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.
Documentation Changes

4th Edition (March 2015)

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

- How to Install CA CSM > Perform Post-Installation Tasks > **Apply Maintenance to CA CSM** (see page 45): updated step 1b to clarify the instruction and the menu option to select
- How to Upgrade CA CSM > Perform Post-Upgrade Tasks > **Apply Maintenance to CA CSM** (see page 45): updated step 1b to clarify the instruction and the menu option to select

3rd Edition (October 2014)

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

- **How to Install CA CSM** (see page 11): updated the process and steps
- How to Install CA CSM > Perform Post-Installation Tasks > **Set Up CAIRIM to Load CA Datacom/MSM PC at IPL** (see page 39): added the topic
- **How to Upgrade CA CSM** (see page 47): updated the process and steps
- How to Upgrade CA CSM > Perform Post-Installation Tasks > **Set Up CAIRIM to Load CA Datacom/MSM PC at IPL** (see page 69): added the topic

2nd Edition (August 2014)

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

- How to Install CA CSM > Prepare for Installation > **Review Installation Prerequisites** (see page 12): added Microsoft Internet Explorer 11 as a supported browser; added a requirement to define MUSASS permission for users who start CA CSM (CA ACF2 for z/OS only)
- How to Upgrade CA CSM > Prepare for Upgrade > **Review Installation Prerequisites** (see page 48): added Microsoft Internet Explorer 11 as a supported browser; added a requirement to define MUSASS permission for users who start CA CSM (CA ACF2 for z/OS only)
1st Edition (April 2014)

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

- **How to Install CA CSM** (see page 11): updated the process and steps
- **How to Upgrade CA CSM** (see page 47): updated the process and steps
- **Options File Worksheet** (see page 73): updated with the information moved from the *Administration Guide*
- **Upgrade Scenarios** (see page 97): added an appendix
# Contents

## Chapter 1: Overview

- Audience .................................................................................................................. 9
- How the Installation Process Works ........................................................................ 9

## Chapter 2: How to Install CA CSM

- Prepare for Installation ............................................................................................. 12
  - Review Installation Prerequisites ........................................................................ 12
  - Set Up USS Paths ................................................................................................. 14
  - Review Options File Keywords ........................................................................... 16
  - Download and Unpack CA CSM Files ................................................................. 16
  - Specifying Installation and Setup Options ......................................................... 18
- Install CA CSM .......................................................................................................... 20
  - Install and Set Up CA CSM ................................................................................ 20
  - Start CA CSM ..................................................................................................... 27
- Configure FTP and HTTP Connections .................................................................... 28
  - FTP Session Options .......................................................................................... 28
  - FTP Proxy Settings ............................................................................................. 31
  - HTTP Proxy Settings ......................................................................................... 37
- Perform Post-Installation Tasks ................................................................................ 39
  - APF—Authorize Libraries Permanently ............................................................... 39
  - Set Up CAIRIM to Load CA Datacom/MSM PC at IPL ..................................... 39
  - Set Up User Security for CA CSM Functions .................................................... 40
  - Update the CA CSM Startup Parameters ......................................................... 40
  - Configure CA CSM ............................................................................................ 41
  - Migrate the CA CSM SMP/E Environment to CA CSM .................................. 42
  - Clean Up the USS Directory ................................................................................ 44
  - Apply Maintenance to CA CSM .......................................................................... 45
  - Configure SDS and SCS ..................................................................................... 46

## Chapter 3: How to Upgrade CA CSM

- Prepare for Upgrade ................................................................................................. 48
  - Review Installation Prerequisites ....................................................................... 48
  - Perform Pre-Upgrade Tasks ................................................................................ 50
  - Download and Unpack CA CSM Files ............................................................... 51
  - Copy Options File Keywords ............................................................................. 53
- Install CA CSM ......................................................................................................... 55
Install and Set Up CA CSM ................................................................. 56
Start CA CSM .............................................................................. 64
Perform Post-Upgrade Tasks .............................................................. 65
Verify CA CSM Data Integrity .............................................................. 66
APF-Authorize Libraries Permanently .................................................. 66
Remove a Previous Version File System ............................................. 66
Set Up User Security for CA CSM Functions ...................................... 67
Update the CA CSM Startup Parameters ............................................. 67
Migrate the CA CSM SMP/E Environment to CA CSM ...................... 68
Configure HTTP Connections ............................................................. 69
Set Up CAIRIM to Load CA Datacom/MSM PC at IPL ......................... 69
Remove the SVC ........................................................................... 70
Clean Up the USS Directory ............................................................... 70
Clean Up Old Deployments ............................................................... 70
Clean Up Data Sets from the Previous Version ................................... 71
Apply Maintenance to CA CSM ......................................................... 71
Configure SDS and SCS .................................................................. 72

Appendix A: Options File Worksheet .................................................... 73
Appendix B: Upgrade Scenarios .......................................................... 97
Chapter 1: Overview

This guide describes how to install CA CSM Version 6.0 or upgrade CA CSM to the latest version.

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

This section contains the following topics:

- Audience (see page 9)
- How the Installation Process Works (see page 9)

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 Version 6.0 (see page 11).
- If you have a previous version of CA CSM installed, upgrade CA CSM to Version 6.0 (see page 47).

STOP

Do not continue until you have completed all security and prerequisite work as noted in the Site Preparation Guide.
You perform the following tasks to install CA CSM:

1. Prepare for installation:
   a. **Review installation prerequisites** (see page 12).
   b. **Set up USS paths** (see page 14).
   c. **Review options file keywords** (see page 16).
   d. **Download and unpack CA CSM files** (see page 16).
   e. **Specify installation and setup options** (see page 18).

2. Install CA CSM:
   a. **Install and set up CA CSM** (see page 20).
   b. **Start CA CSM** (see page 27).
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, perform the following actions:

1. Confirm that you have all prerequisite authorizations using the Prerequisite Validator utility.
2. Confirm that you use a userid with UID(0) or SUPERUSER authority.
3. Review disk space requirements.
   - Hierarchical File System (HFS) or zSeries File System (zFS) space = 2500 cylinders
   - A TSO region = 143360 KB (at minimum)
   - z/OS space = 2400 cylinders
■ DASD space = 100 tracks

■ For SDS, each target system needs 500 cylinders of 3390, except CA Database Management Solutions for DB2 for z/OS, which needs 1500 cylinders

4. Review software requirements:
   ■ CA software — Your system must have CA Common Services for z/OS Release 14.1, or Version 14.0.
   ■ 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 64-bit Java SDK 1.7 for z/OS, we recommend that you use SR5
   ■ PC software — The computer that is used to access CA CSM must have a web browser with access to your mainframe. CA CSM was tested with the following browsers:
     – Mozilla Firefox 28
     – Google Chrome 33
     – Microsoft Internet Explorer 8, 9, and 10 (Page Default document mode only)
     – Microsoft Internet Explorer 11 (document mode 5 or Edge document mode only)

   Note: For more information about document mode, see Microsoft Internet Explorer user documentation.

5. 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

6. Customize the following z/OS OMVS values:
   ■ MAXASSIZE(2147483647)
   ■ MAXCPUTIME(20000)
   ■ MAXFILEPROC(10000)
Prepare for Installation

- MAXTHREADS(1000)
- MAXTHREADTASKS(1000)

7. Set up security on the following systems:
   - The CA CSM application server
   - Target systems

8. (For CA ACF2 for z/OS users only) Define MUSASS permission for users who start CA CSM.

9. Configure the home directory for address space ACIDs.

**Note:** For more information, see the *Site Preparation 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*.

You can define the file systems to mount at system initialization in the SYS1.PARMLIB(BPXPRMxx) member using the MOUNT statement.

Before you download and install CA CSM, 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. However, if your site standards require, you can set up your USS file system using a single file system structure.

Minimally, you require four directories with 775 permissions. The required space is 2500 cylinders.

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 AGRGROW 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')
```

**Note:** 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`

**/parent_path/msmserv/**

Specifies the CA CSM parent path name as defined at your site as the primary mount point, for example:

- `/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 during operation. 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.

The `/mpm` directory should not have a version number. This directory is common and shared between CA CSM versions.

**Note:** If you are planning to run more than one instance of CA CSM on the same system, the `/mpm` directories for these instances must be different.

**/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 cylinders (primary), 100 cylinders (secondary)

**/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 cylinders (primary), 100 cylinders (secondary)
Prepare for Installation

/parent_path/msmserv/version_number/msminstall

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

**Space:** 1000 cylinders (primary), 100 cylinders (secondary)

**Note:** You can delete this directory after the installation is completed.

**Note:** For more information about how to set up USS paths, see the *Best Practices Guide*.

Review Options File Keywords

Before you start installing CA CSM, we recommend that you use the options file worksheet (see page 73). 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](https://www.ca.com/support). Follow these steps:

1. Go to the Download Center on the [CA Support Online website](https://www.ca.com/support).
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.

You are ready to 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 unpack the package:

   ```
   pax -rvf file_name.pax.Z
   ```

   **file_name**

   Specifies the name of the installer file that you downloaded from the Download Center on the CA Support Online website, for example, DVD10155349E.pax.Z.

   **Note:** The full pax file name and its extension are case-sensitive. Verify that you use the exact case when you issue the pax command.

   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.

   Edit the UNZIPJCL file:

   - In the JOB card, update appropriate JOB statement parameters according to your site requirements.
   - 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.
   - (Optional) Make any other updates that your site needs according to the instructions provided in the file.

   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.
Specify 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.

You must customize the contents of this file to reflect your requirements. The options that are marked as required in the description are mandatory.

You can specify installation and setup options either manually (see page 18) or using the ISPF UI tool (see page 18).

Note: If you use CA Allocate with PTF RO60802 applied, you can specify a volume pool name as a value for the volume serial number parameters. The serial number parameters are: CSIVOL, TargetVOL, DlibVOL, RuntimeVOL, and DatabaseVOL.

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 Using the ISPF UI Tool

You can use the CA CSM Installation ISPF UI Tool, which helps to gather site values and prefille some 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 some parameters
- Navigate to edit the options file
- Provide JCLs to create required USS file systems
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.

**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 in the USS MSMSetup/lib 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 to install CA CSM.

The installation utility MSMSetup.sh uses the contents of the options file MSMSetupOptionsFile.properties 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.

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 exit the installation.

If any keywords are not set correctly, the MSMSetup.sh process ends with a list of options in error. Correct the values of the options, and rerun MSMSetup.sh.

If the installation process fails, you can restart it from the point of failure or you can start the process from the beginning. If you updated any keyword in the options file MSMSetupOptionsFile.properties when resolving a previously failed execution, you must start the installation from the beginning. Otherwise, the new keywords will not be processed.

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.

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.

Invoke the MSMSetup.sh utility 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.
If your site has SMS ACS rules to force POU to PDSE, these settings cause the installation job CSMN6001 to fail. The MSMSetup.sh requires POU data sets to be created as PDS data sets.

Follow these steps:

1. Verify that you **extracted the files from the downloaded CA CSM package** (see page 16).
   The MSMSetup and MSMProduct directories exist, and CA CSM files are extracted to the directories.

2. Verify that the required **USS paths** (see page 14) 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. From OMVS, change to the directory where the MSMSetup.sh setup utility resides, and execute the utility:

   ```
   sh MSMSetup.sh
   ```

   This utility verifies that the following statements are true:
   - MSMSetupOptionsFile.properties file is in the current path.
   - The JAVAPATH parameter field in the Options file is valid.
   - Supported Java SDK version is installed.

   **Note:** The setup utility is interactive, requiring some user responses at the beginning. The output is written to a log file, `MsminstallerLogyyyy-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.

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, in particular the OMVS obrowse command.

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.

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

   **A**

   In Automatic mode, the 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. Then, the installation jobs are submitted automatically. This mode lets you adjust JCL space allocation (see page 62).

   **M**

   In Manual mode, you are prompted to review and edit job CSMN6001. Submit each of the remaining installation jobs from the JCL library manually after the setup process in the ISPF environment. This mode lets you adjust JCL space allocation (see page 62).

**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.

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

■ If your site does not require more parameters, enter N. The installation process continues.

■ If your site requires more parameters, enter Y. The JOB statement opens in edit mode. Modify the JOB statement, and press PF3 to save the changes and continue the installation process.

11. 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.

12. (FTP job submission 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 utility.

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 that is required to complete the overall CA CSM installation.

15. (Manual mode only) Submit the installation jobs CSMN60yy (see page 25), as specified in the summary report. yy indicates the sequence number of the job.

16. 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 39).

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

17. 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.

18. 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.
   - 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.

19. Start CA CSM.

CA CSM becomes operational.

**Installation Jobs**

The CA CSM setup utility submits jobs as part of a setup process. The CSMN6001 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 as presented in this section.

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

**CSMN6001 (Unpack CA CSM Product)**

Unpacks the z/OS and USS contents.

**CSMN6002**

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.

**CSMN6003 (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.

**CSMN6004 (Create CA Datacom Custom Data Sets)**

Assembles and link-edits the CA Datacom/MSM IDCUSIB; initializes CUSMAC parmlib members.

**CSMN6005 (Query CA Datacom PC Initialization)**

Runs CA Common Services for z/OS CAIRIMU utility for a report on initialized program calls (PC) that are loaded for CA Datacom.

**CSMN6006 (Load CA Datacom/MSM PC Routines)**

Executes CAIRIM module to load the CA Datacom/MSM PC routines.
**CSMN6007 (Allocate and Initialize CA Datacom/MSM Database System Data Sets)**

Allocates and initializes the CA Datacom/MSM database system environmental data sets.

**CSMN6008 (Start the CA Datacom MUF)**

Starts the CA Datacom/MSM MUF.

**CSMN6009 (Allocate and Initialize CA Datacom/MSM Specific Product Databases)**

Allocate and initialize CA Datacom/MSM specific product databases and confirm tables.

**CSMN6010 (Stop the CA Datacom MUF)**

Stops the CA Datacom/MSM MUF.

---

**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 CSMN6009 performs the initial CA Datacom/MSM disk allocations that are suitable for normal CA CSM usage.

To adjust disk space allocations when executing the MSMSetup.sh installation utility, perform one of the following actions:

- 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.

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 interfering with file allocation, verify that DD statements to exclude such processing are included in the MSMTCSRV JCL member that starts the CA CSM application server.

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

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

Follow these steps:

1. Submit the MSMMUFS JCL member or start the MSMMUF PROCLIB member.
   The CA Datacom/MSM Multi-User Facility (MUF) address space starts.
   Note: All data sets in STEPLIB must be APF-authorized.
   If the MUF starts up successfully, messages similar to the following example appear:

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

2. Submit the MSMDBSVS JCL member or start the MSMDBSRV PROCLIB member.
   The CA Datacom/MSM server address space starts.
   If the server starts up successfully, messages similar to the following example appear:

   ```
   DSV00491I-CA Datacom Server Version 14.0 INITIALIZED --server_name
   ```

3. Submit the MSMTCSRV JCL member or start the MSMTTC PROCLIB member.
   The CA CSM application server address space starts.
   If the server starts up successfully, the following message appears in STDOUT:

   ```
   MSM0091I - CA CSM startup complete.
   ```
   If the startup fails, the following message appears in STDOUT:

   ```
   MSM0101E - CA CSM startup failed.
   ```
Configure FTP and HTTP Connections

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 `RunTimeMVSFLQPrefix.SAMPLIB(PASADVOP)`. This data set is an XML file and has an FTPOPTIONS section defining all the available FTP session options. Each option is set to the FTP client default.
The `<FTPOPTIONS>` XML tag is read for every FTP connection that CA CSM establishes. If the tag is not defined or empty, then the CA CSM FTP client uses the defaults as described in this section.

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

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

You can use the following keys:

**firewall.friendly**

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

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

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

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

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

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

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

```
200 PORT command successful.
```

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

**verify.pasv.ip**

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

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

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

**Important!** We recommend that you do not override this option unless your firewall support absolutely requires it.
Some firewall implementations may intercept and alter the IP address that is returned from the FTP server in response to the PASV command. In this case, you may see the following message in CA CSM application server logs:

Host attempting data connection \textit{ip\_address\_1} is not same as server \textit{ip\_address\_2}

\textit{ip\_address\_1}

Identifies the altered IP address from the firewall server.

\textit{ip\_address\_2}

Identifies the IP address of the FTP server.

\textbf{default.timeout}

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

\begin{verbatim}
<FTPOPTIONS>default.timeout=0</FTPOPTIONS>
\end{verbatim}

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, \texttt{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.

\textbf{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.

\begin{verbatim}
<FTPOPTIONS>default.port=21</FTPOPTIONS>
\end{verbatim}

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

\textbf{Note:} This option has no affect if you enable FTP proxy settings.
control.keep.alive.timeout

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

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

\[
<\text{FTPOPTIONS}>\text{control.keep.alive.timeout=300}</\text{FTPOPTIONS>}
\]

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.
Configure FTP and HTTP Connections

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:

```plaintext
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 RunTimeMVSHLOPrefix.SAMPLIB data set. To see the current location of the PASADVOP, look in FTP Proxy, Advanced Settings Data Set, on the System Settings, Software Acquisition page. This member has a generic template containing advanced FTP settings. You can use the default values in the member or can modify them using ISPF editor to match your FTP and HTTP proxy authentication methods.
Example PASADVOP Member

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

```xml
<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:

```xml
<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_Onine_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:

```xml
<ADV OPTIONS>
  <FIREWALL>
    <FIRE CMD>HOST;</FIRE CMD>
    <FIRE CMD>REMOTE_USER;@REMOTE_HOST; USER;</FIRE CMD>
    <FIRE CMD>REMOTE_PW;</FIRE CMD>
    <FIRE CMD>ACCT; PW;</FIRE CMD>
  </FIREWALL>
</ADV OPTIONS>
```

- 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 `@` 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 `==>`.
Configure FTP and HTTP Connections

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.

```xml
<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:

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

The following sample is not supported:

```xml
<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:

```xml
<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

Follow these steps:
1. On the Settings tab, go to System Settings, Software Acquisition.
2. In the HTTP Proxy section, select the Enable Proxy Settings check box, and provide the HTTP proxy port and address.
3. Click Apply.
   The changes take effect.
4. Go to User Settings, Software Acquisition.
5. In the HTTP Proxy section, provide the NTML domain, user name and password for the HTTP proxy server. The following sample is an example of providing the NTML domain and user name:

   mydomain\user1

6. Click Apply.
   The changes take effect.

Perform Post-Installation Tasks

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

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 PROGxx:

- 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 PROGxx 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 CAIRIM to Load CA Datacom/MSM PC at IPL

Set up CAIRIM to load the PC automatically during each IPL.

Follow these steps:

1. Locate the PARMLIB member referenced by your CAIRIM startup JCL procedure (usually the CAS9 procedure).
Perform Post-Installation Tasks

2. Add the following statements to the PARMLIB member:

```
PRODUCT(CA_DATACOM) VERSION(BD14) INIT(DBCR4PR)
LOADLIB(run_time_caaxload)
PARM(PC=PRD, PCC=DBPCCPR)
PRODUCT(CA_DATACOM) VERSION(BD14) INIT(DBCR4PR)
LOADLIB(run_time_caaxload)
PARM(PC=PRD, PCS=DBPCSPR)
```

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*.

Update the CA CSM Startup Parameters

If you plan to let CA CSM perform external operations on your behalf without saving your password, update the CA CSM startup parameters.

You do so to allow users to perform the following actions:

- Launch CA CSM from CA Chorus without requiring an additional user login.
  
  **Note:** For more information about CA Chorus, see the CA Chorus user documentation.

- Schedule automatic maintenance updates (receiving and applying maintenance) for products that are installed in an SMP/E environment.

Follow these steps:

1. Verify that you configured your security manager (CA ACF2 for z/OS, CA Top Secret for z/OS, or IBM RACF) to use PassTickets for external operations.

  **Note:** For more information about configuring PassTickets, see *Configuring CA CSM to Perform Automatic Maintenance Updates* in the CA CSM bookshelf under User Documentation By Task, and see the *Site Preparation Guide*. 

40 Installation Guide
2. Add the following statement in the SAMPLIB(MSMLIB) member to specify the CA CSM application ID:

```
IJO="$IJO -DmsmApplid=applid"
```

`applid`  
Defines the CA CSM application ID used for PassTicket validation to authenticate connections to the server.  
**Default:** CHORWEBS

3. Restart the CA CSM application server.  
The changes take effect.

**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.
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_specific_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](https://www.ca.com) 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](https://www.ca.com):
   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](https://www.ca.com).
   b. Expand the CA Chorus Software Manager entry in the tree. Right-click the version of CA CSM that you have installed, and select Update Product Release.
      
      The task takes some time to complete, and after it does, a message appears confirming that the software was successfully acquired.
   c. Click Hide.
      
      The message disappears.
   d. Locate the CA CSM maintenance in the right panel.

2. (Optional) Add test fixes using external maintenance.
   
   **Note:** For more information about applying test fixes and managing maintenance downloaded external to CA CSM, see the online help.

3. Review and apply the maintenance.
   
   The contents of the SMP/E target libraries and USS paths for CA CSM are updated. These libraries and paths are set up using the TargetHLQ and MSMPATH keywords in the MSMSSetupOptionsFile.properties options file.
   
   **Note:** For more information about applying and managing maintenance, see the online help.

4. Stop CA CSM.
   
   CA CSM stops operation.
Perform Post-Installation Tasks

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 Configuring SDS and SCS in CA CSM in the CA CSM bookshelf under User Documentation By Task.
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 48).
   b. Perform pre-upgrade tasks (see page 50).
   c. Download and unpack CA CSM files (see page 16).
   d. Copy options file keywords (see page 53).

2. Install CA CSM:
   a. Install and set up CA CSM (see page 55).
   b. Start CA CSM (see page 64).

3. Perform post-upgrade tasks:
   a. Verify CA CSM data integrity (see page 66).
   b. APF-authorize libraries permanently (see page 39).
   c. Remove a previous version file system (see page 66).
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 prerequisite authorizations using the Prerequisite Validator utility.
2. Confirm that you use a userid with UID(0) or SUPERUSER authority.
3. Review disk space requirements.
   - Hierarchical File System (HFS) or zSeries File System (zFS) space = 2500 cylinders
   - A TSO region = 143360 KB (at minimum)
   - z/OS space = 2400 cylinders

After you complete these tasks, you complete the upgrade of CA CSM to the latest version. You can start using CA CSM.

Note: 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

Chapter 3: How to Upgrade CA CSM

4. Review software requirements:
   - CA software — Your system must have CA Common Services for z/OS Release 14.1, or Version 14.0.
   - 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 64-bit Java SDK 1.7 for z/OS, we recommend that you use SR5
   - PC software — The computer that is used to access CA CSM must have a web browser with access to your mainframe. CA CSM was tested with the following browsers:
     - Mozilla Firefox 28
     - Google Chrome 33
     - Microsoft Internet Explorer 8, 9, and 10 (Page Default document mode only)
     - Microsoft Internet Explorer 11 (document mode 5 or Edge document mode only)
     - Note: For more information about document mode, see Microsoft Internet Explorer user documentation.

5. 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
   - sddownloads.ca.com

6. Customize the following z/OS OMVS values:
   - MAXASSIZE(2147483647)
   - MAXCPUTIME(20000)
   - MAXFILEPROC(10000)
Prepare for Upgrade

7. Set up security on the following systems:
   ■ The CA CSM application server
   ■ Target systems

8. (For CA ACF2 for z/OS users only) Define MUSASS permission for users who start CA CSM.

9. Configure the home directory for address space ACIDs.

Note: For more information, see the Site Preparation 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/pre_\_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/pre_\_version\_number/msm/CEGPHFS/MSMSetupOptionsFile.properties options file to point to new version directory paths:
        MSMPATH=/u/users/msmserv/pre_\_version\_number/msm
        RunTimeUSSPath=/u/users/msmserv/pre_\_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](https://www.ca.com). Follow these steps:

1. Go to the Download Center on [the CA Support Online website](https://www.ca.com).
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.

You are ready to 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 unpack the package:

   ```bash
   pax -rvf file_name.pax.Z
   ```

   **file_name**

   Specifies the name of the installer file that you downloaded from the Download Center on [the CA Support Online website](https://www.ca.com), for example, DVD10155349E.pax.Z.

   **Note:** The full pax file name and its extension are case-sensitive. Verify that you use the exact case when you issue the pax command.

   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.

   **Edit the UNZIPJCL file:**

   - In the JOB card, update appropriate JOB statement parameters according to your site requirements.
   - 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.
   - (Optional) Make any other updates that your site needs according to the instructions provided in the file.

   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.

**Important!** Verify that the keyword `PreviousRelease.MSMPATH` in the `MSMSetupOptionsFile.properties` options file is populated with the same value as the previous application installation path. This practice ensures that the migration jobs are automatically generated.

**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
   sh MSMSetup.sh copyOPT PreviousRelease.MSMPATH 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.
   
   Verify that the keywords `MVSHFSDsnPrefix` and `MountPath` in the current version of the options file are the same as in the previous versions of the options file.
   
   During installation, if these parameters are not the same between CA CSM versions, the CA CSM installer displays an error message for the corresponding property, and exits the installation. 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 Keywords

The following keywords were added:

**Applid**
- Specifies a name that is used to identify CA Datacom Server to the CA Datacom/MSM application.

**PROTOCOL**
- Specifies the communication protocol that is used to transmit data between CA CSM and CA Datacom Server.

**TCPIP_HOST**
- Specifies the host name or IP address on which the CA Datacom Server listens for incoming TCP/IP data traffic from CA CSM.

**TCPIP_PORT**
- Specifies the port number on which CA Datacom Server listens for incoming TCP/IP data traffic from CA CSM.

**TCPIP_CONNECT_QUEUE**
- Specifies the number of TCP/IP database requests from CA CSM that the CA Datacom Server can process at once.

Removed Keywords

The following keywords were removed:
- MUFName
- SVCNO
- InstallSVC
- C370linkEditDSN

Other Updates

CA CSM now requires that the CA Datacom/MSM Multi-User Facility CXX name be a unique alphanumeric value that does not exceed seven characters. This name is defined as the CXXNAME keyword. If your site has more than one MUF running, ensure that the MUF CXX name for CA CSM is different from all other MUFs.
Install CA CSM

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

The installation utility MSMSetup.sh uses the contents of the options file MSMSetupOptionsFile.properties 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 upgrade process does not update or delete any previous CA Datacom/MSM data. The upgrade process only backs up your current CA Datacom/MSM environment. This process includes creating a new (latest) CA CSM version environment and populating it with your existing data (previous CA CSM version) that was backed up and converted.

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 exit the installation.

The utility 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 utility also validates that the mount point manager data set HLQ and pathnames are identical to the values in the new options file.

If any keywords are not set correctly, the MSMSetup.sh process ends with a list of options in error. Correct the values of the options, and rerun MSMSetup.sh.

If the installation process fails, you can restart it from the point of failure or you can start the process from the beginning. If you updated any keyword in the options file MSMSetupOptionsFile.properties when resolving a previously failed execution, you must start the installation from the beginning. Otherwise, the new keywords will not be processed.

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.
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.

Invoke the MSMSetup.sh installation utility 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.

If your site has SMS ACS rules to force POU to PDSE, these settings cause the installation job CSMUxx01 to fail. The MSMSetup.sh requires POU data sets to be created as PDS data sets.

Follow these steps:

1. Verify that you extracted the files from the downloaded CA CSM package (see page 16).
   The MSMSetup and MSMProduct directories exist, and CA CSM files are extracted to the directories.

2. Copy the MSMSetupOptionsFile.properties options file (see page 53) to ensure that it conforms to the requirements of your site.

3. Verify that the required USS paths (see page 50) are available.

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. From OMVS, change to the directory where the MSMSetup.sh setup utility resides, and execute the utility:

   sh MSMSetup.sh

   This utility verifies that the following statements are true:
   - MSMSetupOptionsFile.properties file is in the current path.
   - The JAVAPATH parameter field in the Options file is valid.
   - Supported Java SDK version is installed.

   **Note:** The setup utility is interactive, requiring some user responses at the beginning. The output is written to a log file, MsminstallerLogyyyy-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.

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, in particular the OMVS obrowse command.

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.

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

A

In Automatic mode, the 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. Then, the installation jobs are submitted automatically. This mode lets you adjust JCL space allocation (see page 62).

M

In Manual mode, you are prompted to review and edit job CSMUxx01. Submit each of the remaining installation jobs from the JCL library manually after the setup process in the ISPF environment. This mode lets you adjust JCL space allocation (see page 62).

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.

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.

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

■ If your site does not require more parameters, enter N. The installation process continues.

■ If your site requires more parameters, enter Y. The JOB statement opens in edit mode. Modify the JOB statement, and press PF3 to save the changes and continue the installation process.

13. 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.
14. (FTP job submission 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 utility.

15. Monitor the utility as it backs up the CA Datacom/MSM database of the previous CA CSM version, 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 that is required to complete the overall CA CSM installation.
17. (Manual mode only) Submit the installation jobs CSMUxxy (see page 61), as specified in the summary report. xx indicates the version number that you are upgrading from, yy indicates the sequence number of the job.

18. 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 39).

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

19. 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.

20. 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.

- 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.

21. Start CA CSM.

CA CSM becomes operational.

If the latest version of the CA CSM does not start up correctly, you can still use the previous version of CA CSM (see page 63).
Installation Jobs

The CA CSM setup utility submits jobs as part of a setup process. The CSMUxx01 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 CSMUxx02 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 installer submits installation job CSMUxx02 in Automatic and Review modes. In Manual mode, you must submit job CSMUxx02 after the installer completes.
- If you are running in Manual mode, run all jobs in the sequence as presented in this section.

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

CSMUxxyy

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 CSM R5.1, the job numbers will be CSMU5101, CSMU5102, ..., CSMU5110.

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

CSMUxx01 (Unpack CA CSM Product)

Unpacks the z/OS and USS contents.

CSMUxx02 (Backs up existing CA CSM data)

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

CSMUxx03 (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.

CSMUxx04 (Create CA Datacom Custom Data Sets)

Assembles and link-edits the CA Datacom/MSM IDCUSIB; initializes CUSMAC parmlib members.
CSMUxx05 (Query CA Datacom PC Initialization)

Runs CA Common Services for z/OS CAIRIMU utility for a report on initialized program calls (PC) that are loaded for CA Datacom.

CSMNxx06 (Load CA Datacom/MSM PC Routines)

Executes CAIRIM module to load the CA Datacom/MSM PC routines.

CSMUxx07 (Allocate and Initialize CA Datacom/MSM Database System Data Sets)

Allocates and initializes the CA Datacom/MSM database system environmental data sets.

CSMUxx08 (Start the CA Datacom MUF)

Starts the CA Datacom/MSM MUF.

CSMUxx09 (Define, initialize CA Datacom/MSM specific product database and migrate converted data)

Defines and initializes CA Datacom/MSM specific product database, and migrates converted data.

CSMUxx10 (Stop the CA Datacom MUF)

Stops the CA Datacom/MSM MUF.

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 CSMUxx09 performs the initial CA Datacom/MSM disk allocations that are suitable for normal CA CSM usage.

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 installation utility, perform one of the following actions:

■ 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.
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 interfering with file allocation, verify that DD statements to exclude such processing are included in the MSMTCSRV JCL member that starts the CA CSM application server.

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

\[ \text{IJO} = -Xms128m -Xmx768m -Xss768m \]

**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. Submit the MSMMMUSFS 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:

   \[
   \begin{align*}
   &\text{DB00226I - MULTI-USER ACTIVATED XCF SUPPORT} \\
   &\text{DB00222I - MULTI-USER ACTIVATED CCI SUPPORT} \\
   &\text{DB00201I - MULTI-USER ENABLED, CXX=cxx_name MUFNAME=muf_name AD}
   \end{align*}
   \]

5. Submit the MSMDBSFS 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:

   \[
   \begin{align*}
   &\text{DSV00049I-CDatacom Server Version 14.0 INITIALIZED --server_name}
   \end{align*}
   \]

6. Submit the MSMTCSRV JCL member or start the MSMTX PROCLIB member.
   
   The CA CSM application server address space starts.

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

   \[
   \text{MSM0009I - CA CSM startup complete.}
   \]
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.

7. After you successfully bring up CA CSM for the first time, comment out the DBUPDATE DD card in the MSMTCSRV JCL member or MSMTC PROCLIB.

**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.
Perform Post-Upgrade Tasks

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 PROGxx:

- 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 PROGxx 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 Version 6.0 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(BPXPRMxx) 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*.

Update the CA CSM Startup Parameters

If you plan to let CA CSM perform external operations on your behalf without saving your password, update the CA CSM startup parameters.

You do so to allow users to perform the following actions:

- Launch CA CSM from CA Chorus without requiring an additional user login.

  **Note:** For more information about CA Chorus, see the CA Chorus user documentation.

- Schedule automatic maintenance updates (receiving and applying maintenance) for products that are installed in an SMP/E environment.

Follow these steps:

1. Verify that you configured your security manager (CA ACF2 for z/OS, CA Top Secret for z/OS, or IBM RACF) to use PassTickets for external operations.

   **Note:** For more information about configuring PassTickets, see *Configuring CA CSM to Perform Automatic Maintenance Updates* in the CA CSM bookshelf under User Documentation By Task, and see the *Site Preparation Guide*.

2. Add the following statement in the SAMPLIB(MSMLIB) member to specify the CA CSM application ID:

   ```
   IJO="$IJO -DmsmApplid=applid"
   ```

   **applid**
   
   Defines the CA CSM application ID used for PassTicket validation to authenticate connections to the server.

   **Default:** CHORWEBS

3. Restart the CA CSM application server.

   The changes take effect.
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.

### Configure HTTP Connections

If you used an HTTP proxy server with NTLM authentication in a previous version of CA CSM, verify that all users have the NTLM domain in the user name. Do so from the Settings tab, the **User Settings, Software Acquisition page** (see page 38). For example:

```
mydomain\user1
```

### Set Up CAIRIM to Load CA Datacom/MSM PC at IPL

Set up CAIRIM to load the PC automatically during each IPL.

**Follow these steps:**

1. Locate the PARMLIB member referenced by your CAIRIM startup JCL procedure (usually the CAS9 procedure).

2. Add the following statements to the PARMLIB member:

   ```
   PRODUCT(CA DATACOM) VERSION(BD14) INIT(DBCR4PR)
   LOADLIB(run_time_caaxload)
   PARM(PC=PROD,PCC=DBPCCPR)
   PRODUCT(CA DATACOM) VERSION(BD14) INIT(DBCR4PR)
   LOADLIB(run_time_caaxload)
   PARM(PC=PROD,PCS=DBPCSPR)
   ```
Perform Post-Upgrade Tasks

Remove the SVC

CA CSM Version 6.0 does not require the CA Datacom/MSM supervisor call (SVC). If you do not need the SVC for any CA Datacom instances at your site, you can uninstall it.

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_specific_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.

Clean Up Old Deployments

If you upgrade from a version earlier than CA CSM Release 5.1, clean up older deployment snapshots to free up DASD space on your system.

Note: For more information about cleaning up deployment snapshots, see the online help.
Clean Up Data Sets from the Previous Version

After using the latest version for some time, we recommend that you clean up the previous version data sets and folders and free up the DASD.

Review the MSMPWIPE job closely before removing the previous version contents.

You can remove previous version mounts from the system depending on how you set your previous version installation preference for single or multiple mount file systems.

- The previous version is installed in a single file system. The msminstall, msm, msmruntime, msmtmp, and mpm folders are created under one mount file data set. Then, you can remove the msminstall, msm, and msmruntime folders from UNIX System Services (USS).

- The previous version is installed in multiple file systems. The msminstall, msm, msmruntime, msmtmp, and mpm folders use individual mount file data sets. Then, you can remove the msminstall, msm, and msmruntime folders from USS, delete the related mount file data sets, and remove auto-mount entries from SYS1.PARMLIB(BPXPRMxx), if included.

Apply Maintenance to CA CSM

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

Follow these steps:

1. Update the Software Catalog with the CA CSM maintenance information from the CA Support Online website:
   a. Go to the Products tab and locate CA Chorus Software Manager in the Available Products panel on the left.
      
      Note: If you do not see CA Chorus Software Manager in the tree, use one of the products that are installable with CA CSM for this process. These products reflect CA CSM as a component so the maintenance is reflected there also. For more information, see CA Chorus Software Manager Enabled Products in the Recommended Reading section of the CA CSM page on the CA Support Online website.
   b. Expand the CA Chorus Software Manager entry in the tree. Right-click the version of CA CSM that you have installed, and select Update Product Release.
      
      The task takes some time to complete, and after it does, a message appears confirming that the software was successfully acquired.
Perform Post-Upgrade Tasks

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 *Configuring SDS and SCS in CA CSM* in the CA CSM bookshelf under User Documentation By Task.
Appendix A: Options File Worksheet

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

**MSMProdPaxPath**

Specifies the path to the extracted CA CSM files. The value is the path that is defined for the CA CSM Product archive ID in the UNZIPJCL job.

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

*Your value:* ________________________________________________

**JAVAPATH**

Specifies the path to the IBM 64-bit Java SDK for z/OS components.

*Note:* 31-bit Java SDK is not supported.

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

*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.

If you are upgrading to the latest CA CSM version, specify a unique value for this keyword different from the value in any other previous CA CSM version.

*Default:* CAI

*Your value:* ________________________________________________

**TargetHLQ**

Specifies the prefix for the target data sets.

If you are upgrading to the latest CA CSM version, specify a unique value for this keyword different from the value in any other previous CA CSM version. The value of TargetHLQ must be different from RunTimeMVSHLQPrefix and DatabaseHLQ.

*Default:* The value of CSIHLQ

*Your value:* ________________________________________________
Perform Post-Upgrade Tasks

**TargetZoneName**

Specifies the SMP/E environment target zone name.

If you are upgrading to the latest CA CSM version, specify a unique value for this keyword different from the value in any other previous CA CSM version.

**Limits:** Up to 7 characters

**Default:** CAIT0

Your value: ____________________________________________

**DlibHLQ**

Specifies the prefix for the distribution data sets.

If you are upgrading to the latest CA CSM version, specify a unique value for this keyword different from the value in any other previous CA CSM version. The value of DlibHLQ must be different from RunTimeMVSHLQPrefix and DatabaseHLQ.

**Default:** The value of CSIHLQ

Your value: ____________________________________________

**DlibZoneName**

Specifies the SMP/E environment distribution zone name.

If you are upgrading to the latest CA CSM version, specify a unique value for this keyword different from the value in any other previous CA CSM version.

**Limits:** Up to 7 characters

**Default:** CAID0

Your value: ____________________________________________

**MSMPATH**

Specifies the path of the USS directory in which to install CA CSM. This directory becomes the CA CSM root and must be available and writable when you execute the CA CSM setup utility.

You must define the mount point. The required file system space is about 250 cylinders.

If you are upgrading to the latest CA CSM version, specify a unique value for this keyword different from the value in any other previous CA CSM version.

**Example:** /u/users/msmserv/v60/msm

Your value: ____________________________________________
Perform Post-Upgrade Tasks

Appendix A: Options File Worksheet

RunTimeMVSHLQPrefix

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

If you are upgrading to the latest CA CSM version, specify a unique value for this keyword different from the value in any other previous CA CSM version. The value of RunTimeMVSHLQPrefix must be different from TargetHLQ and DlibHLQ.

Example: CAI.CSM60.RT

Your value: ______________________________________________________

RunTimeUSSPath

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

This directory must be available and writable when you execute the CA CSM setup utility. The required space is about 750 cylinders.

If you are upgrading to the latest CA CSM version, specify a unique value for this keyword different from the value in any other previous CA CSM version.

Example: /u/users/msmserv/v60/msmruntime

Your value: ______________________________________________________

DatabaseHLQ

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

If you are upgrading to the latest CA CSM version, specify a unique value for this keyword different from the value in any other previous CA CSM version. The value of DatabaseHLQ must be different from TargetHLQ and DlibHLQ. Starting with CA Datacom/AD Version 14, the CXX name is part of the data set names.

Limits: Up to 27 characters

Default: The value of RunTimeMVSHLQPrefix

Your value: ______________________________________________________

CXXNAME

Specifies the name of the unique identifier for the CA Datacom/MSM database CXX Directory.

The value that you provide for CXXNAME will be part of every CA Datacom/MSM database data set name as the next to last qualifier node.

Limits: 1 through 7 alphanumeric characters

Default: CSM60

Note: For more information about CXXNAME naming conventions, see the CA Datacom/DB DBUTILITY Reference Guide for z/OS.

Your value: ______________________________________________________
**ServerName**

Specifies a name for the CA Datacom/MSM server. CA Datacom uses the name to differentiate between multiple instances of the server. If your site has multiple CA Datacom Multi-User Facility (MUF) servers on a system or in a sysplex, verify that the name is unique within "CAICCI Plex".

The name must be unique across the "CAICCI Plex", and the server name and application ID must be unique within the sysplex. Keeping these values unique ensures that the database servers do not fail during startup. If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

**Limits:** 1 through 32 alphanumeric characters

**Default:** CSM60 or the value that you provided for the CXXNAME keyword

**Note:** We recommend that you keep the default value.

**Example:** CSMV6SRV

**Note:** For more information about ServerName, see the *CA Datacom Server User Guide*.

Your value: ____________________________________________

**Applid**

Specifies a name that is used to identify CA Datacom Server to the CA Datacom/MSM application.

**Limits:** 1 through 20 alphanumeric characters

**Default:** CSM60 or the value that you provided for the CXXNAME keyword

**Note:** For more information about Applid, see the *CA Datacom Server User Guide*.

Your value: ____________________________________________
PROTOCOL

Specifies the communication protocol that is used to transmit data between CA CSM and CA Datacom Server. Data transmission can be done through the CAICCI interface on the system, or by using the simpler TCP/IP interface that listens on a port number. On certain environments, the TCP/IP service may provide better performance during CA CSM operations.

Options include:

CCI

The CAICCI protocol is used.

BOTH

The TCP/IP protocol is used. If you use this option, specify values or use the default values for the keywords TCPIP_HOST, TCPIP_PORT and TCPIP_CONNECT_QUEUE.

Default: CCI

Note: For more information about PROTOCOL, see the CA Datacom Server User Guide.

Your value: __________________________________________________________

TCPIP_HOST

(Only applies when PROTOCOL=BOTH) Specifies the host name or IP address on which the CA Datacom Server listens for incoming TCP/IP data traffic from CA CSM.

This keyword is ignored if PROTOCOL=CCI.

Default: The IP address of the current system

Note: For more information about TCPIP_HOST, see the CA Datacom Server User Guide.

Your value: __________________________________________________________

TCPIP_PORT

(Only applies when PROTOCOL=BOTH) Specifies the port number on which CA Datacom Server listens for incoming TCP/IP data traffic from CA CSM. This port assignment must not be used by any other TCP/IP service in your environment.

This keyword is ignored if PROTOCOL=CCI.

Limits: 1024 through 65535

Default: 5465

Note: For more information about TCPIP_PORT, see the CA Datacom Server User Guide.

Your value: __________________________________________________________
Perform Post-Upgrade Tasks

TCPIP_CONNECT_QUEUE

(Only applies when PROTOCOL=BOTH) Specifies the number of TCP/IP database requests from CA CSM that the CA Datacom Server can process at once.

This keyword is ignored if PROTOCOL=CCI.

Limits: 1 through 9999

Default: 250

Note: We recommend that you keep the default value.

Note: For more information about TCPIP_CONNECT_QUEUE, see the CA Datacom Server User Guide.

Your value: _______________________________________

MSMServerPortNo

(The CA CSM application server HTTP port) Specifies the port number to use for web-based access to CA CSM.

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

Default: 22120

Your value: _______________________________________

MSMDSIPORTNO

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

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

Default: 22130

Your value: _______________________________________

MSMConnectorRedirectPortNo

(The CA CSM application server redirect port) 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.

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

Default: 22140

Your value: _______________________________________
**MSMTomcatServerShutdownPortNo**

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

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

**Default:** 22150

**Your value:** ________________________________

**MVSHFSdsnPrefix**

Specifies the prefix for the names of file system data sets. The value sets the default for the Mount Point Management Data Set Prefix in the web-based interface. A CA CSM administrator can override this value.

**Important!** If you are upgrading to the latest CA CSM version, verify that the value for this keyword is the same as the value for the version that you are upgrading from.

**Default:** OMVSUSR.CAMSM

**Your value:** ________________________________

**MountPath**

Specifies the path to the USS directory that CA CSM can use for work files. This directory must be available when you execute the setup utility. The value sets the default for the Mount Point Management Application root in the web-based interface. A CA CSM administrator can override this value.

**Important!** If you are upgrading to the latest CA CSM version, verify that the value for this keyword is the same as the value for the version that you are upgrading from.

**Example:** /u/users/msmserv/mpm

**Your value:** ________________________________
Perform Post-Upgrade Tasks

mpmAutomount

Specifies whether CA CSM mounts the file systems during startup.

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

Options include:

Y

CA CSM mounts file systems automatically during startup.

N

You must mount file systems manually before starting CA CSM.

Default: Y

Your value: __________________________________________________________

USSFileSystemType

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

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

Options include:

■ HFS
■ ZFS

We recommend that you use 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.

Your value: __________________________________________________________________

mpmAllocation

(Optional) Specifies the storage preference for allocating new data sets for file systems on the Mount Point Management page of the Settings tab.

Options include:

■ SMS
■ NONSMS

Default: SMS

Your value: __________________________________________________________________
mpmStorageClass

(Optional; only applies when mpmAllocation=SMS) Specifies the SMS storage class of the DASD on the Mount Point Management page in the web-based interface. This keyword is used during product installation and maintenance.

Leave this keyword blank to use default site settings.

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

Default: Blank
Example: SYSSC
Your value: _________________________________

mpmMgmtClas

(Optional; only applies when mpmAllocation=SMS) Specifies the SMS management class for file system data sets on the Mount Point Management page of the Settings tab.

Leave this keyword blank to use default site settings.

Default: Blank
Your value: _________________________________

mpmDataClas

(Optional; only applies when mpmAllocation=SMS) Specifies the SMS data class for file system data sets on the Mount Point Management page of the Settings tab.

Leave this keyword blank to use default site settings.

Default: Blank
Example: SYSDC
Your value: _________________________________

mpmUnit

(Optional; only applies when mpmAllocation=NONSMS) Specifies the type of the DASD on which to place data sets on the Mount Point Management page of the Settings tab.

Leave this keyword blank to use default site settings.

Default: Blank
Example: 3390
Your value: _________________________________
mpmVolumeSer

(Optional; only applies when mpmAllocation=NONSMS) Specifies the NONSMS volume serial number of the DASD on the Mount Point Management page in the web-based interface. This value is used during product installation and maintenance.

Leave this keyword blank to use default site settings.

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

**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.

**Limits:** 0; 60 through 1440

**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 the CA CSM Software Installation Service.

Leave this keyword blank to use default site settings.

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

**Default:** Blank

**Example:** SYSSC

**Your value:** __________________________________________

sisExecutorOutputUnit

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

Leave this keyword blank to use default site settings.

**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.

Leave this keyword blank to use default site settings.

**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 the CA CSM Software Installation Service.

Leave this keyword blank or specify an asterisk (*) to use default site settings.

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

**Example:** WRK001

**Your value:** __________________________________________________________

**sisGimunzipTempPrefix**

Specifies the prefix CA CSM uses for GIMUNZIP output temporary data set names during product installation and maintenance. The created temporary work files are not SMP/E controlled data sets. CA CSM deletes them through the product installation process. These files are used as input relative files for SMP/E processing during the receiving of a product into the SMP/E environment global zone.

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

**Limits:** 12 through 19 characters (depending on the number of characters that is used for jobname)

**Note:** If you use the default 6-character jobname, you can enter up to 14 characters for the GIMUNZIP temporary prefix.

**Example:** CAI.CSM.V60.TEMP

**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.DATASETSUFFIXnnnn
```

*nnnn*

Represents the unique numeric identifier that CA CSM automatically appends to the qualifier.

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

**Limits:** 4 characters

**Default:** CASC

**Example:**

MVSHFSDsnPrefix = OMVSUSR.CACSM
DATASETSUFFIX = CASC
Full data set name = OMVSUSR.CACSM.CASC1234

**Your value:** __________________________________________

**sisExecutorServerDsnPrefix**

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

**Limits:** Up to 24 characters

**Example:** PUBLIC

**Your value:** __________________________________________

**safSecurity**

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

If you are upgrading to the latest CA CSM version, you can set this keyword to the same value that you have in the previous CA CSM version.

**Options include:**

**Y**

Enables SAF security.

**N**

Disables SAF security.

**Default:** N

**Your value:** __________________________________________
safResourceClass

(Only applies when safSecurity=Y) Specifies the SAF resource class name that CA CSM uses for security rules in resource profiles.

**Default:** CAMSM

**Your value:** __________________________________________________________

sysTaskDeleteOverrideEnabled

(Only applies when safSecurity=N) Specifies whether to let CA CSM users delete tasks.

Options include:

**Y**

Any user can delete any competed task.

**N**

Users cannot delete completed tasks.

**Default:** N

**Your value:** __________________________________________________________

HASH

Specifies whether to perform SMP/E GIMUNZIP hash validation. We recommend that you use the default value.

Options include:

**Y**

Enables the HASH validation.

**N**

Disables the HASH validation.

**Default:** Y

**Your value:** __________________________________________________________
Perform Post-Upgrade Tasks

ICSF

(Only applies when HASH=Y and the system has Integrated Cryptographic Services Facility (ICSF) installed) Specifies whether to use ICSF for the HASH validation.

Options include:

Y
Uses ICSF for the HASH validation.

N
Does not use ICSF for the HASH validation.

Default: Y
Your value: ________________________________________________

SMPCPATH

(Only applies when both HASH=Y and ICSF=N) Specifies the path to the SMP/E Java application classes.

Default: /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.

To use the SMS default volume, specify an asterisk (*). If you specify CSIVOL=* and your site does not have any default or standard volume that are specified in SMS, the first installation job (CSMN6001 for a new installation, or CSMUxx01 for an upgrade) may fail with an IDCAMS error while allocating the CA CSM SMP/E environment. In that case, specify a valid SMS or non-SMS volume and rerun the installer.

If you use CA Allocate with PTF RO60802 applied, you can specify a volume pool name as a value for this keyword.

Default: *
Your value: ________________________________________________

TargetVOL

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

To use the SMS default volume, specify an asterisk (*).

If you use CA Allocate with PTF RO60802 applied, you can specify a volume pool name as a value for this keyword.

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.

To use the SMS default volume, specify an asterisk (*).

If you use CA Allocate with PTF RO60802 applied, you can specify a volume pool name as a value for this keyword.

**Default:** The value of CSIVOL

Your value: ________________________________________________

RuntimeVOL

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

To use the SMS default volume, specify an asterisk (*).

If you use CA Allocate with PTF RO60802 applied, you can specify a volume pool name as a value for this keyword.

**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.

To use the SMS default volume, specify an asterisk (*).

If you use CA Allocate with PTF RO60802 applied, you can specify a volume pool name as a value for this keyword.

**Default:** The value of RuntimeVOL

Your value: ________________________________________________

TEMPUNIT

Specifies the device name for temporary work data sets.

**Default:** SYSDA

Your value: ________________________________________________
STORAGE

Specifies the storage preference for the SMP/E temporary data sets.

**Note:** If your site uses SMS ACS, ACS overrides the storage parameter values.

Options include:

- SMS
- NONSMS

**Default:** SMS

**Your value:** __________________________________________________________

MGMTCLAS

(Only applies when STORAGE=SMS) Specifies the SMS management class to use for the temporary SMP/E data sets. Management classes define different levels of migration, backup, and retention services.

Leave this keyword blank to use ACS settings.

**Default:** Blank

**Example:** SYSMC

**Your value:** __________________________________________________________

STORCLAS

(Only applies when STORAGE=SMS) Specifies the SMS storage class to use for the temporary SMP/E data sets. Storage classes define different levels of performance and availability services.

Leave this keyword blank to use ACS settings.

**Default:** Blank

**Example:** SYSSC

**Your value:** __________________________________________________________

DATACLAS

(Only applies when STORAGE=SMS) Specifies the SMS data class to use for the temporary SMP/E data sets. Data classes define different allocation defaults.

Leave this keyword blank to use ACS settings.

**Default:** Blank

**Example:** SYSDC

**Your value:** __________________________________________________________
UNIT
(Only applies when STORAGE=NONSMS) Specifies the type of the DASD on which to place temporary SMP/E data sets.

Example: 3390
Your value: ________________________________________________

VOLUME
(Only applies when STORAGE=NONSMS) 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 in which the CAIRIM module resides. The library must be APF-authorized.

Example: CAI.CAW0LOAD
Your value: ________________________________________________

CCScaipdsedsn
Specifies the fully qualified name of the CA Common Services for z/OS CAW0PLD data set in which the LIBCCI and LIBCCI6E load modules reside.

Example: CAI.CAW0PLD
Your value: ________________________________________________

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

You can find this value through the following message:

CAS9850I CAICCI TCP/IP server ready. PORT port-number ADDR host_address

Default: 1202
Your value: ________________________________________________
**ENF SystemID**

Specifies the value of CA Common Services for z/OS CAICCI SYSID on your system. You can find this value through the following console message:

```
CAS9214I - CA-ENF Command: SYSID(caicci_sysid)
```

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

```
ENF DISPLAY,SYSSID
```

**Example:** A91SENF

**Your value:** ____________________________________________

**ActiveJES**

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

- **JES2**
- **JES3**

**Default:** JES2

**Your value:** ____________________________________________

**JOBNAME**

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

**Default:** The ID of the user who executes the CA CSM setup utility appended with S

**Your value:** ____________________________________________

**ACCOUNT**

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

**Default:** Blank

**Example:** ‘1234,dept01,NY NY’

**Your value:** ____________________________________________

**CLASS**

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

**Default:** A

**Your value:** ____________________________________________
MSGCLASS

(Optional) Specifies the JES output class for job logs. The class determines how the logs are handled (for example, held for later review).

Default: X
Your value: __________________________________________

SYSAFF

Specifies the systems that are eligible to process jobs. The keyword specifies the value of the JOBPARM SYSAFF parameter.

You can specify the ID of a particular system so that jobs are processed on that system. If you do not want to use this feature, do not specify a value.

Default: *
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.

Options include:

Y

 Allows the CA CSM installer to add the CA Datacom/MSM data sets to the APF list dynamically. If your site is set with the static APF format, it will be changed to the dynamic format, and data sets will be added to the APF list.

N

 Requires you to add the CA Datacom/MSM data sets manually. Review the summary report after the installation to perform these manual steps to complete the installation.

Default: Y
Your value: __________________________________________

HOSTNAME

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

Default: The IP address of the current LPAR
Example: 110.64.255.255
Your value: __________________________________________

MFASM

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

Default: ASMA90
Your value: __________________________________________
Perform Post-Upgrade Tasks

MFZAP
Specifies the name of the system utility program that is 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. This option may be required depending on your site TCP/IP stack configuration.

You can leave this keyword blank. If errors are encountered during the Apache Tomcat startup job (MSMTCSRVR), you can uncomment the SYSTCPD DD card inside MSMTCSRVR for diagnostic purposes.

Example: VTAM.TCPIP.TCPIP.DATA
Your value: ______________________________________________________

TCPIPLinkDSName
Specifies the name of the TCPIP Services SEZATCP data set. This data set is part of the z/OS Communications Server. This data set is typically program controlled and in the z/OS linklist (LNKLST).

Default: TCPIP.SEZATCP
Your value: ______________________________________________________

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

Default: CEE.SCEELKED
Your value: ______________________________________________________

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

Default: CEE.SCEESPC
Your value: ______________________________________________________
Perform Post-Upgrade Tasks

Appendix A: Options File Worksheet

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.

Example: 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 installer uses to submit jobs, check status, and validate return codes as part of the installation.

Options include:

FTP
Installation jobs are submitted using FTP. The prerequisite is JESINTERFACELEVEL 2. This mode is fully automated.

Note: We recommend that you use this method.

TSO
Installation jobs are submitted using TSO. The CA CSM installer runs in Manual installation mode only: only one job (for a new installation) or two jobs (for an upgrade) are submitted. You have to manually submit the rest of the installation jobs after the utility finishes.

Note: If your local FTP is Secure FTP or FTP Secure, the CA CSM installer does not support this feature. Specify job.submission.mode=TSO and run the CA CSM installer.

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. This field enables you to cancel the process if the system is busy.

Default: 30

Your value: __________________________________________________________

msm.ssl.secure.connection.enable

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

Options include:

Y
Uses HTTPS.

N
Uses HTTP.

Default: N

Your value: __________________________________________________________

first.name.and.last.name

(Optional; only applies when msm.ssl.secure.connection.enable=Y) Specifies your URL domain name.

Default: Blank

Example: www.your.domain

Your value: __________________________________________________________

organization.name

(Optional; only applies when msm.ssl.secure.connection.enable=Y) Specifies your organization name.

Default: Blank

Your value: __________________________________________________________

organization.unit.name

(Optional; only applies when msm.ssl.secure.connection.enable=Y) Specifies your organization unit name.

Default: Blank

Your value: __________________________________________________________
city
(Optional; only applies when msm.ssl.secure.connection.enable=Y) Specifies your city name.

Default: Blank
Your value: ________________________________________________

state
(Optional; only applies when msm.ssl.secure.connection.enable=Y) Specifies your state name.

Default: Blank
Your value: ________________________________________________

country.code
(Optional; only applies when msm.ssl.secure.connection.enable=Y) Specifies your state name.

Default: Blank
Your value: ________________________________________________

keystore.location
(Optional; only applies when msm.ssl.secure.connection.enable=Y) Specifies the location of the keystore. Specify your own value if you need to use a different USS location than the default location.

Note: The Installer prompts you for the keystore password at installation time.

Default: Created in your RunTimeUSSPath
Your value: ________________________________________________

validity.period
(Optional; only applies when msm.ssl.secure.connection.enable=Y) Specifies the validity period, in days, for the generated keystore certificate.

Default: 365
Your value: ________________________________________________

PreviousRelease.MSMPATH
(Only applies when you are upgrading to the latest CA CSM version) Specifies the path of the USS directory in which the previous version of CA CSM is installed. This path has folders, for example, CEGPHFS and CEGPJAR.

See the MSMSummaryReport.txt or the options file available in the CEGPHFS directory of the previous CA CSM version.

Example: /u/users/msmserv/msm
Appendix B: 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 before CA MSM R4.1 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 R4.1 to the latest version

In this scenario, the following actions are performed:

- 12 previous version CA Datacom/MSM database tables are copied, restructured, and data is converted, if any.
- 7 existing CA Datacom/MSM tables are removed.
- 18 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.

CA MSM V5.0 to the latest version

In this scenario, the following actions are performed:

- 8 previous version CA Datacom/MSM database tables are copied, restructured, and data is converted, if any.
- 8 existing CA Datacom/MSM tables are removed.
- 18 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.
Perform Post-Upgrade Tasks

CA CSM R5.1 to the latest version

In this scenario, the following actions are performed:

- 10 previous version CA Datacom/MSM database tables are copied, restructured, and data is converted, if any.
- 12 new CA Datacom/MSM tables are added to their respective database areas.
- System Registry tables are replaced with revised data.