CA Chorus™ Software Manager

Installation Guide

Release 5.1

51000068XIN, Second Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA Chorus™ Software Manager (CA CSM)
- 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 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.

Contents

Chapter 1: Overview

This guide describes how to install CA CSM Release 5.1 or upgrade CA CSM to the latest version.

This section contains the following topics:

Audience

This guide details the tasks that a system programmer can complete to install or upgrade CA CSM.

How the Installation Process Works

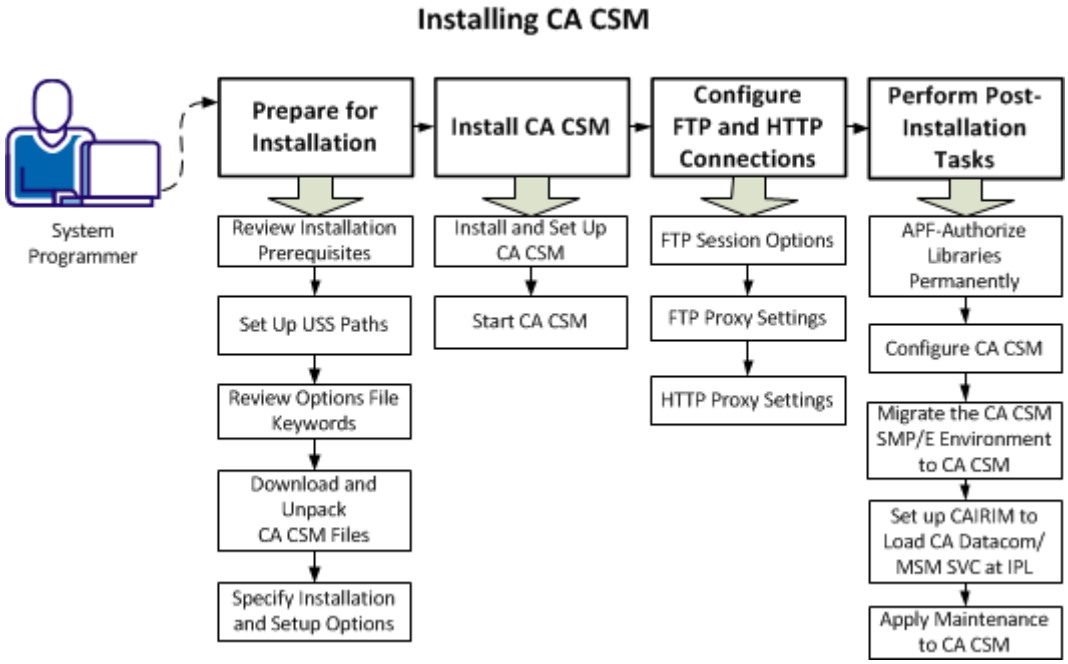
Perform *one* of the following actions:

- If you do not have CA CSM installed, install CA CSM Release 5.1 (see page 9).
- If you have a previous version of CA CSM installed, upgrade CA CSM to Release 5.1 (see page 51).

Important! Before you start installing or upgrading CA CSM Release 5.1, read the *Site Preparation Guide* thoroughly and complete tasks that are described in the guide.

Chapter 2: How to Install CA CSM

You perform the following tasks to install CA CSM:



1. Prepare for installation:
   a. Review installation prerequisites (see page 10).
   b. Set up USS paths (see page 11).
   c. Review options file keywords (see page 14).
   d. Download and unpack CA CSM files (see page 14).
   e. Specify installation and setup options (see page 16).
2. Install CA CSM:
   a. Install and set up CA CSM (see page 18).
   b. Start CA CSM (see page 26).
3. Configure FTP and HTTP connections:
   a. FTP session options (see page 29).
   b. FTP proxy settings (see page 31).
   c. HTTP Proxy Settings (see page 37).

4. Perform post-installation tasks:
   a. APF-authorize llbraries permanently (see page 42).
   b. Configure CA CSM (see page 43).
   c. Migrate the CA CSM SMP/E environment to CA CSM (see page 44).
   d. Set up CAIRIM to load CA Datacom/MSM SVC at IPL (see page 45).
   e. Apply maintenance to CA CSM (see page 48).

Prepare for Installation

This section describes tasks that you perform before you start installing CA CSM.

Review Installation Prerequisites

Before you start installing CA CSM, do the following:

1. Confirm that you have all necessary prerequisite authorizations using the Prerequisite Validator utility.
2. Review disk space requirements.
   - Hierarchical File System (HFS) or zSeries File System (zFS) space = 2500 cylinders
   - z/OS space = 2400 cylinders
   - DASD space = 100 tracks
   - For the SDS, each target system needs 500 cylinders of 3390, except CA Database Management Solutions for DB2 for z/OS, which needs 1500 cylinders
3. Review software requirements:
   - CA software—Your system must have CA Common Services for z/OS Release 14.1, Version 14, or r12.
   - IBM software—Your system must satisfy the following requirements:
     - The latest version of z/OS or the last previous version
     - TCP/IP protocol suite of z/OS Communications Server, with the FTP.DATA data set configured with the JESINTERFACELEVEL 2 statement
     - SMP/E V3R5 at least
     - IBM Java SDK for z/OS

- PC software—The computer that is used to access CA CSM must have one of the following web browsers:
  - Mozilla Firefox 13, 14, 15, or 16
  - Microsoft Internet Explorer 7, 8, or 9
  - Microsoft Internet Explorer 10 (compatibility mode only)

  Note: Microsoft Internet Explorer 10 native mode is *not* supported and causes multiple browser errors.

4. Review web access requirements to the following websites:
   - supportservices.ca.com
   - ftp.ca.com
   - ftpca.ca.com
   - scftpd.ca.com
   - ftpdownloads.ca.com
   - supportftp.ca.com
   - sdownloads.ca.com
5. Customize the following z/OS OMVS values:
   - MAXASSIZE(2147483647)
   - MAXCPUTIME(20000)
   - MAXFILEPROC(10000)
   - MAXTHREADS(1000)
   - MAXTHREADTASKS(1000)
6. Set up security on the following systems:
   - The CA CSM application server
   - Target systems
7. Configure the home directory for address space ACIDs.

Note: For more information, see the *Administration Guide*.

Set Up USS Paths

CA CSM can use HFS or zFS file systems for its download, installation, setup, and general usage.

Note: We recommend using zFS file systems. For information about how to migrate from HFS file systems to zFS file systems, see the latest *IBM z/OS Migration* guide.

Before you download and install CA CSM, your USS administrator must set up directory paths and optionally configure file systems for these files. You can set up the paths in a single file system or multiple file systems, depending on the policy at your site.

Note: We recommend that you set up your USS file system using a multiple file system structure.

Minimally, you require four directories with 775 permissions.

During operation, CA CSM dynamically creates and mounts additional file systems. File systems are mounted during startup, and as a product and maintenance are downloaded.

For a zFS file system to grow dynamically, specify AGGRGROW when you mount the file system. For example:

```
MOUNT FILESYSTEM('yourHLQ.MSM.ZFS') -
     MOUNTPOINT('/parent_path/msmserv/version_number/msm')          -
     TYPE(ZFS)                                  -
     MODE(RDWR)                                 -
     PARM('AGGRGROW')
```

For more information, see the IBM *Distributed File Service zFS Administration*.

CA CSM uses the following z/OS UNIX System Services (USS) directory path structure:

```
/parent_path/msmserv/mpm
/parent_path/msmserv/version_number/msm
/parent_path/msmserv/version_number/msmruntime
/parent_path/msmserv/version_number/msminstall
```

Note: The /mpm directory should not have a version number. This is a common directory that is shared between CA CSM versions.

***/parent_path*/msmserv/**

Specifies the CA CSM parent path name as defined at your site as the primary mount point or directory, for example, one of the following:

```
/u/users/msmserv
/usr/lpp/msmserv
/cai/msmserv
```

Note: We recommend that you use /msmserv as the final portion of the parent path; however, you can change it if necessary for your site standards.

***/parent_path*/msmserv/mpm**

Specifies the mount point for file systems that CA CSM allocates and mounts. The mount point is the directory that CA CSM uses to mount the software catalog root application file system. You specify this path in the MountPath keyword of the options file.

Note: If you are an existing CA CSM customer and are upgrading, you do not need to create this path. The upgrade process reuses the previous version path by default.

***/parent_path*/msmserv/*version_number*/msm**

Specifies the directory for target USS files for CA CSM products. The content is managed through SMP/E.

Space: 750,100 cylinders

***/parent_path*/msmserv/*version_number*/msmruntime**

Specifies the directory for CA CSM runtime files, that is, the directory that the running CA CSM application executes from. You specify this path in the RunTimeUSSPath keyword of the options file.

Space: 750,100 cylinders

***/parent_path*/msmserv/*version_number*/msminstall**

Specifies the directory for CA CSM installation data, including all downloaded and unpacked CA CSM files.

Space: 1000,100 cylinders

Note: This directory can be deleted after the installation is completed.

Note: For more information about how to set up USS paths for multiple versions of CA CSM, see the *Best Practices Guide*.

Using a Single File System

We recommend that you set up your USS file system using a multiple file system structure. However, if you must structure your USS file system as a single file system, ensure that it contains all of the space that is required for the product installation and ongoing operations.

- Use a CA CSM parent path name as defined at your site, for example, one of the following:

  ```
  /u/users/msmserv
  /usr/lpp/msmserv
  /cai/msmserv
  ```

  Note: We recommend that you use /msmserv as the final portion of the parent path; however, you can change it if necessary for your site standards.

- Define the following required directories so that the structure looks like the following:
  /parent_path/msmserv/mpm
  /parent_path/msmserv/*version_number*/msm
  /parent_path/msmserv/*version_number*/msmruntime
  /parent_path/msmserv/*version_number*/msminstall
- Update the UNIX BPXPRM*xx* control member with the single file system and mount point.
- After installation completes, delete the directory */parent_path*/msmserv/*version_number*/msminstall and its contents.

Review Options File Keywords

Before you start installing CA CSM, we recommend that you use the options file worksheet (see page 77). Review the options file keywords, and gather values for them specific for your site. You will need the keywords for installation.

Download and Unpack CA CSM Files

The packed CA CSM product package is available on the CA Support Online website.

Follow these steps:

1. Go to the Download Center on the CA Support Online website.
2. Enter CA Chorus Software Manager in the Select a Product field, select the latest version and the Select all components check box, and click Go.

   Note: If you cannot find CA Chorus Software Manager in the product list, follow the instructions from the Free Service area on the top of the product page.

   A list of product downloads is displayed.
3. Download the software package.

After you download the software package, unpack and extract the files for installation.

Important! Verify that the unpacked CA CSM packages are stored on permanent storage volumes, and not on work or temporary volumes.

Follow these steps:

1. Go to the directory where the CA CSM package is downloaded, and enter the following command to unpack the package:

   ```
   pax -rvf 51000068X01.pax.Z
   ```

   Note: The full pax file name, including the Z suffix, is case-sensitive. Verify that you use the exact case of the file name on the system where you issue the pax command. Rename the file, if necessary.

   The MSMInstaller directory is created, and the package is unpacked into the directory.

2. Customize the UNZIPJCL file in the MSMInstaller directory to conform to the data set and USS directory naming standards at your site. Submit the job (for example, using the submit z/OS shell command in USS OMVS), and review the output for successful completion.

   The UNZIPJCL job creates the MSMSetup and the MSMProduct directories that contain the CA CSM installation files.

   - Replace the following text with the path where the MSMInstaller directory was created:

     ```
     <-- YOUR USS HFS DIRECTORY -->
     ```

   - Replace the following text with the path where you want to create the MSMSetup and MSMProduct directories:

     ```
     <-- YOUR CA CSM USS HFS DIRECTORY -->
     ```

     Note: We recommend that the directories <-- YOUR USS HFS DIRECTORY --> and <-- YOUR CA CSM USS HFS DIRECTORY --> are set to the same path.

   - Replace **yourHLQ** with the high-level qualifier for the ISPF UI Tool data set. The length of the high-level qualifier must not be greater than 26 characters.

   The MSMSetup directory, the MSMProduct directory and the CA CSM Installation ISPF UI tool z/OS data set are created, and the CA CSM files are extracted.

   Note: When you open the UNZIPJCL file, a warning message can appear at the bottom of the screen. This message indicates that any trailing blanks are removed from the UNZIPJCL file. Removing or retaining trailing blanks does not affect job execution. You can ignore this message.

Specifying Installation and Setup Options

The directory (.../MSMSetup) where you extracted the CA CSM files contains the MSMSetupOptionsFile.properties options file. The CA CSM setup utility uses the contents of the MSMSetupOptionsFile.properties options file in the MSMSetup directory to tailor the CA CSM installation and setup process.

The file uses the following keywords to specify the option values in the format *option_keyword=value*.

Important! The keywords that are used in the options file are specific to the CA CSM installation setup process. The values for some keywords are transformed to values that are acceptable to CA CSM during this process. Do not use these values for similar keywords in other areas of CA CSM unless requested by CA Support.

The file contains preset values, but you *must* customize the contents of this file to reflect your requirements.

You can specify installation and setup options either manually (see page 16) or using the ISPF UI tool (see page 16).

Specify Options Manually

To specify installation and setup options manually, review and customize the options in the MSMSetupOptionsFile.properties file using an EBCDIC character set capable text editor. For example, you can use Interactive System Productivity Facility (ISPF). If necessary, consult with other team members at your site to gather the values.

Specify Options Automatically Using the ISPF UI Tool

You can use the CA CSM Installation ISPF UI Tool, which helps to gather site values and prefill most of the options file parameters. You still may have to consult with other team members at your site to review these prefilled values.

Note: If your site uses Storage Management Subsystem (SMS) automatic class selection (ACS), ACS overrides the storage parameter values in the options file.

You can use the CA CSM Installation ISPF UI Tool to specify options automatically. The tool helps you perform the following tasks:

- Gather site values for most of the parameters
- Provide JCLs to create required USS file systems, and make edits to this options file before installing CA CSM

Your 3270 emulator must be able to support ISPF dialogs that are up to 35 rows.

Note: If the setting that shows the ISPF command line at the bottom of the dialog is enabled, the ISPF UI Tool may not display some ISPF dialogs correctly. It may result in displaying an option on the bottom line of the ISPF dialog and out of place with the other options. To avoid this situation, exit the ISPF UI Tool, temporarily disable this option, and then start the UI Tool. You can later enable this option again.

Important! The UI Tool does not detect the complete hostname when the hostname is longer than 26 characters.

Follow these steps:

1. Go to TSO/ISPF option 6 and run the following command:

   exec '*data_set_name*(#RUNTOOL)'

   data_set_name

   Defines the name of the CA CSM Installation ISPF UI Tool z/OS data set extracted using UNZIPJCL.

   Example: CAI.MF20.MSMI.UITOOL

   The main ISPF panel appears.

2. Enter 1 to gather your site values for prefilling the options file parameters.

   You are prompted to provide the Java home path and MSMSetup directory path.

   The programs located in the USS MSMSetup folder get executed through this interface and it gathers site values for some of the parameters. The gathered values are stored in an XML file. This file is used to prefill the options file queries for easier and faster editing of the CA CSM installation options file.

3. Enter 6 or 7 to edit the options file.

   The options in this group let you prefill the options file with site-gathered values, or edit it directly from TSO using the ISPF editor.

   Using prefilled site values

   Use this option (option 6) to review all the installation option parameters and their prefilled value. The values are already included with Installer-set defaults to facilitate editing and reviewing.

   - Values that are prefaced with S indicate gathered site values.
   - Values that are prefaced with D indicate product default values.
   - Values that are prefaced with U indicate that the value has been edited.

   Enter **/** before each parameter to display the available values (S/D/U), which you can also select and modify.

Parameters are listed on multiple pages. You can move forward (Enter) and backward (PF3) to review each screen after all the parameters have been edited and verified.

The ISPF UI tool edits all the panels and it verifies them. Then the tool displays the path and command to invoke the installation utility.

Using ISPF Editor

Use this option (option 7) to edit the options file manually using the ISPF editor from TSO/ISPF.

After the CA CSM Installer is invoked, if any of the parameter validations fail, you can edit the options file again.

Install CA CSM

This section describes tasks that you perform when installing CA CSM.

Install and Set Up CA CSM

The directory (.../MSMSetup) where you extract the CA CSM files contains the MSMSetup.sh setup utility that installs and sets up CA CSM.

Note: CA CSM is an SMP/E-installed and serviceable product.

The utility uses the contents of the options file to tailor the overall process. The utility sets up an Apache Tomcat application server, the CA Datacom/MSM database, the CA CSM service components, and the web-based interface. The utility creates and sets up a runtime environment for CA CSM.

The utility has a restart mechanism to continue installation when reinvoked after addressing an earlier failed run. The utility also lets you select installation from scratch on earlier failed runs. If any of the options file parameters affect the completed stages during restart mode, the utility forces a start from scratch installation.

At the start, the utility checks if data sets and USS folders with the values set in option parameters exist. If they exist, the utility prompts you to overwrite the previous installation files or continue the process without overwriting.

The utility verifies availability of port numbers that are passed through the options file. If they are reserved, already in use or unavailable for other reasons, the utility prompts you to use the provided values and continue the installation.

Consider the following information:

- Before you start installing CA CSM, verify that your TSO region size is at least 143360 KB.
- Invoke the MSMSetup.sh script directly from the TSO OMVS environment (native USS command prompt).
- You cannot invoke the MSMSetup.sh utility from a z/OS Telnet session or an ISHELL command shell.
- MSMSetup.sh requires a userid with UID(0) or SUPERUSER authority.
- If your site has SMS ACS rules to force POU to PDSE, these settings cause the installation job CSMN5102 to fail. The MSMSetup.sh requires POU data sets to be created as PDS data sets.
- If you want to adjust JCL space allocation, run the CA CSM installer in Manual or Review installation mode.

Follow these steps:

1. Verify that you extracted the files from the downloaded CA CSM package (see page 14).

   The MSMSetup and MSMProduct directories exist, and CA CSM files are extracted to the directories.

2. Verify that the required USS paths (see page 52) are available.
3. Verify that you are using a userid with UID(0). If you are not, issue the su command to switch to UID(0).

4. Go to the directory where the MSMSetup.sh setup utility resides, and execute the utility, for example, from OMVS:

   ```
   sh MSMSetup.sh
   ```

   This utility verifies the existence of the following:

   - MSMSetupOptionsFile.properties file in the current path.
   - Valid JAVAPATH parameter field in the Options file.
   - Supported Java SDK version is installed.

   Note: The setup utility is interactive, requiring user responses until completion. The output is written to a log file, MsminstallerLog*yyyy-mm-dd*,*hh-mm-ss*,*ttt*.log, in the MSMSetup directory. If you rerun the utility after a failure, the utility will perform the necessary cleanup steps for the previous execution.

   A panel appears that provides information about the utility. Then, the license agreement appears.

   This license agreement covers an agreement to allow CA Technologies to accumulate minimal information pertaining to the product acquisition activity. 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.

5. Review the license agreement, and press PF3.

   You are prompted to accept the agreement.

   Note: If the license agreement is not displayed, verify that the TSO OMVS libraries are allocated in your TSO environment.

6. Enter **Y** to accept the agreement.

   (Non-UID(0) installation only) If you are executing the installation utility with a userid that is not assigned UID(0), you are asked whether the installer should immediately stop to switch to a userid that is assigned UID(0).

   Note: A userid with UID other than 0 may encounter errors while files are copied and their attributes and permissions are modified. These errors typically indicate that the *Operation is not permitted*. Usually, the installation utility catches this type of errors and results in a premature, unsuccessful termination. In most cases, restarting the installation utility with a userid that has UID(0) assigned successfully restarts and completes the installation.

   However, this type of errors may go undetected. In such cases, a successful restart of the installation utility may be very difficult. You are required to delete all unpaxed files, installed files, and restart the installation from the beginning.

7. (Non-UID(0) installation only) Enter Y (Yes) or N (No) in response to the prompt. We highly recommend that you reply N (No) to the installation utility, stop the installation, and switch to a userid that is assigned UID(0). You do so by running in superuser mode. To run in superuser mode, issue the su command at the OMVS command prompt, and then rerun the installation utility.

   If you reply Y (Yes), the installation continues.

8. Monitor the utility as it verifies that system and software prerequisites are satisfied, and validates the contents of the options file.

   (Optional) If the IP address taken from the system fails to connect, provide a host name or IP address that supports FTP for processing batch jobs.

9. Specify one of the following installation modes for processing the CA CSM installation jobs:

   A

   In Automatic mode, installation jobs are submitted automatically in non-stop mode (the submitted jobs are not shown before submission).

   R

   In Review mode, you are prompted to review each installation job before submission.

   M

   In Manual mode, submit each installation job manually after the setup process.

   Note:

   - If you submit your installation job using TSO, the installer only runs in Manual mode.
   - The installer can require more memory than 17200 KB.
   - If you restarted after an earlier failed point, you are prompted to select a start from an earlier failed point or scratch.
   - If you have selected FTP mode for installation job submission, you are prompted to enter your z/OS credentials.

10. (FTP mode only) Enter your user ID and then your password.

    If you make a mistake entering the user ID or password, you have two more attempts to reenter your credentials. A Yes/No prompt precedes the second and third attempts.

    Yes

    Allows you to reenter your credentials.

    No

    Terminates the installation procedure.

    The installation procedure terminates after the third failed attempt to validate your FTP credentials. Once you resolve this issue, restart the installation script.

    The utility displays the JOB statement, and the JOBPARM statement (for JES2 environment) or the MAIN statement (for JES3 environment) for review and modification (if necessary).

11. Take one of the following steps in response to the Edit Job Card question:

    - If your site does not require additional parameters, enter **N**. The installation process continues.
    - If your site requires additional parameters, enter **Y**. The job card opens in edit mode. Modify the job card, and press PF3 to save the changes and continue the installation process.

      Note: If CA View is running on the host system, uncomment the following statements. Then, fill them in based on the initialization parameters used in SARINIT upon setting up CA View:

      - The OUTPUT statements SARPRT and JESPRT in the JOBCARD
      - The CLASS option in both SARPRT and JESPRT statements

12. Monitor the utility as it customizes all the required installation jobs.

    (Optional) If you selected Review installation mode, you are prompted to review installation jobs one by one. Modify a job and press PF3 to save your changes and submit the job.

13. Monitor the utility as it creates the SMP/E environment for CA CSM, and sets up the CA CSM components.

    The utility performs the following steps:

    - Submits the previously modified jobs one by one and copies the customized JCL into the runtime JCL PDS.

      Note: If executing a job takes longer than the JobCompletionWaitMaxTime options file keyword specifies, the utility asks if you want to continue waiting. Enter **N** to terminate the whole installation process.

    - Customizes the CA Datacom/MSM environment including CA Datacom/MSM address spaces and connection pools.

- Customizes the Apache Tomcat environment including the server.xml and context.xml files, port numbers, the connection pool, and the user XML configuration.
- Customizes and copies JCL for the runtime PROCLIB PDS.
- Customizes and copies JCL for the runtime JCL PDS.
- Prepares CA CSM for the CAICCI interface and copies the LIBCCI and LIBCCI6E modules and the customized job COPYCCI to the run-time JCL PDS member COPYCCI. The COPYCCI job does *not* need to be run as part of the installation process. This job is provided as a convenience to reload these modules, if needed. For example, if these modules are updated through maintenance procedures, you can copy the updates into the CA CSM run time.

After the last step completes, the utility displays an installation summary report (MSMSummaryReport.txt). The report is stored in the MSMSetup directory. This report provides the URL required to access CA CSM from a web browser.

The setup utility completes its process.

14. Review the summary report, MSMSummaryReport.txt, for specific post-installation job submission required to complete the overall CA CSM installation.

    Submit the installation jobs CSMN51yy (see page 24), as specified in the summary report. *yy* indicates the sequence number of the job.

    Note: Submit the installation jobs manually after MSMSetup.sh finishes, regardless of the installation mode that the CA CSM installer is running in.

15. Verify that the following libraries in the STEPLIB of the JCL(MSMMUF) job are APF-authorized:

    - CAAXLOAD and CUSLIB CA Datacom/MSM libraries
    - The CA Common Services for z/OS library that the CCSdsn keyword in the options file specifies

    For the libraries to remain APF-authorized after the next IPL, add the libraries to your permanent APF list (see page 42).

    Note: If the value of the AddAPFauthDSdyn keyword in the options file is N, try to APF-authorize these libraries manually.

16. Verify that the user ID associated with the CA CSM application server (MSMTC job or started task) has the required USS access authority.

    CA CSM can create and mount file systems.

17. Verify that your network configuration permits CA CSM to access 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.

18. Start CA CSM (see page 26, see page 68).

    CA CSM becomes operational.

Installation Jobs

The CA CSM setup utility submits jobs as part of a setup process. The CSMN5102 job that unpacks the CA CSM contents is submitted using a setup process by default regardless of the installation mode. The setup process performs the required configurations and creates the runtime path.

Note: If you are running in Manual mode, run all jobs in the sequence presented in this section.

The following jobs are created when you are performing a new installation of CA CSM:

CSMN5101

This member is only a placeholder to enforce and coincide with the job sequencing for an upgrade. It is not a job and it is not to be executed.

CSMN5102 (Unpack CA CSM Product)

Unpacks the z/OS and USS contents.

CSMN5103 (Customize CA CSM SMP/E Environment)

Customizes the SMP/E environment data set UCLIN statements with the site-specific values provided through the options file.

CSMN5104 (Assemble/Linkedit CA Datacom/MSM db system module)

Assembles and link-edits the CA Datacom/MSM system ID module with the site-specific values provided in the options file.

CSMN5105 (Load CA Datacom/MSM SVC)

Executes CAIRIM module to load the CA Datacom/MSM SVC.

CSMN5106 (Allocate and Load CA Datacom/MSM Database Data Sets)

Allocates and loads the CA Datacom/MSM database data sets.

CSMN5107

This member is only a placeholder to enforce and coincide with the job sequencing for an upgrade. It is not a job and it is not to be executed.

CSMN5108 (Start the CA Datacom MUF)

This job starts the CA Datacom/MSM MUF.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode. The job CSMN5108 is a running task. Before you submit the next job, review the JES Active Queue to determine if the job CSMN5108 is executing.

CSMN5109 (Confirm database tables and backup the new installed database)

Verify that MSMDBSVS (CA Datacom/DB server) and MSMTCSRV (Apache Tomcat) are not active.

This job confirms the CA Datacom/MSM database tables and creates a backup of the latest CA Datacom/MSM installed database.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode.

CSMN5110 (Stop the CA Datacom MUF)

This job stops the CA Datacom/MSM MUF.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode.

Database Allocation Adjustments

You may need to adjust primary and secondary CA Datacom/MSM disk space allocations to any JCL job stream based on your planned usage of CA CSM (including SCS functions), and your current DASD disk pool resources.

The job CSMN5106 performs the initial CA Datacom/MSM disk allocations that are suitable for normal <CASM> usage.

To adjust disk space allocations when executing the MSMSetup.sh shell script, do one of the following:

- If in Review installation mode, enter **Y** (Yes) in response to the prompt if you want to preview JCL before automatic job submission.
- If in Manual installation mode, modify the *runtimeHLQ*.JCL data set as necessary before job submission.

You can adjust the disk allocation based on your expected usage of CA CSM Software Configuration Service (SCS) functions. The following disk allocations can be used for CA Datacom/MSM data area XML, the data set *dbHLQ*.XML4000, where *dbHLQ* is your high-level qualifier for the CA Datacom/MSM data sets:

- A minimum of one cylinder is sufficient if you are not using CA CSM functions to configure products.
- A minimum of 300 cylinders is sufficient if you are using a low volume of CA CSM functions to configure products.
- A minimum of 3,000 cylinders is sufficient if you are using an average to high volume of CA CSM functions to configure products.

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 that interfere 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.

Note: The CA CSM application server uses a default region size of 512 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 -Xmx512m"
```

Follow these steps:

1. (CA CSM upgrade only) Verify that your address spaces from the previous version of CA CSM are down.
2. (CA CSM upgrade only) Unmount the APLROOT, SCROOT, and LJWK mount points from your previous version.
3. (CA CSM upgrade only) Optionally, back up your previous version of CA CSM start procedures and copy the latest version procedures to your production library.

4. If you are starting the latest CA Datacom/MSM MUF for the *first* time, verify that the following post installation jobs have previously been manually executed successfully.
   - For an upgrade (*xx* represents the CA MSM version you are upgrading from)
     - CSMU*xx*08
     - CSMU*xx*09
     - CSMU*xx*10
   - For a new installation
     - CSMN5108
     - CSMN5109
     - CSMN5110
5. 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:

   ```
   DB00215I - CA Datacom/DB r12 at service pack: SP0
   DB00212I - CA Datacom SQL r12   at service pack: SP0
   DB00226I - MULTI-USER ACTIVATED XCF SUPPORT (RIMF20,mufname)
   DB00222I - MULTI-USER ACTIVATED CCI SUPPORT (caicci_sysid,mufname)
   DB00201I - MULTI-USER ENABLED, CXX=cxx_name    MUFNAME=mufname SVC=svc_number
   ```
6. **Important!** Verify that the value of the MUF parameter in the runtime CUSMAC(DBDATIN1) member matches the value of the MUFname keyword in the options file (MSMSetupOptionsFile.properties). Otherwise, you cannot start the MUF.
7. 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:

   ```
   DB00101I - Started Job-MF2SRVR2 number-11326 CXX=CAMSM    Mufname=muf_name
   Svc=svc_number
   BPXM023I (USER01) DSV00049I-CA Datacom Server r11      INITIALIZED -server_name
   ```
8. 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 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, users can log in to CA CSM through a web browser.

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, 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 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.

Configure FTP and HTTP Connections

This section describes how to configure FTP and HTTP connections for CA CSM installations.

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

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*.CUSMAC(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 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*.CUSMAC(PASADVOP) data set:

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

More information:

FTP Proxy Settings (see page 31)

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 31)
- With user credentials (see page 32)

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*.CUSMAC 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 and HTTP 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 34)

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>
  ```

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

Use *one* of the following methods to configure HTTP connection settings and define NTML authorization.

- Specify the NTLM domain in the user name. We recommend that you use this method.

  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 address and port.

3. Verify that the Enable Advanced Settings check box is *not* selected.
4. Click Apply.

   The changes take effect.
5. Go to User Settings, Software Acquisition.
6. In the HTTP Proxy section, provide the NTLM domain, user, and password. This example provides the user name for the NTLM HTTP proxy:

   ```
   myNTLMdomain\user1
   ```
7. Click Apply.

   The changes take effect.

- Specify the NTLM domain as an XML element in the *RunTimeMVSHLQPrefix*.CUSMAC(PASADVOP) member.

  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 address and port.
  3. Select the Enable Advanced Settings check box.
  4. Click Apply.

     The changes take effect.
  5. Go to User Settings, Software Acquisition.
  6. In the HTTP Proxy section, enter the user name and password.

     Note: Do *not* add the NTLM domain in the user name.
  7. Click Apply.

     The changes take effect.
  8. In the *RunTimeMVSHLQPrefix*.CUSMAC(PASADVOP) member, specify the following XML elements. All XML elements must be specified between the tags <ADVOPTIONS></ADVOPTIONS>:

     ```
     <ADVOPTIONS>
       <HTTPPROXY ntlmDomain="myNTLMdomain"> </HTTPPROXY>
     </ADVOPTIONS>
     ```

     Note: The ntlmVersion attribute for the HTTPPROXY tag is obsolete.

Perform Post-Installation Tasks

This section describes tasks that you perform after CA CSM installation is completed.

Set Up CCIDSCSV and CCISPNSV on Each Target System

The load modules and sample procedures for the SDS are delivered as a contributed CA Common Services for z/OS function CETN500. CETN500 is available for all supported CA Common Services for z/OS.

Installing CETN500 creates the address space CCIDSCSV or CCISPNSV as needed on the target system. Do not start the CCIDSCSV or CCISPNSV address space manually. CCIDSCSV is started for every Validate action that users trigger in the CA CSM System Registry. CCISPNSV is started for each Deployment action users trigger in the Software Deployment Service (SDS). CCIDSCSV and CCISPNSV end after the completion of their associated tasks. The system discovery module resides in the CA Common Services for z/OS base FMID and its associated non-PDSE load library.

Follow these steps:

1. Verify that the following CA Common Services for z/OS maintenance and functions are installed:

   CA Common Services for z/OS r12

   - CETN500
   - RO17488
   - RO19624

   CA Common Services for z/OS Version 14

   - CETN500

   In addition, install any additional maintenance that is associated with any of these versions when it becomes available.

   CETN500 installs modules into one of the following locations:

   - CAIPLD for CA Common Services for z/OS r12
   - CAW0PLD for CA Common Services for z/OS Version 14.0 and above

2. Create an independent file system (HFS or zFS) to house the SMPWKDIR directory and the SDS FTP landing directory.

   ETNI0100 provides a sample job that creates a zFS file system.

3. Mount the file system that you created. Create the SMP/E SMPWKDIR directory and the SDS FTP landing directory under the file system mount point.

   ETNI0200 provides a sample job that creates the mount point, mounts the zFS file system, and creates the SMP/E SMPWKDIR directory and the SDS FTP landing directory.

4. Verify that you update your BPXPRM*xx* member in SYS1.PARMLIB with the file system and mount point that you defined earlier.

5. Modify your CAIENF procedure to append the CAIOPTN library member MSMSPNPM, delivered by CETN500, to SPNPARMS DD statements.

6. Verify that nodes and connect statements that point to the CAICCI running on the CA CSM host exist in the target system CCIPARM statements. These nodes and connect statements ensure CAICCI network connectivity to the CA CSM host and all target systems.

   Note: CAICCI can use protocols VTAM LU0 and/or TCPIP and/or XCF for a connection path between systems. Use one or a mixture of protocols that best meet your organizational policies, procedures, and standards. Verify that the CAICCI Spawn Facility is active in both the CA CSM host system and target system CAIENF and CAICCI.

7. Copy CCISPNSV and CCIDSCSV sample procedures from the CA Common Services for z/OS target zone PROC library (CCS*hlq*.CAIPROC for r12; and CCS*hlq*.CAW0PROC for Version 14.0 and above) to your STC PROC library.

8. Modify CCISPNSV and CCIDSCSV procedures to meet your organizational standards.

   - Verify that SMPWKDIR is correctly set up for your installed file system and mount point as done in steps 2 and 3.

     The subdirectory should be created as a mount point directory for the shared DASD switched file system, if used, for example, /cai/ccispnsv/msmMPm.

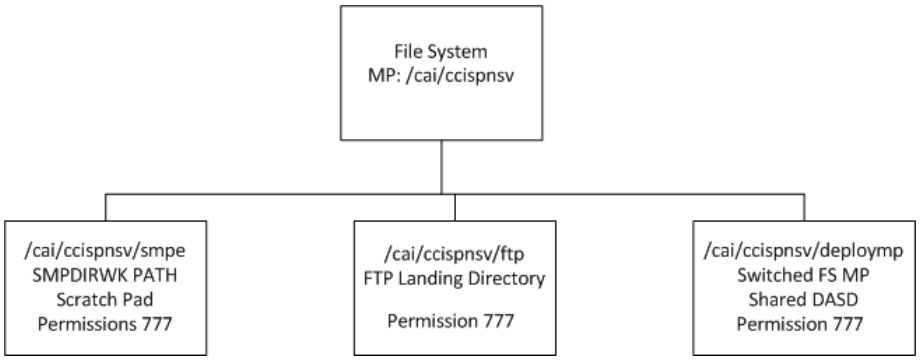
   - Verify that the SMPJHOME and SMPCPATH point to the Java home directory and home SMP classes for your system.

   You can change the name of these procedures. However, you must change the CAICCI SPAWN parameters that reference MSMD_DSC_APPLICATION for System Discovery and MSMD-DPL_APPLICATION for the SDS in all systems. The CAICCI SPAWN parameters are defined in the CAIOPTN library member MSMSPNPM referenced by the SPNPARMS DD statement.

9. Verify that the user ID associated with the CCISPNSV procedure has the correct security access and privileges. The associated user ID should have a valid OMVS segment, and all security items that are associated with the user ID for CAIENF and CAICCI. You can use the CAIENF user ID or you can use your owned defined ID.

10. Verify that the CA Common Services for z/OS load libraries are APF-authorized.

CCISPNSV Sample Directory Tree



APF-Authorize Libraries Permanently

To ensure that the MUF is started as an APF-authorized job step, APF-authorize all libraries you include in the MUF STEPLIB concatenation.

Add the following libraries to your APF list in the member PROG*xx:*

- CAAXLOAD and CUSLIB CA Datacom/MSM libraries
- The CA Common Services for z/OS library that the CCSdsn keyword in the options file specifies

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*.

Set Up User 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 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.

Note: For more information about security for CA CSM functions, see the *Administration Guide*.

Configure CA CSM

After you set up and install CA CSM, you configure it so that it can access the CA Support Online website for you to acquire products. You are prompted to configure CA CSM on the first login.

Follow these steps:

1. Start your web browser, and enter the access URL.

   The login page appears.

   Note: If the Notice and Consent Banner appears, read and confirm the provided information.

2. Enter your z/OS login user name and password, and log in.

   The initial page appears, and you are prompted to configure CA CSM.

   Note: For more information, click the online help link at the top right corner of the page.

3. Configure the following settings:

   - Proxies that CA CSM uses to communicate with the CA Support Online website

     If proxies are not used, CA CSM uses HTTPS Port Number 443 and FTP Port Number 21.

     Important! If your site uses proxies, review your proxy credentials on the User Settings, Software Acquisition page.

   - The USS path to the temporary directory for downloaded software packages

     If you do not specify the directory, CA CSM sets it up using default settings that you can change later.

   Note: These settings are also available on the System Settings, Software Acquisition page.

   Click Next.

   You are prompted to define your account on the CA Support Online website.

4. Click New.

   You are prompted for the credentials to use on the CA Support Online website.

5. Specify the credentials, click OK, and then click Next.

   You are prompted to review your user settings.

   Note: These settings are available on the User Settings page.

6. Change the settings or keep the defaults, and then click Finish.

   A dialog opens, which shows the progress of the configuration task. You can click Show Results to view the details of the actions in a finished task.

7. Click the Settings tab, and review other configuration settings.

You have configured CA CSM. Users can log in and can begin downloading mainframe products.

Migrate the CA CSM SMP/E Environment to CA CSM

Migrate the SMP/E environment that you created during the CA CSM installation into CA CSM.

Follow these steps:

1. Click the SMP/E Environments tab, and click the Migrate SMP/E Environment link in the Actions section on the left side.

   You are prompted to identify the SMP/E environment.

2. Enter the name of the SMP/E environment you created during the installation of CA CSM, specify the SMP/E environment data set name, and click Next.

   The functions in the SMP/E environment are listed.

3. Review the information, and click Next.

   A list of zones with DDDEF associations appears.

4. Review the zones, and click Next.

   A list of file systems appears, if any are found mounted to the path specified in the DDDEFs.

5. Review the file systems. If there are file systems that you want to add as managed product USS file systems, select them. Click Next.

   Zones of the migrated SMP/E environment are listed.

   Note: Only the zones that exist and to which you have access appear.

6. Specify a prefix for each zone and click Next. Prefixes are only used as high-level qualifier (HLQ) defaults during future base installations into the same SMP/E environment. These defaults can be overridden during the base installation, if needed.

   A list of advanced options appears.

   Note: The prefix for the global zone is defined automatically, and you cannot change it.

7. Review the list of options available and select the options that you want to apply to the migrated SMP/E environment:

   Add SMP/E Environment to Working Set

   Adds the migrated SMP/E environment to your working set.

8. Click Next.

   The summary page appears.

9. Review the information, and click Migrate.

   Note: To see UCLIN statements for the zone DDDEFs, click Show UCLIN at the bottom.

   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.

   After the migration is successfully completed, information about the SMP/E environment and associated products is saved in the CA CSM database. The migrated environment appears on the tree in the SMP/E Environments section on the left side.

Set Up CAIRIM to Load CA Datacom/MSM SVC at IPL

The CAIRIM service is the common driver in the CA Common Services for z/OS for a collection of dynamic initialization routines. The CA CSM setup utility loads the CA Datacom/MSM supervisor call (SVC) for the current initial program load (IPL). Set up CAIRIM to load the SVC automatically during each IPL.

Follow these steps:

1. Add *one* of the following statements to your CAIRIM startup procedure:

   - If you have only the CA Datacom/MSM SVC to load, use the following statement:

     ```
     //DBLIB DD DSN=run_time_caaxload,DISP=SHR
     ```

   - If you want to load a CA Datacom/MSM SVC that is different to an existing CA Datacom SVC, use the following statement:

     ```
     //DBLIBx DD DSN=run_time_caaxload,DISP=SHR
     ```

   run_time_caaxload

   Specifies the name of the CAAXLOAD CA Datacom/MSM library.

   x

   Specifies a suffix for the ddname to differentiate from other CAAXLOAD CA Datacom libraries.

   Limits: One to three alphanumeric characters

   The CAIRIM service is configured to load the CA Datacom/MSM SVC at IPL.

2. Add the following statement to the STEPLIB:

   ```
   DSN=run_time_caaxload,DISP=SHR
   ```

   run_time_caaxload

   Specifies the name of the CAAXLOAD CA Datacom/MSM library.

   Note: As with all data sets that are a part of this STEPLIB, the CA Datacom/MSM CAAXLOAD target library must be APF-authorized.

3. Add *one* of the following statements to the PARMLIB member that is referenced by your CAIRIM startup JCL procedure (usually the CAS9 procedure):

   - If you have only the CA Datacom/MSM SVC to load, use the following statement:

     ```
     PRODUCT(CA DATACOM) VERSION(BD12) INIT(DBRIMPR)    -
     PARM(Dsvc,DBSVCPR,TYP=3)
     ```

   - If you want to load a CA Datacom/MSM SVC that is different to an existing CA Datacom SVC, use the following statement:

     ```
     PRODUCT(CA DATACOM) VERSION(BD12) INIT(DBRIMPR)    -
     PARM(Dsvc,DBSVCPR,TYP=3,L=x)
     ```

   svc

   Specifies the SVC number that is set by the SVCNO keyword in the options file for the CA CSM setup utility.

Clean Up the USS Directory

After you download and process the CA CSM installation pax files, remove the files from your USS directory. These actions free file system disk space for subsequent downloads. You can delete the following entities:

- The pax file
- The package-specific directory that the pax command created and all the files in it

Note: Retain non-SMP/E installation data sets for future reference.

Follow these steps:

1. Navigate to your USS directory for downloaded packages.
2. Delete the pax file by entering the following command:

   `rm paxfile`

   paxfile

   Specifies the name of the pax file that you downloaded.
3. Delete the package-specific directory by entering the following command:

   `rm -r package_specific_directory`

   package_specfic_directory

   Specifies the directory that the pax command created.

   Note: You can also use TSO ISHELL to navigate to the pax file and package-specific directory, and delete them using the D line command.

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. Right-click CA Chorus Software Manager and select Update Product.

      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.

   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.

Configure SDS and SCS

If you plan to use CA CSM to deploy and configure your products, configure the Software Deployment Service (SDS) and the Software Configuration Service (SCS).

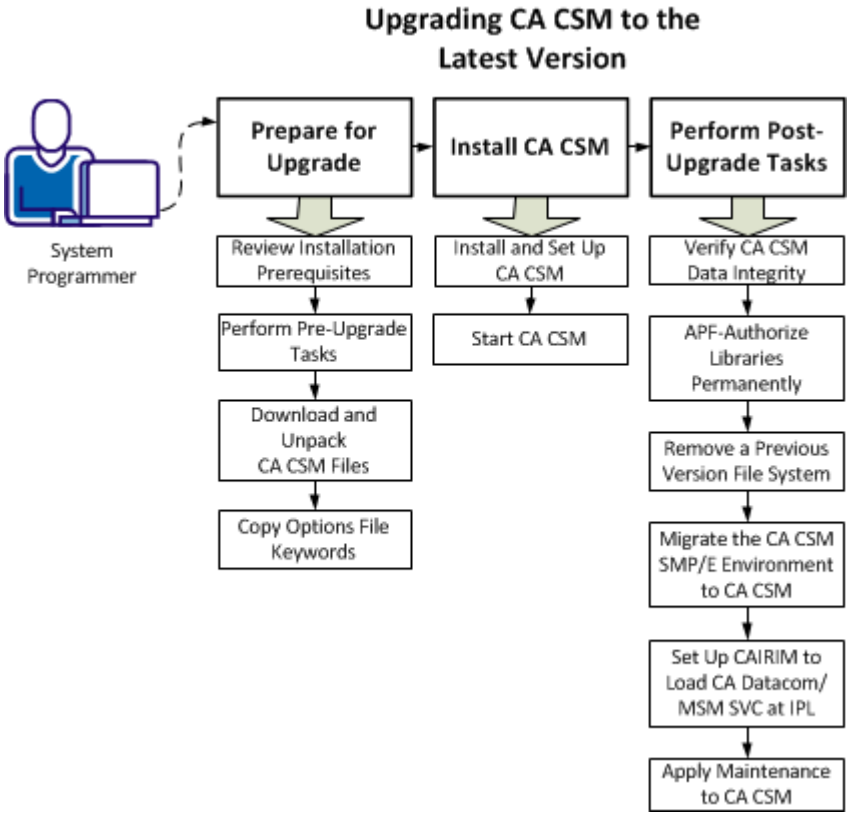
Note: For more information about configuring SDS and SCS, see the scenario *Configuring SDS and SCS in CA CSM*.

You completed the installation of CA CSM.

You can now communicate the URL and appropriate login credentials to users and start using CA CSM.

Chapter 3: How to Upgrade CA CSM

You perform the following tasks to upgrade CA CSM:



1. Prepare for upgrade:
   a. Review installation prerequisites (see page 52).
   b. Perform pre-upgrade tasks (see page 54).
   c. Download and unpack CA CSM files (see page 14).
   d. Copy options file keywords (see page 56).
2. Install CA CSM:
   a. Install and set up CA CSM (see page 58).
   b. Start CA CSM (see page 68).

3. Perform post-upgrade tasks:
   a. Verify CA CSM data integrity (see page 70).
   b. APF-authorize libraries permanently (see page 42).
   c. Remove a previous version file system (see page 71).
   d. Migrate the CA CSM SMP/E environment to CA CSM (see page 44).
   e. Set up CAIRIM to load CA Datacom/MSM SVC at IPL (see page 73).
   f. Apply maintenance to CA CSM (see page 48).

The upgrade process does not affect data in your previous version of CA CSM in any way. A new CA CSM environment is set up with an upgraded database. The previous version CA CSM mount points for the products that are managed using CA CSM are still used after the upgrade. If you can run the latest CA CSM version successfully, you should not use the previous version anymore.

Prepare for Upgrade

This section describes tasks that you perform to get prepared for the CA CSM upgrade.

Review Installation Prerequisites

Before you start upgrading CA CSM, perform the following actions:

1. Confirm that you have all necessary prerequisite authorizations using the Prerequisite Validator utility.
2. Review disk space requirements.
   - Hierarchical File System (HFS) or zSeries File System (zFS) space = 2500 cylinders
   - z/OS space = 2400 cylinders
   - DASD space = 100 tracks
   - For the SDS, each target system needs 500 cylinders of 3390, except CA Database Management Solutions for DB2 for z/OS, which needs 1500 cylinders
3. Review software requirements:
   - CA software—Your system must have CA Common Services for z/OS Release 14.1, Version 14, or r12.
   - IBM software—Your system must satisfy the following requirements:
     - The latest version of z/OS or the last previous version
     - TCP/IP protocol suite of z/OS Communications Server, with the FTP.DATA data set configured with the JESINTERFACELEVEL 2 statement

- SMP/E V3R5 at least
- IBM Java SDK for z/OS

- PC software—The computer that is used to access CA CSM must have one of the following web browsers:
  - Mozilla Firefox 13, 14, 15, or 16
  - Microsoft Internet Explorer 7, 8, or 9
  - Microsoft Internet Explorer 10 (compatibility mode only)

  Note: Microsoft Internet Explorer 10 native mode is *not* supported and causes multiple browser errors.

4. Review web access requirements to the following websites:
   - supportservices.ca.com
   - ftp.ca.com
   - ftpca.ca.com
   - scftpd.ca.com
   - ftpdownloads.ca.com
   - supportftp.ca.com
   - sdownloads.ca.com
5. Customize the following z/OS OMVS values:
   - MAXASSIZE(2147483647)
   - MAXCPUTIME(20000)
   - MAXFILEPROC(10000)
   - MAXTHREADS(1000)
   - MAXTHREADTASKS(1000)
6. Set up security on the following systems:
   - The CA CSM application server
   - Target systems
7. Configure the home directory for address space ACIDs.

Note: For more information, see the *Administration Guide*.

Perform Pre-Upgrade Tasks

Before you start upgrading CA CSM, perform the following tasks:

1. In the CA CSM web-based interface, navigate to the Settings tab, click Mount Point Management under System Settings, and select Unmount at Shutdown. Click Apply.
2. Shut down CA CSM address spaces of the previous CA CSM version.
3. Depending on your file system configuration, choose one of the following options:
   - For a single CA CSM file system configuration:
     a. Unmount the CA CSM file systems for the previous version.
     b. Create a CA CSM file system, and mount it at the previous version mount point (that is, /u/users/msmserv).
     c. Create the following directories: mpm, msm, msmruntime, msminstall.
     d. Create the new mount point for the previous version: /u/users/msmserv/*previous_version_number*. The path node *previous_version_number* must start with a letter followed by two digits, for example, V50.
     e. Mount the CA CSM previous version file system to this new mount point that you created in step 3d.
     f. Edit the following parameters in the /u/users/msmserv/*previous_version_number*/msm/CEGPHFS/MSMSetupOptionsFile.properties options file to point to new version directory paths:

        ```
        MSMPATH=/u/users/msmserv/previous_version_number/msm
        RunTimeUSSPath=/u/users/msmserv/previous_version_number/msmruntime
        ```

   - For a multiple CA CSM file system configuration:
     a. Create the following new version directories:

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

     b. Create the following new version file systems: msm, msmruntime, and msminstall.
     c. Mount the file systems to the new version directories at /u/users/msmserv/*version_number*/msm, /u/users/msmserv/*version_number*/msmruntime, and /u/users/msmserv/*version_number*/msminstall.

Download and Unpack CA CSM Files

The packed CA CSM product package is available on the CA Support Online website.

Follow these steps:

1. Go to the Download Center on the CA Support Online website.
2. Enter CA Chorus Software Manager in the Select a Product field, select the latest version and the Select all components check box, and click Go.

   Note: If you cannot find CA Chorus Software Manager in the product list, follow the instructions from the Free Service area on the top of the product page.

   A list of product downloads is displayed.
3. Download the software package.

After you download the software package, unpack and extract the files for installation.

Important! Verify that the unpacked CA CSM packages are stored on permanent storage volumes, and not on work or temporary volumes.

Follow these steps:

1. Go to the directory where the CA CSM package is downloaded, and enter the following command to unpack the package:

   ```
   pax -rvf 51000068X01.pax.Z
   ```

   Note: The full pax file name, including the Z suffix, is case-sensitive. Verify that you use the exact case of the file name on the system where you issue the pax command. Rename the file, if necessary.

   The MSMInstaller directory is created, and the package is unpacked into the directory.
2. Customize the UNZIPJCL file in the MSMInstaller directory to conform to the data set and USS directory naming standards at your site. Submit the job (for example, using the submit z/OS shell command in USS OMVS), and review the output for successful completion.

   The UNZIPJCL job creates the MSMSetup and the MSMProduct directories that contain the CA CSM installation files.

   - Replace the following text with the path where the MSMInstaller directory was created:

     ```
     <-- YOUR USS HFS DIRECTORY -->
     ```

- Replace the following text with the path where you want to create the MSMSetup and MSMProduct directories:

  ```
  <-- YOUR CA CSM USS HFS DIRECTORY -->
  ```

  Note: We recommend that the directories <-- YOUR USS HFS DIRECTORY --> and <-- YOUR CA CSM USS HFS DIRECTORY --> are set to the same path.

- Replace **yourHLQ** with the high-level qualifier for the ISPF UI Tool data set. The length of the high-level qualifier must not be greater than 26 characters.

The MSMSetup directory, the MSMProduct directory and the CA CSM Installation ISPF UI tool z/OS data set are created, and the CA CSM files are extracted.

Note: When you open the UNZIPJCL file, a warning message can appear at the bottom of the screen. This message indicates that any trailing blanks are removed from the UNZIPJCL file. Removing or retaining trailing blanks does not affect job execution. You can ignore this message.

Copy Options File Keywords

You can copy keyword values from a previous version of CA CSM for easier and quicker customization.

Follow these steps:

1. Go to the directory where the MSMSetup.sh setup utility resides.

   You can use one of the following methods to find the MSMPATH for the previous version:

   - The path that is specified in CA CSM Product Installed Path of the summary report for the previous version (MSMSummaryReport.txt) for CA CSM Product Installed Path
   - The path that is specified in the MSMPATH keyword in MSMSetup folder MSMSetupOptionsFile.properties options file for the previous version

2. Execute the utility.

   For example, use the following command to execute the utility from USS OMVS:

   `sh MSMSetup.sh copyOPT` *`PreviousRelease.MSMPATH`*

   PreviousRelease.MSMPATH

   Path where CA CSM target files for the previous version are located.

   Example: /u/users/msmserv/msm

   The utility looks for the previous version options file in the following location:

   `PreviousRelease.MSMPATH``/CEGPHFS/MSMSetupOptionsFile.properties.`

   The utility copies all available values from the previous version options file to the current options file to fill in missing corresponding keywords.

   When the utility finishes, the modified MSMSetupOptionsFile.properties options file appears in edit mode. You can customize it to conform to the requirements of your site.

3. Review keyword values against the previous system version and user configuration settings in the previous version of CA CSM user interface. During migration, two keywords, MVSHFSDsnPrefix and MountPath, specified in the options file must be the same as in the previous version. All other system and user setting keywords can be modified during the migration.

Options File Keyword Updates

Updates were made to the MSMSetupOptionsFile.properties options file in the MSMSetup directory.

Added the following keywords:

TempSpaceCleanupInterval

Specifies the time interval, in minutes, for CA CSM to clean up temporary work space. A value of zero (0) disables this feature.

safResourceClass

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

Removed the following keywords:

- USSTempDwnldPath
- sisServerUnpaxTempDir

Note: For more information about option file keywords, see the *Administration Guide*.

Install CA CSM

This section describes tasks that you perform to install the latest version of CA CSM.

If any keywords are not set correctly, the MSMSetup.sh process prompts you to select correct values from the available install options.

The script validates whether the previous version values for the SMP/E installation, run-time and database parameters are different. The upgrade related jobs and steps are performed based on the installation mode.

The upgrade process first backs up the database for the previous version, and then migrates its contents to the database for the new version.

The MSMSetup.sh discovers the previous version details and processes the upgrade steps and generated jobs specific to the previous version.

When you have successfully completed the MSMSetup.sh utility, read the generated summary report and complete the post-installation steps.

Install and Set Up CA CSM

The directory (.../MSMSetup) where you extract the CA CSM files contains the MSMSetup.sh setup utility that installs and sets up CA CSM.

Note: CA CSM is an SMP/E-installed and serviceable product.

The utility uses the contents of the options file to tailor the overall process. The utility sets up an Apache Tomcat application server, the CA Datacom/MSM database, the CA CSM service components, and the web-based interface. The utility creates and sets up a runtime environment for CA CSM.

The utility has an option to migrate the previous version database based on the options file values.

The utility has a restart mechanism to continue installation when reinvoked after addressing an earlier failed run. The utility also lets you select installation from scratch on earlier failed runs. If any of the options file parameters affect the completed stages during restart mode, the utility forces a start from scratch installation.

At the start, the utility checks if data sets and USS folders with the values set in option parameters exist. If they exist, the utility prompts you to overwrite the previous installation files or continue the process without overwriting.

The utility verifies availability of port numbers that are passed through the options file. If they are reserved, already in use or unavailable for other reasons, the utility prompts you to use the provided values and continue the installation.

Consider the following information:

- Before you start installing CA CSM, verify that your TSO region size is at least 143360 KB.
- Invoke the MSMSetup.sh script directly from the TSO OMVS environment (native USS command prompt).
- You cannot invoke the MSMSetup.sh utility from a z/OS Telnet session or an ISHELL command shell.
- MSMSetup.sh requires a userid with UID(0) or SUPERUSER authority.
- If your site has SMS ACS rules to force POU to PDSE, these settings cause the installation job CSMU*xx*02 to fail. The MSMSetup.sh requires POU data sets to be created as PDS data sets.
- If you want to adjust JCL space allocation, run the CA CSM installer in Manual or Review installation mode.

Follow these steps:

1. Verify that you extracted the files from the downloaded CA CSM package (see page 14).

   The MSMSetup and MSMProduct directories exist, and CA CSM files are extracted to the directories.

2. Copy the MSMSetupOptionsFile.properties options file (see page 56) to help ensure that it conforms to the requirements of your site.

   To set options for migrating CA CSM to the new version, you can migrate your current database.

3. Verify that the required USS paths are available (see page 52).
4. Verify that you are using a userid with UID(0). If you are not, issue the su command to switch to UID(0).
5. Verify that the previous CA CSM version is not running.

6. Go to the directory where the MSMSetup.sh setup utility resides, and execute the utility, for example, from OMVS:

   ```
   sh MSMSetup.sh
   ```

   This utility verifies the existence of the following:

   - MSMSetupOptionsFile.properties file in the current path.
   - Valid JAVAPATH parameter field in the Options file.
   - Supported Java SDK version is installed.

   Note: The setup utility is interactive, requiring user responses until completion. The output is written to a log file, MsminstallerLog*yyyy-mm-dd*,*hh-mm-ss*,*ttt*.log, in the MSMSetup directory. If you rerun the utility after a failure, the utility will perform the necessary cleanup steps for the previous execution.

   A panel appears that provides information about the utility. Then, the license agreement appears.

   This license agreement covers an agreement to allow CA Technologies to accumulate minimal information pertaining to the product acquisition activity. 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.

7. Review the license agreement, and press PF3.

   You are prompted to accept the agreement.

   Note: If the license agreement is not displayed, verify that the TSO OMVS libraries are allocated in your TSO environment.

8. Enter **Y** to accept the agreement.

   (Non-UID(0) installation only) If you are executing the installation utility with a userid that is not assigned UID(0), you are asked whether the installer should immediately stop to switch to a userid that is assigned UID(0).

   Note: A userid with UID other than 0 may encounter errors while files are copied and their attributes and permissions are modified. These errors typically indicate that the *Operation is not permitted*. Usually, the installation utility catches this type of errors and results in a premature, unsuccessful termination. In most cases, restarting the installation utility with a userid that has UID(0) assigned successfully restarts and completes the installation.

   However, this type of errors may go undetected. In such cases, a successful restart of the installation utility may be very difficult. You are required to delete all unpaxed files, installed files, and restart the installation from the beginning.

9. (Non-UID(0) installation only) Enter Y (Yes) or N (No) in response to the prompt. We highly recommend that you reply N (No) to the installation utility, stop the installation, and switch to a userid that is assigned UID(0). You do so by running in superuser mode. To run in superuser mode, issue the su command at the OMVS command prompt, and then rerun the installation utility.

   If you reply Y (Yes), the installation continues.

10. Monitor the utility as it verifies that system and software prerequisites are satisfied, and validates the contents of the options file.

    (Optional) If the IP address taken from the system fails to connect, provide a host name or IP address that supports FTP for processing batch jobs.

11. Specify one of the following installation modes for processing the CA CSM installation jobs:

    A

    In Automatic mode, installation jobs are submitted automatically in non-stop mode (the submitted jobs are not shown before submission).

    R

    In Review mode, you are prompted to review each installation job before submission.

    M

    In Manual mode, submit each installation job manually after the setup process.

    Note:

    - If you submit your installation job using TSO, the installer only runs in Manual mode.
    - The installer can require more memory than 17200 KB.
    - If you restarted after an earlier failed point, you are prompted to select a start from an earlier failed point or scratch.
    - If you have selected FTP mode for installation job submission, you are prompted to enter your z/OS credentials.

12. (FTP mode only) Enter your user ID and then your password.

    If you make a mistake entering the user ID or password, you have two more attempts to reenter your credentials. A Yes/No prompt precedes the second and third attempts.

    Yes

    Allows you to reenter your credentials.

    No

    Terminates the installation procedure.

    The installation procedure terminates after the third failed attempt to validate your FTP credentials. Once you resolve this issue, restart the installation script.

    The utility displays the JOB statement, and the JOBPARM statement (for JES2 environment) or the MAIN statement (for JES3 environment) for review and modification (if necessary).

13. Take one of the following steps in response to the Edit Job Card question:

    - If your site does not require additional parameters, enter **N**. The installation process continues.
    - If your site requires additional parameters, enter **Y**. The job card opens in edit mode. Modify the job card, and press PF3 to save the changes and continue the installation process.

      Note: If CA View is running on the host system, uncomment the following statements. Then, fill them in based on the initialization parameters used in SARINIT upon setting up CA View:

      - The OUTPUT statements SARPRT and JESPRT in the JOBCARD
      - The CLASS option in both SARPRT and JESPRT statements

14. Monitor the utility as it customizes all the required installation jobs.

    (Optional) If you selected Review installation mode, you are prompted to review installation jobs one by one. Modify a job and press PF3 to save your changes and submit the job.

15. Monitor the utility as it creates the SMP/E environment for CA CSM, and sets up the CA CSM components.

    The utility performs the following steps:

    - Submits the previously modified jobs one by one and copies the customized JCL into the runtime JCL PDS.

      Note: If executing a job takes longer than the JobCompletionWaitMaxTime options file keyword specifies, the utility asks if you want to continue waiting. Enter **N** to terminate the whole installation process.

    - Customizes the CA Datacom/MSM environment including CA Datacom/MSM address spaces and connection pools.

- Customizes the Apache Tomcat environment including the server.xml and context.xml files, port numbers, the connection pool, and the user XML configuration.
- Customizes and copies JCL for the runtime PROCLIB PDS.
- Customizes and copies JCL for the runtime JCL PDS.
- Prepares CA CSM for the CAICCI interface and copies the LIBCCI and LIBCCI6E modules and the customized job COPYCCI to the run-time JCL PDS member COPYCCI. The COPYCCI job does *not* need to be run as part of the installation process. This job is provided as a convenience to reload these modules, if needed. For example, if these modules are updated through maintenance procedures, you can copy the updates into the CA CSM run time.

After the last step completes, the utility displays an installation summary report (MSMSummaryReport.txt). The report is stored in the MSMSetup directory. This report provides the URL required to access CA CSM from a web browser.

The setup utility completes its process.

16. Review the summary report, MSMSummaryReport.txt, for specific post-installation job submission required to complete the overall CA CSM installation.

    Submit the installation jobs CSMUxxyy (see page 64), as specified in the summary report. *xx* indicates the version number that you are upgrading from, *yy* indicates the sequence number of the job.

    Note: Submit the installation jobs manually after MSMSetup.sh finishes, regardless of the installation mode that the CA CSM installer is running in.

17. Verify that the following libraries in the STEPLIB of the JCL(MSMMUF) job are APF-authorized:

    - CAAXLOAD and CUSLIB CA Datacom/MSM libraries
    - The CA Common Services for z/OS library that the CCSdsn keyword in the options file specifies

    For the libraries to remain APF-authorized after the next IPL, add the libraries to your permanent APF list (see page 42).

    Note: If the value of the AddAPFauthDSdyn keyword in the options file is N, try to APF-authorize these libraries manually.

18. Verify that the user ID associated with the CA CSM application server (MSMTC job or started task) has the required USS access authority.

    CA CSM can create and mount file systems.

19. Verify that your network configuration permits CA CSM to access the following websites:

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

- ftpca.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.

20. Start CA CSM (see page 26, see page 68).

    CA CSM becomes operational.

Installation Jobs

The CA CSM setup utility submits jobs as part of a setup process. The CSMU*xx*02 job that unpacks the CA CSM contents is submitted using a setup process by default regardless of the installation mode. The setup process performs the required configurations and creates the runtime path.

Notes:

- The installation job CSMU*xx*01 backs up your existing version data and prepares converted data for the latest version population. When upgrading from a previous version of CA CSM, the installation job CSMU*xx*01 is submitted first for all installation modes. In Manual mode, the script submits the installation jobs CSMU*xx*01 and CSMU*xx*02.
- If you are running in Manual mode, run all jobs in the sequence presented in this section.

The installer generates unique JCL necessary for the type of installation and installation options that you specified according to the following rules:

CSMU*xxyy*

xx

Indicates the version number that you are upgrading from.

yy

Indicates the sequence number of the job.

For example, if you are upgrading from CA MSM R4.1, the job numbers will be CSMU4101, CSMU4102, …, CSMU4110.

The following jobs are created if you are performing an upgrade of your current CA CSM database to the latest CA CSM version:

CSMU*xx*01 (Backs up existing CA CSM data)

Backs up your existing previous version CA Datacom/MSM data.

CSMU*xx*02 (Unpack CA CSM Product)

Unpacks the z/OS and USS contents.

CSMU*xx*03 (Customize CA CSM SMP/E Environment)

Customizes the SMP/E environment data set UCLIN statements with the site-specific values provided through the options file.

CSMU*xx*04 (Assemble/Linkedit CA Datacom/MSM db system module)

Assembles and link-edits the CA Datacom/MSM system ID module with the site-specific values provided in the options file.

CSMU*xx*05 (Load CA Datacom/MSM SVC)

Executes CAIRIM module to load the CA Datacom/MSM SVC.

CSMU*xx*06 (Allocate and Load CA Datacom/MSM Database Data Sets)

Allocates and loads the CA Datacom/MSM database data sets.

CSMU*xx*07 (Data migration)

Migrates the previous CA Datacom/MSM database to the latest version.

CSMU*xx*08 (Start the CA Datacom MUF)

This job starts the CA Datacom/MSM MUF.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode. The job CSMU*xx*08 is a running task. Before you submit the next job, review the JES Active Queue to determine if the job CSMU*xx*08 is executing.

CSMU*xx*09 (Confirm database tables and backup the new installed database)

Verify that MSMDBSVS (CA Datacom/DB server) and MSMTCSRV (Apache Tomcat) are not active.

This job matches the requirements specific to the CA CSM version that you are upgrading from. For all versions, this job confirms the CA Datacom/MSM database tables and creates a backup of the latest CA Datacom/MSM installed database. However, if you are upgrading to the latest version, this job contains additional JCL steps specific to the CA CSM version that you are upgrading from.

If this job fails, review the error message to determine the cause of the problem. Take appropriate actions to correct the situation. Before you resubmit this job, perform the following actions:

- Bring down the CA Datacom/MSM MUF by submitting the CSMU*xx*10 JCL member.
- Resubmit job CSMU*xx*07.
- Bring up the CA Datacom/MSM MUF by submitting the CSMU*xx*08 JCL member, or start the MSMMUF PROCLIB member.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode.

CSMU*xx*10 (Stop the CA Datacom MUF)

This job stops the CA Datacom/MSM MUF.

Note: Run this job manually, even if you are running the CA CSM installer in Automatic or Review mode.

Database Allocation Adjustments

You may need to adjust primary and secondary CA Datacom/MSM disk space allocations to any JCL job stream based on your planned usage of CA CSM (including SCS functions), and your current DASD disk pool resources.

The job CSMU*xx*06 performs the initial CA Datacom/MSM disk allocations that are suitable for normal CA CSM usage.

xx

Indicates the version number that you are upgrading from.

Verify that the new disk allocations are at least equal to the CA Datacom/MSM disk space currently in use.

To adjust disk space allocations when executing the MSMSetup.sh shell script, do one of the following:

- If in Review installation mode, enter **Y** (Yes) in response to the prompt if you want to preview JCL before automatic job submission.
- If in Manual installation mode, modify the *runtimeHLQ*.JCL data set as necessary before job submission.

You can adjust the disk allocation based on your expected usage of CA CSM Software Configuration Service (SCS) functions. The following disk allocations can be used for CA Datacom/MSM data area XML, the data set *dbHLQ*.XML4000, where *dbHLQ* is your high-level qualifier for the CA Datacom/MSM data sets:

- A minimum of one cylinder is sufficient if you are not using CA CSM functions to configure products.
- A minimum of 300 cylinders is sufficient if you are using a low volume of CA CSM functions to configure products.
- A minimum of 3,000 cylinders is sufficient if you are using an average to high volume of CA CSM functions to configure products.

Fallback

If the latest version of the CA CSM does not start up correctly, you can still use the previous version of CA CSM.

If you can run the latest version successfully, we recommend that you do not use the previous version anymore. If the latest CA CSM application server names and port numbers are the same as for the previous version, you cannot run both versions simultaneously.

Your previous CA CSM system libraries (CXX, DBIDs 002, and 015) and their associated data (DBID 4000) are not removed during the CA CSM upgrade process. The upgrade process adds unique libraries and data sets that permit functional execution of the new CA CSM version and the previous version of CA CSM. The upgrade process copies and converts data from the database of the previous version, and incorporates it into the new version. The new version uses the same file systems and the same mount points as the previous version.

Imagine that you upgraded and you are using the latest version. If you now use the previous version, any changes that you make in one version are not reflected in the other version. The previous version data is isolated from the new version data. Use caution when attempting to use a previous CA CSM version after using the latest version.

Note: To obtain full benefits and functionality of the new version, we recommend that you immediately begin using the new version after you complete the upgrade process.

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 that interfere 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.

Note: The CA CSM application server uses a default region size of 512 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 -Xmx512m"
```

Follow these steps:

1. Verify that your address spaces from the previous version of CA CSM are down.
2. Unmount the APLROOT, SCROOT, and LJWK mount points from your previous version.
3. (Optional) Back up your previous version CA CSM start procedures and copy the latest version procedures to your production library.
4. (CA CSM upgrade only) Verify that your address spaces from the previous version of CA CSM are down.
5. (CA CSM upgrade only) Unmount the APLROOT, SCROOT, and LJWK mount points from your previous version.
6. (CA CSM upgrade only) Optionally, back up your previous version of CA CSM start procedures and copy the latest version procedures to your production library.
7. If you are starting the latest CA Datacom/MSM MUF for the *first* time, verify that the following post installation jobs have previously been manually executed successfully.
   - For an upgrade (*xx* represents the CA MSM version you are upgrading from)
     - CSMU*xx*08
     - CSMU*xx*09
     - CSMU*xx*10
   - For a new installation
     - CSMN5108
     - CSMN5109
     - CSMN5110

8. 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:

   ```
   DB00215I - CA Datacom/DB r12 at service pack: SP0
   DB00212I - CA Datacom SQL r12   at service pack: SP0
   DB00226I - MULTI-USER ACTIVATED XCF SUPPORT (RIMF20,mufname)
   DB00222I - MULTI-USER ACTIVATED CCI SUPPORT (caicci_sysid,mufname)
   DB00201I - MULTI-USER ENABLED, CXX=cxx_name    MUFNAME=mufname SVC=svc_number
   ```

   Important! Verify that the value of the MUF parameter in the runtime CUSMAC(DBDATIN1) member matches the value of the MUFname keyword in the options file (MSMSetupOptionsFile.properties). Otherwise, you cannot start the MUF.

   If you are performing an upgrade and this job fails, review the error message to determine the cause of the problem. Take appropriate actions to correct the situation. Before you resubmit this job, perform the following actions:

   - Bring down the CA Datacom/MSM database by submitting the MSMMUFP JCL member.
   - Resubmit job MSMDBMIG.
   - Bring up the CA Datacom/MSM database by submitting the MSMMUFS JCL member, or start the MSMMUF PROCLIB member.

9. 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:

   ```
   DB00101I - Started Job-MF2SRVR2 number-11326 CXX=CAMSM    Mufname=muf_name
   Svc=svc_number
   BPXM023I (USER01) DSV00049I-CA Datacom Server r11      INITIALIZED -server_name
   ```

10. 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 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, users can log in to CA CSM through a web browser.

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, 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 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.

Perform Post-Upgrade Tasks

This section describes tasks that you perform after you upgrade to the latest version of CA CSM.

Verify CA CSM Data Integrity

After you upgrade CA CSM to the latest version, verify that the data that you had in the previous version are correct and not corrupted.

To verify data integrity, log in to the latest version of CA CSM using the web-based interface, and verify that all previous CA CSM data is available in the latest version of CA CSM.

APF-Authorize Libraries Permanently

To ensure that the MUF is started as an APF-authorized job step, APF-authorize all libraries you include in the MUF STEPLIB concatenation.

Add the following libraries to your APF list in the member PROG*xx:*

- CAAXLOAD and CUSLIB CA Datacom/MSM libraries
- The CA Common Services for z/OS library that the CCSdsn keyword in the options file specifies

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*.

Remove a Previous Version File System

CA CSM Release 5.1 does not use the msmtmp directory. If you are not reusing the msmtmp file system from the previous version in the latest version, you can remove it. Delete the file system data set, and remove the auto-mount entry from the SYS1.PARMLIB(BPXPRM*xx*) member.

Set Up User 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 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.

Note: For more information about security for CA CSM functions, see the *Administration Guide*.

Migrate the CA CSM SMP/E Environment to CA CSM

Migrate the SMP/E environment that you created during the CA CSM installation into CA CSM.

Follow these steps:

1. Click the SMP/E Environments tab, and click the Migrate SMP/E Environment link in the Actions section on the left side.

   You are prompted to identify the SMP/E environment.

2. Enter the name of the SMP/E environment you created during the installation of CA CSM, specify the SMP/E environment data set name, and click Next.

   The functions in the SMP/E environment are listed.

3. Review the information, and click Next.

   A list of zones with DDDEF associations appears.

4. Review the zones, and click Next.

   A list of file systems appears, if any are found mounted to the path specified in the DDDEFs.

5. Review the file systems. If there are file systems that you want to add as managed product USS file systems, select them. Click Next.

   Zones of the migrated SMP/E environment are listed.

   Note: Only the zones that exist and to which you have access appear.

6. Specify a prefix for each zone and click Next. Prefixes are only used as high-level qualifier (HLQ) defaults during future base installations into the same SMP/E environment. These defaults can be overridden during the base installation, if needed.

   A list of advanced options appears.

   Note: The prefix for the global zone is defined automatically, and you cannot change it.

7. Review the list of options available and select the options that you want to apply to the migrated SMP/E environment:

   Add SMP/E Environment to Working Set

   Adds the migrated SMP/E environment to your working set.

8. Click Next.

   The summary page appears.

9. Review the information, and click Migrate.

   Note: To see UCLIN statements for the zone DDDEFs, click Show UCLIN at the bottom.

   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.

   After the migration is successfully completed, information about the SMP/E environment and associated products is saved in the CA CSM database. The migrated environment appears on the tree in the SMP/E Environments section on the left side.

Alternatively, you can remove the previous version of the CA CSM SMP/E environment from the latest version of CA CSM.

Note: For more information about removing the previous version of the CA CSM SMP/E environment, or deleting an SMP/E environment, see the online help.

Set Up CAIRIM to Load CA Datacom/MSM SVC at IPL

This procedure only applies if you are upgrading CA CSM from CA MSM r3.1 to the latest version, or you do not have CA Datacom/MSM Version 12.0 SVC already installed in your environment.

The CAIRIM service is the common driver in the CA Common Services for z/OS for a collection of dynamic initialization routines. The CA CSM setup utility loads the CA Datacom/MSM supervisor call (SVC) for the current initial program load (IPL). Set up CAIRIM to load the SVC automatically during each IPL.

Follow these steps:

1. Add *one* of the following statements to your CAIRIM startup procedure:
   - If you have only the CA Datacom/MSM SVC to load, use the following statement:

     ```
     //DBLIB DD DSN=run_time_caaxload,DISP=SHR
     ```

   - If you want to load a CA Datacom/MSM SVC that is different to an existing CA Datacom SVC, use the following statement:

     ```
     //DBLIBx DD DSN=run_time_caaxload,DISP=SHR
     ```

   run_time_caaxload

   Specifies the name of the CAAXLOAD CA Datacom/MSM library.

   x

   Specifies a suffix for the ddname to differentiate from other CAAXLOAD CA Datacom libraries.

   Limits: One to three alphanumeric characters

   The CAIRIM service is configured to load the CA Datacom/MSM SVC at IPL.

2. Add the following statement to the STEPLIB:

   DSN=*run_time_caaxload*,DISP=SHR

   run_time_caaxload

   Specifies the name of the CAAXLOAD CA Datacom/MSM library.

   Note: As with all data sets that are a part of this STEPLIB, the CA Datacom/MSM CAAXLOAD target library must be APF-authorized.

3. Add *one* of the following statements to the PARMLIB member that is referenced by your CAIRIM startup JCL procedure (usually the CAS9 procedure):

   - If you have only the CA Datacom/MSM SVC to load, use the following statement:

     ```
     PRODUCT(CA DATACOM) VERSION(BD12) INIT(DBRIMPR)    -
     PARM(Dsvc,DBSVCPR,TYP=3)
     ```

   - If you want to load a CA Datacom/MSM SVC that is different to an existing CA Datacom SVC, use the following statement:

     ```
     PRODUCT(CA DATACOM) VERSION(BD12) INIT(DBRIMPR)    -
     PARM(Dsvc,DBSVCPR,TYP=3,L=x)
     ```

   svc

   Specifies the SVC number that is set by the SVCNO keyword in the options file for the CA CSM setup utility.

Clean Up the USS Directory

After you download and process the CA CSM installation pax files, remove the files from your USS directory. These actions free file system disk space for subsequent downloads. You can delete the following entities:

- The pax file
- The package-specific directory that the pax command created and all the files in it

Note: Retain non-SMP/E installation data sets for future reference.

Follow these steps:

1. Navigate to your USS directory for downloaded packages.
2. Delete the pax file by entering the following command:

   rm *paxfile*

   paxfile

   Specifies the name of the pax file that you downloaded.

3. Delete the package-specific directory by entering the following command:

   `rm -r package_specific_directory`

   package_specfic_directory

   Specifies the directory that the pax command created.

   Note: You can also use TSO ISHELL to navigate to the pax file and package-specific directory, and delete them using the D line command.

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. Right-click CA Chorus Software Manager and select Update Product.

      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.

   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.

Configure SDS and SCS

If you plan to use CA CSM to deploy and configure your products, configure the Software Deployment Service (SDS) and the Software Configuration Service (SCS).

Note: For more information about configuring SDS and SCS, see the scenario *Configuring SDS and SCS in CA CSM*.

You completed the upgrade of CA CSM to the latest version. You can now start using CA CSM.

Appendix A: Options File Worksheet

Review options file keywords, and gather the required values for your enterprise.

Note: For more information about the keywords, see the *Administration Guide*.

MSMProdPaxPath

Specifies the path to the extracted CA CSM files.

Example: /u/users/msmserv/msminstall/MSMProduct

Your value: _____

JAVAPATH

Specifies the path to the IBM Java SDK for z/OS components.

Example: /usr/lpp/java/J6.0

Your value: _____

CSIHLQ

Specifies the prefix (high-level qualifier) for the consolidated software inventory (CSI) data set, and other SMP/E data sets such as SMPPTS and SMPSTS.

Default: CAI

Your value: _____

TargetHLQ

Specifies the prefix for the target data sets.

Default: The value of CSIHLQ

Your value: _____

TargetZoneName

Specifies the SMP/E environment target zone name.

Default: CAIT

Your value: _____

DlibHLQ

Specifies the prefix for the distribution data sets.

Default: The value of CSIHLQ

Your value: _____

DlibZoneName

Specifies the SMP/E environment distribution zone name.

Default: CAID

Your value: _____

MSMPATH

Specifies the path of the USS directory in which to install CA CSM.

Example: /u/users/msmserv/r51/msm

Your value: _____

RunTimeMVSHLQPrefix

Specifies the prefix for CA CSM run-time data sets, which are runtime copies of the target data sets.

Example: CAI.MSM.RUN

Your value: _____

RunTimeUSSPath

Specifies the path of the USS directory for CA CSM run-time use.

Example: /u/users/msmserv/r51/msmruntime

Your value: _____

DatabaseHLQ

Specifies the prefix for CA Datacom data sets that are created during the installation process.

Default: The value of RunTimeMVSHLQPrefix

Your value: _____

MUFname

Specifies your preferred name for the CA Datacom/MSM Multi-User Facility (MUF).

Example: MSMR5MUF

Your value: _____

ServerName

Specifies your preferred name for the CA Datacom/MSM server.

Example: MSMR5SRV

Your value: _____

CXXNAME

Specifies the name of the identifier for the CA Datacom/AD Directory when it is initialized.

Default: CAMSM

Your value: _____

SVCNO

Specifies an SVC number for CA Datacom/MSM.

Example: 246

Your value: _____

MSMServerPortNo

Specifies the port number to use for web-based access to CA CSM.

Default: 22120

Your value: _____

MSMDSIPORTNO

Specifies the port number for CA DSI Server, which CA CSM uses internally to provide security features.

Default: 22130

Your value: _____

MSMConnectorRedirectPortNo

Specifies the port number to which a request is redirected. Redirection occurs if a request comes in on a non-SSL port and is subject to a security constraint with a transport guarantee that requires SSL.

Default: 22140

Your value: _____

MSMTomcatServerShutdownPortNo

Specifies the port number to which the CA CSM application server listens for the shutdown command.

Default: 22150

Your value: _____

MVSHFSDsnPrefix

Specifies the prefix for the names of file system data sets.

Default: OMVSUSR.CAMSM

Your value: _____

MountPath

Specifies the path to the USS directory that CA CSM can use for work files.

Example: /u/users/msmserv/r51/mpm

Your value: _____

mpmAutomount

Specifies whether CA CSM mounts the file systems during startup.

Options include:

- Y (Yes)
- N (No)

Default: Y

Your value: _____

USSFileSystemType

Specifies whether an HFS or a zFS file system be used for temporary files.

Default: ???

Your value: _____

mpmAllocation

(Optional) Specifies whether to use SMS when allocating new data sets for file systems on the Mount Point Management page of the Settings tab.

Default: SMS

Your value: _____

mpmStorageClass

(Optional) Specifies the SMS storage class of the DASD on the Mount Point Management page in the web-based interface. This value is used during product installation and maintenance.

Default: Blank

Your value: _____

mpmMgmtClas

(Optional) Specifies the SMS management class for file system data sets on the Mount Point Management page of the Settings tab.

Default: Blank

Your value: _____

mpmDataClas

(Optional) Specifies the SMS data class for file system data sets on the Mount Point Management page of the Settings tab.

Default: Blank

Your value: _____

mpmUnit

(Optional) Specifies the type of the DASD on which to place data sets on the Mount Point Management page of the Settings tab.

Default: Blank

Example: 3390

Your value: _____

mpmVolumeSer

(Optional) Specifies the NONSMS volume serial number of the DASD on the Mount Point Management page in the web-based interface.

Default: Blank

Example: DASD01

Your value: _____

TempSpaceCleanupInterval

Specifies the time interval, in minutes, for CA CSM to clean up temporary workspace. A value of zero (0) disables this feature.

Default: 60

Your value: _____

sisExecutorOutputStorclas

(Optional) Specifies the SMS storage class for the data sets that executed programs use for temporary data during product installation through CA CSM Software Installation Service.

Default: Blank

Your value: _____

sisExecutorOutputUnit

(Optional) Specify the type of the DASD to use for the data sets that executed programs use for temporary data.

Default: Blank

Example: 3390

Your value: _____

sisExecutorOutputVolser

(Optional) Specify the volume serial number of the DASD to use for the data sets that executed programs use for temporary data.

Default: Blank

Example: DASD01

Your value: _____

sisGimunzipTempVolser

Specifies the volume serial number (SMS or NONSMS managed) of the DASD to use for the temporary data sets created by GIMUNZIP during product installation through CA CSM Software Installation Service.

Example: *

Your value: _____

sisGimunzipTempPrefix

Specifies the prefix CA CSM uses for GIMUNZIP output temporary data set names during product installation and maintenance.

Example: USER1

Your value: _____

DATASETSUFFIX

Specifies a qualifier CA CSM uses for the names of the file system data sets allocated for the software catalog to store packages during product installation and maintenance. The full data set name appears in the format: MVSHFSDsnPrefix.DATASETSUFFIX

Default: CASC

Your value: _____

sisExecutorServerDsnPrefix

Specifies the data set prefix for storing temporary output files created by the execution of SMP/E during a product installation and maintenance.

Default: *SAF_userid*

Your value: _____

safSecurity

Specifies whether to enable security checking for the resources on the web-based interface.

Default: N

Your value: _____

safResourceClass

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

Default: CAMSM

Your value: _____

sysTaskDeleteOverrideEnabled

Specifies whether to let CA CSM users delete tasks.

Default: N

Your value: _____

HASH

Specifies whether to perform SMP/E GIMUNZIP hash validation.

Default: Y

Your value: _____

ICSF

Specifies whether the system has Integrated Cryptographic Services Facility (ICSF) installed.

Default: Y

Your value: _____

SMPCPATH

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

Example: /usr/lpp/smp/classes

Your value: _____

CSIVOL

Specifies the volume serial number of the DASD on which to place CA CSM SMP/E data sets.

Default: *

Your value: _____

TargetVOL

Specifies the volume serial number of the DASD on which to place CA CSM SMP/E target data sets.

Default: The value of CSIVOL

Your value: _____

DlibVOL

Specifies the volume serial number of the DASD on which to place CA CSM SMP/E distribution data sets.

Default: The value of CSIVOL

Your value: _____

RuntimeVOL

Specifies the volume serial number of the DASD on which to place CA CSM runtime data sets.

Default: *

Your value: _____

DatabaseVOL

Specifies the volume serial number of the DASD on which to place CA Datacom data sets created during the installation process.

Default: The value of RuntimeVOL

Your value: _____

TEMPUNIT

Specifies the esoteric unit for temporary work data sets.

Default: SYSDA

Your value: _____

STORAGE

Specifies whether to let SMS manage the SMP/E temporary data sets.

Example: SMS

Your value: _____

MGMTCLAS

Specifies the SMS management class to use for the temporary SMP/E data sets.

Default: Blank

Your value: _____

STORCLAS

Specifies the SMS storage class to use for the temporary SMP/E data sets.

Default: Blank

Your value: _____

DATACLAS

Specifies the SMS data class to use for the temporary SMP/E data sets.

Default: Blank

Your value: _____

UNIT

Specifies the type of the DASD on which to place temporary SMP/E data sets.

Example: 3390

Your value: _____

VOLUME

Specifies the volume serial number of the DASD on which to place temporary SMP/E data sets.

Example: DASD01

Your value: _____

JVMdsn

Specifies the name of the data set where the JVM load module is located.

Example: SYS1.SIEALNKE

Your value: _____

CCSdsn

Specifies the fully qualified name of the CA Common Services for z/OS target load library.

Example: CAI.CAW0LOAD

Your value: _____

CCScaipdsedsn

Specifies the fully qualified name of the CA Common Services for z/OS CAIPDSE data set.

Example: CAI.CAW0PLD

Your value: _____

CCISSLPortNo

Specifies the CA Common Services for z/OS CCITCP or CCISSL port number configured on your system.

Default: 1202

Your value: _____

ENF SystemID

Specifies the value of CA Common Services for z/OS CAICCI SYSID on your system.

You can issue the following operator command to obtain the value:

```
ENF DISPLAY,SYSID
```

Example: A31SENF

Your value: _____

ActiveJES

Specifies the type of job entry subsystem (JES) used on the z/OS system.

Default: JES2

Your value: _____

JOBNAME

Specifies the job name that is used in the JOB statement for all jobs that are submitted as part of installation.

Default: ID of the user who executes the CA CSM setup utility concatenated with #.

Your value: _____

MSGCLASS

(Optional) Specifies the JES output class for job logs.

Default: X

Your value: _____

CLASS

(Optional) Specifies the JES initiator class to use for jobs.

Default: A

Your value: _____

ACCOUNT

(Optional) Specifies the job accounting string to use in the JOB statement for all jobs.

Example: ’1234,dept01,NY NY’

Your value: _____

SYSAFF

Specifies the systems that are eligible to process jobs.

Default: Blank

Your value: _____

AddAPFauthDSdyn

Specifies whether the CA CSM installer dynamically adds data sets that the CA Datacom/MSM job requires to be APF-authorized to the APF list.

Default: Y

Your value: _____

InstallSVC

Specifies whether Datacom/MSM SVC should be installed.

Default: Y

Your value: _____

HOSTNAME

(Optional) Specifies the host name or IP address of your system.

Default: Blank

Your value: _____

MFASM

Specifies the name of the z/OS assembler program SMP/E is to use.

Default: ASMA90

Your value: _____

MFZAP

Specifies the name of the system utility program used to install changes for modules, load modules, or CSECTs within modules.

Default: IMASPZAP

Your value: _____

MFLKED

Specifies the name of the link-edit program or procedure to use.

Default: IEWL

Your value: _____

TCPdsn

Specifies the name of the TCPIP.DATA data set.

Example: TCPIP.TCPIP.DATA

Your value: _____

TCPIPLinkDSName

Specifies the name of the TCPIP Services SEZATCP data set.

Default: TCPIP.SEZATCP

Your value: _____

LangEnvLinkEditorDSN

Specifies the name of the Language Environment linkage editor data set.

Default: CEE.SCEELKED

Your value: _____

C370LinkEditDSN

Specifies the name of the C/370 linkage editor data set.

Default: CEE.SCEESPC

Your value: _____

LangEnvSPCdsn

Specifies the name of the C/C++ Language library functions data set.

Default: CEE.SCEESPC

Your value: _____

CSSLibDSN

Specifies the name of the IBM Linkage Assist Library data set.

Default: SYS1.CSSLIB

Your value: _____

SSLLIBRARY

Specifies the data set name of the System SSL library.

Default: SYS1.SIEALNKE

Your value: _____

SysUtilitiesPath

Specifies the path to the z/OS UNIX utilities such as mount and unmount.

Default: /usr/sbin

Your value: _____

job.submission.mode

Specifies the method that the CA CSM installation script (installer / MSMSetup.sh) uses to submit jobs, check status, and validate return codes as part of the installation.

Default: FTP

Your value: _____

JobStatusCheckPollPeriod

Specifies the period in seconds to poll the status of the jobs submitted during the installation and setup process for CA CSM.

Default: 2

Your value: _____

JobCompletionWaitMaxTime

Specifies the time in seconds to wait for job completion before prompting the user whether to continue.

Default: 30

Your value: _____

msm.ssl.secure.connection.enable

(Optional) Specifies whether CA CSM uses HTTP or HTTPS.

Default: N (for HTTP)

Your value: _____

first.name.and.last.name

Specifies your URL domain name.

Example: www.your.domain

Your value: _____

organization.name

Specifies your organization name.

Default: Blank

Your value: _____

organization.unit.name

Specifies your organization unit name.

Default: Blank

Your value: _____

city

Specifies your city name.

Default: Blank

Your value: _____

state

Specifies your state name.

Default: Blank

Your value: _____

country.code

Specifies your state name.

Default: Blank

Your value: _____

keystore.location

Specifies the location of the keystore. Specify your own value if you need to use a different USS location than the default location.

Default: Created in your RunTimeUSSPath

Your value: _____

validity.period

Specifies the validity period for the generated keystore certificate, in days.

Default: 365

Your value: _____

Chapter 4: Upgrade Scenarios

The latest version of CA CSM includes the following changes:

- Updated versions of prepackaged CA CSM components, including CA Datacom/MSM and Apache Tomcat
- Change in USS folder structure and CA CSM component names
- Removal of some CA CSM components and inclusion of new CA CSM components

Note: Upgrades from versions of CA MSM previous to r3.1 are not supported. You should uninstall your current version and install the latest version as a new installation.

The following upgrade scenarios are possible:

CA MSM r3.1 to the latest version

In this scenario, the following actions are performed:

- Four z/OS data sets added to support new CA Datacom/MSM database areas.
- Eight previous version CA Datacom/MSM database tables are copied, restructured, and data is converted, if any.
- 50 CA Datacom/MSM tables are added to their respective database areas.
- Four system registry database tables are populated with initial data.
- Additional data added to the following database tables:
  - IDC (IDCONTROL)
  - LIS (LISTTASKTYPE)

CA MSM V4.0 to the latest version

In this scenario, the following actions are performed:

- Six previous version CA Datacom/MSM database tables are copied, restructured, and data is converted, if any.
- Six existing CA Datacom/MSM tables are removed.
- 12 new CA Datacom/MSM tables are added to their respective database areas.
- Additional data is added to the following database tables:
  - IDC (IDCONTROL)
  - LIS (LISTTASKTYPE)
- System Registry tables are replaced with revised data.