control sequence using the character string *'&amp;'*.

Example: '&SYSNAME..MSM', dsnhlq='&amp;SYSNAME..MSM'

Default: &SYSUID..MSMDATA

unit

Specifies unit name that is used when allocating z/OS data sets created for data recovery purposes.

Limits: 1-8 bytes

Default: None

volser

Specifies the volume serial number that is used when allocating data sets created for data recovery purposes.

Limits: 1-6 bytes. The characters of the serial number must be alphabetic, national, or a hyphen.

Default: None

mgmtclas

Specifies the SMS management class that is used when allocating data sets created for data recovery purposes.

Limits: 1-8 bytes. The first character of the class name must be alphabetic or national. The remaining characters must be alphanumeric or national.

Default: None

storclas

Specifies the SMS storage class that is used when allocating data sets created for data recovery purposes.

Limits: 1-8 bytes. The first character of the class name must be alphabetic or national. The remaining characters must be alphanumeric or national.

Default: None

TCP/IP

Specifies the address space parameters for the interface between the SCS address space and TCP/IP for communicating with other components of CA CSM.

The TCP/IP parameters are specified using the following attributes:

ipaddr

Specifies the IP address of the interface through which the SCS address space accepts TCP connection requests from other CA CSM components.

Limits: IPv4 address using standard dotted decimal notation.

(Optional) IPv6 address using one of the standard text forms that are defined in RFC 4291, IPv6

Example 1: 0.0.0.0

Example 2: ::

Note: The IPv4 unspecified address, 0.0.0.0, is used to indicate that the SCS address space accepts TCP connection requests through all IPv4 interfaces. The IPv6 unspecified address, :: , can be used to indicate that the SCS address space accepts TCP connection requests through all IPv4 and IPv6 interfaces.

Default: ::

port

Specifies the port number the SCS address space uses to listen for TCP connection requests from other CA CSM components.

Limits: 65535

Default: 49152

Console

Sets the parameters that are related to the SCS address space usage of extended MCS consoles that issue z/OS commands, receive command responses, and receive unsolicited message traffic.

The console parameters are specified using the following attributes:

prefix

Used in the construction of extended MCS console names.

Limits: 1-5 bytes. The first character must be alphabetic or national. The remaining characters must be alphanumeric or national.

Default: CAMSM

auth

Specifies the authority the extended MCS consoles have to issue z/OS commands.

The assigned authority specifies the commands that can be entered from the console. Separate multiple values with a blank space or a comma.

Enter one or more of the following values from the console:

MASTER

Allows the consoles to act as a master console, which issues all MVS commands.

ALL

Allows the consoles to issue system control commands, input/output commands, console control commands, and informational commands.

SYS

Allows the consoles to issue system control commands and informational commands.

IO

Allows the consoles to issue input/output commands and informational commands.

CONS

Allows the consoles to issue console control commands and informational commands.

INFO

Allows the consoles to issue informational commands.

Default: INFO

Note: SYS, IO, and CONS can be specified together in any combination. All others are mutually exclusive.

See the IBM *z/OS MVS System Commands Reference* guide for information about which commands can be entered from a console with a specific authority level.

Note: The security product settings override the console command authority settings for z/OS commands that a security product protects. For example, CA ACF2 for z/OS, if the OPERCMDS class is active and a profile is defined to protect the command.

SAF

Sets the parameters that are related to the SCS address space interface to the System Authorization Facility (SAF).

The SAF parameters are specified using the following attributes:

application

Specifies the application name that is assigned to the SCS address space.

Limits: 1-8 bytes. The first character must be alphabetic or national. The remaining characters must be alphanumeric or national.

Default: MSMCAPPL

requestor

Specifies the name that is assigned to the SCS address space that assigns a unique control point within a set of control points that exist in a subsystem.

Note: If you specify a requestor name and IBM RACF is installed, update the IBM RACF router table with a matching entry. If you do not update the table, IBM RACF processing is bypassed.

Limits: 1-8 bytes. The first character must be alphabetic or national. The remaining characters must be alphanumeric or national.

Default: None

subsystem

Specifies the subsystem name, version, and release level that are assigned to the SCS address space.

Note: If you specify a subsystem name and IBM RACF is installed, update the IBM RACF router table with a matching entry. If you do not update the table, IBM RACF processing is bypassed.

Limits: 1-8 bytes. The first character must be alphabetic or national. The remaining characters must be alphanumeric or national.

Default: None

class

Specifies the resource class name that CA CSM uses for security rules in resource profiles.

Limits: 1-8 bytes. All characters of the name must be alphanumeric or national.

Default: CAMSM

SSL

Sets the parameters that are related to the SCS address space interface to the System SSL Cryptographic Services.

The SSL parameters are specified using the following attributes:

keyring

Specifies the path and file name of the key ring database file that is used for encrypting data from remote systems, or the SAF key ring label that is defined in the external security manager(CA ACF2 for z/OS, CA Top Secret for z/OS, or IBM RACF) for the user ID assigned to the SCS address space.

Used to retrieve the default certificate to send to the client side to begin the process of securing the connection for communication.

Default: None

stashfile

Specifies the path and file name of the stashfile if the key ring attribute is set to the path and file name of a key ring database file.

The stashfile contains the password to access the key ring database file.

Limits: Required if the key ring attribute is set to a key ring database file name.

Default: None

AUX

Sets the parameters that are related to the SCS AUX address space.

The SCS AUX address space parameters are specified using the following attributes:

procname

Specifies the name of a JCL procedure library member that contains the source JCL for the SCS AUX address space.

Limits: 1-8 bytes. The first character must be alphabetic or national. The remaining characters must be alphanumeric or national.

Default: MSMCAUX (see page 153)

jobname

Specifies the job name that is assigned to the SCS AUX address space.

Limits: 1-8 bytes. The first character must be alphabetic or national. The remaining characters must be alphanumeric or national.

Default: The JCL procedure library member name (if the source JCL is a procedure), or the job name that is assigned on the JOB statement (if the source JCL is a job).

reusasid

Determines if a reusable ASID is requested for the SCS AUX address space.

The SCS AUX address space receives one of the following values:

YES

The SCS AUX address space is assigned a reusable ASID if REUSASID (YES) is also specified in the DIAG*xx* PARMLIB member.

NO

The SCS AUX address space is not assigned reusable ASID.

Default: YES

Note: Using a reusable ASID results in an ABEND of system 0D3 if products or programs that are used in the configuration of a CA Technologies product are not upgraded to tolerate reusable ASIDs.

See the IBM *z/OS MVS Programming: Extended Addressability Guide* for more information about reusing ASIDs.

maxactive

Specifies the maximum number of concurrently active SCS AUX address spaces.

Limits: 1 to 20 numeric

Default: 20

SCS Address Space Message Log (SCSLOG)

The SCS address space message log (SCSLOG) is a detailed log of all messages that the SCS address space writes.

SCS address space messages that are written to the z/OS hardcopy message log are also written to the SCSLOG. In addition, the SCSLOG is used for messages that are more detail-oriented and that can be useful when diagnosing problems. The SCSLOG is therefore a more complete record of the activities of the SCS address space.

The SCSLOG is implemented using the z/OS UNIX System Services (USS) syslog daemon. The syslog daemon is part of the z/OS system product. The syslog daemon must be explicitly started using the USS syslogd command.

Note: For more information about the syslog daemon, see the IBM *z/OS Communications Server: IP Configuration Guide* and the *z/OS Communications Server: IP Configuration Reference*.

Configure Syslog Daemon

A configuration file controls the syslog daemon (syslogd) processing.

Default: /etc/syslog.conf

Statements in the configuration file define logging rules and output destinations for log messages. You define logging rules in the syslog daemon configuration file to send SCS address space messages to specific destinations.

The logging rules are defined using a facility name and a priority code. The user ID and job name of the program that generates the message can also be specified in the logging rule.

Note: AUX address space messages are written to the syslog daemon by a process executing in the SCS address space. Only define logging rules for the SCS address space job name. No logging rules are needed for the AUX address space job name.

All SCS address space messages that are written to the syslog daemon specify a facility name of ‘user’.

Each SCS address space message that is written to the syslog daemon specifies one of the following priority codes:

info

Messages with this priority code are informational messages.

warning

Messages with this priority code are warning messages.

error

Messages with this priority code are error messages.

crit

Messages with this priority code are severe error messages.

debug

Messages with this priority code are debugging messages.

Example: Add statements to the syslog daemon

To allow all messages that job MSMCPROC writes to write to the file /tmp/syslogd/msmcproc.syslog, add the following statements to the syslog daemon configuration file and activate the changes.

```
#
#  CA CSM SCS message log (SCSLOG)
#
*.MSMCPROC.*.* /tmp/syslogd/msmcproc.scslog
```

Activate Syslog Daemon Configuration Changes

After you update the syslog daemon configuration file, send a SIGHUP signal to the syslog daemon. You do so to cause the daemon to reread the configuration file and activate any modified parameters.

Use the USS kill command to send the SIGHUP signal.

This command has the following format:

```
kill –s SIGHUP pid
```

pid

Specifies the syslog daemon process ID.

Depending on how it is started, the syslog daemon stores its process ID in a file. The file can be used to reconfigure the daemon.

- If the syslog daemon is started in normal or local-only mode, the file is named as follows:

  /etc/syslog.pid

- If the syslog daemon is started in network-only mode, the file is named as follows:

  /etc/syslog_net.pid

The syslog daemon continues to append log messages to the files you specify in the configuration, after reading the configuration file again.

Note: All log files that the syslog daemon uses must be created in the z/OS UNIX file system before the syslog daemon is started or reconfigured, unless the syslog –c option is specified. If the –c option is specified, the syslog daemon dynamically creates log files that are not already in existence.

Generalized Trace Facility

The SCS address space uses the generalized trace facility (GTF) to capture data for diagnostic purposes. GTF is a part of the z/OS system product. GFT must be explicitly activated by issuing a START GTF command.

Note: For more information about GTF, see the *IBM MVS Diagnosis Tools and Service Aids*.

Start the GTF

To start the GTF, enter a START GTF command. You can start the GTF by using the IBM-supplied procedure or your internal procedure for starting GTF.

Note: Multiple instances of GTF can be active simultaneously. Each instance operates as a system task in its own address space.

Each instance of GTF can be assigned a unique identifier that is specified on the START GTF command. The identifier lets you recognize and control specific instances of GTF. If a unique identifier is not specified, the operating system assigns the device number of the device where the trace data set resides.

The events that GTF traces are specified as options. You specify the USRP and JOBNAMEP options for the SCS address space.

After you specify the USRP GTF option, GTF prompts you for the list of event identifiers (EIDs).

The SCS address space uses the following EIDs:

301

Captures diagnostic data for the infrastructure component of the SCS address space.

302

Captures diagnostic data for the communications server component of the SCS address space.

303

Captures diagnostic data for the communications server event API component of the SCS address space

304

Captures diagnostic data for the container section component of the SCS address space.

305

Captures diagnostic data for the implementation engine component of the SCS address space.

306

Captures diagnostic data for the services section component of the SCS address space.

307

Captures diagnostic data for the system information agent component of the SCS address space.

Note: To avoid unwanted information, limit the GTF trace output using the USRP option.

If the JOBNAMEP GTF option is specified, you are prompted for the list of job names that trace output is captured for. Specify the names of the SCS address space, both main and auxiliary. The common names are MSMCPROC (see page 153) and MSMCAUX (in this order).

Example

CA CSM includes the MSMCGTFP sample member that contains the following GTF trace options:

```
TRACE=USRP,JOBNAMEP
USR=(301,302,303,304,305,306,307)
JOBNAME=(MSMCPROC,MSMCAUX)
END
```

Stop the GTF

To stop the GTF, issue a STOP GTF command. Specify the identifier on the START GTF command. If an identifier is not specified on the START GTF command, specify it on the device number of the device where the trace data set resides.

Appendix A: CA CSM Implementation and Status

This section contains the following topics:

Implementation Checklist

Use the checklists in this section to confirm that each role has completed the tasks that are associated with them.

Network Administrator

Configure access to the following websites:

- supportservices.ca.com (using HTTPS Port Number 443)
- ftp.ca.com (using FTP Port Number 21)
- ftpca.ca.com (using FTP Port Number 21)

  Note: CA CSM uses this FTP server to accumulate minimal information. This information includes the site ID, the product, and the user ID for the CA Support Online website. Sometimes site access rules deny an FTP connection that is established for this purpose or the connection cannot be established for any other reason. Then CA CSM still continues to function.
- scftpd.ca.com (using FTP Port Number 21)

- ftpdownloads.ca.com (using FTP Port Number 21)
- supportftp.ca.com (using FTP Port Number 21)
- sdownloads.ca.com (using HTTPS Port Number 443)

  Note: sdownloads.ca.com is only required if you use the Use HTTPS for Downloads acquisition option under System Settings, Software Acquisition on the Settings page. If you authorize the ca.com domain for both ports 80 and 443, you do not need to authorize sdownloads.ca.com.

In addition, your network administrator must define a Domain Name System (DNS) entry for localhost.

Security Administrator

1. Grant UPDATE authority to the following data sets or libraries to the user who implements CA CSM:
   - SYS*x*.PARMLIB
   - Procedure library that stores the JCL jobs that are used to start the CA CSM address spaces, for example, SYS3.PROCLIB
   - (Optional) The master catalog if you decide to define alias entries for the CA CSM data set prefixes
2. Grant the following access to the user ID associated with the CA CSM setup utility, MSMSetup.sh:
   - Access to USS
   - Permission to access the following FACILITY class profiles that are related UNIX:
     - BPX.FILEATTR.APF (READ authority)
     - BPX.FILEATTR.PROGCTL (READ authority)
     - BPX.FILEATTR.SHARELIB (READ authority)
     - BPX.SERVER (UPDATE authority)
     - BPX.CONSOLE (READ authority)
     - BPX.DAEMON (READ authority)
   - Permission to access the SERVAUTH class profile, EZB.STACKACCESS (READ authority)
   - Permission to access the CSFSERV class profile, CSFOWH (READ authority) providing you want to perform SMP/E GIMUNZIP hash validation

- Permission to create and modify data sets for the qualifiers (CA CSM MVS SMP/E and runtime data sets) specified in the options file.

  Note: Your user ID can have BPX.SUPERUSER access and it can switch to SUPERUSER. Then the switched SU ID requires a CREATE and MODIFY access to the MVS data set qualifiers that are specified in the options file.

- If you are using IBM RACF, access to the following data sets for program control:

  - SYSx.MIGLIB
  - CEE.SCEERUN2
  - Members IEANTCR, IEANTDL, and IEANTRT of SYS1.CSSLIB
  - Member JVMLDM76 (for 64-bit Java 7.0) of the data set where Java load modules are installed
  - (Optional) Member IDIXCEE of SYS1.IDI.SIDIAUTH, only if you use IDIXCEE as an optional exit

  Note: To display the resources, issue the RLIST command.

  You can set IBM RACF to control programs. If the resources do not exist, issue the following command:

  ```
  RDEFINE PROGRAM member ADDMEM('hlq.libraryname'//NOPADCHK) UACC(READ)
  ```

  For example:

  ```
  RDEFINE PROGRAM IEANTCR ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
  ```

  If the resources exist, issue the following command:

  ```
  RALTER PROGRAM member ADDMEM('hlq.libraryname'//NOPADCHK) UACC(READ)
  ```

  For example:

  ```
  RALTER PROGRAM IEANTCR ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
  ```

  Note: To set all members of a data set as a controlled program, replace the member name with an asterisk (*). For example:

  ```
  RDEFINE PROGRAM * ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
  ```

  Important! If you are planning to use zFS, add IOE.SIOELMOD (or equivalent library) to program control.

3. Grant the following access to the user ID associated with the CA CSM application server (MSMTC job or started task):

   - Access to USS
   - Authority to create and mount file systems
   - Permissions for MSMMUF and MSMDBSRV to the data sets that are referenced in the following option file keywords:
     - DatabaseHLQ (READ, UPDATE, and ALTER authority)
     - CCSdsn, CCScaipdsedsn, and RunTimeMVSHLQPrefix (READ authority)
   - Permissions for MSMTC to the data sets that are referenced in the following option file keywords:
     - RunTimeMVSHLQPrefix (READ authority)
     - MVSHFSDsnPrefix, sisGimunzipTempPrefix, and the sisExecutorServerDsnPrefix (CREATE, READ, UPDATE, and ALTER authority)
   - Permission to access the following FACILITY class profiles that are related UNIX:
     - BPX.FILEATTR.APF (READ authority)
     - BPX.FILEATTR.PROGCTL (READ authority)
     - BPX.FILEATTR.SHARELIB (READ authority)
     - BPX.SERVER (UPDATE authority)
     - BPX.CONSOLE (READ authority)
     - BPX.DAEMON (READ authority)
   - Permission to access the SERVAUTH class profile, EZB.STACKACCESS (READ authority)
   - CA ACF2 for z/OS only: MUSASS permission for users who start CA CSM
   - If your site uses CA SAF HFS security, the following access:
     - BPX.CAHFS.SET.RLIMIT (READ authority)
     - BPX.CAHFS.PTRACE (READ authority)
     - BPX.CAHFS.MOUNT (READ authority)
     - BPX.CAHFS.UNMOUNT (READ authority)
     - BPX.CAHFS.CHANGE.FILE.MODE (READ authority)
     - BPX.CAHFS.CHANGE.FILE.TIME (READ authority)

     Note: CA SAF HFS security is a feature in CA ACF2 for z/OS and CA Top Secret for z/OS.

4. Set up OMVS segments for CA CSM users.

USS Administrator

Set up the USS paths using the following structure:

```
/u/users/msmserv (primary mount point)
     msminstall (1000 cylinders)
     msm (750 cylinders)
     msmruntime (750 cylinders)
     mpm (mount point for CA CSM use)
```

Systems Programmer

1. Ensure that prerequisite requirements are met.
2. Review the options file keywords and gather the required values.
3. Download CA CSM.
4. Unpack CA CSM:

   ```
   pax -rvf DVD10155349E.pax.Z
   ```

   Note: The full pax file name and its extension are case-sensitive. Verify that you use the exact case when you issue the pax command.
5. Customize and submit UNZIPJCL to extract CA CSM product files.
6. Customize the MSMSetupOptionsFile.properties file.
7. Execute MSMSetup.sh.
8. Start CA CSM using the following members in sequence:
   - MSMMUFS JCL member or MSMMUF PROCLIB member
   - MSMDBSVS JCL member or MSMDBSRV PROCLIB member
   - MSMTCSRV JCL member or MSMTC PROCLIB member
9. Access CA CSM using a web browser and perform initial configuration.
10. Clean up the USS directory.
11. To support product deployment, ensure that the deployment activation elements for each CA Technologies product have been acquired and installed.

    Note: For more information about product deployment, see the online help.

CA CSM Software Deployment Spawn Procedure Entities

The following entities are installed within the CA CSM software deployment procedure, which is a component-dependent function for CA Common Services for z/OS and CAIENF/CAICCI.

SMPCPATH

Specifies the path to the SMP/E Java application classes.

Preset: /usr/lpp/smp/classes/

SMPJHOME

Specifies the Java home directory.

Example: /sys/java64bt/v7r0m0/usr/lpp/java/J7.0_64

Note: If your installation has a different Java home directory, use that directory name.

SMPDRIWK

This entity must be defined with the permissions of 775.

Preset: /cai/msm/ccispnsv/smpe

Note: The procedure is set to /cai/msm/ccispnsv/smpe. Tailor it to your company standard.

USS File Systems

This section provides more information about setting up your z/OS UNIX System Services (USS) and file systems.

CA CSM Installation and Setup

Before you execute the MSMSetup.sh utility, define a mount point for the installation of CA CSM. The mount point includes the following directories:

- The installation directory (for example, /u/users/msmserv/msminstall) that the MSMPATH keyword refers to in MSMSetupOptionsFile.properties
- The runtime directory (for example, /u/users/msmserv/msmruntime) that the RunTimeUSSPath keyword refers to in MSMSetupOptionsFile.properties

CA CSM Download

CA CSM is delivered as a pax file, which is downloaded and installed into a mounted file system or a directory (for example, /u/users/msmserv/msminstall). The name of the file is DVD10155349E.pax.Z. When the file is expanded, new directories are created.

CA CSM Startup

This section describes the CA CSM startup process for both new and existing CA CSM installations.

At startup, CA CSM allocates and mounts file systems and USS directories. Before you execute MSMSetup.sh, define a mount point (for example, /u/users/msmserv/mpm) for the APLROOT file system. CA CSM allocates the file system and mounts it to this mount point.

Note: The MountPath keyword in MSMSetupOptionsFile.properties specifies the APLROOT directory. MSMSetup.sh populates the mpmPath parameter in the SAMPLIB(DBINIT) member with this value. The DBINIT member is used when CA CSM starts for the first time. On startup, the value is stored in the database. You can modify the value using the Application Root field on the Mount Point Management page on the Settings tab in the web-based interface.

Under the APLROOT file system, CA CSM creates four USS directories: sdsroot, scroot, ljroot, and tmproot. The USS directory ljwk is created under the ljroot directory.

The following list identifies the permanent file systems and their mount points:

- *hfs_prefix*.APLROOT mounted at *mountpath* (105,105 tracks)
- *hfs_prefix*.LJWK mounted at *mountpath*/ljroot/ljwk (2370,105 tracks)
- *hfs_prefix*.SDSROOT mounted at *mountpath*/sdsroot (105,105 tracks)

hfs_prefix

This prefix is specified by the MVSHFSDsnPrefix keyword in MSMSetupOptionsFile.properties. MSMSetup.sh populates the mpmHlq parameter in the SAMPLIB(DBINIT) member with this value. On startup, the value is stored in the database. You can modify it using the Data Set Prefix field on the Mount Point Management page on the Settings tab in the web-based interface.

The tmproot USS directory is used for allocating and mounting temporary file systems (see page 108) as required during CA CSM operation.

You can define whether CA CSM mounts file systems at startup. The Mount Point Management page on the Settings tab in the web-based interface has an Automount option. If the option is enabled, CA CSM looks for and mounts all the file systems that it manages. If the option is not enabled, you manage the mount points by updating the BPXPRM*xx* member in SYS*x*.PARMLIB.

Use of Temporary File Systems

In addition, CA CSM allocates temporary file systems as required during product acquisition, product installation, and other tasks. By default, CA CSM keeps a temporary file system for 60 minutes. After the file system has been idle for 60 minutes, CA CSM deallocates and releases it.

The names of the file systems have the following format: *hfs_prefix*.T*x.*

x

Is an internally generated number of up to seven characters.

CA CSM mounts temporary files at the following path:

```
mountpath/tmproot/MSM.unique_number.scratchpad
```

You can modify the time slot during which CA CSM keeps a file system allocated and mounted. In the SAMPLIB(MSMLIB) member, set the following parameter to the required number of minutes, and restart the CA CSM application server:

```
IJO="$IJO –DCSM_MPM.TEMPSPACE.MINIMUM.IDLE.MINUTES=60"
```

The minimum allowed value is 60. If you set the parameter to a value less than 60, CA CSM resets it back to 60.

If this parameter is set to 0, CA CSM allocates the temporary space during execution and deallocates it at termination.

Software Catalog

CA CSM allocates and mounts file systems for use by the software catalog as required. CA CSM mounts these file systems under *mountpath*/scroot.

The names of the file systems have the following format: *hfs_prefix*.*suffixn*.

suffix

Defines the last part of the file system name and is specified by the scDatasetPrefix parameter in the SAMPLIB(DBINIT) member.

n

Defines an internally generated counter of up to four characters.

More information:

CA CSM Startup (see page 107)

CA CSM Data Sets and File Systems

This section provides more information about the CA CSM data sets and file systems.

This section contains the following topics:

CA CSM Data Set Types

CA CSM has six groups of data sets. They are organized in the following types:

Application Root: *hlq*.APLROOT

This data set is used as the root USS file system that stores the directory structure for CA CSM.

Temporary Areas: *hlq*.Tx

These data sets are temporary file systems that are used as temporary areas for CA CSM processing. These data sets are allocated during CA CSM operation as required and are deleted when no longer needed.

Log Journal: *hlq*.LJWK*x*

These data sets are used to store task output results, and their content appears in the Tasks tab for the finished tasks. To delete this content using CA CSM, use the Delete Task button on the Task tab.

Software Catalog: *hlq*.CASC*x*

These data sets store all the downloaded products and maintenance packages that can be viewed in the software catalog. A data set with a suffix CASC is usually configurable, with a default value of CASC. The data sets are removed after deployment is completed or deleted.

Note: In previous versions of CA CSM, the default software catalog data set had the suffix MSMT.

Deployment Temporary Area: *hlq*.SDSROOT

This data set is a temporary file system that is used as a temporary area for CA CSM deployment processing. CA CSM deletes the content of this file system after the data is no longer needed. If any content remains there after CA CSM shuts down, you can manually delete the content from the appropriate USS directories without affecting CA CSM.

Deployment: *hlq*.D*x*

These data sets are used for deployment processing and contain deployment data. To remove this content using CA CSM, select Remove from the Action drop-down list on the Deployment tab.

Important! Do not delete these data sets or the content from these data sets manually outside of CA CSM. Manually deleting data sets causes missing task output or CA CSM to fail.

CA CSM File Systems

The following table lists the file systems that CA CSM allocates and uses. The following terms are used in the table:

mpm

Specifies the UNIX path to the application root. mpm specifies the mount point directory for the file systems. An initial mount point is configured during the CA CSM installation.

hlq

Specifies the HLQ for the data set names that are created for new file systems that CA CSM allocates.

Data Set Name (DSN)

Specifies the DSN of the file system that is mounted to this directory, or of the file system that contains this directory if no file system is mounted to this directory.

Typical Size

Specifies the typical size of the file system. The value is specified only for paths that have a file system mounted to them.

Path	Data Set Name	Data Set Mounted to Path	Type	Purpose	Typical Size
mpm	*hlq*.APLROOT	Yes	Application root	The main mount point directory for CA CSM. This directory resides in the *hlq*.APLROOT data set.	14400 KB
mpm/ljroot	*hlq*.APLROOT	No	Log journal root	The root directory for the log journal (task output).	N/A
mpm/scroot	*hlq*.APLROOT	No	Software catalog root	The root directory for the software catalog (stored products and maintenance packages).	N/A
mpm/sdsroot	*hlq*.SDSROOT	Yes	Deployment root	The root directory for deployment packages.	158400 KB
mpm/ljroot/ljwk	*hlq*.LJWK	Yes	Log journal	This directory resides in the *hlq*.LJWK data set.	137760 KB
mpm/scroot/tmp	*hlq*.APLROOT	No	Software catalog	The directory that contains Software catalog temporary directories.	N/A
mpm/scroot/tmp/tmpx	*hlq*.CASCn	Yes	Software catalog	The Software catalog temporary directory.	400000 KB
mpm/scroot/DatabaseM	*hlq*.APLROOT	No	Software catalog	The directory that contains the Software catalog database.	N/A
mpm/scroot/DatabaseM/CA	*hlq*.APLROOT	No	Software catalog	The CA Technologies vendor directory that contains all downloads for a vendor.	N/A
mpm/scroot/DatabaseM/CA/error_hold_data	*hlq*.APLROOT	No	Software catalog	The directory that contains the ALL-HOLDDATA.txt file. This file contains HOLDDATA for all CA Technologies products.	N/A

Path	Data Set Name	Data Set Mounted to Path	Type	Purpose	Typical Size
mpm/scroot/DatabaseM/CA/COMMONS	*hlq*.APLROOT	No	Software catalog	The directory that contains the installation for CA Common Services.	N/A
mpm/scroot/DatabaseM/cars	*hlq*.CASCn	Yes	Software catalog	The directory that contains CA RS files.	4800 KB
mpm/scroot/DatabaseM/CA/MAINTENANCE	*hlq*.CASCn	Yes	Software catalog	The directory that contains all maintenance packages	4800 KB
mpm/scroot/DatabaseM/CA/*product_name*	*hlq*.CASCn	Yes	Software catalog	The product directory for a specific product.	4800 KB
mpm/scroot/DatabaseM/CA/*product_name* */release/servicepack/packagename* */date*	*hlq*.CASCn	Yes	Software catalog	The directory for a specific product package that does not fit into the product directory.	4800 KB
mpm/sdsroot/*deployment_ID*	*hlq*.Dn	Yes	Software Deployment Service (SDS)	The directory that contains data stored for deployment with ID *deployment_ID*. This directory resides in the *hlq.deployment_ID* data set.	21024 KB
mpm/tmproot	*hlq*.APLROOT	Yes	Temporary area	The directory contains temporary mount points for temporary file systems.	N/A
mpm/tmproot/MSM.*n*.scraptchpad	*hlq*.T*n*	Yes	Temporary area	The directory serves as a mount point for a temporary file system that CA CSM allocates as required during product acquisition, product installation, and other tasks.	57408 KB

CA Common Services Component Requirements

CA Common Services for z/OS includes distributed services common to CA Technologies implementations and solutions specific to z/OS. CA Common Services for z/OS provides a common interface and event services to create multiple, unified resource views.

CA Common Services for z/OS Software Services provide CA CSM with a number of software components that perform various functions, including the following components:

- CAICCI
- CAIENF (Base)
- CAIRIM
- CA-C Runtime

Note: For more information about CA Common Services for z/OS, see the CA Common Services for z/OS user documentation.

FMIDs

CA CSM requires CA Common Services for z/OS Release 14.1 or Version 14.0 components to perform various functions. The function modification identifiers (FMIDs) are provided for these components.

The FMIDs in the following table are based on CA Common Services for z/OS Version 14.0:

FMID	Component
CAF3E00	CA-C Runtime
CAS9E00	CAIRIM
CAW1E00	CAIENF
CAW4E00	CAICCI with SSL

The FMIDs in the following table are based on CA Common Services for z/OS Release 14.1:

FMID	Component
CAF3E00	CA-C Runtime
CAS9E10	CAIRIM
CAW1E10	CAIENF
CAW4E10	CAICCI with SSL

The FMID in the following table is based on CA Common Services for z/OS Version 14.0 and above. This FMID is a CA Common Services for z/OS dependent function that is only used for SDS and SCS.

FMID	Component
CETN600	CA CSM Common Services, which uses CAICCI

Note: For information about setup and configuration steps that must be completed, see the *CA Common Services for z/OS Installation Guide.*

Set Up CAICCI

Use this procedure if you have not set up CAICCI at all. For more information, see the *CA Common Services for z/OS Installation Guide*.

Follow these steps:

1. Define the CAICCI SYSID, either in the CAIENF parameter file or as a separate CCIPARM PDS member concatenated to ENFPARMS, using the following format:

   ```
   SYSID(sysid)
   ```

   sysid

   Specifies the CAICCI identifier.

   Limit: Eight characters

2. Define the CAICCI data collection module (DCM), CAS9DCM3, in your CAIENF parameter file. For example:

   ```
   DCM(CAS9DCM3)         * ENF V1.0 CCI Event
   ```

Security for CA CSM Functions

Many of the resources and activities that CA CSM provides are protected by security profiles that are defined to your external security manager (ESM). When you attempt to perform an action in the web-based interface (for example, logging in or changing a setting), CA CSM invokes the System Authorization Facility (SAF) with the associated resource profile. CA CSM resource profiles (see page 116) are defined in the CA CSM resource class. The resource profiles enable your site to assign authorities to various resources and actions to specific users or to provide generic access with few settings.

Resource Names

CA CSM does not use the distinctions of READ, UPDATE, CONTROL, and ALTER for access to resources. Instead, access is encoded into the resource name. If you have access to a resource, you can perform the specified action on the resource.

The granted authority level is immaterial. Access to the resource is managed in a binary manner: either you can access the resource (any combinations of READ, UPDATE, CONTROL, or ALTER), or you cannot access the resource. For example, the following resource profiles control access to the system settings on the Settings tab:

ADMIN.SETTINGS.SYSTEM

Enables a user to display and update the system settings.

ADMIN.SETTINGS.SYSTEM.@DISPLAY

Enables a user to display the system settings.

ADMIN.SETTINGS.SYSTEM.@UPDATE

Enables a user to update the system settings.

For resources that have both an @DISPLAY and an @UPDATE profile, granting access to only the @UPDATE profile is an error. Because you have no authority to display the value, you cannot change the value, even though that level of access is granted.

Because all the system settings are organized under ADMIN.SETTINGS.SYSTEM, you can give access to all system settings by granting one or more users to the ADMIN.SETTINGS.SYSTEM profile. These users would be taking on the administration role for CA CSM.

User settings are organized under ADMIN.SETTINGS.USER. The settings are maintained separately in CA CSM for each user. Access to display or update a resource is managed through the @SELF qualifier in the resource profile. For example, authorizing the user IDs, USER01 and USER02, to the ADMIN.SETTINGS.USER.@SELF.@DISPLAY and ADMIN.SETTINGS.USER.@SELF.@UPDATE profiles enable the users to update their own web-based interface settings. However, USER01 cannot display or update the settings for USER02. We recommend that you grant permission to ADMIN.SETTINGS.USER.@SELF to all CA CSM users.

Resource Profiles

You can secure certain parts of CA CSM by granting or denying access using security rules, which are named *resource profiles*. Create these resource profiles in their associated security package using resource class CAMSM.

Important! If you grant a user permission to a *.@UPDATE resource profile, you must also grant that user permission to the corresponding *.@DISPLAY resource profile.

LOGON

Grants access to CA CSM.

ADMIN.SETTINGS

Grants full access to all settings on the Settings tab.

ADMIN.SETTINGS.SYSTEM

Grants full access to all system settings.

ADMIN.SETTINGS.SYSTEM.@DISPLAY

Grants DISPLAY authority to all system settings.

ADMIN.SETTINGS.SYSTEM.@UPDATE

Grants UPDATE authority to all system settings.

ADMIN.SETTINGS.USER.@SELF

Grants full access to a user's own settings, including the user's account on the CA Support Online website.

ADMIN.SETTINGS.USER.@SELF.@DISPLAY

Grants DISPLAY authority to a user's own settings, including the user's account on the CA Support Online website.

ADMIN.SETTINGS.USER.@SELF.@UPDATE

Grants UPDATE authority to a user's own settings, including the user's account on the CA Support Online website.

ADMIN.LMPKEY

Grants full access to the resources on the LMP Keys Browser page.

ADMIN.LMPKEY.UPDTKEYS

Grants access to Update Keys on the LMP Keys Browser page.

ADMIN.LMPKEY.REFRSITE

Grants access to Refresh Site IDs on the LMP Keys Browser page.

CONFIG

Grants full access to the resources on the Configurations tab.

CONFIG.@DISPLAY

Grants display only access to the resources related to SCS.

CONFIG.@ACTION.CREATE

Grants full access to create or update the resources that are related to SCS.

CONFIG.@ACTION.REMOVE

Grants full access to the resources on the Deployments tab.

CONFIG.@ACTION.IMPL

Grants access to implement configurations on remote systems.

DEPLOY

Grants full access to the resources on the Deployment tab.

DEPLOY.@DISPLAY

Grants read-only authority to information provided on the Deployments tab.

DEPLOY.@SELF

Grants authority to create deployments, assign systems and custom data sets, and all actions for the deployment if your CA CSM user ID is marked as the owner of that deployment.

DEPLOY.@BUILD

Grants authority to create and update deployments, assign systems and custom data sets, and previewing the deployment.

DEPLOY.@EXECUTE

Grants authority to perform a snapshot, transmit, deploy, and confirm a deployment.

METHOD

Grants full access to all methodologies.

METHOD.@DISPLAY

Grants read access to all methodologies.

METHOD.@SELF

Grants full access to only those methodologies where you are listed as the owner.

METHOD.@UPDATE

Grants access to create, edit, and remove methodologies from within the Maintain Methodologies page. This profile also controls the availability of the Edit button next to the methodology within the deployment view.

SC

Grants full access to the resources on the Products tab.

SC.@ACTION

Grants full access to the actions on the Products tab.

SC.@ACTION.UPDTCAT

Grants access to all Update Catalog actions on the Products tab.

SC.@ACTION.SHOWLMP

Grants access to the Show License Keys action in the Actions section on the Products tab.

SC.@ACTION.INSRTPRD

Grants access to the Add Product action in the Actions section on the Products tab.

SC.@ACTION.INSTPKG

Grants access to the Install External Package action in the Actions section on the Products tab.

SC.@HIDE

Grants access to the Hide Product action in the Products tree and to the Show Products button on the Show Hidden Products dialog on the Products tab.

SIS.BASE.@SELF.WORKDD.@UPDATE

Grants access to the action to update work DDDEF settings during product installation.

SMPE.@ACTION

Grants full access to the actions on the SMP/E Environments tab.

SMPE.@ACTION.MIGRATE

Grants access to the action to migrate an SMP/E environment.

SMPE.@ACTION.REMOVECSI.*csidatasetname*

Grants access to Remove SMP/E Environment from CA CSM on the SMP/E Environments, SMP/E Environment Information tab. The permission is for the specified SMP/E environment.

.csidatasetname

Specifies the data set names of the SMP/E environments that the user can remove.

The value can be a full name that matches one SMP/E environment or a prefix that can match multiple SMP/E environment data set names.

SYSREG

Grants full access to the resources on the System Registry tab.

SYSREG.@DISPLAY

Grants display authority to all System Registry values.

Note: Users who are defined with this access are not allowed to create, delete, or update any information on any of the panels.

SYSREG.@ACTION

Grants full access to the actions on the System Registry tab.

SYSREG.@ACTION.CREATE

Grants access to the Create Non-Sysplex System link, the Create Sysplex link, the Create Shared DASD Cluster link and the Create Staging System link. This profile also enables the Create button from within the display for each primary node of the System Registry tree, and the Create button within Data Destinations. Create authority also implies Update authority.

SYSREG.@ACTION.REMOVE

Grants access to the Select check box and the Remove item from within the Actions button from within each primary node of the System Registry tree.

Note: If the user does not have this authority, these items are disabled.

SYSREG.@PROFILE

Grants full access to the information within each primary node of the system registry. The information is applicable to those CA CSM users within your organization that create or implement configurations. If this access is not granted, the system information is not displayed within the web-based user interface.

Note: Implementations can result in changes on the remote system that, if done incorrectly, could adversely affect the stability of that system. We recommend that you restrict authorization to this resource profile.

SYSREG.@PROFILE.DISPLAY

From within each system node of the system registry, a user with this access does not have authority to modify any values within a system. These items are displayed but all Action buttons are disabled.

SYSREG.@PROFILE.UPDATE

From within each system node of the system registry, grants access to update any existing values within a system registry profile or to create an occurrence of a repeatable system registry profile. If the system registry is secured with the resource rule SYSREG@PROFILE.DISPLAY, this access rule is required to allow updating of any system information.

SYSREG.@PROFILE.UPDATE.*systemname*

Grants access to update any existing values within a system registry profile or create an occurrence of a repeatable system registry profile for system *systemname*.

SYSREG.@SYSTEM

Grants full access to all systems defined within the System Registry tab.

SYSREG.@SYSTEM.*systemname*

Grants access to system *systemname* within the System Registry tab. If a system is created within a CA CSM session and specific system level security is desired, the security administrator must grant access to the newly defined system before it becomes visible to the CA CSM user. Security at this level simply controls which defined systems are available to the user. The ability to update or delete information with the defined system is permitted using the SYSREG.@ACTION.CREATE, SYSREG.@ACTION.REMOVE, and SYSREG.@PROFILE.UPDATE resources.

TM.TASK.ARCHIVE

Grants access to Manage History functionality within the Task tab and allows authorized users to create, run, or delete task archive policies.

TM.TASK.@SELF.DELETE

Grants access to delete user's own tasks.

TM.TASK.SYSTEM.DELETE

Grants access to delete any tasks.

SAF Check During SMP/E Processing

All CA CSM features that execute SMP/E commands do it in the security context of the user that is logged in to CA CSM and drives these features. Depending on the CA CSM feature, users must have READ access to different sets of SMP/E SAF facility class resources.

Note: CA CSM executes GIMUNZIP in the security context of the CA CSM application server ID. If SMP/E security is active, the CA CSM application server ID must have READ access to the GIM.PGM.GIMUNZIP resource in the SAF FACILITY class.

SMP/E Environment Migration

If new DDDEFs are added to a migrated SMP/E environment using customer-provided JCL, you must have READ access to the following SMP/E SAF facility class resources:

- GIM.CMD.SET
- GIM.CMD.UCLIN

Base Product Installation

To install products, you must have READ access to the following SMP/E SAF facility class resources:

- GIM.PGM.GIMUNZIP
- GIM.CMD.SET
- GIM.CMD.UCLIN
- GIM.CMD.RECEIVE
- GIM.CMD.APPLY
- GIM.CMD.ACCEPT

If an error occurs when installing a product to an existing SMP/E environment, CA CSM performs UNDO operations to restore the SMP/E environment to its state before starting the installation.

Depending on the level of UNDO operations that CA CSM performs, you must have READ access to the following SMP/E SAF facility class resources:

- GIM.CMD.SET
- GIM.CMD.UCLIN
- GIM.CMD.RESTORE
- GIM.CMD.REJECT

Maintenance Management

You must have READ access to the GIM.CMD.SET SAF facility class resource to manage maintenance.

Other requirements depend on a particular maintenance operation:

- To install maintenance, you must have READ access at least to the following SMP/E SAF facility class resources:
  - GIM.CMD.RECEIVE
  - GIM.CMD.APPLY
- To accept maintenance, you must also have READ access to the GIM.CMD.ACCEPT SAF facility class resource.

- To perform elementary SMP/E commands on one or more maintenance packages, you must have READ access to the following corresponding SAF facility class resources:
  - GIM.CMD.RECEIVE (for RECEIVE operation)
  - GIM.CMD.APPLY (for APPLY operation)
  - GIM.CMD.ACCEPT (for ACCEPT operation)
  - GIM.CMD.RESTORE (for RESTORE operation)
  - GIM.CMD.REJECT (for REJECT operation)

Deployment

SDS relies on the SMP/E GIMZIP program. If you perform a deployment operation, you must have READ access to the GIM.PGM.GIMZIP SAF facility class resource on the CA CSM driving system. Also, you must have READ access to the GIM.PGM.GIMUNZIP SAF facility class resource on the CA CSM remote system.

DBINIT and DBUPDATE Settings

The DBINIT member, *RunTimeMVSHLQPrefix*.SAMPLIB(DBINIT), is used when CA CSM starts for the first time. The CA CSM installer sets the content of this member.

Important! Change the member content only when CA Support requests it. The values set for some keywords may vary between the CA CSM Setup Options file and *RunTimeMVSHLQPrefix*.SAMPLIB(DBINIT) member. Therefore, it is important that you closely follow the instructions from CA Support.

The DBINIT member is allocated to DBINIT DD of the CA CSM startup JCL (*RunTimeMVSHLQPrefix*.JCL(MSMTCSRV)). The DBINIT member is used only when CA CSM is run for the first time.

At startup, values from the DBINIT member are stored in the database. Some of the values can be set only once. You cannot change them, or changing the values does not have any effect. You can modify the other values later using the web-based CA CSM interface.

To modify the values that cannot be modified using the web-based interface, you can use the DBUPDATE DD (see page 129). The DBUPDATE DD is processed during CA CSM startup.

Important! Update these values only when CA Support requests it. Otherwise, you may cause data inconsistency.

The contents of DBINIT and DBUPDATE are records that can be either comments starting with # or value settings in the following format:

```
setting=value
```

The values are not verified during DBINIT or DBUPDATE processing.

The following settings are available for the Mount Point Manager:

mpmPath

Defines the path to the USS directory that CA CSM uses for work files. This directory must be available when you execute the setup utility.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Application Root field.

Note: Changing this value does not copy existing data to the new path. Ensure that the new path is valid.

mpmHlq

Defines a prefix that is used for file system allocation.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Data Set Prefix field.

Limits: 40 characters

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmStorclas

Defines the SMS storage class on the Mount Point Management page of the Settings tab.

The value can be blank.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Storage Class field.

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmVolser

Defines the volume serial number of the corresponding DASD on the Mount Point Management page of the Settings tab.

The value can be blank. If defined, mpmVolser must be the volume serial number of an online volume.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the VOLSER field.

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmFilesystemType

Specifies the file system type that is used for file system allocation.

Options include:

- HFS
- zFS

Note: We recommend using zFS file systems.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page.

Note: If you change this setting, it will be used for newly allocated data sets only. Existing data sets remain intact.

mpmAutomount

Specifies whether CA CSM mounts all file systems during startup.

Options include:

- true
- false

This value can be changed in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, the Automount check box.

mpmunit

Specifies the type of the DASD on which to place data sets on the Mount Point Management page of the Settings tab.

This value can be changed in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Unit field.

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmDataClas

Specifies the SMS data class for file system data sets on the Mount Point Management page of the Settings tab.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Data Class field.

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmMgmtClas

Specifies the SMS management class for file system data sets on the Mount Point Management page of the Settings tab.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Storage Class field.

Note: If you change this setting, it will be used for newly allocated data sets only.

mpmAllocation

Specifies whether to use SMS when allocating new data sets for file systems on the Mount Point Management page of the Settings tab.

Options include:

- SMS
- NONSMS

If mpmStorclas is defined, mpmAllocation is treated as SMS. Otherwise, it is treated as NONSMS.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Mount Point Management page, in the Use SMS or Use Non-SMS fields.

Note: If you change this setting, it will be used for newly allocated data sets only.

The following settings are available for the Software Catalog:

scDatasetPrefix

Specifies a suffix for the data set name, which also has an internally generated counter.

The name has the following format:

`mpmHlq.scDatasetPrefix`*n*

You can change this value in the web-based interface using the Settings tab, on the System Settings, Software Catalog page, in the Data Set Suffix field.

Note: If you change this setting, it will be used for newly allocated data sets only.

scRoot

Defines the root directory of the Software Catalog database where packages from the CA Support Online website are stored on a customer site. The directory is relative to the CA CSM application root, mpmPath.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Software Catalog page, in the Root Directory field.

Note: Ensure that the new path points to a valid Software Catalog root.

scPrimBig

Specifies the default value for primary quantity for data sets implicitly mounted at the product or release level in the USS database.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Software Catalog page, in the Primary Quantity field.

scSecBig

Specifies the default value for secondary quantity for data sets implicitly mounted at the product or release level in the USS database.

You can change this value in the web-based interface using the Settings tab, on the System Settings, Software Catalog page, in the Secondary Quantity field.

The following settings are available for CA DSI Server:

dsiHost

Specifies the host name for CA DSI Server that CA CSM uses internally to provide security features.

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

dsiPort

Specifies the port number for CA DSI Server that CA CSM uses internally to provide security features.

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

dsiConf

Specifies the path of the CA DSI Server configuration file.

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

The following settings are available for the Software Installation Service:

sisGimunzipTempPrefix

Defines the prefix that CA CSM uses to allocate GIMUNZIP output temporary data sets during product installation and maintenance. The name of the resulting data set is *prefix.jobname*.*unpacked_file_name*. The created temporary work files are not SMP/E controlled data sets. CA CSM deletes them through the product installation process. These files are used as input relative files for SMP/E processing during the receiving of a product into the SMP/E environment global zone.

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the GIMUNZIP Temporary Prefix field (for both System Settings and User Settings).

Limits: 12 through 19 characters (depending on the number of characters used for *jobname*)

Note: If you use the default 6-character *jobname*, you can enter up to 14 characters for the GIMUNZIP temporary prefix.

sisExecutorServerDsnPrefix

Defines the prefix for temporary data sets used by executed programs.

The name of a temporary data set has the following format: *prefix*.R*n*.*ddname* (*n* is the execution request number).

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the Temporary Data Set Prefix field (for both System Settings and User Settings).

Default: *userid*.CAMSM.*jobname*

Limits: 24 characters

sisGimunzipTempVolser

Specifies the volume serial number of the DASD to use for the temporary data sets created by GIMUNZIP during installation.

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the GIMUNZIP Temporary VOLSER field (for both System Settings and User Settings).

Limits: 1-6 alphanumeric characters or an asterisk (*). If an asterisk is specified, SMS assigns a volume for a new VSAM data set if the automatic class selection (ACS) routines allow it.

sisExecutorOutputStorclas

Specifies the SMS storage class for the data sets that executed programs use for temporary data.

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the Storage Class field (for both System Settings and User Settings).

sisExecutorOutputVolser

Specifies the volume serial number of the DASD to use for the data sets that executed programs use for temporary data.

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the VOLSER field (for both System Settings and User Settings).

Limits: 1-6 alphanumeric characters

sisExecutorOutputUnit

Specifies the type of the DASD on which to place the data sets that executed programs use for temporary data.

You can change this value in the web-based interface using the Settings tab, on the Software Installation page, in the Unit field (for both System Settings and User Settings).

The following settings are available for the PAS component keys:

PASAdvancedSettingsPDS

Defines the data set where the member containing a sample of FTP proxy advanced settings is located.

Default: *RunTimeMVSHLQPrefix*.SAMPLIB

RunTimeMVSHLQPrefix

Specifies the prefix for CA CSM runtime data sets, which are runtime copies of the target data sets.

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

PASAdvancedSettingsMember

Defines the member that contains a sample of FTP proxy advanced settings where you can configure FTP advanced proxy settings.

Default: PASADVOP

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

The following setting is available for the Task Management:

sysTaskDeleteOverrideEnabled

Lets all CA CSM users delete completed tasks when the security feature in CA CSM is disabled.

true

Any user can delete any competed task.

false

Users cannot delete completed tasks.

Note: If the security feature is enabled in CA CSM, the task deletion is managed by security resources (see page 116), and the parameter is ignored.

Default: None.

This value cannot be changed in the web-based interface, but can be modified using DBUPDATE.

Modify Values Using the DBUPDATE DD

To modify entry values in the CA CSM database using the DBUPDATE DD, add the DBUPDATE DD to the CA CSM startup JCL (*RunTimeMVSHLQPrefix*.JCL(MSMTCSRV)).

Follow these steps:

1. Create a *RunTimeMVSHLQPrefix*.SAMPLIB(DBUPDATE) member.
2. Add only the settings (see page 122) and their values in the *RunTimeMVSHLQPrefix*.SAMPLIB(DBUPDATE) member that you want to modify.
3. Add the DBUPDATE DD pointing to the *RunTimeMVSHLQPrefix*.SAMPLIB(DBUPDATE) member to the CA CSM startup JCL (*RunTimeMVSHLQPrefix*.JCL(MSMTCSRV)).
4. Restart the CA CSM application server.
5. Comment out the DBUPDATE DD in the *RunTimeMVSHLQPrefix*.JCL(MSMTCSRV).

ASCII Configuration Files

All files in the tomcat/conf folder and all configuration files in tomcat/webapps/MSM folder are stored in ASCII. Therefore, you cannot edit these files in the standard way. This section describes some of the ASCII files and how to edit them.

Edit an ASCII File

Some text files are stored on USS in ASCII. If you attempt to open the file as EBCDIC, it may appear to be binary.

The ASCII requirement is due to Java, which only runs in ASCII. USS (OMVS) can run code that is ASCII and EBCDIC.

Note: OEDIT and ISHELL are for EBCDIC and cannot be used to edit ASCII files.

You can edit a file in ASCII mode using one of the following methods:

- Use a third-party utility that allows direct editing of ASCII files from USS.
- Edit the ASCII file locally with a text editor:
    1. Download the file to your computer using FTP in binary mode, so that the encoding is not changed during the transfer.
    2. Edit the file on your computer with a text editor.
    3. Upload the file back in binary using FTP.

- Edit the ASCII file with the ISPF UI Tool within USS:

  1. Select UTILITIES from the ISPF primary option menu.

     The Utility Selection Panel opens.

  2. Select Udlist.

     The z/OS UNIX Directory List Utility opens.

  3. Type the pathname, then use normal USS commands to step down the path to the required directory.

  4. Make yourself a superuser and enter the EA command on the appropriate file.

The file is in a readable form, and you can update it.

context.xml Parameters

You can edit values in the context.xml file. The context.xml file is an ASCII file. Use special handling when editing this file (see page 129).

Some parameters in context.xml depend on corresponding parameters in the CUSMAC(SRVLIB) member:

- If you change the value for ServerName in context.xml, change the SERVERNAME parameter in the CUSMAC(SRVLIB) member accordingly.

- If you change the value for ApplicationID in context.xml, change the APPLID parameter in the CUSMAC(SRVLIB) member accordingly.

- If you have defined PROTOCOL=BOTH in the CUSMAC(SRVLIB) member, configure the following parameters in context.xml:

  HostPort

  Verify that this parameter matches the TCPIP_PORT option in the CUSMAC(SRVLIB) member.

  ConnectType

  Set this parameter to TCP.

- If you have defined PROTOCOL=CCI, or have not defined PROTOCOL and it was set to its default value PROTOCOL=CCI, configure the following parameters in context.xml:

  HostPort

  Verify that this parameter matches the CA CCITCP or CCISSL port number that is configured in CA Common Services for z/OS on your system.

  ConnectType

  Set this parameter to CCI.

The following example is a sample from context.xml:

```
url="jdbc:datacom:/ServerName=SRVMUF,SystemID=A31SENF, ApplicationID=SRVMUF,
HostPort=1202,ConnectType=CCI, HostName=AA01,UserID=SWMGRQA"
```

The URL string consists of the following parameters:

ServerName

Defines the CA Datacom/MSM server that the CA CSM application server uses.

SystemID

Defines the CA-ENF CAICCI SYSID on the system that the CA CSM application server uses.

ApplicationID

Defines the CA Datacom/MSM server name.

HostPort

Depending on how you have configured the PROTOCOL parameter in the CUSMAC(SRVLIB) member, defines the CA CCITCP or CCISSL port number that is configured in CA Common Services for z/OS on your system (for example, 1202), or the value of the TCPIP_PORT parameter in the CUSMAC(SRVLIB) member.

ConnectType

Defines the type of connection between the CA CSM application server (see page 151) and the CA Datacom/MSM server. Depending on how you have defined the PROTOCOL parameter in the CUSMAC(SRVLIB) member, set this parameter to CCI or TCP.

HostName

Defines the name or IP address of the host system on your system.

UserID

Defines the user ID used by CA CSM to access the database.

Job Allocation Details

This section provides details about the z/OS and USS files and folders that are created after CA CSM is installed.

The following jobs are submitted based on whether you are performing a CA CSM installation or an upgrade. The job name has the format CSM*axxyy*.

a

Indicates a new installation (N) or an upgrade (U).

xx

Indicates the version number that you are upgrading from or has a value of 60 for a new installation.

yy

Indicates the sequence number of the job.

This section contains the following topics:

- CSMaxx01 (see page 132) (new installation and upgrade)
- CSMaxx04 (see page 134) (new installation and upgrade)
- CSMaxx07 (see page 135) (new installation and upgrade)
- CSMN6009 (see page 136) (new installation only)
- CSMU5102 (see page 136) (upgrade from CA CSM R5.1 only)
- CSMU5002 (see page 138) (upgrade from CA MSM V5.0 only)
- CSMU4102 (see page 140) (upgrade from CA MSM R4.1 only)
- CSMUxx09 (see page 141) (upgrade only)

CSMaxx01

The following table lists the data sets and USS files that are created when this job runs.

Note: The total primary quantity of cylinders is 922 of 3390 DASD space.

Name	Space Units	Primary Quantity	Secondary Quantity
<CSIHLQ>.SMPCSI.CSI	NA	NA	NA
<CSIHLQ>.SMPCSI.CSI.DATA	CYLS	15	
<CSIHLQ>.SMPCSI.CSI.INDEX	CYLS	2	
<CSIHLQ>.SMPHOLD	CYLS	5	1
<CSIHLQ>.SMPLOG	CYLS	5	5
<CSIHLQ>.SMPLOGA	CYLS	5	5
<CSIHLQ>.SMPLTS	CYLS	5	5
<CSIHLQ>.SMPMTS	CYLS	5	5
<CSIHLQ>.SMPPTS	CYLS	187	10
<CSIHLQ>.SMPSCDS	CYLS	4	1

Name	Space Units	Primary Quantity	Secondary Quantity
<CSIHLQ>.SMPSTS	CYLS	5	5
<DatabaseHLQ>.MSM.ADCXX.BKP	CYLS	1	17
<DatabaseHLQ>.MSM.DB002.BKP	CYLS	7	17
<DatabaseHLQ>.MSM.DB015.BKP	CYLS	3	17
<DatabaseHLQ>.MSM.JNL4000.BKP	CYLS	1	15
<DatabaseHLQ>.MSM.PCY4000.BKP	CYLS	1	15
<DatabaseHLQ>.MSM.SRG4000.BKP	CYLS	1	15
<DlibHLQ>.AAAXDATV	CYLS	40	6
<DlibHLQ>.AAAXHFS	CYLS	10	10
<DlibHLQ>.AAAXMAC	CYLS	6	2
<DlibHLQ>.AAAXMOD0	CYLS	140	1
<DlibHLQ>.AAAXSAMP	CYLS	10	1
<DlibHLQ>.AAAXML	CYLS	5	1
<DlibHLQ>.AEG1JAR	CYLS	30	2
<DlibHLQ>.AEG1SHSC	CYLS	1	1
<DlibHLQ>.AEGPHFS	CYLS	30	10
<DlibHLQ>.AEGPJAR	CYLS	80	10
<DlibHLQ>.AEGPJCL	CYLS	1	1
<DlibHLQ>.AEGPPROC	CYLS	1	1
<DlibHLQ>.AEGPSAMP	CYLS	1	1
<MSMPATH>/CEG1JAR	NA		
<MSMPATH>/CEG1SHSC	NA		
<MSMPATH>/CEGPHFS	NA		
<MSMPATH>/CEGPJAR	NA		
<MSMPATH>/datacom/dbsrv	NA		
<MSMPATH>/dsi	NA		
<RunTimeMVSHLQPrefix>.CAAXLOAD	CYLS	140	5
<RunTimeMVSHLQPrefix>.CAAXLOAD.BO1	CYLS	50	5
<RunTimeMVSHLQPrefix>.CAAXLOAD.BO2	CYLS	50	5

Name	Space Units	Primary Quantity	Secondary Quantity
<RunTimeMVSHLQPrefix>.CAAXMAC	CYLS	6	1
<RunTimeMVSHLQPrefix>.CAAXSAMP	CYLS	10	2
<RunTimeMVSHLQPrefix>.CUSLIB	TRKS	100	15
<RunTimeMVSHLQPrefix>.CUSMAC	TRKS	30	15
<RunTimeMVSHLQPrefix>.DEPLOYIN	CYLS	1	1
<RunTimeMVSHLQPrefix>.JCL	CYLS	1	2
<RunTimeMVSHLQPrefix>.PROCLIB	CYLS	1	1
<RunTimeMVSHLQPrefix>.SAMPLIB	CYLS	2	1
<RunTimeMVSHLQPrefix>.SYSPRINT	CYLS	1	1
<RunTimeUSSPath>/dsi	NA		
<RunTimeUSSPath>/tomcat	NA		
<TargetHLQ>.CAAXDATV	CYLS	40	6
<TargetHLQ>.CAAXLOAD	CYLS	140	5
<TargetHLQ>.CAAXLPA	TRKS	12	6
<TargetHLQ>.CAAXMAC	CYLS	6	1
<TargetHLQ>.CAAXSAMP	CYLS	10	1
<TargetHLQ>.CABDXML	CYLS	10	2
<TargetHLQ>.CEGPJCL	CYLS	2	1
<TargetHLQ>.CEGPPROC	CYLS	1	1
<TargetHLQ>.CEGPSAMP	CYLS	1	1

CSMaxx04

The following table lists the data sets that are created when this job runs.

Note: The total primary quantity of cylinders is 10 of 3390 DASD space.

Name	Space Units	Primary Quantity	Secondary Quantity
<dbHLQ>.CUSMAC	TRKS	30	15
<dbHLQ>.CUSLIB	TRKS	100	15

CSMaxx07

The following table lists the data sets that are created when this job runs.

Note: The total primary quantity of cylinders is 540 of 3390 DASD space.

Name	Space Units	Primary Quantity	Secondary Quantity
<dbHLQ>.CBS1006	CYLS	15	15
<dbHLQ>.CXX	CYLS	35	10
<dbHLQ>.DDD015	CYLS	15	15
<dbHLQ>.DD1002	CYLS	60	15
<dbHLQ>.FXX	CYLS	90	15
<dbHLQ>.IXX002	CYLS	45	15
<dbHLQ>.IXX006	CYLS	15	15
<dbHLQ>.IXX015	CYLS	15	15
<dbHLQ>.IXX016	CYLS	5	5
<dbHLQ>.IXX016	CYLS	5	5
<dbHLQ>.IXX1006	CYLS	15	15
<dbHLQ>.IXX1007	CYLS	10	5
<dbHLQ>.LXX	CYLS	90	15
<dbHLQ>.MSG015	CYLS	15	15
<dbHLQ>.PXX	CYLS	90	15
<dbHLQ>.SIT015	CYLS	5	5
<dbHLQ>.SQ1016	CYLS	5	5
<dbHLQ>.TTM017	CYLS	10	5

CSMN6009

The following table lists the data sets that are created when this job runs.

Note: The total primary quantity of cylinders is 2,180 of 3390 DASD space.

Name	Space Units	Primary Quantity	Secondary Quantity
<dbHLQ>.A011007	CYLS	15	5
<dbHLQ>.A021007	CYLS	15	5
<dbHLQ>.AUD4000	CYLS	500	350
<dbHLQ>.DEL1020	CYLS	15	5
<dbHLQ>.INV4000	CYLS	600	100
<dbHLQ>.IXX1007	CYLS	15	15
<dbHLQ>.IXX1018	CYLS	15	5
<dbHLQ>.IXX1019	CYLS	15	15
<dbHLQ>.IXX1020	CYLS	15	5
<dbHLQ>.IXX4000	CYLS	120	30
<dbHLQ>.JNL4000	CYLS	120	30
<dbHLQ>.PCY4000	CYLS	35	15
<dbHLQ>.SCS4000	CYLS	130	60
<dbHLQ>.SDS4000	CYLS	180	60
<dbHLQ>.SNP1019	CYLS	15	5
<dbHLQ>.SRG4000	CYLS	60	15
<dbHLQ>.STA1018	CYLS	15	15
<dbHLQ>.XML4000	CYLS	300	300

CSMU5102

The following table lists the data sets that are created when this job runs.

Primary quantity space allocation reflects what is defined in the associated z/OS job stream and should be sufficient. However, the total quantity will be adjusted to the actual quantity required based on your current environment usage.

The following values are required if you are upgrading from CA CSM R5.1 to CA CSM Version 6.0:

Note: The total primary quantity of cylinders is 2,060 of 3390 DASD space.

Name	**Space Units**	**Primary Quantity**	**Secondary Quantity**
<PREVDBHLQ>.CXX.BACKUP	CYLS	35	10
<PREVDBHLQ>.DB4000.BACKUP	CYLS	350	300
<PREVDBHLQ>.DDDBBU.BACKUP	CYLS	60	10
<PREVDBHLQ>.DDDDBU.BACKUP	CYLS	15	15
<PREVDBHLQ>.BEXCLAUD>	CYLS	200	200
<PREVDBHLQ>.BEXCLINV	CYLS	200	200
<PREVDBHLQ>.BEXCLJNL	CYLS	200	200
<PREVDBHLQ>.BEXCLPCY	CYLS	200	200
<PREVDBHLQ>.BEXCLSCS	CYLS	200	200
<PREVDBHLQ>.BEXCLSDS	CYLS	200	200
<PREVDBHLQ>.ESDSM94	CYLS	150	150
<PREVDBHLQ>.NSDSM94	CYLS	150	150
<PREVDBHLQ>.ESDSC12	CYLS	150	150
<PREVDBHLQ>.NSDSC12	CYLS	150	150
<PREVDBHLQ>.ESDSC23	CYLS	50	25
<PREVDBHLQ>.NSDSC23	CYLS	50	25
<PREVDBHLQ>.ESDSC24	CYLS	50	25
<PREVDBHLQ>.NSDSC24	CYLS	50	25
<PREVDBHLQ>.EAUDAOP	CYLS	15	15
<PREVDBHLQ>.EAUDAVR	CYLS	15	15
<PREVDBHLQ>.ESCSCNP	CYLS	15	15
<PREVDBHLQ>.ESCSCRS	CYLS	15	15
<PREVDBHLQ>.ESCSICP	CYLS	15	15
<PREVDBHLQ>.ESCSOPE	CYLS	15	15
<PREVDBHLQ>.ESRGSR1	CYLS	15	15
<PREVDBHLQ>.NAUDAOP	CYLS	15	15

Name	Space Units	Primary Quantity	Secondary Quantity
<PREVDBHLQ>.NAUDAVR	CYLS	15	15
<PREVDBHLQ>.NSCSCNP	CYLS	15	15
<PREVDBHLQ>.NSCSCRS	CYLS	15	15
<PREVDBHLQ>.NSCSICP	CYLS	15	15
<PREVDBHLQ>.NSCSOPE	CYLS	15	15
<dbHLQ>.CXX?NAME.BK60CXX	CYLS	35	10
<dbHLQ>.CXX?NAME.BK600002	CYLS	60	15
<dbHLQ>.CXX?NAME.BK6000015	CYLS	15	15
<dbHLQ>.CXX?NAME.BK604000	CYLS	350	300

CSMU5002

The following values are required if you are upgrading from CA MSM V5.0 to CA CSM Version 6.0:

Note: The total primary quantity of cylinders is 2,645 of 3390 DASD space.

Name	Space Units	Primary Quantity	Secondary Quantity
<PREVDBHLQ>.CXX.BACKUP	CYLS	35	10
<PREVDBHLQ>.DB4000.BACKUP	CYLS	350	300
<PREVDBHLQ>.DDDBBU.BACKUP	CYLS	60	10
<PREVDBHLQ>.DDDDBU.BACKUP	CYLS	15	15
<PREVDBHLQ>.BEXCLAUD>	CYLS	200	200
<PREVDBHLQ>.BEXCLINV	CYLS	200	200
<PREVDBHLQ>.BEXCLJNL	CYLS	200	200
<PREVDBHLQ>.BEXCLPCY	CYLS	200	200
<PREVDBHLQ>.BEXCLSCS	CYLS	200	200
<PREVDBHLQ>.BEXCLSDS	CYLS	200	200
<PREVDBHLQ>.ESDSM94	CYLS	150	150
<PREVDBHLQ>.NSDSM94	CYLS	150	150

Name	Space Units	Primary Quantity	Secondary Quantity
<PREVDBHLQ>.ESDSC12	CYLS	150	150
<PREVDBHLQ>.NSDSC12	CYLS	150	150
<PREVDBHLQ>.ESDSC23	CYLS	50	25
<PREVDBHLQ>.NSDSC23	CYLS	50	25
<PREVDBHLQ>.ESDSC24	CYLS	50	25
<PREVDBHLQ>.NSDSC24	CYLS	50	25
<PREVDBHLQ>.EAUDAOP	CYLS	15	15
<PREVDBHLQ>.EAUDAVR	CYLS	15	15
<PREVDBHLQ>.ESCSCNP	CYLS	15	15
<PREVDBHLQ>.ESCSCRS	CYLS	15	15
<PREVDBHLQ>.ESCSICP	CYLS	15	15
<PREVDBHLQ>.ESCSOPE	CYLS	15	15
<PREVDBHLQ>.ESRGSR1	CYLS	15	15
<PREVDBHLQ>.NAUDAOP	CYLS	15	15
<PREVDBHLQ>.NAUDAVR	CYLS	15	15
<PREVDBHLQ>.NSCSCNP	CYLS	15	15
<PREVDBHLQ>.NSCSCRS	CYLS	15	15
<PREVDBHLQ>.NSCSICP	CYLS	15	15
<PREVDBHLQ>.NSCSOPE	CYLS	15	15
<dbHLQ>.CXX?NAME.BK60CXX	CYLS	35	10
<dbHLQ>.CXX?NAME.BK600002	CYLS	60	15
<dbHLQ>.CXX?NAME.BK6000015	CYLS	15	15
<dbHLQ>.CXX?NAME.BK604000	CYLS	350	300

CSMU4102

The following values are required if you are upgrading from CA MSM R4.1 to CA CSM Version 6.0:

Note: The total primary quantity of cylinders is 3,495 of 3390 DASD space.

Name	Space Units	Primary Quantity	Secondary Quantity
<PREVDBHLQ>.CXX.BACKUP	CYLS	35	10
<PREVDBHLQ>.DB4000.BACKUP	CYLS	350	300
<PREVDBHLQ>.DDDBBU.BACKUP	CYLS	60	10
<PREVDBHLQ>.DDDDBU.BACKUP	CYLS	15	15
<PREVDBHLQ>.BEXCLAUD>	CYLS	200	200
<PREVDBHLQ>.BEXCLINV	CYLS	200	200
<PREVDBHLQ>.BEXCLJNL	CYLS	200	200
<PREVDBHLQ>.BEXCLPCY	CYLS	200	200
<PREVDBHLQ>.BEXCLSCS	CYLS	200	200
<PREVDBHLQ>.BEXCLSDS	CYLS	200	200
<PREVDBHLQ>.ESDSM94	CYLS	150	150
<PREVDBHLQ>.NSDSM94	CYLS	150	150
<PREVDBHLQ>.ESDSC12	CYLS	150	150
<PREVDBHLQ>.NSDSC12	CYLS	150	150
<PREVDBHLQ>.EAUDAOP	CYLS	15	15
<PREVDBHLQ>.EAUDAVR	CYLS	15	15
<PREVDBHLQ>.ESCSCNP	CYLS	15	15
<PREVDBHLQ>.ESCSCRS	CYLS	15	15
<PREVDBHLQ>.ESCSDUF	CYLS	50	25
<PREVDBHLQ>.ESCSICP	CYLS	15	15
<PREVDBHLQ>.ESCSOPE	CYLS	15	15
<PREVDBHLQ>.ESDSC13	CYLS	50	25
<PREVDBHLQ>.ESDSC23	CYLS	50	25
<PREVDBHLQ>.NSDSC23	CYLS	50	25

Name	Space Units	Primary Quantity	Secondary Quantity
<PREVDBHLQ>.ESDSC24	CYLS	50	25
<PREVDBHLQ>.NSDSC24	CYLS	50	25
<PREVDBHLQ>.ESDSSYS	CYLS	15	15
<PREVDBHLQ>.ESRGSR1	CYLS	15	15
<PREVDBHLQ>.NAUDAOP	CYLS	15	15
<PREVDBHLQ>.NAUDAVR	CYLS	15	15
<PREVDBHLQ>.NSCSCNP	CYLS	15	15
<PREVDBHLQ>.NSCSCRS	CYLS	15	15
<PREVDBHLQ>.NSCSICP	CYLS	15	15
<PREVDBHLQ>.NSCSOPE	CYLS	15	15
<PREVDBHLQ>.NSDSC13	CYLS	50	25
<PREVDBHLQ>.NSDSC24	CYLS	50	25
<PREVDBHLQ>.NSDSSYS	CYLS	15	15
<dbHLQ>.CXX?NAME.BK60CXX	CYLS	35	10
<dbHLQ>.CXX?NAME.BK600002	CYLS	60	15
<dbHLQ>.CXX?NAME.BK6000015	CYLS	15	15
<dbHLQ>.CXX?NAME.BK604000	CYLS	350	300

CSMUxx09

The following table lists the data sets that are created when this job runs.

Note: The total primary quantity of cylinders is 460 of 3390 DASD space.

Name	Space Units	Primary Quantity	Secondary Quantity
<dbHLQ>.BK60CXX	CYLS	35	10
<dbHLQ>.BK600002	CYLS	60	15
<dbHLQ>.BK600015	CYLS	15	15
<dbHLQ>.BK604000	CYLS	350	300

Appendix B: External Interfaces

Some of the tasks that you perform using the web-based interface can also be performed outside of CA CSM using external interfaces. CA CSM is able to accept commands from external applications, translate them into an appropriate format, and generate tasks based on them.

Performing Tasks Outside of CA CSM

You can regularly perform some PAS tasks such as updating the catalog tree and obtaining updates for products and product releases using external schedulers. You can also execute task management policies and change log4j settings.

You set up the scheduler to issue commands that are translated into the MVS command MODIFY (F). This command obtains a set of parameters such as your user ID, the command type you want to execute, and its properties.

Note: For information about how to configure your scheduler, see its documentation.

Every time a scheduled task is executed, CA CSM validates the received command. If the validation is successful, the appropriate task is created and performed in CA CSM. You can view the task status from the Tasks tab.

Note: To set up the automatic updates, you must have a valid TSO user ID, and an account set up on the CA Support Online website.

MVS MODIFY Command

The MODIFY (F) command allows you to perform the following actions:

- Update the product tree
- Update for products and product releases
- Execute task management policies
- Change log4j settings

For each action, the command contains a particular set of parameters.

The MODIFY command has the following format:

```
F jobname,APPL=command,parameter=value[,parameter=value,…]
```

jobname

Defines the name of the job which is started.

APPL=*command*

Defines the command that is issued.

command

Specifies the command type. The following options are available:

UPDTTREE

Updates the product tree.

UPDTCAT

Updates products and product releases.

CHNGLOG

Temporarily changes log4j settings at run time.

EXECPLCY

Executes a task management policy.

parameter=value

Defines a parameter that may vary depending on the type of the command that you issue: updating the product tree, (see page 144) updating products or product releases (see page 145), changing log4j settings (see page 148), or execute task management policies (see page 149).

Update the Product Tree

For updating the product tree, this command has the following format:

```
F jobname,APPL=UPDTTREE,USERID=user_id[,FILTER=filter_name][,VENDOR=vendor_name]
```

USERID=*user_id*

Defines the user who issues the command.

FILTER=*filter_name*

(Optional) Defines the name of the site ID filter to use for updating the catalog tree.

Note: If the filter name is not defined, the command is rejected. If no filter is defined, all site IDs are used. If the VENDOR parameter is specified, the FILTER parameter must come before the VENDOR parameter.

VENDOR=*vendor_name*

(Optional) Defines the name of the vendor for which you update the catalog tree.

Note: If the vendor name is not defined, the command is executed for the default vendor, CA.

Note: Do not change the order of the command parameters. Doing so may result in parsing errors.

Example

This example updates the product list for the CA Technologies mainframe products:

```
F MSMTC,APPL=UPDTTREE,USERID=MYUSERID,VENDOR=CA
```

Update Products and Product Releases

For obtaining updates for products and product releases, this command has the following format:

```
F jobname,APPL=UPDTCAT,USERID=user_id,PRODUCT=product_name
[,RELEASE=release_number][,TYPE=FULL|PTFS][,MODE=EXECUTE|CHECK|ATOMIC]
```

USERID=*user_id*

Defines the user who issues the command.

PRODUCT=*product_name*

Defines the name of the product for which you want to obtain updates.

Note: To distinguish between products whose names are not unique (they share part of the name), put *product_name* in single quotes. For example, PRODUCT='CA IDMS SQL OPTION - MVS' searches for the product named *CA IDMS SQL OPTION - MVS* and ignores *CA Easytrieve Report Generator CA IDMS SQL OPTION - MVS*.

RELEASE=*release_number*

(Optional) Defines the product release for which you want to obtain updates.

TYPE=FULL|PTFS

(Optional) Specifies the type of a product or release update to be obtained.

Note: If the type is not explicitly defined in the command syntax, the command is executed with the FULL type.

FULL

Retrieves all product packages and maintenance packages. This is the default.

PTFS

Retrieves only maintenance packages that have been released since the product release was updated last time.

MODE=EXECUTE|CHECK|ATOMIC

(Optional) Specifies the mode in which the command for obtaining updates for products and product releases is executed.

Note: When the mode is not explicitly defined in the command syntax, the command is executed with EXECUTE mode.

EXECUTE

Validates the command and executes any tasks generated based on it. This is the default.

CHECK

Validates the command, returns any errors but does not execute any tasks.

ATOMIC

Runs the command in the CHECK mode, validating the command and generating task based on it, but does not execute tasks immediately: it stores all the validated tasks and only executes them if all tasks have been validated.

Note: All found validation errors that are defined as WARNING are treated as SEVERE. Any error with a severity level of WARNING or SEVERE causes the entire command to fail.

Note: Do not change the order of the command parameters. Doing so may result in parsing errors.

Examples

Obtain Available Updates for One or Multiple Products

These examples obtain updates for all available releases of CA Panvalet:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA PANVALET – MVS,TYPE=FULL
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA PANVALET - MVS
```

This example obtains updates for all available releases of CA Panvalet, CA Auditor for z/OS, and CA SMF Director:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA PANVALET - MVS, CA AUDITOR - MVS,
CA SMF DIRECTOR - MVS
```

This example obtains updates for all available releases of CA IDMS SQL OPTION MVS and ignores updates for any products whose names contain the part *CA IDMS SQL OPTION MVS*:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT='CA IDMS SQL OPTION MVS'
```

Obtain Specific Updates for One Product

This example obtains updates for releases 6.0, 11.0, and 12.0 of CA SMF Director in the CHECK mode:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA SMF DIRECTOR -
MVS,RELEASE=6.0,11.0,12.0,MODE=CHECK
```

This example obtains updates for release 16.0 of CA IDMS SQL OPTION MVS and ignores updates for any products whose names contain the part *CA IDMS SQL OPTION MVS*:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT='CA IDMS SQL OPTION
MVS',RELEASE=16.0
```

Obtain Specific or Available Updates for Multiple Products

This example obtains updates for releases 6.0 and 11.0 of CA SMF Director and updates for all available releases of CA Panvalet in the ATOMIC mode:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA SMF DIRECTOR -
MVS,RELEASE=6.0,11.0,PRODUCT=CA PANVALET - MVS,MODE=ATOMIC
```

This example obtains updates for release 12.0 of CA SMF Director, and release 14.5 of CA Panvalet:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA SMF DIRECTOR -
MVS,RELEASE=12.0,PRODUCT=CA PANVALET - MVS,RELEASE=14.5
```

This example obtains only maintenance packages for release 12.1 of CA Auditor for z/OS that have been released since the product release was updated last time:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA AUDITOR -
MVS,RELEASE=12.1,TYPE=PTFS
```

This example obtains only maintenance packages for all releases of CA Panvalet that have been released since the product release was updated last time:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA PANVALET - MVS,TYPE=PTFS
```

This example obtains updates for release 16.0 of CA IDMS SQL OPTION MVS, and release 16.0 of CA IDMS/DB - MVS, and ignores updates for any products whose names contain the part *CA IDMS SQL OPTION MVS* or *CA IDMS/DB - MVS*:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT='CA IDMS SQL OPTION
MVS',RELEASE=16.0,PRODUCT='CA IDMS/DB - MVS',RELEASE=16.0
```

This example obtains updates for all available releases of CA IDMS SQL OPTION MVS, and all available releases of CA IDMS/DB - MVS, and ignores updates for any products whose names contain the part *CA IDMS SQL OPTION MVS* or *CA IDMS/DB - MVS*:

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT='CA IDMS SQL OPTION MVS,CA IDMS/DB
- MVS'
```

Change log4j Settings

For temporarily changing log4j settings at run time, this command has the following format:

```
F jobname,APPL=CHNGLOG,logger[*]:loglevel
```

logger

Defines the log4j logger, which is usually the class or package name.

loglevel

Specifies the lowest log4j level of messages to display, such as DEBUG, INFO, WARN, ERROR, or FATAL.

Notes:

- Do not change the order of the command parameters. Doing so may result in parsing errors.
- Do not change log4j settings at run time unless instructed to do so by CA Support.

Example

This example temporarily changes the log4j settings of the SCS logger to warning or higher (WARN, ERROR, or FATAL):

```
F MSMTC,APPL=CHNGLOG,com.ca.scs:WARN
```

This example temporarily changes the log4j settings of all the SAM Communications loggers to debug or higher (DEBUG, INFO, WARN, ERROR, or FATAL):

```
F MSMTC,APPL=CHNGLOG,com.ca.SAM.Communications.*:DEBUG
```

This example temporarily changes the log4j settings of all loggers to informational or higher (INFO, WARN, ERROR, or FATAL):

```
F MSMTC,APPL=CHNGLOG,*:INFO
```

Execute Task Management Policy

For executing a task management policy, this command has the following format:

```
F jobname,APPL=EXECPLCY,USERID=user_id,POLICY=policy_name
```

USERID=*user_id*

Defines the user who issues the command.

POLICY=*policy_name*

Specifies the name of the policy that you want to execute.

The policy name must be a valid policy name in CA CSM.

Note: Do not change the order of the command parameters. Doing so may result in parsing errors.

Example

This example executes a task management policy with the name MYARCHIVEPOLICY:

```
F MSMTC,APPL=EXECPLCY,USERID=MYUSERID,POLICY=MYARCHIVEPOLICY
```

Command Validation

Every time a scheduled update is executed, CA CSM validates that the following criteria are met:

- The command format and syntax is correct.
- Data that is defined in the command (product names, release numbers) is valid and correspond with the data in CA CSM database.
- The user issuing the command has appropriate credentials.

If any of these statements are false, the following events take place:

- The command is not executed.
- The task is not generated.
- An error is logged in the STDOUT DDNAME in the JOBLOG for the CA CSM region.

Log Messages

When a command for a scheduled update is issued, a set of messages is recorded in STDOUT DDNAME in the CA CSM region JOBLOG. These messages reflect the steps CA CSM performs while processing the request.

Each message starts with MSMM, followed by a four-digit number and the message status code. The message status code can be:

- I – Information
- E – Error
- S – Serious

Example

This example displays messages that are recorded in the STDOUT DDNAME in the CA CSM region JOBLOG after USER1 issued a command obtaining updates for CA Panvalet, release 14.5.

```
MSMM0101I - MODIFY command received: UPDTCAT
MSMM0100I - Handling command: UPDTCAT - USERID=USER1,PRODUCT=CA PANVALET -
MVS,RELEASE=14.5
MSMM0191I - Authenticating user: USER1.
MSMM0153E - Release 14.5 for product CA PANVALET - MVS not found in software catalog.
MSMM0162I - PAS task executed for specific product releases.
```

Note: For more information about CA CSM messages, see the *Message Reference Guide*.

Glossary

CA CSM application server

The *CA CSM application server* is the CA CSM Tomcat region that supports the CA CSM application code.

CA CSM Common Services

The *CA CSM Common Services* (CETN600) is a contributed component of CA Common Services for z/OS that consists of the Software Deployment Service (SDS) and the Software Configuration Service (SCS).

CA Datacom/MSM server

The *CA Datacom/MSM server* is a server that lets workstation-based applications use the CA Datacom/MSM database.

CA Recommended Service (CA RS)

CA Recommended Service (CA RS) is a set of maintenance packages that have been tested in a mainframe integrated system test environment. We recommend that you install CA RS maintenance to keep your products up-to-date. To keep yourself informed about new CA RS maintenance available, download (manually or automatically) all CA RS files that list published maintenance for that CA RS level.

configurations

A *configuration* is a CA CSM object that you create to tailor your installed software or CA CSM deployed software. Configuration makes your software usable in your environment. A configuration contains the profiles, variables, and resources specific to your environment.

confirm

Confirms that the deployment is complete. This is the final action by the user. A deployment is not completed until it is confirmed. After it is confirmed the deployment moves to the Confirmed deployment list.

contact system

The *contact system* defines which system the deployment is unpackaged on. That is, which system CAICCI is spawned to run the unpackaging.

custom data set

A *custom data set* is a data set that contains either a z/OS data set or USS path.

data destination

A *data destination* must be defined for every system. The data destination is how you tell CA CSM which technique to use to transport the deployment data to the remote system. Data destinations are assigned to non-sysplex systems, sysplexes, and shared DASD clusters. Data destinations are named objects, and thus can be assigned to multiple entities in the system registry and have their own independent maintenance dialogs.

data set name mask

A d*ata set name mask* is a unique name that identifies each data set. It consists of one or more qualifiers separated by periods, and has a maximum input length of 64 characters, including the periods. When the data set name mask is translated, it has a maximum length of 44 characters including the periods.

deploy

The *deploy* functionality combines the snapshot, transmit, and deploy actions into one action, letting you copy your CA CSM product onto systems across your enterprise. For example, you can send one or many products to one or many systems by copying it to a shared DASD or through FTP.

deployment

A *deployment* is a CA CSM object that you create to deploy libraries and data sets using a process that copies target libraries defined to SMP/E and user data sets across both shared DASD and networked environments.

directory path

The root d*irectory path* is the base directory to which the FTP server is allowed access. The FTP server will be allowed to create files to or read files from this directory and any of its subdirectories. The directory path is a USS path name, it consists of one or more directory leaves separated by forward slashes, and has a maximum input length of 255 characters including slashes. When the directory path is translated, it has a maximum length of 255 characters.

driving system

A *driving system* is the system where the CA CSM application server is running.

FTP port

An *FTP port* is the point of connection through which files are transferred. The default is 21.

GIMZIP

GIMZIP is an IBM utility that creates portable packages of software with a suffix of *z*.

monoplex

A *monoplex* is a sysplex that has only one member system and minimally a single coupling facility. Currently, a monoplex is tracked in the same manner as a sysplex, except the sysplex name shown in the web-based interface is actually the monoplex system name.

MSMCAUX

MSMCAUX is the JCL procedure that is used to start the auxiliary address space. CA Common Services for z/OS that CA CSM uses includes a sample procedure in the member MSMCAUX of the CA Common Services for z/OS CAW0PROC (CCS*hlq*.CAW0PROC) library. You must copy this procedure to a system PROCLIB that z/OS START commands use and modify it to suit your installation environment. The MSMCAUX sample member describes the changes that are required. Do not start the MSMCAUX procedure manually. The MSMCAUX procedure is started by the SCS address space (MSMCPROC).

MSMCPROC

MSMCPROC is the JCL procedure that is used to start the SCS address space. CA Common Services for z/OS that CA CSM uses includes a sample procedure in the member MSMCPROC of the CA Common Services for z/OS CAW0PROC (CCS*hlq*.CAW0PROC) library. You must copy this procedure to a system PROCLIB that the z/OS START commands use and modify it to suit your installation environment. The MSMCPROC sample member describes the changes that are required.

MSMTC/MSMTCSRV

MSMTC/MSMTCSRV is the job stream or started task associated with the CA CSM application server (see page 151).

MUF

MUF is the CA Datacom/MSM Multi-User-Facility.

non-sysplex

A *non-sysplex* is a stand-alone z/OS system that is not part of a sysplex or a monoplex system.

preview

Preview identifies the deployment by name and briefly states the products, systems, means of transport, target libraries including source, target and resolution, as well as SMP/E environment and snapshot information.

Product Acquisition Service (PAS)

The *Product Acquisition Service (PAS)* facilitates the acquisition of mainframe products and the service for those products, such as program temporary fixes (PTFs). PAS retrieves information about products to which your site is entitled. Then it records these entitlements in a software inventory that is maintained on your driving system.

SCS address space

The *SCS address space* is a specially defined location where the system registry and commands for interrogating output and console traffic reside within the operating system. The SCS address space provides the services and processing necessary to implement configurations across your targeted z/OS systems. Each target system that is expected to support SCS processing must execute an SCS address space.

shared DASD clusters

A s*hared DASD clusters* system is a set of systems that shared DASD and it can be composed of sysplex and/or non-sysplex systems. Staging system cannot be part of a shared DASD cluster.

snapshot

A *snapshot* is a copy of the set of target libraries that CA CSM makes using the IBM utility GIMZIP. CA CSM uses GIMZIP to create a compressed archive of these libraries, including a list of applied maintenance. The SMP/E environment is locked during this archive creation process to verify the integrity of the archived data.

Software Configuration Service (SCS)

The *Software Configuration Service* (SCS) facilitates product configuration. Configuration is a process of copying target libraries to run-time libraries and customizing the product for your site to bring it to an executable state.

Software Deployment Service (SDS)

The *Software Deployment Service* (SDS) facilitates product deployment. Deployment is a process of copying SMP/E target libraries from a driving system (where the CA CSM application server is running) to a target (remote destination) system. The target system could be the local z/OS system, a remote z/OS system, a staging system, or a sysplex.

Software Installation Service (SIS)

The *Software Installation Service (SIS)* facilitates the installation and maintenance of mainframe products in the software inventory of the driving system. This facilitation includes browsing downloaded software packages, managing SMP/E consolidated software inventories on the driving system, and automating installation tasks.

staging system

A *staging system* is a virtual system that you can use to deploy and configure product before activating it on a target system. If the target system is the same as the CA CSM driving system, the software is activated locally. To use a staging system, the CA CSM driving system must be registered in the CA CSM system registry.

storage classes

storage classes apply only to SMS-managed data sets and objects. They allow you to define different levels of performance and availability services for your data sets. Using them, you can separate the level of service needed by a data set or object from its physical characteristics. Storage classes can supply such information as attributes for dynamic cache management, sequential data set striping, and concurrent copy.
It is the association of a storage class with a data set or object which causes the data set or object to be SMS-managed. Because of this, such functions as dynamic cache management and sequential data set striping apply only to SMS managed data sets. Data sets may be SMS-managed or non-SMS managed. Objects must be SMS-managed.

sysplex

A *sysplex* (SYStem comPLEX) is the IBM mainframe system complex which is a single logic system running on one or more physical systems. Each of the physical systems that make up a sysplex, is often referred to as a “member” system.

system registry

The *system registry* is a repository of variable data that all CA CSM managed products share. The system registry repository contains information about the systems that have been defined to CA CSM and selected as a target for deployments and configurations. You can create non-sysplex, sysplex, shared DASD cluster, and staging systems. You can maintain, validate, view, and delete a registered system and you can investigate a failed validation.

topology

The enterprise system *topology* can include shared DASD environments, networked environments, and z/OS systems.

transmit

The *transmit* functionality lets you copy a product onto systems across the enterprise through FTP, in preparation for a subsequent deployment.

Uniform Resource Identifier (URI)

A *Uniform Resource Identifier (URI)* is a string of characters used to identify a name or a resource on the Internet. Such identification enables interaction with representations of the resource over a network (typically the World Wide Web) using specific protocols. Schemes specifying a concrete syntax and associated protocols define each URI.
For a shared DASD cluster or sysplex, the URI must be the URI of the Contact System.

UNIX System Services (USS) files

For *UNIX System Services* (*USS*) *files* for z/OS systems, there are three types of files system: HFS (Hierarchical File Systems), zFS (zSeries File Systems), and NFS (Network File Systems). USS files are any one, or combination, of these file systems, and start with the root directory, which is denoted by a single forward slash (/).

validation

The *validation* process is started by the user when they select the Validate button in the Actions drop down for a sysplex system, non-sysplex system, and shared DASD cluster on that system’s System Registry Page (staging systems are not validated). This starts a background security procedure using the CAICCI validation services to validate this system.

VOLSER

A *VOLSER* is the Volume Serial Number that places the data on an explicit volume.