CA IDMS - 19.0
Installation and Maintenance for z/OS

Date: 12-Jan-2018
This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2017 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.
Table of Contents

Audience ................................................................................................... 11

Methodologies .......................................................................................... 11
Acquisition Methods .................................................................................. 11
SMP/E Environment Create Methods ...................................................... 12
Maintenance Application Methods ............................................................ 12
Deployment Methods .................................................................................. 12

How the Installation Process Works .......................................................... 13

Preparing for Installation .......................................................................... 13
Hardware Requirements ............................................................................... 13
  Mainframes Supported ........................................................................... 14
  CPU Requirements .................................................................................. 14
  Disk Drives Supported ........................................................................... 14
  Disk Space Requirements ....................................................................... 14
Software and Interface Requirements ........................................................ 14
  Operating Systems Supported ............................................................... 15
  CA Chorus Software Manager Versions Supported ................................. 15
  SVC Supported ...................................................................................... 15
CA Common Services for z/OS Requirements ............................................ 15
  Required CA Common Services for z/OS Components ............................. 15
  Other CA Common Services for z/OS Components ................................ 16
Other Requirements ................................................................................... 16
  VTAM Requirements ............................................................................. 17
  TCP/IP Requirements ............................................................................ 17
  SQL Web Connect .................................................................................. 17
  CICS Support ....................................................................................... 17
  Library Requirements ............................................................................ 17
  SMP/E Requirements ............................................................................ 18
  CA LMP Keys ...................................................................................... 18
  Key Certificate Contents ....................................................................... 18
Starting Your Product .......................................................... 47
Before You Begin .................................................................. 47
Configuration Process Overview ........................................... 48
Unlicensed Products ............................................................. 48
Installation Libraries ........................................................... 48
Configuration Libraries ....................................................... 49
Configuration Types ........................................................... 50
  Complete Base Configuration ........................................... 51
  Upgrade Configuration ..................................................... 51
  Add-On Configuration ...................................................... 52
Configuring Your Product Using CA CSM ......................... 53
Configuring Your Product Without CA CSM ....................... 53
  Create the CAISAG Library ............................................. 53
  Customizing the CAISAG Library Members ....................... 53
  Customizing the JOBCARD Member .................................. 54
  Customizing the SETUP Member ..................................... 54
  Customizing the VARBLIST Member ............................... 54
  Execute CAISAG ............................................................ 55
Generated Configuration Tasks ............................................ 56
  Generated Configuration Jobs ........................................... 56
    Configuration Files Allocation ....................................... 57
    Customized Source ..................................................... 57
    Customized Load Modules .......................................... 60
    Load SVC Using CAIRIM ............................................ 60
    Database Files Allocation ............................................ 62
    DD Statement Members ............................................... 62
    DMCL and DB Table in Bootstrap Catalog ....................... 62
    Selected Product Updates ............................................ 63
    SYSTEM and SYSDIRL Dictionaries .............................. 63
    APPLDICT Dictionary .................................................. 64
    ASFDICT Dictionary ................................................... 64
    Format Tools Files ..................................................... 65
    Tools Dictionaries and Database Files ............................. 65
    Non-SQL Commonweather Database ............................... 65
    SQL Demo Database and Web Services Consumer Demo ........ 66
    Change Control Database ............................................. 66
    Generate SYSTEM 90 .................................................. 66
    Database Files Backup ................................................ 67
Post-Configuration Tasks ................................................... 67
  The Environment After Configuration is Complete .............. 68
  z/OS Environment ......................................................... 68
Preparing TP Access Environment ........................................................................................................... 68
VTAM Access ........................................................................................................................................ 68
TCP/IP Access ....................................................................................................................................... 69
TSO Access .......................................................................................................................................... 69
CICS Access .......................................................................................................................................... 70
CA IDMS Task Analyzer Storage Requirements ................................................................................. 70
CA IDMS Log Analyzer and CA IDMS Task Analyzer Statistics Gathering ........................................ 70
CA IDMS Performance Monitor ........................................................................................................... 71
CA IDMS Web Services .......................................................................................................................... 71
  Web Services Consumer Demo Service ............................................................................................... 71
  Add-On Install SYSGEN Updates ......................................................................................................... 72
Configuring Default JCL for CA IDMS Extractor and CA IDMS Dictionary Migrator Assistant .......... 72
CA ADS Trace Dictionary Updates ......................................................................................................... 73
CA IDMS/DC Sort Dictionary Updates ................................................................................................ 73
CA IDMS DOF Dictionary Updates ...................................................................................................... 73
  Security Classification Modules ........................................................................................................... 74
Linking a Dictionary to the CA Endevor/DB Change Monitor ................................................................. 74
Creating an Executable System .............................................................................................................. 74
Modify the Startup JCL .......................................................................................................................... 75
  CA IDMS Enforcer ............................................................................................................................... 77
  CA IDMS/DC Sort under CICS ........................................................................................................... 77
Verifying the System Configuration ....................................................................................................... 77
  System Startup ................................................................................................................................... 78
  Online Verification .............................................................................................................................. 78
  Batch Verification .............................................................................................................................. 79
CAIRIM .................................................................................................................................................. 80
SVC ....................................................................................................................................................... 80
Refreshing Required Modules ................................................................................................................. 81
Numbered Options ................................................................................................................................. 81
Security .................................................................................................................................................. 82

Setup SQL Web Connect for z/OS ......................................................................................................... 82
CA IDMS Server Installation ................................................................................................................... 82
SQL Usage .......................................................................................................................................... 83
  Usage Considerations .......................................................................................................................... 83
  CAISAG Implementation .................................................................................................................... 84
  CSM Implementation .......................................................................................................................... 85

Installing CA IDMS Visual DBA ......................................................................................................... 85
Software Requirements ......................................................................................................................... 86
VARBLIST Variables ........................................................................................................... 100
Member Name .................................................................................................................. 101
Products .............................................................................................................................. 101
Global DMCL ...................................................................................................................... 101
Upgrade Configuration 1 .................................................................................................... 101
Tape Class .......................................................................................................................... 102
Disk VOLSER and Disk Contention .................................................................................. 102
CV Number .......................................................................................................................... 103
DC System Number .......................................................................................................... 103
Free Storage ....................................................................................................................... 103
Uppercase Terminal Support ............................................................................................. 104
Authorized Userid .............................................................................................................. 104
VTAM ID .............................................................................................................................. 104

Install CA IDMS Visual DBA Version 18 on the PC ............................................................. 86
Prepare Your Mainframe Environment .............................................................................. 88
   CA IDMS r16 .................................................................................................................... 88
   CA IDMS r17 .................................................................................................................... 88
Install CA IDMS Visual DBA Version 18 ........................................................................ 88
How to Convert to SQL, Create additional SQL Catalogs, Set Up Server and CCI .......... 89
   Convert CATSYS .......................................................................................................... 90
   Create SYSSID Catalog ............................................................................................... 91
   Create an Updated DMCL Module, Update the DBTABLE, and Format SYSSID ......... 91
   Load the Catalogs with SQL System Definitions ...................................................... 92
   Set Up CCI ...................................................................................................................... 92
   Set Up CA IDMS Server ............................................................................................... 93
How to Install the CA IDMS Visual DBA Version 18 SQL Definitions ............................. 93
   Install CA IDMS Visual DBA SQL Definitions Using IDMSBCF ................................. 94
   Install CA IDMS Visual DBA SQL Definitions Using CA IDMS Visual DBA ........... 95
Uninstall and Reinstall CA IDMS Visual DBA ................................................................. 96
   Uninstall the PC Client Component ............................................................................ 97
      Uninstall CA IDMS Visual DBA r16 ......................................................................... 97
      Uninstall CA IDMS Visual DBA r17 ......................................................................... 97
      Uninstall CA IDMS Visual DBA Version 18 ............................................................ 97
   Uninstall the Mainframe SQL Definitions ................................................................... 98
      Uninstall CA IDMS Visual DBA r16 ......................................................................... 98
      Uninstall CA IDMS Visual DBA r17 ......................................................................... 99
      Uninstall CA IDMS Visual DBA Version 18 ............................................................ 100
CA IDMS Visual DBA Version 18 Reinstallation ............................................................... 100
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWA Displacement</td>
<td>104</td>
</tr>
<tr>
<td>Add-On Variables</td>
<td>105</td>
</tr>
<tr>
<td>Page Size</td>
<td>105</td>
</tr>
<tr>
<td>CA Common Services for z/OS</td>
<td>106</td>
</tr>
<tr>
<td>CVKEY</td>
<td>106</td>
</tr>
<tr>
<td>Log and Task Analyzer Billing Information</td>
<td>106</td>
</tr>
<tr>
<td>CA Endevor/DB Message Library</td>
<td>106</td>
</tr>
<tr>
<td>Variables for SQL Web Connect</td>
<td>107</td>
</tr>
<tr>
<td>Base Configuration</td>
<td>107</td>
</tr>
<tr>
<td>Upgrade Configuration</td>
<td>107</td>
</tr>
<tr>
<td>Add-On Configuration</td>
<td>108</td>
</tr>
<tr>
<td>Installing Your Product from Tape</td>
<td>108</td>
</tr>
<tr>
<td>Download the SAMPJCL Library from Tape</td>
<td>108</td>
</tr>
<tr>
<td>Modify the Receive Job</td>
<td>109</td>
</tr>
<tr>
<td>Customize the AGJEDIT Edit Macro</td>
<td>109</td>
</tr>
<tr>
<td>Make the AGJEDIT Edit Macro Accessable</td>
<td>110</td>
</tr>
<tr>
<td>Create Your SMP/E System</td>
<td>110</td>
</tr>
<tr>
<td>How to Use an Edit Macro</td>
<td>110</td>
</tr>
<tr>
<td>Customize and Submit Jobs in SAMPJCL</td>
<td>111</td>
</tr>
<tr>
<td>Install Maintenance on Your SMP/E System</td>
<td>111</td>
</tr>
<tr>
<td>Apply Preventive Maintenance</td>
<td>112</td>
</tr>
<tr>
<td>HOLDDATA</td>
<td>114</td>
</tr>
<tr>
<td>Deploy and Configure Your Product</td>
<td>114</td>
</tr>
</tbody>
</table>
Installation and Maintenance for z/OS

This section describes how to acquire, install, deploy and configure CA IDMS to make it available to the staff who implement and use the product.
Audience

There are multiple steps in the CA IDMS installation process, and some steps can be performed in multiple ways. Different steps may be performed by different people, depending on access authority, skill set, site policies, etc. This section is for people taking part in the installation of CA IDMS. The following installation breakdown is intended to aid you in identifying the people required and coordinating their efforts.

Configuration (creating customized loadlibs and creating or updating database files) should be done by the CA IDMS DBA. The DBA may need to work with the following personnel:

- Systems programmer, for VTAM definitions, SVC selection, CV key, LMP keys, library names.
- Storage administrator, for DASD allocations.
- CICS administrator, for CWA displacement, CICS library names.

Methodologies

There are several methods you can use to acquire your software, set up your SMP/E environment, apply maintenance, and configure your software after installation is complete.

Acquisition Methods

Use one of the following methods to acquire (download) CA IDMS:

- CA CSM
  CA Chorus Software Manager (CA CSM) standardizes the installation process for CA mainframe products. To acquire your product using CA CSM, you must have CA CSM installed. A CA Support Online account is required.

- PAX-Enhanced ESD
  The ESD (Electronic Software Delivery) process requires knowledge of UNIX System Services and USS write authority. A Support Connect user ID associated with a CA Support Online account is required.

- Tape
  This acquisition method is not encouraged, but is still available for sites where security rules disallow acquiring files from the internet.
SMP/E Environment Create Methods

Use one of the following methods to create your SMP/E environment:

- **CA CSM**
  Using CA CSM to create your SMP/E environment requires no SMP/E knowledge, and there is no JCL to customize or submit. However, the authority to execute the SMP/E program, GIMSMP, is required. You can set up your SMP/E environment using CA CSM after acquiring your software using CA CSM or by Pax-Enhanced ESD. You cannot use CA CSM if you acquired your software from tape. If acquisition is by PAX-Enhanced ESD, execute the CA CSM dialog, Insert New Product, before using CA CSM to create the SMP/E environment.

- **Manual**
  The SMP/E environment can be created manually (JCL in SAMPJCL) following ESD or tape acquisition. It requires customizing an edit macro and making the edit macro available to a TSO session.

As a result of either method, the same SMP/E environment containing the same uncustomized software is set up at every site.

Maintenance Application Methods

Use one of the following methods to apply any available maintenance to CA IDMS:

**Note:** Applying maintenance should be done before performing deployment.

- **CA CSM**
  Using CA CSM standardizes the application of maintenance for CA mainframe products. Minimal SMP/E vocabulary is required. To acquire your product using CA CSM, you must have CA CSM installed. If you created the SMP/E environment manually, run the CA CSM Import CSI dialog before installing maintenance.

- **Manual**
  There is JCL to install maintenance in the same SAMPJCL library containing the jobs to create the SMP/E environment. You must be able to download PTFS and HOLDDATA from CA Support Online.

Deployment Methods

Deploying CA IDMS can be done with CA CSM and requires that CA CSM be installed at your site. Deployment copies the SMP/E target libraries (or a subset of them) to a different system or location. Performing deployment using CA CSM is a prerequisite to performing configuration using CA CSM. Otherwise deployment is optional.

**Note:** SMP/E does not update the deployed libraries. If you have performed deployment, perform the deployment again after you install maintenance to update your deployed libraries.
How the Installation Process Works

The following steps describe the installation process:

1. Prepare for the installation by confirming that your site meets all installation requirements as described in Preparing for Installation (see page 13).

2. Acquire the product using one of the supported acquisition methods (see page 10).

3. Install your product based on your acquisition method:
   - CA CSM -- see Installing Your Product Using CA CSM (see page 24)
     
     **Note:** If you do not have CA CSM, you can download it from the Download Center. Follow the installation instructions in the CA Chorus Software Manager documentation bookshelf on the CA Chorus Software Manager product page.
   - PAX-Enhanced ESD -- see Installing Your Product From Pax-Enhanced ESD (see page 30)
   - Tape -- see Installing CA IDMS from Tape (see page 108)

4. Apply maintenance, if applicable.

5. Deploy your target libraries.

6. Configure the minimum settings to start your product. For more information, see Starting Your Product (see page 47).

7. Start your product.

Preparing for Installation

The following topics describe information you need to know before you install CA IDMS.

- Hardware Requirements (see page 13)
- Software and Interface Requirements (see page 14)
- CA Common Services for z/OS Requirements (see page 15)
- Other Requirements (see page 16)

Hardware Requirements

The following sections describe the hardware requirements for installing CA IDMS:

- Mainframes Supported (see page 14)
- CPU Requirements (see page 14)
- Disk Drives Supported (see page 14)
Mainframes Supported

Any processor that supports 64-bit z/Architecture.

CPU Requirements

The default configuration requires a 6 MB region for execution. Region requirements depend on your specific system configuration.

Disk Drives Supported

The following DASDs are supported:

- 3380
- 3390

Disk Space Requirements

Disk space requirements are estimated in tracks in the following table:

| Disk installation files (ESD)          | 5,400 |
| SMP/E Environment                     | 14,000|
| Configuration files (only non-CSM installations) | 650   |
| Configuration files (only CSM installations) | 13,800|
| Database files                         | 5,800 |
| Deployment files (only CSM installations) | 7,500 |

You can delete the PAX-enhanced ESD disk installation files after the SMP/E environment is created.

Software and Interface Requirements

This section provides the software and interface requirements for installing CA IDMS.

- Operating Systems Supported (see page 15)
- CA Chorus Software Manager Versions Supported (see page 15)
- SVC Supported (see page 15)
Operating Systems Supported

This release requires z/OS.

CA Chorus Software Manager Versions Supported

CA IDMS requires Version 5.1 of CA CSM (formerly CA MSM).

SVC Supported

CA IDMS uses a Type 1 SVC to communicate between address spaces. Within CAIRIM, a CA Common Service, SVC numbers 172 through 176 are reserved for CA IDMS. Other valid user SVC numbers are 200 through 255.

The SVC number you plan to use must be selected during configuration. The SVC load module, IGC.xxx (where xxx is the SVC number), is assembled and linked during the configuration process. The SVC is downward compatible.

CA Common Services for z/OS Requirements

CA Common Services for z/OS is a group of system services that protect your investment in software and help you manage your data center more efficiently. Each of the components offers individual benefits. CA Technologies products require various CA Common Services for z/OS. The components you need for CA IDMS may already be installed at your site. Check with your systems group.

Required CA Common Services for z/OS Components

The following CA Common Services for z/OS components are required for installing CA™ IDMS:

- **CAIRIM (Resource Initialization Manager)**
  Eliminates the need for permanent installation of user SVCs and other installation requirements commonly encountered when installing systems software by providing a common driver for a collection of dynamic initialization routines. CAIRIM dynamically installs the CA IDMS SVC when requested, typically at IPL time.

- **CAISSF (Standard Security Facility)**
  Allows CA solutions to offer standardized security interfaces regardless of the particular needs of the underlying access control software. CAISSF invokes CA IDMS system security features. CAISSF is a subcomponent of CAIRIM and is installed with CAIRIM.

- **CA LMP (License Management Program)**
  Automated software tracking and validation service. CA LMP is a subcomponent of CAIRIM and is installed with CAIRIM.
Other CA Common Services for z/OS Components

The following CA Common Services for z/OS components are also used with and benefit CA IDMS:

- **CAICCI (Common Communication Interface)**
  Allows your software solutions to work together across platforms, making your software more powerful. CAICCI optional. How you define your CA IDMS system defines how you use CAICCI.

- **CAIENF (Event Notification Facility)**
  Insulates software solutions from changes in the operating system and environment. CAIENF is optional. How you define your CA IDMS system defines how you use CAIENF.

- **CA LMP Seat License Registration Service**
  The LMP Seat License Registration common service enables tracking and reporting on concurrent users of a CA product. This common service is a complimentary service used with the LMP license management service.
  If you do not have a license for the CA IDMS SQL Option or CA IDMS Server, you must have the CA LMP Seat License Registration Service installed on their system to use the SQL Web Connect feature. The Common Services releases that contain the Seat License Registration Service are:
  - CCS r12 with PTF RO40748
  - CCS r14.0 with PTF RO33298
  - CCS r14.1 (or greater)

Other Requirements

The following sections explain additional installation requirements:

- VTAM Requirements (see page 17)
- TCP/IP Requirements (see page 17)
- SQL Web Connect (see page 17)
- CICS Support (see page 17)
- Library Requirements (see page 17)
- SMP/E Requirements (see page 18)
- CA LMP Keys (see page 18)
- Key Certificate Contents (see page 18)
- Member Keys Parameter (see page 19)
- Installation Considerations (see page 20)
- Secured CA IDMS System on z/OS (see page 20)
- Accidental Deletion of Previous Release (see page 23)
- PDSE Considerations (see page 23)
- Maintenance Considerations (see page 23)
VTAM Requirements

You can use a VTAM application ID (APPLID) to access your DC/UCF system. The following sample statement assigns an APPLID for IDMSDC:

IDMSDC APPL AUTH= (ACQ, NOPASS, NVPACE, NOTSO, NOPO)

TCP/IP Requirements

You can use TCP/IP to access your CA IDMS system. To do so, you must provide a port number to the CA IDMS listener during configuration.

SQL Web Connect

The SQL Web Connect feature allows all IDMS/DB customers to run two concurrent instances of SQL and two concurrent instances of either ODBC or JDBC:

- JDBC users must use a Type-4 JDBC connection.
- ODBC users must configure their Data Source to use the ‘IDMS’ communications protocol.

You need to install CA IDMS Server for ODBC/JDBC connectivity. The following releases of CA IDMS Server are required:

- JDBC users must run CA IDMS Server r16.0 or greater.
- ODBC users must run CA IDMS Server r17.0 or greater.

CICS Support

The CA IDMS installation does not require CICS. However, if your site wants to access CA IDMS from CICS, you must use CICS at a release level that is supported by IBM. To implement the CICS interface, CA IDMS requires the exclusive use of a fullword in the CICS CWA. Typically, only the CICS systems programming staff assigns fullwords in the CWA.

⚠️ Note: For more information on CICS implementation, see Standard CICS Interface (https://docops.ca.com/display/IDMS19/Standard+CICS+Interface).

Library Requirements

The installation and operation of some products in the CA IDMS product line require the following libraries:
The z/OS system macro library (SYS1.MACLIB) is required by CA IDMS/DB.

The z/OS Callable Services Library (SYS1.CSSLIB) is required by CA IDMS/DB.

A COBOL subroutine library is required to install the Commonweather demonstration database.

Access to the IBM Language Environment (LE) runtime support is required in all CV and local mode batch CA IDMS environments. If the LE runtime library (usually CEE.SCEERUN) must be in the CDMSLIB concatenation or in the MVS LPA when executing a CA IDMS Central Version. It must be in the STEPLIB concatenation or in the link list for batch jobs.

CICS libraries are required by CICS Support.

**SMP/E Requirements**

CA IDMS cannot be installed without SMP/E. SMP/E Release V3R4 or higher is required if you are using Electronic Software Delivery to acquire the software.

You can make configuration choices without modification to the delivered software. Virtually all sites create the same SMP/E environment containing the same non-customized software.

**CA LMP Keys**

Some CA IDMS products, options, and interfaces require an LMP key. If your site uses any of these products, options, or interfaces, the LMP keys associated with them must be installed.

CA LMP keys are valid across product releases but not across CPUs. If you are running a previous release of a product and performing configuration on the same CPU, you can skip this section. If you are adding new product or you are performing configuration on a different CPU, you must install CA LMP keys.

**Key Certificate Contents**

The CA LMP key certificates contain the following information:

- **Product Name**
  Specifies the trademarked or registered name of the CA product licensed for the designated site and CPUs.

- **Supplement**
  Specifies the reference number of your license for the particular product, in the format nnnnnn - nnn. This format differs slightly inside and outside North America, and in some cases may not be provided at all.

- **Expiration Date**
  Specifies the date your license expires for this product, in the format MONTH dd, yyyy, for example JANUARY 15, 2016.
- **Technical Contact**
  Specifies the name of the technical contact at your site. This person is responsible for the installation and maintenance of the designated product. CA addresses all CA LMP correspondence to this contact person.

- **MIS Director**
  Specifies the name of the director of MIS or the person who performs that function at your site. If the title, but not the name, of the individual is indicated on the certificate, supply the actual name when correcting and verifying the certificate.

- **CPU Location**
  Specifies the address of the building where the CPU is installed.

- **Execution Key**
  Specifies an encrypted code required by CA LMP for product initialization. During installation, it is referred to as the LMP code.

- **Product Code**
  Specifies a two-character code that corresponds to this particular product.

- **CPU ID**
  Specifies the code that identifies the specific CPU for which installation of your product is valid.

If your site is already running software from CA Technologies, your systems group probably is already running a CAS9 proc (cataloged procedure). If so, add the CA LMP keys for the products you are installing to the CA LMP keys already being used.

The CAS9 proc runs the CAIRIM program, which uses a KEYS DD statement. The KEYS DD statement points to your CA LMP keys. The KEYS DD statement usually points to a member named KEYS in a PARMLIB or OPTLIB. Each line contains the information from one key certificate. If the information does not fit on one line, code a hyphen in column 72 for a continuation character.

### Member Keys Parameter

The parameter structure for member KEYS is as follows:

```
PROD(pp) DATE(ddmmyyy) CPU(tttt-mmmm/ssssss) LMPCODE(kkkkkkkkkkkkkk)
```

**Note:** The parentheses in the parameter list are required.

The member key parameter contains the following information:

- **pp**
  Specifies the two-character product code. For any CA LMP software solution, this code agrees with the product code already in use by the CAIRIM initialization parameters for earlier gen levels of the product.

- **ddmmyyyy**
  Specifies the CA LMP licensing agreement expiration date.
• \textit{tttt-mm}
  Specifies the CPU type and model (for example: 3090-600) on which the CA LMP software solution is to run. If the CPU type and the model require less than four characters, insert blank spaces for the unused characters.

• \textit{ssssss}
  Specifies the serial number of the CPU on which the CA LMP software solution is to run.

• \textit{kkkkkkkkkkkk}
  Specifies the execution key required to run the CA LMP software solution. This CA LMP execution key is provided on the Key Certificate shipped with each CA LMP software solution.

**Example: Control Card for the CA LMP Execution Software Parameter**

The following example shows a control card for the CA LMP execution software parameter:

\begin{verbatim}
PROD(FE) DATE(15JAN07) CPU(3090-600 /370623) LMPC0DE(52H2K06130Z7RZ06)
\end{verbatim}

\textbf{Note:} This execution key is only an example; the CA LMP execution key is invalid.

**Installation Considerations**

If you are upgrading from a previous release, always review the Release Notes for each of the releases higher than your current release. If you are upgrading from a release prior to Release 18.0, be aware that there are substantial differences in the installation process. These changes are described in detail in the Release Notes for CA IDMS Version 18.0.0, located on the Support Documentation site.

Additional Instructions, which may be added in the release announcement letter or PMLs, supersede the instructions in this documentation.

**Secured CA IDMS System on z/OS**

If you comply with the following requirements when configuring CA IDMS and its related products, there are no known system integrity exposures introduced within the z/OS operating systems.

• Specify the following parameters to generate a secured SVC when configuring using CA CSM or customizing the VARBLIST member:

\begin{verbatim}
GJCVKEY=primary-protect-keyAUTHREQ=YES
\end{verbatim}

\textbf{Note:} For more information on these parameters, see CVKEY, AUTHREQ, and the article "Setting Up Interpartition Communication and the SVC (https://docops.ca.com/display/IDMS19/Setting+Up+Interpartition+Communication+and+the+SVC)."
Update the Program Properties table (PPT) in SYS1.PARMLIB(SCHEDnn) to include the protect key chosen for CA IDMS.

Specify STORPROT=YES during configuration.

Protect the library containing the CA IDMS system code against unauthorized updates. This includes user written exits, database procedures, and system mode SQL procedures.

Verify that all user application programs are specified in the CA IDMS sygjen with the PROTECT option. This option helps ensure that CA IDMS system code runs in this primary key while user mode application code runs in a separate key.

There are two forms of storage protection: standard storage protection and high performance storage protection.

Standard storage protection protects CA IDMS system code from update by an application program. It also protects an application program from update from other application programs.

High performance storage protection protects CA IDMS system code from update by an application program.

Note: Running a CA IDMS system with standard storage protection requires more storage and more CPU use than running an unsecured CA IDMS system. High performance storage protection requires the same storage as standard storage protection, but it does not incur any significant CPU overhead. For this reason, high performance storage protection may be more suitable for a production system. Standard storage protection is often used on development or test systems to prevent inadvertent updates by untested user code. For more information on standard and high performance storage protection, see the Administrating section.

Control access to the CA IDMS Debugger, because this facility permits changing both programs and storage in the CA IDMS address space.

Use the discrete security functions of DCMT to prevent unauthorized users from performing the following activities:

- Dynamic program registration
- Dynamic task code creation
- Dynamic alteration of memory (core zaps) in the CA IDMS address space

Control user access to online applications using CA IDMS internal security or an external security manager such as CA ACF2 for z/OS or CA Top Secret for z/OS.

Secure all online user application tasks. The only tasks that could run unsecured are the SIGNON task and the BYE task.

Although not an operating system integrity issue, you also want to prevent unauthorized disclosure of corporate information by taking the following actions:

- Carefully tailor all subschemas to permit access to only those data items to which the user is entitled.
Carefully control the use of both batch Printlog and Online Printlog (OLP) facilities. Any personnel with appropriate security clearance must obtain and review any necessary information before releasing it to the user or to software vendors.

CVKEY Parameter Specification

The SVC source created during configuration contains CVKEY=n. You can specify the CVKEY parameter in one of the following ways:

- As the value of the GJCVKEY variable within the IDMS_DB/CV variable group in CA CSM configuration.
- As the value of the GJCVKEY variable in VARBLIST during manual configuration.

Valid values for CVKEY are 1 through 15 and asterisk (*). Use of 8 or 9 is not recommended. A value of asterisk (*) permits the intentional creation of the unsecured version of the SVC.

Certain functions of the CA IDMS SVC must be invoked only from within a CA IDMS Central Version. Privileged instructions are used during the execution of these functions. If a numeric CVKEY value is specified and one of these functions is invoked, then the SVC verifies that the invoking routine job or address space has the primary protect key. If the routine does not have the primary protect key, the SVC does not allow the routine to use the SVC function. This prevents unsecured programs, such as batch application programs, from invalidly invoking these functions.

These checks help ensure that these functions are issued only by code running in the specified protect key. They also cause the z/OS ECSA used by CA IDMS to be both fetch- and store-protected from ordinary batch jobs. An abend with a system completion code of SE\text{xx} is issued when these functions are misused, where \text{xx} is the hexadecimal representation of the SVC number. This function includes all attempts to access the CA IDMS SVC from V=R jobs.

Programs that execute with a key of less than 8 are privileged in z/OS. CA IDMS does not require these privileges; a key in the range of 10 to 15 is recommended. However, the z/OS parameter AllowUserKeyCSA(NO) requires that the CA IDMS primary key be less than 8.

Note: For more information on key designation, see z/OS Considerations (https://docops.ca.com/pages/viewpage.action?pageId=328584243).

CA IDMS operates successfully in any key other than 9, which is due to a z/OS limitation in IOS. Specifying a system key (1 through 7) can be useful for preventing batch or V=R jobs from directly viewing or altering the ECSA storage used by CA IDMS.

Note: V=R jobs refer to the type of region that the job is running in. There are two types of user regions: Virtual (V=V) and Real (V=R). Programs that require a one-to-one mapping from virtual to central storage, such as channel programs, are candidates for real regions. A user can assign jobs to virtual or real regions by coding a value of VIRT or REAL on the ADDRSPC parameter on the job’s JOB or EXEC statement.
AUTHREQ Parameter Specification

The SVC source created during configuration contains AUTHREQ=YES/NO. You can specify the AUTHREQ parameter in one of the following ways:

- As the value of the AUTHREQ variable within the IDMS_DB/CV variable group in CA CSM Configuration.
- As the value of the AUTHREQ variable in VARBLIST during manual configuration.

If AUTHREQ=YES is specified, all Central Version Startup modules must reside in an authorized library and must be linked as authorized, that is, with SETCODE AC(1). This setting allows the startup module to set up PC routines to perform certain necessary system functions. After these PC routines are established, the startup module unauthorizes itself. As a result, application programs and nucleus modules, such as system exits, are prevented from using privileged operating system instructions. Specifying AUTHREQ=YES completely disables certain SVC functions. Setting AUTHREQ to YES requires no additional storage or CPU use.

Accidental Deletion of Previous Release

SMP/E deletes previously installed FMIDs and load modules if you install into an existing CSI using the same zones. If you want to use your previous release while installing a new release, install to a new CSI to avoid deleting the previous release.

PDSE Considerations

If you want to make your loadlib a PDSE, then you must have an SVC= parameter in the parameter list of the startup JCL.

Maintenance Considerations

Installing maintenance on a system created by CA CSM is different from installing maintenance on a system created manually. After installing the maintenance on the SMP/E libraries, you must redeploy and reconfigure. During reconfiguration, you are required to select a new prefix for each data set allocated during configuration, including the runtime and custom libraries. As a result, you must change any JCL containing the name of any of these loadlibs.

Develop a maintenance strategy for your site that handles changes at a high level. This helps you avoid changing user JCL and CV startup JCL whenever maintenance is installed.

Consider the following options to minimize disruption due to library name changes:

Note: For more information on region types, see the z/OS MVS Initialization and Tuning Guide on the IBM InfoCenter website.
Create aliases in the operating system catalog for CA IDMS loadlibs and macro libraries.

Create JCL procedures (PROCs) for end-user JCL and CV startup JCL.

Modify user JCL to include a JCLLIB statement after the JOB card and an INCLUDE statement for the bulk of the JCL.

After you run configuration, make a copy of the runtime and custom libraries and point your JCL to these copies. These copies are now your runtime libraries. Each time you run configuration again to apply maintenance, copy those libraries again, replacing the original copies. This way, you keep your runtime library names the same and do not need to modify your JCL every time you apply maintenance.

Upgrading

Before you upgrade from an earlier release, review the Release Notes or Release Summary information for each of the releases between your current release and the release that you are installing. You can find release information for releases earlier than 19.0 on the Support Documentation site.

Note: Release Notes are not cumulative.

Installing Your Product Using CA CSM

As a system programmer, your responsibilities include acquiring, installing, maintaining, deploying, and configuring CA Technologies mainframe products on your system. CA CSM is an application that simplifies and unifies the management of your CA Technologies mainframe products on z/OS systems. As products adopt the CA CSM services, you can install your products in a common way according to industry best practices.

This scenario describes the following procedures for a system programmer to acquire, install, deploy, and configure products and maintenance. Not all tasks may apply to your organization. For example, you may decide not to deploy and configure products. In this case, do not perform the product deployment task and the product configuration task.

Before you use this scenario, you must have CA CSM installed at your site. If you do not have CA CSM installed, you can download it from the Download Center at CA Support. You access CA CSM from a web browser.

Note: This scenario applies to the latest version of CA CSM. If you are using an earlier version, see the appropriate bookshelf on the CA Chorus Software Manager product page.

This scenario is a high-level overview of steps that you perform using CA CSM. For more detailed information, use the online help that is included in CA CSM.
Perform the following tasks to install products and manage them on your system:

- Access CA CSM Using the Web-Based Interface (see page 25)
- Acquire a New Product (see page 25)
- Install a Product (see page 26)
- Maintain the Installed Products (see page 27)
- Deploy the Product to the Destination System (see page 28)
- Configure the Deployed Product (see page 29)

Access CA CSM Using the Web-Based Interface

You need the URL of CA CSM from the CA CSM administrator.

Follow these steps:

1. Start your web browser, and enter the access URL to access the login page.
   
   **Note:** If the Notice and Consent Banner appears, read and confirm the provided information.

2. Enter your z/OS login user name and password.
   The initial page appears. If you log in for the first time, you are prompted to define your account on the CA Support Online website.
   
   **Note:** For more information about the interface, click the online help link at the top right corner of the page.

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

4. 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.

5. 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.

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

Acquire a New Product

Acquisition allows you to download products and product maintenance from the CA Support Online website to a USS directory structure on your system. The products to which your site is entitled and the releases available are displayed in the Available Products section on the Products page.
You perform the following high-level tasks to acquire a product using CA CSM:

1. Set up a CA Support Online account.
   
   To use CA CSM to acquire or download a product, you must have a CA Support Online account.

2. Determine the CA CSM URL for your site.
   
   To access CA CSM (see page 25), you require its URL. You can get the URL from your site CA CSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA CSM account with your credentials that you use to access CA Support. This account enables you to download product packages.

3. Log in to CA CSM and go to the Products page to locate the product that you want to acquire.
   
   After you log in to CA CSM, you can see the products to which your organization is entitled on the Products tab.
   
   If you cannot find the product that you want to acquire, update the product list. CA CSM refreshes the product list through CA Support using the site IDs associated with your credentials.

4. Download the product installation packages.
   
   After you find your product in the product list, you can download the product installation packages. To do so, use the Update Product Release action.
   
   CA CSM downloads (acquires) the packages (including any maintenance packages) from the CA Support Online website.

   After the acquisition process completes, the product is ready for you to install or apply maintenance.

### Install a Product

CA CSM simplifies and manages SMP/E installation tasks. You can browse and install a product that you acquired and that is available in the product list on the Products page. You can also install the maintenance for the products that are currently installed in a managed SMP/E environment on the driving system.

Perform the following high-level tasks to install a product using CA CSM:

1. (Optional) On the Settings tab, click Software Installation under System Settings, and configure base installation settings.

2. (Optional) Click the SMP/E Environments tab, and configure a working set of SMP/E environments.

3. Click the Products tab and select a product that you want to install. Start the installation wizard and review product information.

4. Select an installation type.

5. Review installation prerequisites if any are presented.

6. Take one of the following steps to select an SMP/E environment:
- Create an SMP/E environment:
  a. Set up the global zone.
  b. Create a target zone.
  c. Create a distribution zone.

- Use an existing SMP/E environment from your working set:
  a. Update the global zone.
  b. Set up the target zone: Create a target zone or use an existing target zone.
  c. Set up the distribution zone: Create a distribution zone or use an existing distribution zone.

**Note:** If you install a product or its components into an existing target or distribution zone, older versions are deleted from the zone and associated data sets. We recommend that you use new target and distribution zones for this installation so that you can apply maintenance to your current version, if necessary.

**Note:** When defining the datasets for your SMP/E environment, there is the option DSN TYPE. The default option in CSM is LIBRARY. If LIBRARY is used, the SMP/E datasets will be created as type PDSE. There are special considerations when using PDSE datasets. See PDSE Support (https://docops.ca.com/display/IDMS19/PDSE+Support) for more information.

7. Review the installation summary and start the installation.

8. (Optional) Review pending tasks for the SMP/E environment where you are installing your product. If applicable, continue the installation.

CA CSM installs the product.

After the installation process completes, check for and install available product maintenance. The product is ready for you to deploy. Sometimes, there are other steps to perform manually outside of CA CSM before continuing.

## Maintain the Installed Products

You can migrate existing SMP/E environments into CA CSM to maintain all your installed products in a unified way from a single web-based interface.

You can use CA CSM to maintain a CA Technologies product.
You perform the following high-level tasks to maintain a product using CA CSM:

1. Verify that CA CSM recognizes the SMP/E environment where your product is installed. If not, migrate the SMP/E environment to CA CSM. During the migration, CA CSM stores information on the SMP/E environment in the database.

2. From the Product tab, download the latest maintenance for the installed product releases. If you cannot find the required release, perform the following steps to download the maintenance:
   
   a. Add the release to the catalog manually.

   b. Update the added release.

3. Apply the maintenance. CA CSM applies the maintenance to your product.

   After the maintenance process completes, the product is ready for you to deploy to systems that are defined in the system registry.

---

**Deploy the Product to the Destination System**

Deployment is a process of copying SMP/E target libraries to a destination system. The destination system could be the local z/OS system, a remote z/OS system, or a sysplex. You identify the destination system, deployed data set names, and the transport mechanism as part of the deployment process. Deploying a product makes it available for configuration.

**Important!** Before you deploy a product, set up the destination systems and remote credentials in the system registry.

You perform the following high-level tasks to deploy your products using CA CSM:

1. On the Deployments tab, set up methodologies.

   **Note:** You can also set up methodologies when creating a deployment, or use existing methodologies, if you have set up any previously. If you do so, you can skip this step.
2. Start the New Deployment wizard to create a deployment. Complete each of the steps in the wizard. The wizard guides you through choosing deployment settings for your site. At any point, you can save your work and come back to it later.

3. Deploy:
   
   a. Take a snapshot of the deployment.
   
   b. Transmit the deployment to a destination system.
   
   c. Deploy (unpack) to the mainframe environment.

   CA CSM deploys the product to the destination system.

   After the deployment process completes, the product is ready for you to configure.

**Configure the Deployed Product**

Configuration is a process of copying the deployed libraries to run-time libraries and customizes the product for your site to bring it to an executable state. You can configure CA Technologies products that you have already acquired, installed, and deployed using CA CSM. You cannot use CA CSM to configure a product unless you have already used CA CSM to deploy the product.

You perform the following high-level tasks to configure your products using CA CSM:

1. Select a configurable deployment on the Deployments tab to view details and products for that deployment.

2. Select a product in the deployment and start the Configuration wizard to create a configuration. Complete each of the steps in the wizard. The wizard has multiple levels of detailed instructions and guides you through choosing configuration settings for your site. At any point, you can save your work and come back to it later. Configurations where you have partially completed the steps in the wizard are listed on the Configurations tab. The steps in the wizard include the following:

   a. Define a configuration name and select a system for the configuration.

   b. Select configuration functions and options.

   c. Define system preferences.

   d. Create target settings.

   e. Select and edit resources.

3. Build the configuration. The last step of the Configuration wizard lets you build the configuration. If needed, you can edit the configuration and can build the configuration again. Building the configuration closes the wizard and creates a configuration with all your settings.
4. (Optional) Validate the configuration. Validation verifies access to resources that are going to be used when you implement the configuration.

5. Implement the configuration. You implement a configuration to make your deployed software fully functional. Implementation executes on the destination system, applying the variables, resources, and operations that are defined in the configuration. CA CSM configures the product.

After the configuration process completes, the product is ready for you to use.

Installing Your Product from Pax-Enhanced ESD

- How to Install a Product Using Pax-enhanced ESD (see page 30)
- Allocate and Mount a File System (see page 33)
- Copy the Product Pax Files into Your USS Directory (see page 35)
- Create a Product Directory from the Pax File (see page 39)
- Copy Installation Files to z/OS Data Sets (see page 40)
- Install Products Using Native SMP/E JCL (see page 41)
- Clean Up the USS Directory (see page 44)
- Apply Preventive Maintenance (see page 45)

How to Install a Product Using Pax-enhanced ESD

This section describes the Pax-enhanced ESD process. We recommend that you read this overview and follow the entire procedure the first time you complete a Pax-enhanced ESD installation. For experienced UNIX users, the Pax-enhanced ESD Quick Reference section has sufficient information for subsequent installations.

- How the Pax-enhanced ESD Download Works (see page 31)
- USS Environment Setup (see page 32)

**Important!** Downloading pax files for the SMP/E installation as part of the Pax-enhanced ESD process requires write authority to the UNIX System Services (USS) directories that are used for the ESD process.

To perform Steps 1 through 4, CA IDMS installers should have the list of the unpacked MVS data sets to the product installer. USS is not required for the actual SMP/E RECEIVE of the product or for any of the remaining installation steps.

To install files using Pax-enhanced ESD, use the following process:
Allocate and mount the file system. This process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system that is dedicated to Pax-enhanced ESD and create the directory in this file system. Ensure that all users who are working with pax files have write authority to the directory.

Copy the product pax files into your USS directory. To download files, choose one of the following options:

- Download a zip file from CA Support Online to your PC, unzip the file, and then upload the product pax files to your USS file system.
- FTP the pax files from CA Support Online directly to your USS directory.

Note: Perform Steps 3 through 6 for each pax file that you upload to your USS directory.

Create a product directory from the pax file. Set the current working directory to the directory containing the pax file, and create a directory in your USS directory by entering the following command:

```
pax -rvf pax-filename
```

Use the SMP/E GIMUNZIP utility to create z/OS installation data sets. The file UNZIPJCL in the directory that the pax command that is created in Step 3 contains a sample JCL to GIMUNZIP the installation package. Edit and submit the UNZIPJCL JCL.

Receive the SMP/E package. Use the data sets that GIMUNZIP created in Step 4. Perform a standard SMP/E RECEIVE using the SMPPTFIN and SMPHOLD (if applicable) DASD data sets. Also, specify the high-level qualifier for the RELFILEs on the RFPREFIX parameter of the RECEIVE command.

Proceed with product installation. Consult product-specific documentation, including AREADME files and installation notes to complete the product installation.

(Optional) Clean up the USS directory. Delete the pax file, the directory that the pax command created, all the files in it, and the SMP/E RELFILEs, SMPMCS, and HOLDDATA data sets.

How the Pax-enhanced ESD Download Works

Important! To download pax files for the SMP/E installation as part of the Pax-enhanced ESD process, you must have write authority to the UNIX System Services (USS) directories that are used for the ESD process and available USS file space before you start the procedures in this guide.

Use the following process to download files using Pax-enhanced ESD:

1. Log in to CA Support Online (https://support.ca.com/us.html).
2. Select DOWNLOAD MANAGEMENT.
3. Locate your product in the download management tool. Your product entry opens at the Product Downloads tab.

4. Locate the appropriate software package.

   Tip: To change the release, select the package and use the release drop-down.

If applicable, agree to the end-user license agreement (EULA).

5. Select a download method:

   Tip: Review the CA Support Online download and FTP Help topics.

   - If you select Enhanced Download Manager, a dialog opens. Follow the prompts to download the installer. The installer then downloads your product files to the location on your PC, as specified in the installer. Go to Step 10.

   - If you select FTP, you are redirected to Cart History. You receive an email notification when your files are ready. The email includes a link to your Cart History. Go to Step 7.

   - If you have previously set your download preference, the installer begins the download process. Go to Step 7 or 10 based on your download setting.


USS Environment Setup

You need a UNIX System Services (USS) directory and a file system with adequate space to perform the following tasks:

- Receive product pax files from CA Support Online.

- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

We recommend that you allocate and mount a file system that is dedicated to Pax-enhanced ESD. The amount of space that you need for the file system depends on the following variables:

- The size of the pax files that you intend to download.
Whether you plan to keep the pax files after unpacking them. We do not recommend this practice.

We recommend that you use one directory for downloading and unpacking pax files. Reusing the same directory minimizes USS setup. The USS setup is done only once. You reuse the same directory for subsequent downloads. Alternatively, you can create a directory for each pax download.

**Important!** Downloading pax files for the SMP/E installation as part of the Pax-enhanced ESD process requires write authority to the UNIX System Services (USS) directories that are used for the ESD process.

**Important!** The USS file system that is used for Pax-enhanced ESD must have sufficient free space to hold the directory, which the pax command created, and its contents. You need approximately 3.5 times the pax file size in free space to download the pax file and unpack its contents. For example, to download and unpack a 14-MB pax file, you need approximately 49 MB of free space in the file system hosting your ESD directory.

### Allocate and Mount a File System

You can use the zSeries File System (zFS) or hierarchical file system (HFS) for ESD downloads.

This procedure describes how to perform the following tasks:

- Allocate a zFS or an HFS.
- Create a mount point in an existing maintenance USS directory of your choice.
- Mount the file system on the newly created mount point.

**Note:** You must have either SUPERUSER authority, or the required SAF profile setting to allow you to issue the USS mount command for the file system.

- Optionally, permit write access to anyone in the same group as the person who created the directory.

**Important!** USS commands are case-sensitive.

**Follow these steps:**

1. Allocate the file system by customizing one of the following samples to your site requirements:

   - On a zFS, use the following sample:

     ```
     //DEFINE EXEC PGM=IDCAMS
     //SYSPRINT DD SYSOUT=* 
     //SYSUDUMP DD SYSOUT=* 
     ```
On an HFS, use the following sample:

```
//ALCHFS EXEC PGM=IEFBR14
//CAESD DD DSN=yourHFS_data_set_name,
// DISP=(NEW,CATLG,DELETE),UNIT=3390,
// DSNTYPE=HFS,SPACE=(CYL,(primary,secondary,1))
```

The file system is allocated.

⚠️ **Note:** Ensure that the zFS or HFS data set name that you use conforms to your data set naming conventions for USS file systems. If the allocation of the file system data set fails, it is because of environmental settings not allowing for the allocation. On an HFS, try using the ISPF 3.2 Data Set Utility to allocate your HFS data set.

2. Create a mount point for the file system. This example shows how to create a /CA/CAESD directory in an existing directory, /u/maint. From the TSO OMVS shell, enter the following commands:

```
cd /u/maint/
mkdir CA
```
```
cd CA
```
```
mkdir CAESD
```

⚠️ **Note:** This document refers to this structure as yourUSSESDDirectory.

The mount point is created.

3. Mount the file system by customizing one of the following samples to your site requirements:

- On a zFS, use the following sample:

```
MOUNT FILESYSTEM('your_zFS_data_set_name')
MOUNTPOINT('yourUSSESDDirectory')
TYPE(ZFS) MODE(RDWR)
PARM(AGGRGROW)
```
On an HFS, use the following sample:

```
MOUNT FILESIPstem('your HFS data set name')
MOUNTPOINT('yourUSSESDdirectory')
TYPE(HFS)   MODE(RDWR)
```

The file system is mounted.

4. (Optional) Set security permissions for the directory. You can use the chmod command to let other users access the ESD directory and its files. For example, to allow write access to the ESD directory for other users in your USS group, from the TSO OMVS shell, enter the following command:

```
chmod -R 775 /yourUSSESDdirectory/
```

Write access is granted.

**Note:** For more information on the chmod command, see the IBM z/OS UNIX System Services Using section (SA22-7802).

---

**Copy the Product Pax Files into Your USS Directory**

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up. Use one of the following methods:

- Download the product pax files directly from the CA Support Online FTP server to your z/OS system.
- Download the product pax file from the CA Support Online FTP server to your computer, and upload it to your z/OS system.
- Download the product file from CA Support Online to your computer. If your download included a zip file, unzip the file, and upload the unzipped pax files to your z/OS system.

This section includes a sample batch job to download a product pax file from the CA Support Online FTP server directly to a USS directory on your z/OS system and sample commands to upload a pax file from your computer to a USS directory on your z/OS system.

**Important!** The FTP procedures vary due to local firewall and other security settings. Consult your local network administrators to determine the appropriate FTP procedure to use at your site.

Ensure that sufficient free space is available in the USS file system that you are using for Pax-Enhanced ESD to hold the product pax file. If you do not have sufficient free space, error messages similar to the following appear:
When the download finishes, the pax file size in your USS directory matches the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

**Download Using Batch JCL**

Use this process to download a pax file from the CA Support Product Downloads window by running batch JCL on the mainframe. Use the sample JCL attached to the PDF file as CAtoMainframe.txt to perform the download.

**Important!** To simplify the Pax-Enhanced ESD process, the PDF version of this section includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the file to view the sample JCL.

**Note:** We recommend that you follow the preferred method as described on CA Support Online. This procedure is our preferred download method; however, we do include the procedure to download to the mainframe through a PC in the next section.

**Follow these steps:**

1. Supply a valid JOB statement.

2. Replace `yourTCP/IP.PROFILE.dataset` with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.
   The job points to your profile.

3. Replace `YourEmailAddress` with your email address.
   The job points to your email address.

4. Replace `yourUSSESDdirectory` with the name of the USS directory that you use for ESD downloads.
   The job points to your USS directory.

5. Locate the product component to download on the CA Support Product Download window.
   You have identified the product component to download.

6. Click Download for the applicable file.

**Note:** For multiple downloads, add files to a cart.
The Download Method window opens.

7. Click FTP Request.

The Review Download Requests window displays any files that you have requested to download. **Note:** We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

   - **Preferred FTP**
     
     Uses CA Technologies worldwide content delivery network (CDN). If you cannot download using this method, review the security restrictions for servers that company employees can download from that are outside your corporate network.
     
     **Host Name:** ftp://ftpdownloads.ca.com

   - **Alternate FTP**

     Uses the original download servers that are based on Long Island, New York.
     
     **Host Name:** ftp://scftpd.ca.com for product files and download cart files and ftp://ftp.ca.com for individual solution files.

Both methods display the host, user name, password, and FTP location, which you then can copy into the sample JCL.

**Note:** The following links provide details regarding FTP: the FTP Help document link in the Review Download Requests window and the Learn More link available in the Download Methods window.

9. Submit the job.

   **Important!** If your FTP commands are incorrect, it is possible for this job to fail and still return a zero condition code. Read the messages in the job DDNAME SYSPRINT to verify the FTP succeeded.

After you run the JCL job, the pax file resides in the mainframe USS directory that you supplied.

**Example CAtoMainframe.txt, JCL**

The following text appears in the attached CAtoMainframe.txt JCL file:
Download Files to Mainframe through a PC

If you download pax or zip files from CA Support Online to your PC, use this procedure to upload the pax file from your PC to your z/OS USS directory.

Follow these steps:

1. Follow the procedures in How the Pax-Enhanced ESD Download Works to download the product pax or zip file to your PC. If you download a zip file, first unzip the file to use the product pax files.

   The pax or zip file resides on your PC.

2. Open a Windows command prompt.

   The command prompt appears.

3. Customize and enter the following FTP commands:

   ```
   ftp mainframeuseridpassword
   lcd C:\PC\folderfor\thePAXfile
   put paxfile.pax.Z
   exit
   ```

   - **mainframe**
     
     Specifies the z/OS system IP address or DNS name.
userid
Specifies your z/OS user ID.

password
Specifies your z/OS password.

C:\\PC\\folder\\for\\thePAXfile
Specifies the location of the pax file on your PC.

Note: If you specify a location that has blanks or special characters in the path name, enclose that value in double quotation marks.

yourUSSpaxdirectory
Specifies the name of the USS directory that you use for pax downloads.

paxfile.pax.Z
Specifies the name of the pax file to upload.


Create a Product Directory from the Pax File

Contents
- Sample Job to Execute the Pax Command (Unpackage.txt) (see page 40)

Use the sample job attached to the PDF file as Unpackage.txt to extract the product pax file into a product installation directory.

Important! To simplify the Pax-Enhanced ESD process, the PDF version of this section includes a sample JCL job that you can copy directly to the mainframe. To access this job, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click the file to view the sample JCL.

Follow these steps:
1. Supply a valid JOB statement.
2. Replace yourUSSESDdirectory with the name of the USS directory that you use for ESD downloads.
   The job points to your specific directory.
3. Replace `paxfile.pax.Z` with the name of the pax file. The job points to your specific pax file.

4. Submit the job. The job runs and creates the product directory.

**Note:** If the PARM= statement exceeds 71 characters, uncomment and use the second form of UNPAXDIR instead. This sample job uses an X in column 72 to continue the PARM= parameters to a second line.

---

**Sample Job to Execute the Pax Command (Unpackage.txt)**

The following text appears in the attached Unpackage.txt JCL file:

```plaintext
//ESDUNPAX JOB (ACCOUNTNO), 'UNPAX ESD PACKAGE ',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//===============================================================================
/* This sample job can be used to invoke the pax command to create */
/* the product-specific installation directory. */
/*
/* 1. Supply a valid JOB statement. */
/* 2. Replace "yourUSSESDirectory" with the name of the USS */
/* directory used on your system for ESD downloads. */
/* 3. Replace "paxfile.pax.Z" with the name of the pax file. */
/* NOTE: If you continue the PARM= statement on a second line, make */
/* sure the 'X' continuation character is in column 72. */
//===============================================================================
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSESDirectory/; pax -rvf paxfile.pax.Z'
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSESDirectory/; pax -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=* 
//STDERR DD SYSOUT=* 
```

---

**Copy Installation Files to z/OS Data Sets**

Use the SMP/E GIMUNZIP utility to create MVS data sets from the files in the product-specific directory.

1. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:

   - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file without quotes. The path name ends in Packaging/IDMS/R<release number>/GJJS0B/UNZIPJCL.

   - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.

   The job is edited.
2. Change the SMPDIR DD PATH to the product-specific directory created by the pax command. Your view is of the product-specific directory.

3. If ICSF is not active, perform the following steps:
   a. Change the SMPJHOME DD PATH to your Java runtime directory. This directory varies from system to system.
   b. Perform one of the following steps:
      - Change the SMPCPATH DD PATH to your SMP/E Java application classes directory, usually /usr/lpp/smp/classes/.
      - Change HASH=YES to HASH=NO on the GIMUNZIP parameter.

One of the following occurs: ICSF is active or you are using Java.

4. Change all occurrences of YourHLQ to the high-level qualifier for z/OS data sets used by the installation process. We suggest that you use a unique HLQ for each expanded pax file to uniquely identify the package. Do not use the same value for yourHLQ as you will use for the SMP/E RELFILEs.
   All occurrences of YourHLQ are set to your high-level qualifier for z/OS data sets.

5. Submit the UNZIPJCL job.
   The UNZIPJCL job should complete with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.
   GIMUNZIP creates z/OS data sets with the high-level qualifier you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed at this point.

⚠️ **Note:** For more information, see the IBM Reference Manual, *SMP/E for z/OS Reference (SA22-7772).*

---

### Install Products Using Native SMP/E JCL

The following steps describe the process to install products using native SMP/E JCL:

1. Download external HOLDDATA.
2. Allocate product data sets and SMP/E data sets.
3. Create SMP/E CSI.
4. Receive base functions.
5. Apply base functions.
6. Accept base functions.
Prepare the SMP/E Environment for Pax Installation

The members in the SAMPJCL library prepare the data sets, initialize the zones, and create the DDDEFs for CA IDMS. External DDDEF data sets are required. The default is NULLFILE.

For information on the members, see the comments in the JCL.

Follow these steps:

1. Customize the edit macro AGJSEDIT, a member in SAMPJCL, with your site-specific information. Replace the rightmost parameters for each ISREDIT CHANGE command with values for your site. Copy the customized edit macro to a library in your SYSPROC concatenation. To list the libraries in your SYSPROC concatenation, enter the following command on any ISPF command line: TSO ISRDDN ONLY SYSPROC. The macro is now ready to customize your AGJ.SAMPJCL members. Each time you edit an installation member, type AGJSEDIT on the command line and press Enter to replace the defaults with your specifications.
   
   **Note**: Set the DASD HLQ to the same value specified for yourHLQ in the UNZIPJCL job which copied files to z/OS DASD.

2. Open the SAMPJCL member AGJ1HOLD in an edit session and execute the AGJSEDIT macro from the command line.
   AGJ1HOLD is customized.

3. Submit AGJ1HOLD.
   This job downloads the error and FIXCAT HOLDDATA from CA Support.

4. Open the SAMPJCL member AGJ2ALL in an edit session and execute the AGJSEDIT macro from the command line.
   AGJ2ALL is customized.

5. Submit AGJ2ALL.
   This job produces the following results:

   - The target and distribution data sets for CA IDMS are created.
Unique SMPLTS, SMPMTS, SMPSCDS, and SMPSTS data sets for this target zone are created.

6. Open the SAMPJCL member AGJ3CSI in an edit session and execute the AGJEDIT macro from the command line. AGJ3CSI is customized.

7. Submit AGJ3CSI.
This job produces the following results:

- The CSI data set is defined.
- The SMPPTS and SMPLOG data sets are allocated.
- The global, target, and distribution zones are initialized.
- The DDDEF entries for your product are created.
- The DDDEFs for the required SMP/E data sets are created.

Run the Installation Jobs for a Pax Installation

Submit and run these SAMPJCL members in sequence. Do not proceed with any job until the previous job has completed successfully.

Note: The following steps include instructions to execute the AGJEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the AGJAREAD member, and submit the AGJEDALL member.

Follow these steps:

1. Open the SAMPJCL member AGJ4RECD in an edit session and execute the AGJEDIT macro from the command line.
   AGJ4RECD now contains basic customization. In addition, comment out any unwanted FMIDs by adding a slash/asterisk combination in columns 2 and 3.

2. Submit the yourhlq.SAMPJCL member AGJ4RECD to receive SMP/E base functions.
   CA IDMS is received and now resides in the global zone.

3. Open the SAMPJCL member AGJ5APP in an edit session and execute the AGJEDIT macro from the command line.
   AGJ5APP now contains basic customization. In addition, comment out the same FMIDs as in the AGJ4RECD (Receive) job.

4. Submit the yourhlq.SAMPJCL member AGJ5APP to apply SMP/E base functions.
   CA IDMS is applied and now resides in the target libraries.
   The listing shows IDENTIFY statements and these statements contain unprintable characters. The IDENTIFY statements enable CA Support to quickly locate the source matching your load module. There is a separate line of IDENTIFY text for each object module. Unprintable characters in your SMP/E output are not a cause for concern.
5. Open the SAMPJCL member AGJ6ACC in an edit session and execute the AGJSEDIT macro from the command line.
   AGJ6ACC now contains basic customization. In addition, comment out the same FMIDs as in the AGJ4RECD (Receive) job.

6. Submit the `yourhlq.SAMPJCL` member AGJ6ACC to accept SMP/E base functions.
   Your product is accepted and now resides in the distribution libraries.

---

**Clean Up the USS Directory**

---

**Important!** This procedure is optional. Do not use this procedure until you complete the entire installation process.

To free file system disk space for subsequent downloads after downloading and processing the pax files for your CA Technologies product, we recommend removing the files from your USS directory and deleting unnecessary MVS data sets. You can delete the following items:

- Pax file
- Product-specific directory that the pax command created and all of the files in it
- SMP/E RELFILEs, SMPMCS, and HOLDDATA MVS data sets
  These data sets have the HLQ that you assigned in the UNZIPJCL job.

**Note:** Retain non-SMP/E installation data sets such as `yourHLQ.INSTALL.NOTES` for future reference.

**Follow these steps:**

1. Navigate to your Pax-Enhanced ESD USS directory.
   Your view is of the applicable USS directory.

2. Delete the pax file by entering the following command:
   ```
   rm paxfile
   ```
   *paxfile*
   Specifies the name of the CA Technologies pax file that you downloaded.
   
   The pax file is deleted.

3. Delete the product-specific directory by entering the following command:
   ```
   rm -r product-specific_directory
   ```
   *product-specific_directory*
   Specifies the product-specific directory that the pax command created.
   
   The product-specific directory is deleted.
Apply Preventive Maintenance

Important! We strongly recommend that you use CA CSM to maintain your CA Technologies z/OS-based products. The procedure that is discussed in this section is fully automated when you use CA CSM.

CA Support Online has maintenance and HOLDDATA published since the installation data was created. After the maintenance process completes, the product is ready to deploy.

Use this procedure during product installation and for ongoing preventive maintenance in non-installation use cases according to your maintenance strategy.

Note: To review the CA Technologies mainframe maintenance philosophy, see your Best Practices Guide or visit the CA Next-Generation Mainframe Management page (https://support.ca.com/phpdocs/0/8319/mainframe20_support.html).

This procedure directs you to use the CAUNZIP utility. The CAUNZIP utility processes ZIP packages directly on z/OS without the need for an intermediate platform, such as a Microsoft Windows workstation. If you are not familiar with this utility, see the CA Common Services for z/OS Administering section. This section includes an overview and sample batch jobs. To use this utility, you must be running CA Common Services for z/OS Version 14.0 with PTF RO54887 or CA Common Services for z/OS Release 14.1 with PTF RO54635.

Follow these steps:

1. Check the Download Center for PTFs that have been published since this release was created. If the base release was created recently, no PTFs will have been published yet. If PTFs exist, add published solutions for your product to your Download Cart, and click Checkout.

2. Specify that you want a complete package. When processing completes, a link appears on the Review Download Requests page. You also receive an email notification.

3. Click the Alternate FTP link for your order to obtain FTP login information and the ZIP file location. Download the ZIP file into a USS directory on your z/OS system.
4. Run the CAUNZIP utility.
CAUNZIP unzips the package of published solutions and creates a SMPNTS file structure that the SMP/E RECEIVE FROMNTS command can process. For sample JCL to run the utility that is located in `yourHLQ.CAW0JCL(CAUNZIP)`, see the CA Common Services for z/OS CAUNZIP Administering section. After execution completes, the ZIPRPT data set contains the summary report. The summary report does the following:

- Summarizes the content of the product order ZIP file.
- Details the content of each data set and the z/OS UNIX files produced.
- Provides a sample job to receive the PTFs in your order.

5. Review the sample job that is provided in the CAUNZIP output ZIPRPT file. Cut and paste the JCL into a data set, specify your SMP/E CSI on the SMPCSI DD statement and submit the job to receive the PTFs in your order.

6. Verify that you have the values from the base installation in the AGJSEDIT macro that was customized in the installation steps.

**Note:** Skip the two following steps if you have already received HOLDDATA according to steps 2 and 3 in the Prepare the SMP/E Environment for Pax Installation (see page ) section.

7. Open the SAMPJCL member AGJ1HOLD in an edit session and execute the AGJSEDIT macro from the command line.

**Note:** Update AGJ1HOLD SAMPJCL to download the HOLDDATA file.

AGJ1HOLD is customized.

8. Submit AGJ1HOLD.
The job downloads the external HOLDDATA file.

9. Open the SAMPJCL member AGJ7RECH in an edit session and execute the AGJSEDIT macro from the command line.
AGJ7RECH is customized.

10. Submit AGJ7RECH.
The job receives the external HOLDDATA file.

11. Open the SAMPJCL member AGJ8APYP in an edit session and execute the AGJSEDIT macro from the command line.
AGJ8APYP is customized.
CA IDMS - 19.0

12. Submit AGJ8APYP.
The PTFs are applied.

13. (Optional) Open the SAMPJCL member AGJ9ACCP in an edit session and execute the AGJSEDIT macro from the command line.
AGJ9ACCP is customized.

14. (Optional) Submit AGJ9ACCP.
The PTFs are accepted.

**Note:** You do not have to submit the job at this time. You can accept the PTFs according to your site policy.

**HOLDDATA**

When you apply maintenance, you typically encounter SMP/E HOLDDATA. We use HOLDDATA to notify your SMP/E system of SYSMODs that have errors or special conditions. We support system and external HOLDDATA. **Note:** When you have completed the procedures in this section, go to Starting Your Product. (see page 47)

**Starting Your Product**

This following topics describe what you need to know and the configuration tasks you need to complete before starting CA IDMS:
- Configuration Process Overview (see page 48)
- Unlicensed Products (see page 48)
- Installation Libraries (see page 48)
- Configuration Libraries (see page 49)
- Configuration Types (see page 50)
- Configuring Your Product Using CA CSM (see page 53)
- Configuring Your Product Without CA CSM (see page 53)
- Generated Configuration Tasks (see page 56)
- Post-Configuration Tasks (see page 67)

**Before You Begin**

Before you begin the configuration process, familiarize yourself with the following resources:
- The CA IDMS release announcement letter
- Any available PMLs
- The Release Notes
Preparing for Installation

- Security information in Creating a Secured CA IDMS System on z/OS

**Important!** The instructions in the announcement letter or PMLs supersede the instructions in this documentation.

## Configuration Process Overview

You can perform the configuration process using either CA CSM or CAISAG. The configuration process creates customized load modules in a non-SMP/E loadlib. The configuration process also creates or updates your database files, depending on whether you are doing a full base configuration, an add-on configuration, or an upgrade configuration.

Before you begin the configuration process, use one of the methods that are described in this section to perform the following steps:

1. Create the SMP/E environment containing the CA IDMS software.
2. Install all the available and recommended maintenance.
3. Complete deployment, which creates a copy of some or all of your SMP/E target libraries. For CA CSM, deployment is a prerequisite for configuration. For CAISAG, deployment is optional.

## Unlicensed Products

Modules belonging to products for which you are not licensed are in your loadlib. If you try to use these unlicensed products that require a LMP (license product management) key, messages and auditing problems occur.

You specify which products you intend to use during the configuration process, which creates a product intent module named RHDCPINT. For more information, see Product Intent Module [here](https://docops.ca.com/display/IDMS19/Product+Intent+Module).

## Installation Libraries

The low-level qualifiers of your deployed libraries are the same as the low-level qualifiers of your SME/E target libraries. Configuration uses your deployed libraries if you did deployment. It uses your target libraries if you configure your product manually and did not do deployment. The following list describes libraries identified by the low-level qualifiers:

- **CAGJSRC**
  Source library
- **CAGJMAC**
  Macro library

- **CAGJMSG**
  Messages for CA Endevor/DB

- **CAGJSAMP**
  Various sample members

- **CAGJLOAD**
  Load library that contains generic executable CA IDMS modules which may need to be updated by maintenance. This library should not contain any modules which are customized for your site.

- **CAGJMDU**
  Load library for special uppercase support. Most sites do not need uppercase modules. This library is for sites that have terminals that cannot display mixed-case characters and for sites that use double-byte character support (DBCS).

- **CAGJCICS**
  Library for CA IDMS/DC Sort use within CICS

- **CAGJSASO**
  SPG text for SASO

- **CAGJCULP**
  CA Culprit test file

- **CAGJSKEL**
  CAISAG skeleton

- **CAGJDATV**
  IDMSDIRL input data and VDBA code

- **CAGJXML**
  Deployment metadata

---

**Important!** Do not customize the modules in these libraries because they are replaced when you apply maintenance. Libraries that contain maintenance replace the existing deployed libraries.

---

**Configuration Libraries**

The configuration process creates the configuration libraries described in the following list. These libraries rarely require maintenance.

- **CUSTOM.SRCLIB**
  Customized source library
CUSTOM.LNKLIB
Customized link library

CUSTOM.LOADLIB
Customized load library

CUSTOM.JCLLIB
Customized JCL library

DBA.LOADLIB
DBA load library

APFLIB
Load library containing the SVC and related load modules.

ENFORCER.LOADLIB
Enforcer load library

INTBLOAD
Load library for the 10.2 batch interface

These libraries contain members that are customized for your site or some operational environment within your site. The custom libraries contain the customized source, binder input, and load modules for the option modules and interface routines that are specific to your environment. These libraries do not need to change, except in response to changing business requirements.

Configuration Types

Contents
- Complete Base Configuration (see page 51)
- Upgrade Configuration (see page 51)
- Add-On Configuration (see page 52)

There are three types of mutually exclusive configurations:

- **Complete base configuration (see page 51)** for sites installing CA IDMS for the first time.
- **Upgrade configuration (see page 51)** for sites upgrading a current installation.
- **Add-on configuration** for sites that want to configure additional CA IDMS products.

The following table provides more information on the three different configurations:

<table>
<thead>
<tr>
<th>Jobs</th>
<th>Complete Base Configuration</th>
<th>Upgrade Configuration</th>
<th>Add-on Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates or updates custom libraries</td>
<td>Creates</td>
<td>Creates</td>
<td>Updates</td>
</tr>
<tr>
<td>Allocates and formats database areas</td>
<td>Yes</td>
<td>No</td>
<td>Depends on product being installed</td>
</tr>
</tbody>
</table>
Complete Base Configuration

A complete base configuration performs the following functions:

- Creates a set of runtime libraries from the deployed libraries
- Creates a set of custom libraries
- Allocates, formats, and initializes new dictionaries
- Creates new DMCL and DB name table load modules
- Creates a new DC system

Upgrade Configuration

If you are already running an earlier release of CA IDMS, select an upgrade configuration. An upgrade configuration performs the following functions:

- Preserves and operates with your existing dictionaries and database files.
- Does not allocate, format, or initialize dictionaries or database files.
- Ignores allocation and page range parameters for database files.
- Allocates new runtime and custom libraries for CA IDMS.
- Populates runtime libraries by copying the deployed libraries.
- Populates custom libraries with customized members tailored to your operational environment.

You can envision an upgrade configuration as containing a software side and a database side. Everything on the database side is preserved, although some files can be updated. Everything on the software side is replaced. As part of the software side, the SVC load module and all of your CICS interface load modules must be created as part of the configuration process using the newly created libraries.

⚠️ Note: If modules from multiple releases are used at runtime, the results are unpredictable.
Although an upgrade configuration does not replace dictionaries, it does update dictionaries with entities that have changed since an earlier release, such as:

- Messages and codes
- Systems records
- CA IDMS protocols
- System classes and attributes
- Built-in functions
- CA IDMS reports
- CA IDMS load modules

⚠️ **Note:** Load modules created by punching and linking source from dictionaries need not be recreated. These load modules include the DMCL and the DB name table.

When upgrading your release, review the *Release Notes* and *Release Summary* guides to find all the new functionality introduced between the release from which you are upgrading and the current release.

### Add-On Configuration

An add-on configuration allows you to configure additional CA IDMS products.

Perform an add-on configuration if you have already completed a base or upgrade configuration and want to configure additional CA IDMS products, such as CA ADS, CA Culprit, or CA IDMS Enforcer. An add-on configuration allows you to purchase licenses for and configure additional CA IDMS products.

For manual configurations, the VARBLIST product settings for an add-on configuration are different from the settings for a base or upgrade configuration. Change the settings in the product section at the top of the VARBLIST member to YES for each product you have previously configured and the new products you are configuring. In the add-on section at the bottom of the VARBLIST, specify YES for each of the new products you are adding.

⚠️ **Note:** For more information on the modifying the VARBLIST member for add-on configurations, see *Add-On Variables* (see page 105).
Configuring Your Product Using CA CSM

You can use the SCS component of CA CSM to configure a CA Technologies product that you have already acquired, installed, and deployed.

**Note:** For more information on using SCS to configure CA IDMS, see How to Configure a Product.

Configuring Your Product Without CA CSM

The manual configuration process is based on the Specify and Generate (CAISAG) program. This program reads the specified configuration and a prototype JCL skeleton containing default values, and generates the customized configuration jobs.

The database administrator can perform the CA IDMS configuration that consists of the following steps:

1. **Create the CAISAG library** (see page 53).
2. **Customize the CAISAG library members** (see page 53).
3. **Execute the CAISAG program** (see page 55).
4. Review the configuration jobs generated by CAISAG. Repeat steps two to four until the configuration jobs are generated correctly for your site.
5. **Submit the generated configuration jobs.**

Create the CAISAG Library

To allocate and populate a CAISAG library, customize and submit the CFIG#JCL member in your CAGJSRC library, which contains an IEBCOPY job. To customize this job, use the AGJSEDIT macro that you use to customize the SMP/E jobs. If you performed the SMP/E installation using CSM, the AGJSEDIT edit macro does not exist. You need to customize the job manually, and supply a prefix for the configuration data sets to be allocated on the SET statement. This job allocates a PDS with the low-level qualifiers CAISAG.CONFIG and populates it by copying four members from CAGJSRC.

Customizing the CAISAG Library Members

The CAISAG library contains the following members, which you must customize for your site:
Customizing the JOBCARD Member

Customize the JOBCARD member for your site for long-running jobs without tape mounts. This member is copied into the top of each generated job.

You can customize this member by executing the AGJSEDIT edit macro and then deleting the two comment lines.

Customizing the SETUP Member

The SETUP member is copied into the beginning of each job requiring a tape mount. If your site uses /*SETUP cards, customize the SETUP member with /*SETUP cards appropriate for tape use.

The following example shows the default SETUP member:

```
//
```

**Important!** Do not delete the SETUP member.

Customizing the VARBLIST Member

The VARBLIST contains a list of variables that are used by the Specify and Generate program (CAISAG) to generate customized JCL. For each variable, supply the appropriate value for your site.

The following syntax is used for each variable:

```
variable-name = value <optional comment>
```

The following rules apply when coding the VARBLIST member:

- An asterisk in column 1 denotes a comment.
- Blank lines can be used for readability.
- Values containing blanks must be enclosed in single quotes.
- Two single quotes indicate a null value.
All values are translated to uppercase unless they are enclosed in single quotes.

Many values in VARBLIST begin and end with an at "@" symbol. If the values inside the symbol are previously defined, CAISAG replaces the "@" string with the previously defined values. In the following example, the second LOADLIB statement shows the replacement of the LOADLIB "@" string:

```plaintext
PREFIX = IDMS.V<release number>
LOADLIB = @PREFIX@.LOADLIB
PREFIX = IDMS.V<release number>
LOADLIB = IDMS.V<release number>.LOADLIB
```

If a variable is specified more than once, CAISAG uses the last value.

**Execute CAISAG**

The CAISAG job generates customized configuration jobs as new members in the CAISAG library, see Generated Configuration Tasks. (see page 56)

To execute the CAISAG program to generate the installation jobs, follow these steps:

1. Customize the variables PREFIX, CONFIG, WORK, and SYSOUT in the CAISAG member as shown next.
   ```plaintext
   //* SET PREFIX='CAI.IDMSV<release number>'
   */
   //* PREFIX USED IN SMP/E JOB
   //* SET CONFIG='CAI.IDMSV<release number>.CAISAG.CONFIG'
   //* NAME OF THIS LIBRARY
   //* SET WORK=SYSDA
   //* DISK UNIT FOR TEMPORARY DATASETS
   //* SET SYSOUT='**'
   //* SYSOUT CLASS
   ```

2. Run CAISAG. New members in the configuration library are created.

3. Browse the generated jobs. If they are not correct, correct the variables in VARBLIST and regenerate the JCL.
   New members in the configuration library are created.

![Note: VARBLISTs from previous installations are an invaluable tool for documenting your system.](image)

**Important!** Do not submit any of the generated configuration jobs until you have verified the JCL in all the configuration jobs.

The following JCL shows a sample CAISAG member:

```plaintext
//CAISAG EXEC PGM=CAISAG
//* EXPECTED RETURN CODE: 00
//STEPLIB DD DISP=SHR,DSN=&PREFIX..CAGJLOAD
//GENJCL DD DISP=NEW,PASS,DSN=&GENJCL..UNIT=&WORK,
```
Generated Configuration Tasks

Generated Configuration Jobs

The following sections describe the configuration jobs that are generated by CAISAG (the Specify and Generate program), if you configure your product without CA CSM:

**Job 1:** Configuration Files Allocation (see page 57)

**Job 2:** Source and Link Members Customization (see page 57)

**Job 3:** Customized Load Modules (see page 60)

**Job 4:** Load SVC Using CAIRIM (see page 60)

**Job 5:** Database Files Allocation (see page 62)

**Job 6:** DD Statement Members (see page 62)

**Job 7:** DMCL and DB Table in Bootstrap Catalog (see page 62)

**Job 8:** Selected Product Updates (see page 63)

**Job 9:** SYSTEM and SYSDIRL Dictionaries (see page 63)

**Job 10:** APPLDICT Dictionary (see page 64)

**Job 11:** ASFDICT Dictionary (see page 64)

**Job 12:** Formats Tools Files (see page 65)

**Job 13:** Tools Dictionaries and Database Files (see page 65)
Configuration Files Allocation

Job 1 allocates the configuration files.

Restart Information: This job can be rerun if it abends.

Customized Source

Job 2 creates customized source and link members that are then assembled into load modules in Job 3. The source members document your configuration choices. If your configuration requirements change, you can modify and use these members at any time.

Restart Information: This job can be rerun.

The following table describes the modules that are created and customized in Jobs 2 and 3. Some modules are created only if certain products or features are being installed.

<table>
<thead>
<tr>
<th>Modules</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source: #PMOPT, Link: #PMOPT, Load: #PMOPT</td>
<td>CA IDMS Performance Monitor option module (<a href="https://docops.ca.com/display/IDMS19/Modifying+%23PMOPT+Parameters">https://docops.ca.com/display/IDMS19/Modifying+%23PMOPT+Parameters</a>)</td>
</tr>
<tr>
<td>Source: #SVOPT, Link: IGCnnn, Load: IGCnnn</td>
<td>SVC option module (<a href="https://docops.ca.com/display/IDMS19/Generating+the+SVC">https://docops.ca.com/display/IDMS19/Generating+the+SVC</a>)</td>
</tr>
<tr>
<td>Source: ADSOVCON, Link: ADSOVCON</td>
<td>CA ADS user-defined BIF module skeleton (<a href="https://docops.ca.com/display/IDMSCU19/Linking+Built-In+Functions+With+The+Runtime+System">https://docops.ca.com/display/IDMSCU19/Linking+Built-In+Functions+With+The+Runtime+System</a>)</td>
</tr>
<tr>
<td>Source: CICSOPTS, Link: IDMSINTC, Load: IDMSINTC</td>
<td>CA IDMS CICS interface option module (<a href="https://docops.ca.com/display/IDMS19/Standard+CICS+Interface">https://docops.ca.com/display/IDMS19/Standard+CICS+Interface</a>)</td>
</tr>
<tr>
<td>Source: CULPPROF, Link: CULPPROF, Load: CULPPROF</td>
<td>CA Culprit option module (<a href="https://docops.ca.com/display/IDMSCU/Profile+Options+v19_Next">https://docops.ca.com/display/IDMSCU/Profile+Options+v19_Next</a>)</td>
</tr>
<tr>
<td>Source:</td>
<td>CA IDMS DQF option module (<a href="https://docops.ca.com/display/IDMS19/Site+Specific+Assemblies">https://docops.ca.com/display/IDMS19/Site+Specific+Assemblies</a>)</td>
</tr>
<tr>
<td>Modules</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source: DADTPARM</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: DADTPARM</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: DADTPARM</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: ESSTPARM</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: ESSTPARM</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: ESSTPARM</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: ESXTPARM</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: ESXTPARM</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: ESXTPARM</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Source: GSISVCX</td>
<td>CA IDMS SASO option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Site+Specific+Assemblies))</td>
</tr>
<tr>
<td>Link: GSISVCX</td>
<td>CA IDMS Enforcer option module ([<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters](<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a> /Modify+CA+IDMS+Enforcer+Tuning+Parameters))</td>
</tr>
<tr>
<td>Load: GSISVCX</td>
<td>CA IDMS Log Analyzer and CA IDMS Task Analyzer SVC exit module (<a href="https://docops.ca.com/display/IDMS19/What+GSISVCX+Does">https://docops.ca.com/display/IDMS19/What+GSISVCX+Does</a>)</td>
</tr>
<tr>
<td>Modules</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Source: SSKTPARM</td>
<td>Link: SSKTPARM Load: SSKTPARM</td>
</tr>
<tr>
<td>Source: TPSPARM</td>
<td>CA IDMS/DC Sort option module (<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a>/Site+Specific+Assemblies)</td>
</tr>
<tr>
<td>Link: TPSPARM Load: TPSPARM</td>
<td>CA IDMS UCF CICS interface option module (<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a>/UCF+Front-End)</td>
</tr>
<tr>
<td>Source: UCFCICS</td>
<td>CA IDMS UCF CICS interface option module (<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a>/UCF+Front-End)</td>
</tr>
<tr>
<td>Link: UCFCICS Load: UCFCICS</td>
<td>TSO CLIST to invoke CA IDMS from TSO through UCF (see page 67)</td>
</tr>
<tr>
<td>Source: UCFTSO</td>
<td>CA IDMS Online option module (<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a>/CA+IDMS+DMLO+Features)</td>
</tr>
<tr>
<td>Link: USDTTPARM Load: USDTTPARM</td>
<td>CA IDMS Online Log Display option module (<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a>/Set+Product+Runtime+Parameters)</td>
</tr>
<tr>
<td>Source: USDTTPARM</td>
<td>CA IDMS Dictionary Migrator option module (<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a>/CA+IDMS+Dictionary+Migrator+Runtime+Parameters)</td>
</tr>
<tr>
<td>Link: USKTPARM Load: USKTPARM</td>
<td>CA IDMS Extractor option module (<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a>/Customizing+the+CA+IDMS+Extractor+Environment--USVTPARM)</td>
</tr>
<tr>
<td>Source: USKTPARM</td>
<td>CA IDMS Extractor option module (<a href="https://docops.ca.com/display/IDMS19">https://docops.ca.com/display/IDMS19</a>/Customizing+the+CA+IDMS+Extractor+Environment--USVTPARM)</td>
</tr>
<tr>
<td>Source: WTOEXIT</td>
<td>Link: WTOEXIT Load: WTOEXIT</td>
</tr>
</tbody>
</table>
Customized Load Modules

Job 3 performs assemblies and links, populating the CUSTOM loadlib.

Job 3 creates an SVC load module—IGCxxx (where xxx is your SVC number) in the APFLIB loadlib. An SVC is a Supervisor Call load module that must be loaded into the operating system before it is executable.

Restart Information: This job can be rerun.

Load SVC Using CAIRIM

Job 4 uses CAIRIM to load the SVC. Failure to use CAIRIM causes an error when CA IDMS is started.

Note: At your site, the use of CAIRIM might be restricted to the systems group. If so, they must execute Job 4.

More information:

- See the SVC (see page 80) section for information about how to share the SVC across releases of CA IDMS.
- See the Refreshing Required Modules (see page 81) topic for more modules that must be loaded using CAIRIM.

CAIRIM Execution

The CAIRIM program reads its input parameters from the sequential file that is pointed to by a PARMLIB DD statement. The installation generates the following CAIRIM product parameter line:

```
PRODUCT(CA IDMS) VERSION(GJJ0) INIT(GJJ0INIT) PARM(SVC=your-SVC-number)
```

Required Modules

The nine modules that are shown in the following table must be available when CAIRIM is run. The CA Common Services for z/OS installation creates the CAW0LOAD and CAW0LINK load libraries, and APFLIB is a load library created during configuration of CA IDMS.
To achieve required authorization, the APFLIB modules must be copied to an authorized load library, or the APFLIB loadlib must be authorized before running Job 4.

The following modules must be available when CAIRIM is run:

<table>
<thead>
<tr>
<th>Module Name</th>
<th>Module Type</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAIRIM</td>
<td>CA Common Services for z/OS modules</td>
<td>CA Common Services for z/OS Loadlib (CAW0LOAD)*</td>
</tr>
<tr>
<td>CAS9SEC</td>
<td>CA Common Services for z/OS modules</td>
<td>(already loaded from CAILIB; see QI75813)</td>
</tr>
<tr>
<td>CAILPAM</td>
<td>CA Common Services for z/OS modules</td>
<td>CA Common Services for z/OS Loadlib (CAW0LINK)</td>
</tr>
<tr>
<td>GJJJOIN1</td>
<td>CA IDMS</td>
<td>CA IDMS Loadlib (APFLIB)</td>
</tr>
<tr>
<td>IGGxxx</td>
<td>CA IDMS</td>
<td>CA IDMS Loadlib (APFLIB)</td>
</tr>
<tr>
<td>RHDCSSFM</td>
<td>CA IDMS</td>
<td>CA IDMS Loadlib (APFLIB)</td>
</tr>
<tr>
<td>CAIXDOA$</td>
<td>CA IDMS</td>
<td>CA IDMS Loadlib (APFLIB)</td>
</tr>
<tr>
<td>IDMSMSVA</td>
<td>CA IDMS</td>
<td>CA IDMS Loadlib (APFLIB)</td>
</tr>
<tr>
<td>PMRTDATA</td>
<td>CA IDMS</td>
<td>CA IDMS Loadlib (APFLIB)*</td>
</tr>
</tbody>
</table>

* Note: Library must be APF authorized.

CAIRIM Authorization

The CAIRIM module must run authorized. The CAW0LOAD loadlib or the loadlib that contains CAIRIM must be APF authorized.

If CAW0LOAD and CAW0LINK are in the operating system LNKLSTxx concatenation, you can use APFLIB as the sole STEPLIB library in Job 4. If APFLIB is the only library that STEPLIB points to, it does not have to be authorized.

If CAW0LOAD and CAW0LINK are not in the operating system LNKLST concatenation, the STEPLIB DD statement in Job 4 must point to them to make CAIRIM available. If CAILIB is in the STEPLIB concatenation of Job 4, the six CA IDMS modules must come from an authorized library. Select one of the following options for the APFLIB modules:

- If your site established an authorized library for holding SVC and INIT modules, copy the six APFLIB modules there. If that library is not in the operating system LNKLST concatenation, concatenate it to the STEPLIB DD statement in Job 4.

- APF authorizes the APFLIB loadlib (or a copy) and concatenates that library to the STEPLIB DD statement in Job 4.
Important! If unauthorized libraries are included in a STEPLIB concatenation with authorized libraries, all modules from STEPLIB are treated as unauthorized.

The CAS9SEC module must be loaded at IPL time or by running a CAIRIM job using the appropriate parameter input. The following example shows the parameter input:

`PRODUCT( CA SECURITY/INIT ) VERSION(S910) INIT(S910INIT)`

Return Codes

The possible return codes are as follows:

- **0** -- Specifies processing was successful.
- **S806** -- Indicates that the LOADLIB parameter is specified on the CAIRIM input line and a STEPLIB is specified.

Restart Information: This job can be rerun but requires modification before it is rerun. If the installed SVC must be replaced, change the PARM value as follows. The following example shows the change of the PARM value:

`PARM(SVC=xxx)`
`PARM(REFRESH(SVC=xxx))`

Important! All CA IDMS central versions using the SVC must go through a normal shutdown, before replacing the SVC.

Database Files Allocation

Depending on the type of configuration, Job 5 does the following:

- **Complete base installation** -- Allocates database files.
- **Upgrade installation** -- Copies the old DMCL and database name table load modules to the new DBA loadlib.

Restart Information: This job cannot be rerun. Restart the Job at the failing step.

DD Statement Members

Job 6 creates groups of DD statements in members in the CAISAG library. Subsequent jobs require these members.

Restart Information: This job can be rerun.

DMCL and DB Table in Bootstrap Catalog

The SVC must successfully load using CAIRIM, before submitting Job 7. This job executes CA IDMS SVC and abends SFnn unless it is loaded into the z/OS CSA.
Depending on the type of configuration, Job 7 does the following:

- **Complete base configuration** -- Creates a global DMCL and a database name table using the bootstrap catalog, and punches and links them into the DBA loadlib. This configuration also formats the dictionary files and adds definitions, protocols, and messages to the dictionaries and catalogs.

- **Upgrade configuration** -- Definitions, protocols, and messages are loaded.

**Note:** When installing from 18.5 to a later release, CA IDMS loads only dictionary entities that are changed. The changed entities are in the CAGJSRC dataset, member IDDXISJ0. PTF R093158 is required for this function.

If Job 7 fails with an SFnn completion code, the system cannot find SVC ddd, where nn is a hexadecimal SVC number. Convert the number in SFnn to a three-digit decimal number, ddd. If it is the right number, verify the following:

- The CA IDMS APFLIB loadlib contains an IGCddd load module.
- The RHDCSRTT source in CUSTOM.SRCLIB is assembled with the right SVC=ddd parameter. The SVC number in RHDCSRTT must be valid even if external security is not being used.
- The IGCddd load module is loaded into the operating system since the last IPL.

**Example:** SVC Usage

A job abends with a SFAD, indicating the system is trying to use SVC 173 (173 = 10x16 + 13x1).

**Restart Information:** This job can be rerun.

**Selected Product Updates**

Depending on the type of configuration, Job 8 does the following:

- **Complete base configuration** -- Updates the global DMCL and DBTABLE with segments for selected products.

- **Upgrade configuration** -- No JCL is generated.

- **Add-on Configuration** – Updates the sysgen, DMCL, and DB name table with the added selected products.

**SYSTEM and SYSDIRL Dictionaries**

Depending on the type of configuration, Job 9 does the following:

- **Complete base configuration** -- Builds the CA IDMS dictionary, including the catalog component, and the SYSDIRL dictionary. This configuration also creates the global DMCL, the DB name table, and generates System 99, which is later used to generate System 90. The actual steps that are generated for this Job depend on the product mix selected for configuration.
- **Upgrade configuration** -- No dictionaries or catalogs are built. Existing dictionaries and catalogs are updated. Your existing global DMCL and DB name table are used.

  **Note:** When installing from 18.5 to a later release, CA IDMS loads only dictionary entities that are changed. The changed entities are in the CAGJSRC dataset, member IDDXI5J0. PTF R093158 is required for this function.

**Return Codes**

The possible return codes are as follows:

- **0** -- Specifies processing was successful for most steps.
- **4** -- Specifies processing was successful for DLODPROT and DIRLPROT steps in a complete base configuration. Specifies processing was successful for many steps in an upgrade configuration.

**Restart Information:** This job can be rerun.

**APPLDICT Dictionary**

Job 10 creates or updates the APPLDICT dictionary.

Depending on the type of configuration, Job 10 does the following:

- **Complete base configuration** -- Formats the APPLDICT dictionary and loads miscellaneous items like protocols, definitions, and ADS records.
- **Upgrade configuration** -- Updates the APPLDICT with protocols and definitions.

  **Note:** When installing from 18.5 to a later release, CA IDMS loads only dictionary entities that are changed. The changed entities are in the CAGJSRC dataset, member IDDXI5J0. PTF R093158 is required for this function.

**Restart Information:** This job cannot be rerun. Restart the job at the failing step, provided it does not require a temporary data set created earlier.

  **Note:** Run the steps that update the APPLDICT dictionary against every application dictionary in your environment.

**ASFDICT Dictionary**

Job 11 creates or updates the ASFDICT dictionary.

Depending on the type of configuration, Job 11 does the following:
**Format Tools Files**

Depending on the type of configuration, Job 12 does the following:

- **Complete base configuration** -- Formats the Tools files.
- **Upgrade configuration** -- No JCL is generated.

**Restart Information:** This job can be rerun.

**Tools Dictionaries and Database Files**

Job 13 creates or updates dictionaries and database files for Tools products.

Depending on the type of configuration, Job 13 does the following:

- **Complete base configuration** -- Creates the Tools dictionary and the database files for selected Tools products.
- **Upgrade and add-on configurations** -- Updates the SYSTEM and TOOLDICT dictionaries.

**Restart Information:** This job cannot be rerun. Use the `RESTART=` parameter on the `JOB` statement to restart the job at the failing step.

**Non-SQL Commonweather Database**

Job 14 builds the Commonweather demonstration database and is optional. Specify `EMPDEMO=YES` in your `VARBLIST` if you want to generate this Job. Specify `EMPDEMO=NO` if you do not want to generate this job.

Depending on the type of configuration, Job 14 does the following:

- **Complete base configuration** -- Creates a second DMCL (EMPDMCL) and builds the Commonweather demonstration database, a non-SQL version of the Employee Skills Demonstration database.
- **Upgrade and add-on configurations** -- Load items which have changed since your earlier base install.

**Restart Information:** This job cannot be rerun. Restart the job at the failing step provided it does not require a temporary data set created earlier.
SQL Demo Database and Web Services Consumer Demo

Job 15 builds the SQL demonstration database and provides the Web Services Consumer Demo. Specify SQLDEMO=YES in your VARBLIST if you want the SQL Demo Database to be provided. If you are installing Web Services, and ADS is installed, the Web Services Consumer Demo is provided. An IEFBR14 is generated if you are not installing CA IDMS SQL and CA IDMS Web Services.

Depending on the type of configuration, Job 15 does the following:

- **Complete base configuration** -- Builds the SQL demonstration database and the Web Services Consumer Demo.
- **Upgrade configuration** -- No JCL is generated.
- **Add-on configuration** -- A JCL is not generated unless you are installing CA IDMS SQL, or CA IDMS Web Services and ADS is installed.

**Restart Information:** This job can be restarted at any step that failed, provided it does not require a previously created, temporary data set.

Change Control Database

Job 16 performs database configuration tasks for CA Endevor/DB.

Modify and rerun to install a change control database, for each IDD you want to monitor.

**Important!** Backup your SYSTEM and SYSDIRL segments, before running this Job.

**Restart Information:**

To restart this job:

1. Restore the SYSTEM and SYSDIRL files from backup.
2. Rerun the job.

Generate SYSTEM 90

Job 17 builds the sample DC/UCF system, System 90. System 90 is intended as a test system only. You can bring up System 90 to verify the configuration. It will be modified by future CA IDMS changes.

Depending on the type of configuration, Job 17 does the following:

- **Complete base configuration** -- Formats the journal files in addition to building System 90.
- **Upgrade configuration** -- Copies all programs and tasks from System 99, adding entities that are new for this release and regenerates System 90 to include these updates.
Note: The release literal placed into records in the DDLDCLOG is changed to the current release number. If you do not want to mix the records from multiple releases in your log file, offload the log file using the ARCHIVE LOG utility. You then use the batch command facility, IDMSBCF, to FORMAT your DDLDCLOG area before starting your system for the first-time.

Restart Information: This job can be restarted at any step that failed, provided it does not require a temporary data set created earlier.

Database Files Backup

Job 18 performs a backup of all the installed database files depending on configuration options.

Restart Information: This job can be rerun.

Post-Configuration Tasks

Perform these tasks if you configure your system manually or using CA CSM.

- The Environment After Configuration is Complete (see page 68)
- z/OS Environment (see page 68)
- Preparing TP Access Environment (see page 68)
- CA IDMS Task Analyzer Storage Requirements (see page 70)
- CA IDMS Log Analyzer and CA IDMS Task Analyzer Statistics Gathering (see page 70)
- CA IDMS Performance Monitor (see page 71)
- CA IDMS Web Services (see page 71)
- Configuring Default JCL for CA IDMS Extractor and CA IDMS Dictionary Migrator Assistant (see page 72)
- CA ADS Trace Dictionary Updates (see page 73)
- CA IDMS/DC Sort Dictionary Updates (see page 73)
- CA IDMS DQF Dictionary Updates (see page 73)
- Linking a Dictionary to the CA Endevor/DB Change Monitor (see page 74)
- Creating an Executable System (see page 74)
- Modify the Startup JCL (see page 75)
- Verifying the System Configuration (see page 77)
- CAIRIM (see page 80)
- SVC (see page 80)
- Refreshing Required Modules (see page 81)
- Numbered Options (see page 81)
- Security (see page 82)
The Environment After Configuration is Complete

The entire installation process (SMP/E installation, deployment and configuration) creates various source and executable load libraries.

A complete base configuration process creates the following environment:

- **Dictionary environment** -- Configures a system and application dictionary environment.

- **DBA loadlib** -- Contains the following two customized load modules whose names were specified as configuration variables:
  - The DMCL load module -- A load module describing the configured runtime environment for the current release.
  - The database name table load module -- A load module defining the databases and data dictionaries accessible by the DMCL load module.

- **Configures the following systems**:
  - System 90 -- A sample of the current CA IDMS DC/UCF system that can be copied to your DC system number.
  - System 99 -- A non-executable system containing CA IDMS programs and tasks that can be copied to the new systems you define and generate.

**z/OS Environment**

Modules from prior releases of CA IDMS or CA Dispatch should not exist in the z/OS LPA. The SYS1.LPALIB should not contain modules beginning with ADS, IDMS, or RHDC.

1. If you specified the z/OS option "AllowUserKeyCSA(NO)", update the PPT to indicate the system key that RHDCOMVS (the startup module) should run in. You can specify any system key in the range of 1 to 7. If you specified the z/OS option "AllowUserKeyCSA(YES)", you can use any key in the range of 8 to 15.

**Preparing TP Access Environment**

This task involves preparing the TP access method for your CA IDMS system. The access methods covered are VTAM, TCP/IP, TSO, and CICS.

**VTAM Access**

To use VTAM to access CA IDMS/DC, the following two definitions must be in place:
A VTAM line (VTAMLIN) must be defined in the CA IDMS/DC system. The definition is already in place because the configuration process defined the VTAM line using the value of the CA CSM variable DcSystemVtamApplid or the CAISAG variable GJVTAMID. One VTAM line supports multiple concurrent users.

An application ID (APPLID) must be defined in VTAM to identify the CA IDMS/DC system.

**Note:** The APPLID defined to VTAM must match the APPLICATION ID parameter of the VTAMLIN statement specified during configuration.

**TCP/IP Access**

If you plan to use TCP/IP communication protocol for your DDS communications, or if you are configuring CA IDMS for use with CA Server, you must define a TCP/IP environment, socket line and listener PTERM to the CA IDMS system. For DNS functions to operate correctly, add a SYSTCPD DD statement to the startup JCL deck of your central version, pointing to the TCPIP.DATA file of your site.

**TSO Access**

The RHDCUCFT load module is in the CAGJLOAD library. RHDCUCFT is required to access DC/UCF through TSO.

To access a DC/UCF system from TSO, use the CLIST in CUSTOM.SRCLIB member UCFTSO to invoke RHDCUCFT. For reference purposes, the UCFTSO member follows. Modify it to reflect your data set naming conventions.

```
PROC 0
CONTROL NOMSG LIST
FREE F(SYSPRINT, SYSOUT, SYSOUD, SYSLST, SYSUDUMP, SYSCTL, DCMSG)
FREE F(SYSJRNAL, J1JRNAL, J2JRNAL, J3JRNAL, J4JRNAL, CDMSLIB)
CONTROL MSG
ALLOC F(SYSPRINT) DA(*)
ALLOC F(SYSOUT) DA(*)
ALLOC F(SYSOUD) DA(*)
ALLOC F(SYSUDUMP) DA(*)
ALLOC F(SYSCTL) DA('CAI.IDMSTEST.SYSCTL') SHR
ALLOC F(DCMSLIB) DA('CAI.IDMSTEST.SYSMSG.DDLCMSLIB') SHR
ALLOC F(SYSJRNAL) DUMMY
ALLOC F(J1JRNAL) DUMMY
ALLOC F(J2JRNAL) DUMMY
ALLOC F(J3JRNAL) DUMMY
ALLOC F(J4JRNAL) DUMMY
ALLOC F(CDMSLIB) DA('CAI.IDMSTEST.DBA.LOADLIB', - 'CAI.IDMSTEST.CUSTOM.LOADLIB', - 'idms.CAGJLOAD') SHR
CALL 'idms.CAGJLOAD(RHDCUCFT)'
```

You can access CA IDMS DML Online from TSO.

**Follow these steps:**

1. Create a CLIST to execute CA IDMS DML Online using the USDTSO member in the CAGJSAMP library as a sample.

2. Modify the CLIST for your site requirements.
3. Add the CA IDMS loadlibs to the TSO signon STEPLIB.

4. Execute the CLIST.

CICS Access

To access a DC/UCF system from CICS, CA IDMS CICS Support must be configured by selecting CA IDMS CICS Support during the CA CSM configuration or in the CAISAG VARBLIST.

Once the configuration steps execute successfully, add the CA IDMS CSD entries to your CICS system to define the resources required by CA IDMS to CICS. This is usually done by a CICS systems programmer using the CICS resource definition online (RDO) or the DFHCSDUP utility to update the CSD file.

Sample CSD resources required by CA IDMS are shown in CAGJSRC member CICSCSD. Additional optional CSD resources are shown in CAGJSAMP members TPSCICS (CA IDMS/DC Sort) and USDCICS (CA IDMS DML Online). Consult the appropriate IBM documentation to help ensure that these definitions take precedence over any previously configured definitions for the corresponding entities.

More information:

- For a complete description of CA IDMS CICS support, see the Administrating section.
- For complete instructions on updating the CICS CSD file, see the IBM documentation.

CA IDMS Task Analyzer Storage Requirements

Before you start CA IDMS/DC, consider the following storage requirements of CA IDMS Task Analyzer that can affect the sysgen:

- Storage pool
- Program pool
- Stacksize

CA IDMS Log Analyzer and CA IDMS Task Analyzer Statistics Gathering

CA IDMS Log Analyzer and CA IDMS Task Analyzer gather statistical data for all activities except dialogs from the by-task statistics records. Statistical information for dialogs is gathered from the transaction statistics records. For CA IDMS to capture this data, the statistics must be requested at the system level.

You can gather statistical data for CA IDMS Log Analyzer and CA IDMS Task Analyzer.

Follow these steps:
1. **By-task Statistics** are controlled through the STATISTICS subparameter of the SYSTEM statement. The minimum specification required is as follows:

   \[
   \text{STATISTICS TASK WRITE COLLECT}
   \]

   **Note:** For CA IDMS Log Analyzer, you must specify WRITE, otherwise COLLECT is sufficient.

   Usually, CV writes the by-task statistic records to the log. With CA IDMS Task Analyzer, this action is controlled by the DC STATISTICS option field of the CA IDMS Task Analyzer Statistics Plan screen. For more information, see Task Analyzer z/OS Operation (https://docops.ca.com/pages/viewpage.action?pageId=328584806).

2. **Dialog Statistics** are specified in the ADSO statement of the sysgen. The DIALOG STATISTICS subparameter of the ADSO statement generates the transaction statistics. The specification required is as follows:

   \[
   \text{DIALOG STATISTICS ON SELECTED ALL}
   \]

   **Note:** If you specify SELECTED, CA IDMS Log Analyzer and CA IDMS Task Analyzer can report only on dialogs defined with a PROGRAM statement specifying ADSO DIALOG STATISTICS ON. Note: For more information on gathering statistics, see the appropriate CA IDMS guides.

### CA IDMS Performance Monitor

Customize the execution of CA IDMS Performance Monitor by tailoring the PMAMINIT, PMIMINIT, and PMRTINIT modules.

### CA IDMS Web Services

#### Web Services Consumer Demo Service

If you purchase the ADS/Online product, a Consumer Demo ADS Dialog—IDMSWSDM—is included with the CA IDMS Web Services installation component. IDMSWSDM is coded to seed the Map Port number with the CA IDMS Web Services default listener port 3850. You can customize the port number to your site requirements during product installation. If you change the port number, you may also want to change the port assignment in the Demo Dialog process code. Otherwise, you need to amend the port number when you run IDMSWSDM.

To change the port number, use IDD to modify the highlighted line within Process Module IDMSWSDM-PM, as follows:
MODIFY
PROCESS NAME IS IDMSWSDM-PM
VERSION IS 1
PROCESS SOURCE FOLLOWS
MOVE '0472' TO MAP-EMP-ID.
MOVE '127.0.0.1' TO MAP-IP-ADDRESS.
MOVE 3850 TO MAP-CV-PORT.
MOVE 'EMPDEMO' TO MAP-DBNAME.
DISPLAY MSG TEXT 'ENTER EMPLOYEE ID AND PRESS <ENTER>.'.
MSEND

Once the Process Module is updated, use ADSC to compile Dialog IDMSWSDM, to realize the source code change.

Add-On Install SYSGEN Updates

These post-configuration tasks are only performed when CA IDMS Web Services is configured as part of an Add-On configuration.

The Web Services programs that are defined in SYSGEN are set with MULTIPLE ENCLAVE IS ON. To enable the reuse of your LE Enclaves, your CV SYSTEM statement must specify MULTIPLE ENCLAVE IS ON.

The following is an example for setting MULTIPLE ENCLAVE:

SIG DIC SYSTEM
USA UPD FOR DDLDML
USA UPD FOR DDLDCLOD.
MOD SYS xxx (where "xxx" is your system number)
MULTIPLE ENCLAVE IS ON.
GENERATE.

⚠️ Note: If you intend to use the Web Services Client/Provider demo, we recommend that there is at least one XA storage pool with a minimum of 10k.

Configuring Default JCL for CA IDMS Extractor and CA IDMS Dictionary Migrator Assistant

At the initial configuration, configure the default JCL used by CA IDMS Extractor and CA IDMS Dictionary Migrator Assistant (DMA).

CA IDMS Extractor JCL is used to execute the batch components of CA IDMS Extractor. The default CA IDMS Extractor JCL is contained in the following CAGJSRC library members:

- **USVEXEC** -- Extracts and loads a database
- **USVPSPC** -- Prints extract specifications
- **USVPJCL** -- Prints extract and load JCL
The DMA JCL and CA IDMS Extractor JCL allow you to submit Jobs to the internal reader from a CA IDMS system. The DMA JCL is used for the online job submission of CA IDMS Dictionary Migrator Jobs by DMA. The DMA JCL is any JCL for CA IDMS Dictionary Migrator that you are already using or the CAGJSRC library member USMXTRCT. Edit USMXTRCT to tailor the JCL and parameter statements appropriately for your CA IDMS environment and required migration.

The JCL to upload CA IDMS Extractor and DMA JCL is included in CAGJSRC library members USVUJCL and XDMBJCL respectively.

CA ADS Trace Dictionary Updates

All application dictionaries using CA ADS Trace must be updated with the attributes, records, and elements for CA ADS Trace.

Follow these steps to update each dictionary:

1. Create an IDMSDDL job with ATDDDL as input. ATDDDL is located in the CAGJSRC library.
2. Execute the job.
3. Review the output and verify that the entities were added to the dictionary.

CA IDMS/DC Sort Dictionary Updates

All application dictionaries using CA IDMS/DC Sort must be updated with the records and modules for CA IDMS/DC Sort.

Follow these steps to update each dictionary:

1. Create an IDMSDDL job with TPSDDDL as input. TPSDDDL is located in the CAGJSRC library. The TPSDDDL set in Job 13 can be used as a guide.
2. Submit the job.
3. Review the output and verify that the entities were added to the dictionary.

CA IDMS DQF Dictionary Updates

CA IDMS DQF is a CA ADS application. The configuration process adds the CA IDMS DQF application to the CA IDMS Task Application Table (TAT) in the TOOLDICT dictionary. Each application dictionary using CA IDMS DQF must be updated with the CA IDMS DQF ADS application.

Follow these steps to update the dictionary:

1. In the CAGJSRC library, modify the member DADS12OP.
2. Submit DADS12OP for execution.
3. Review the output and verify that the application was added to the dictionary.

Security Classification Modules

If you are upgrading and your site maintains customized versions of IDMSCTAB, IDMSGTAB or IDMSUTAB, you should reassemble and link your customized source. If you are performing a complete base install, you can optionally create customized versions of these modules. See Administrating Security for IDMS (https://docops.ca.com/display/IDMS19/Administrating+Security+for+IDMS) for more information on the security services that these modules provide and information on their modification.

Note: Versions of these modules with no security set are installed into your base installation libraries.

Linking a Dictionary to the CA Endevor/DB Change Monitor

If you selected CA Endevor/DB for CA IDMS for configuration, the configuration process created a CCDB (Change Control Data Base) segment but did not associate the CCDB to a dictionary dbname. A dictionary you want to monitor is linked, or hooked by subschema mapping of IDMSNWKA to NDVRNWKA. Run the Batch Command Facility (IDMSBCF) using the following sample as input to establish change monitoring for a dictionary. Specify the dbtable you want to update and the dictionary segment you want to monitor.

```
ALTER DBNAME dbtablename.dbname
SEGMENT ccdname
    SUBSCHEMA IDMSNWKA MAPS TO NDVRNWKA;
GENERATE DBTABLE dbtablename;
PUNCH DBTABLE LOAD MODULE dbtablename;
```

For more information on seeding the CCDB and assigning a security administrator, see Monitoring Change Activity (https://docops.ca.com/display/IDMS19/Monitoring+Change+Activity).

Creating an Executable System

For either an upgrade or a complete base configuration, additional configuration is required to complete the definition of your DC System.

For a complete base configuration, configure the following:

- **SYSTEM statement** -- Specify the values for the SYSTEM statement parameters, for example:
  
  - REENTRANT POOL
  - STORAGE POOL
- PROGRAM POOL
- STACKSIZE
- SVC
- SYSCTL
- MAX ERUS

Some products have additional requirements.

- CA IDMS Task Analyzer storage requirements
- CA IDMS Log Analyzer and CA IDMS Task Analyzer statistics-gathering

**Important!** These requirements may be critical to the proper functioning of your environment.

- **Task and program definitions** -- The configuration process copied System 90 to your specified DC system.

- **Line definitions** -- Add the line definitions for your site. Add the LTERMs and PTERMs for each line.

- **Generate the new system** -- Submit an RHDCSGEN job to execute the sysgen compiler.

For an upgrade configuration, do the following:

- **Task and program definitions** -- Copy the tasks and programs from System 99 to your specified DC system. Do not alter the task or program definitions copied from System 99.

- **Generate the new system** -- Submit an RHDCSGEN job to execute the sysgen compiler.

**Modify the Startup JCL**

The STARTUP member in the CUSTOM.JCLLIB library contains a partially customized startup job. Depending on hardware (zIIPs) and software in use at your site, you may need to modify one or more of the following:

- The EXEC parameters
- The STEPLIB concatenation
- The CDMSLIB concatenation

DC/UCF systems use the services of the IDMS SVC to enable themselves automatically to run non-swappable in z/OS regardless of the value specified in the z/OS PPT or SYS1.PARMLIB.
To prevent CA IDMS from automatically forcing itself to run non-swappable, do one of the following actions:

- Code SWAP=Y on the EXEC statement in your CV startup JCL if you are using keyword parameters.
- Code an S in column 24 of the EXEC parm of the proc that starts CA IDMS if you are using positional parameters.

CA IDMS now runs exactly as defined in the z/OS definitions.

The startup JCL contains four SET statements. Change the following commands to reflect your environment:

- **SET CLASS**
  The class for the job to be submitted under

- **SET AJNL**
  Point to your archive journal job. See the Archive Journal (https://docops.ca.com/display/IDMSCU/ARCHIVE+JOURNAL) section for more information.

- **SET PLOG**
  Point to your archive log job. See the Archive Log (https://docops.ca.com/display/IDMSCU/ARCHIVE+LOG) section for more information.

- **SET PTRC**
  Point to your archive trace job. See the Archive Trace section for more information.

Many parameters can be specified in the PARM on the EXEC statement in the startup job.

You may need to increase the region size to accommodate increased storage requirements for the current release.

You may need to include DD statements in your CDMSLIB concatenation for libraries of other vendors and products (for example, LE runtime) to load properly when used with your CA IDMS central version.

You may need to add the following libraries to the CDMSLIB concatenation:

- CA IDMS Enforcer load library
- CA IDMS/DC Sort CICS load library

You can add DD statements for database files to the startup JCL, if desired. This action is optional because CA IDMS supports dynamic allocation. If the file names are specified in the DMCL, they are not required in the JCL. The following products use their own database files:

- CA IDMS SQL
- ASF Option
- CA IDMS Tools Dictionary
Under certain circumstances, there are minimum requirements for successfully starting any CA IDMS CV, as follows:

- If you are implementing CA IDMS support for zIIP, certain modules must be loaded from authorized libraries. For more information on zIIP support, see [zIIP Exploitation](https://docops.ca.com/display/IDMS19/zIIP+Exploitation).

- If the z/OS operating system runs with AllowUserKeyCSA(NO), which is the default for z/OS v1r9 and above, the STEPLIB must be authorized and certain other procedures must be followed. For more information on configuring your system to run with AllowUserKeyCSA(NO), see [Storage Key Considerations for z/OS CSA Subpools](https://docops.ca.com/pages/viewpage.action?pageId=328584246).

- If AUTHREQ=YES is specified for the CA IDMS SVC, then the STEPLIB must be authorized. For more information on configuring your system to run with AUTHREQ=YES, see [Installation Considerations](https://docops.ca.com/display/IDMS19/installationConsiderations).

CA IDMS Enforcer

Identify the CA IDMS systems where you want CA IDMS Enforcer to run. Add the CA IDMS Enforcer load library to the CDMSLIB concatenation.

CA IDMS/DC Sort under CICS

Add the CA IDMS/DC Sort CICS load library to the startup JCL for CICS.

Verifying the System Configuration

Before you begin the verification process, the configuration must be completed successfully. The verification process consists of the following phases:

- System startup (see page 78)
- Online verification (see page 78)
- Batch verification (see page 79)
System Startup

To start your DC/UCF system, submit the STARTUP member in the CUSTOM.JCLLIB library. The system is active when the Enter Next Task Code message appears in the JES log.

Online Verification

The online verification process consists of the following steps:

1. **DCMT verification** -- A CLIST that executes a large percentage of the DCMT DISPLAY xxxx functions has been placed in your SYSTEM dictionary. To use this CLIST, enter the following commands at the DC/UCF ENTER NEXT TASK CODE prompt:

   DCUF SET DICTNAME SYSTEM
   CLIST DCMT-DEMO-CLIST

   This step invokes the CLIST and allows you to view the new DCMT DISPLAY output.

2. **DCUF verification** -- A CLIST that executes a large percentage of the DCUF DISPLAY xxxx functions has been placed in your SYSTEM dictionary. To use this CLIST, enter the following commands at the DC/UCF ENTER NEXT TASK CODE prompt:

   DCUF SET DICTNAME SYSTEM
   CLIST DCUF-DEMO-CLIST

   This step invokes the CLIST and allows you to view the new DCUF DISPLAY output.

3. **IDMSLOOK verification** -- A CLIST that executes a large percentage of the online LOOK xxxx functions has been placed in your SYSTEM dictionary. To use this CLIST, enter the following commands at the DC/UCF ENTER NEXT TASK CODE prompt:

   DCUF SET DICTNAME SYSTEM
   CLIST L00K-DEMO-CLIST

   This step invokes the CLIST and allows you to view the IDMSLOOK output.

4. **IDD verification** -- To validate IDD, sign on to the APPLDICT dictionary and try various IDD commands, such as DISPLAY ALL MODULES, DISPLAY ALL USERS, and DISPLAY ALL SCHEMAS.

5. **Online Command Facility (OCF) verification** -- To verify OCF, enter the following commands:

   - DCUF SET DICTNAME SYSTEM
   - OCF
   - DISPLAY SEGMENT SYSTEM -- Displays the definitions of the segment, files and areas that comprise the SYSTEM segment.
   - DISPLAY DMCL R185DMCL -- Displays the DMCL created during the configuration process.
   - DISPLAY DBTABLE R185DBTB -- Displays the database name table created during the configuration process.
Most other online products are optional. Exercise additional products, such as CA ADS, CA OLQ, and CA IDMS Performance Monitor to verify their installation.

**Batch Verification**

Many CA IDMS tools and utilities can be tested. Most of these tools have already been verified by completing configuration, including the following:

- **ADSOBTAT** -- The batch CA ADS application table load utility (ADSOBTAT) is run to define the $TOOLTCF (Transfer Control Facility) as a valid CA ADS runtime application.

- **IDMSBCF** -- The CA IDMS Batch Command Facility (IDMSBCF) controls the execution of most of the CA IDMS utility programs, DBTABLE processing, and SQL processing. IDMSBCF invokes the following utilities during configuration:
  - BACKUP
  - FORMAT
  - PRINT PAGE
  - PRINT SPACE
  - RESTORE

- **IDMSCHEM** -- The non-SQL, Commonweath Demonstration Database schema, EMPSCHM version 100, is added to the APPLDICT DDLDML area using the schema compiler.

- **IDMSDDL** -- Several data dictionary utilities are run to load various entity types (messages, elements, records, and modules) into the DDLDML and DDLDCLOD areas.

- **IDMSDMLC** -- Various programs, including EMPLOAD, are processed using the CA IDMS COBOL precompiler (IDMSDMLC) during the creation of the non-SQL demonstration database.

- **IDMSRPTS** -- The CA IDMS Schema Reporter program is executed to list various reports for EMPSCHM Version 100 during the configuration of the non-SQL demonstration database.

- **IDMSUBSC** -- The subschema used to define the non-SQL demonstration database, EMPSS01, is loaded and generated using the subschema compiler.

- **RHDCMAP1** -- The batch mapping compiler is used to load the map, EMPMAP, into the APPLDICT DDLDML area.

- **RHDCMPUT** -- The batch mapping utility module is run to do a PROCESS=ALL for map EMPMAP in the APPLDICT dictionary.

- **RHDCSGEN** -- The batch system generation compiler is executed to create SYSTEM 90 and SYSTEM 99.

If you chose local mode for the configuration process, consider testing some of these tasks running against your central version once it is established. You can test any other programs not executed during configuration at your convenience.
CAIRIM

The configuration process loads a customized IDMS SVC that is resident only until the next IPL. Your systems group can enable the SVC to install automatically at each IPL by running the CAIRIM proc (usually the CAS9 procedure) at each IPL. This proc is described in the CA Common Services for z/OS documentation.

The CAS9 proc requires the CAIRIM parameter line for CA IDMS and the location of the six APFLIB modules.

The CAS9 proc reads CAIRIM product parameter lines from the CARIMPRM member in SYS1.PARMLIB. The format for this line can vary as follows:

- If the location of the six APFLIB modules is specified by adding a DD statement to the CAS9 proc (concatenated to STEPLIB), the CAIRIM parameter line format is as follows:

  \[ \text{PRODUCT(CA IDMS) \ Version(GJJ0) \ INIT(GJJ0INIT) \ PARM(SVC=xxx)} \]

- If no DD statement is added to the CAS9 proc, the format is as follows:

  \[ \text{PRODUCT(CA IDMS) \ Version(GJJ0) \ LOADLIB(dsname) \ INIT(GJJ0INIT) \ PARM(SVC=xxx)} \]

  where \text{dsname} is the name of the authorized loadlib containing the six APFLIB modules.

If you are running multiple releases of CA IDMS using one SVC, supply a CAIRIM parameter line for each release. All but the first line must have the REFRESH parameter. See SVC (see page 80).

⚠️ Note: Maintenance may update the SVC load module. If the CA IDMS APFLIB loadlib is authorized and CAIRIM loads the SVC directly from the APFLIB at each IPL, you are loading an updated (and possibly untested) SVC with the first IPL after installing maintenance affecting the SVC. For this reason, do not load the SVC for your production system directly from APFLIB.

SVC

When an SVC is refreshed, all CVs using it must be brought down before the REFRESH. After the SVC has been refreshed, the CV can be restarted. Unpredictable results can occur for any ERUS task that is accessing a CV while its SVC is being refreshed. Batch jobs and CICS regions that access CA IDMS are affected.

The CA IDMS SVC load module is downward compatible. If you are using multiple supported versions of CA IDMS, you can run all your releases on the new SVC. For multiple releases to share the same SVC, the CAIRIM input statements must be modified to avoid CA IDMS CAIRIM errors. Failure to modify the CAIRIM statement results in the following message:

\[ \text{CA IDMS SVC MUST BE INSTALLED BY CAIRIM BEFORE STARTING THE DATABASE} \]
**Example**

The site is running releases 18.0 and 19.0 and uses SVC 173. The following are the CAIRIM PARMLIB input statements:

```
PRODUCT(CA IDMS) VERSION(GJI0) INIT(GJI0INIT) PARM(SVC=173)
PRODUCT(CA IDMS) VERSION(GJJ0) INIT(GJJ0INIT) PARM(REFRESH(SVC=173))
```

**Explanation** The first statement installs SVC 173 with version code GJI0 (Release 18.0). The second statement inserts version code GJJ0 (Release 19.0.02) into the CPU where CAIRIM is running while refreshing the same SVC load module. This allows releases 18.0 and 19.0 CA IDMS CVs to use the same SVC.

⚠️ **Note:** The INIT parameter on both lines should name the GJJOINT load module.

---

**Refreshing Required Modules**

The required modules—IDMSMSVA, RHDCSSFM, CAIXDOA$ and PMRTDATA—are downward compatible. If you are using an earlier release of CA IDMS, the versions of these modules in the ECSA may not have been refreshed when the new SVC was installed. Refresh these modules using the following syntax:

```
PRODUCT(CA IDMS) VERSION(GJJ0) INIT(GJJ0INIT) PARM(REFRESH(RHDCSSFM))
PRODUCT(CA IDMS) VERSION(GJJ0) INIT(GJJ0INIT) PARM(REFRESH(IDMSMSVA))
PRODUCT(CA IDMS) VERSION(GJJ0) INIT(GJJ0INIT) PARM(REFRESH(CAIXDOA$))
PRODUCT(CA IDMS) VERSION(GJJ0) INIT(GJJ0INIT) PARM(REFRESH(PMRTDATA))
```

When a `module-name` is refreshed, all CVs and batch Jobs that are using the module being refreshed must be ended before the REFRESH. When the module has been refreshed, CVs and batch jobs can be restarted.

---

**Numbered Options**

Numbered options provide a means for you to tailor CA IDMS behavior to meet your processing needs. You enable numbered options by turning on a bit in the options table, RHDCOPTF.

The following shows the default RHDCOPTF with no bits turned on. It can be found in your CUSTOM. SRCLIB (RHDCOPTF)

```plaintext
#DEFOPTF TYPE=GENERATE
END
```

To turn on bits 5 and 81, code the following:

```plaintext
#DEFOPTF OPT00005
#DEFOPTF OPT00081
#DEFOPTF TYPE=GENERATE
END
```
Assemble and link RHDCOPTF by running the RHDCOPTF jobs in the CUSTOM.SRCLIB and CUSTOM.LNKLIB libraries.

Security

A list of CA Technologies supplied user mode programs that issue bind run units can be found in the CAGJSRC library in members whose names begin with SEC. This list may be useful for sites that choose to secure RESTYPE=SPGM or RESTYPE=DB.

Setup SQL Web Connect for z/OS

SQL Web Connect allows all CA IDMS™/DB customers to take advantage of SQL, ODBC, and JDBC connectivity functions. Previously, these functions were only available to customers who licensed CA IDMS™ SQL and CA IDMS™ Server options. SQL Web Connect provides access for two concurrent users of dynamic SQL through ODBC and JDBC from the Web, Windows, Java, and other non-mainframe platforms, and through the usual CA IDMS tools (for example, OCF, BCF). SQL Web Connect is automatically activated when SQL, ODBC, or JDBC access is attempted when an LMP key is required and there is no valid LMP key on the system for the interface being invoked.

SQL Web Connect uses TCP/IP to communicate with CA IDMS, for example:

- JDBC users must use a Type-4 JDBC connection.
- ODBC users must configure their Data Source to use the ‘IDMS’ communications protocol.

Using these communication interfaces requires that CA IDMS Server is installed, as follows:

- JDBC users must run CA IDMS Server r16.0 or greater.
- ODBC users must run CA IDMS Server r17.0 or greater.

SQL Web Connect only operates when no valid LMP key is installed for the product that is invoked. Customers who have full licenses of the product cannot use this feature to limit resource usage.

Note: If you apply the enhancement PTF RO96807, SQL Web Connect is no longer necessary, because the LMP keys for CA IDMS SQL and CA IDMS Server product options are contained in the base CA IDMS product.

CA IDMS Server Installation

Clients who must install the CA IDMS Server client component can acquire the software in one of two ways:
1. All CA IDMS clients can download the CA IDMS Server product directly from the Download Center link on CA Support Online, at: https://support.ca.com/. From the drop-down lists, select the product and release number for CA IDMS/DB - MVS and click Go. On the Product Downloads page, click Download next to IDMS SRVR CD ZIP FILE ESD ONLY. The install image for the latest release of CA IDMS Server is included in the CA IDMS r<release number> installation PAX file. Once the SMP APPLY step is run, this image is available in the CAGJDATV SMP library under member IDSERV17. You must FTP this member (in BINARY mode) to an appropriate location on the hard drive of your PC. Once downloaded, rename the file to have an extension of .zip.

Once the ZIP file is downloaded, extract the installation files and then invoke the setup.exe file to initiate the installation.

2. SQL Usage

You must create an SQL Catalog for your system to use SQL Web Connect if you:

- Do not have the CA IDMS SQL Option, and
- Have not already created an SQL Catalog for your system (for use with CA IDMS Visual DBA for example).

You may also want to create and populate the SQL version of the Employee Skills Demo Database on one or more of your CVs. The following sections describe how these actions can be performed using either CAISAG or CSM.

- Usage Considerations (see page 83)
- CAISAG Implementation (see page 84)
- CSM Implementation (see page 85)

Usage Considerations

If you attempt to create and populate the SQL version of the Employee Skills Demo Database you may encounter an error. This error occurs when performing a Base or Upgrade installation if the following conditions are fulfilled:

- The SQL product is licensed (the LMP key for SQL is installed), and
- The RHDCPINT module is configured to indicate that the SQL product is not used.

Do not add the SQL Demo Database if your installation fulfills the conditions in the preceding list. If you want to use SQL on the target CV, set the SQL product flag to indicate this fact in the RHDCPINT module.
CAISAG Implementation

Several new VARBLIST configuration variables are available to assist you in creating an SQL Catalog and Demo Database on your system.

Use the following variables for a Base CA IDMS configuration:

- SYSSQL = YES -- Governs the creation of System SQL catalog.
- SQLDEMO = YES -- Governs the creation of the SQL Demo Database.

Use the following variables for an Upgrade CA IDMS configuration:

- UPGSYSQL = YES -- Governs the creation of System SQL catalog.
- UPGQDEMO = YES -- Governs the creation of the SQL Demo Database.

Clients who already upgraded their CA IDMS system, but would like to create an SQL catalog, SQL Demo Database, or both can perform an Add-On installation to accomplish this task.

Use the following variables for an Add-On CA IDMS configuration:

- BEGINMEM = SQL -- Sets the prefix for generated members to ‘SQL’.
- ADDSYSQL = YES -- Governs the creation of System SQL catalog.
- ADDQDEMO = YES -- Governs the creation of the SQL Demo Database.

When the CAISAG job is run, several new SQL-prefixed members are added into your CAISAG configuration library. The following jobs contain the steps necessary to add the SQL catalog and Demo Database to your system for an Add-On installation:

- SQL05 -- This job allocates the SQL catalog and Demo Database files.
- SQL08 -- This job builds the new SQL catalog.
- SQL10 -- This job formats and populates the new SQL catalog.
- SQL15 -- This job builds, formats, and populates the new SQL Demo Database.

⚠️ **Note:** For more information on modifying the VARBLIST member, see the SQL Web Connect for VSE (https://docops.ca.com/display/IDMS19/SQL+Web+Connect+for+VSE) section in the appendix.
CSM Implementation

Customers using CSM have the same options for adding the SQL catalog and SQL Demo Database as described in the preceding section for customers using CAISAG. The process for adding the SQL catalog and Demo Database is described within the CSM interface itself. CSM refers to an ‘Add-On installation’ as an ‘Update installation’ (or ‘Update configuration’). The same variables that are noted in the preceding section are also present in the CSM interface.

**Important!** The addition of the SQL Catalog, SQL Demo Database, or both requires updates to both the global DMLC and Database name Table (DBTB) of your CV. These updates are performed automatically in the job steps that are generated by both CAISAG and CSM. Backups of both the global DMCL and DBTB are also performed during these job steps.

**Note:** Specify NO for the CA IDMS™ SQL option if you do not have a license for it. This creates an RHDCPINT module without SQL selected and assembles the IDMISCINT macro with SQL=NO. New configuration variables (detailed above) allow you to select whether to install the SYSSQL catalog component and the SQL Demo Database. These two choices are independent of your product selection. This process allows you to install the SYSSQL catalog component and the SQL Demo Database even if you do not have a license for the CA IDMS SQL Option. The SYSSQL catalog component is a prerequisite for the SQL Demo Database. The SYSSQL database uses 600 tracks (40 CYL) and the SQL Demo Database uses 25 tracks (<2 CYL).

Installing CA IDMS Visual DBA

This section contains instructions on how to install CA IDMS Visual DBA on the PC and on the mainframe. To enable Enhanced Object Security for Visual DBA in an IDMS Central Version, an additional mainframe configuration step is required. This information is covered in "Enhanced Object Security" of CA IDMS VDBA Using section, which also contains extensive examples illustrating its benefits.

If an installation in an IDMS CV is done without \Enhanced Object Security, it can always be added in a later phase. Also Enhanced Object Security can be turned off and on at any time. For more information, see the CA IDMS VDBA Using section and the CA IDMS Visual DBA readme file on the installation CD.

For more information, see the following topics:

- Software Requirements (see page 86)
- Install CA IDMS Visual DBA Version 18 on the PC (see page 86)
- Prepare Your Mainframe Environment (see page 88)
Software Requirements

The following software requirements for running CA IDMS Visual DBA Version 18 apply:

- To run CA IDMS Visual DBA Version 18 on a mainframe, you need CA IDMS Release 16.0 or above on z/OS or z/VSE.


Notes:

- The client component of CA IDMS Server can be obtained from:
  - The CA IDMS Visual DBA installation CD.
  - The installation image that can be downloaded from Support Connect.
  - The installation image in the VDBA180 member of the SMP/E target library, CAGJDATV.
  - Customers without a license for CA IDMS Server must reinstall CA IDMS Server on their PC from the CA IDMS Visual DBA Version 18 installation CD or image.

Install CA IDMS Visual DBA Version 18 on the PC

CA IDMS Visual DBA can be installed from any of these media:

- From the installation CD
  To install CA IDMS Visual DBA from the installation CD, place the installation CD in your CD drive. If the setup program does not automatically start when you insert your CD, you can run setup.exe from the setup folder on the CD.
From Support Connect
To install CA IDMS Visual DBA from Support Connect at https://support.ca.com, go to the download page. Select 'CA IDMS/DB - MVS' from the product drop-down list and '18.5' from the release drop-down list, and click the 'Go' button. On the following screen, click the 'Download' function next to the 'CA IDMS VISUAL DBA MEDIA' item.

From a library that is created during the mainframe installation of CA IDMS
To install CA IDMS Visual DBA from the mainframe CAGJDATV library, the SMP/E APPLY of CA IDMS 18.5 must have completed successfully. FTP the VDBA180 member (in BINARY mode) to a hard drive of your PC. Rename the file to have an extension of zip. Extract the installation files and then invoke the setup.exe file to initiate the installation.

The setup program displays the CA IDMS Visual DBA Product Explorer. Select Install CA IDMS Visual DBA and click Install. The setup program guides you through the installation process. You can optionally start the installation process by double-clicking or right-clicking on Install CA IDMS Visual DBA and selecting Install.

CA IDMS Visual DBA offers three installation options:

- **Typical**
  Covers all of the product components into the folder you specified during the installation. This includes the following files:
  - Program files and help files that are needed for execution on the PC
  - SQL script files that optionally can be uploaded to the mainframe if running them on the mainframe is preferred as opposed to running them from Visual DBA. The SQL script files are copied into three CA subfolders: IdmsR16x contains the scripts which are used for IDMS r16, IdmsR17x is for IDMS r17 and IdmsV18x is for IDMS Versions 18.0 and later.
  - The example file (demo180.cfg)
  - **CA IDMS Visual DBA Using section and CA IDMS Visual DBA Release Notes**
  - ReadMe file (readme.txt), which is also provided in HTML format for viewing through your browser (readme.htm)
  - Files for a bookshelf application to easily view and search the documentation.

- **Compact**
  Copies the required program files, help files, and readme files for the PC into the folder you specified during the installation. However, it does not copy the SQL installation scripts into the CA IDMS release specific subfolders, the example file, the Using section and the Release Notes, or the bookshelf application to the product folder.

- **Custom**
  Allows you to select which product components get installed. By default, all of the components are selected for installation. You can optionally select or deselect components, such as the SQL script files, documentation files, and example files. The required program files, help files, and readme files are always installed.
Prepare Your Mainframe Environment

Contents

- CA IDMS r16 (see page 88)
- CA IDMS r17 (see page 88)

This topic describes APARs and other maintenance that you must apply to your mainframe CA IDMS systems before installing the mainframe component of CA IDMS Visual DBA.

CA IDMS r16

Apply APAR QO57823 to your system if you have not installed any Service Pack.

Customers that have no license for CA IDMS SQL Option require SP2 or later, and also need to apply Apar RO12770.

CA IDMS r17

No maintenance is required if you have a license for CA IDMS SQL Option.

Customers that do not have a license for CA IDMS SQL Option need to apply the following PTFs:

- For zOS apply PTF RO12719
- For zVSE apply PTF RO12720.

Install CA IDMS Visual DBA Version 18

CA IDMS Visual DBA uses SQL to access all of the CA IDMS mainframe objects that it manages. CA IDMS Visual DBA requires that the following components be installed in your mainframe environment:

- **SQL definitions**
  Installs the SQL DDL for schemas, views, functions, and table procedures which are required by CA IDMS Visual DBA into each dictionary you want to manage using CA IDMS Visual DBA.

**Important!** Installation of CA IDMS Visual DBA Version 18 on the mainframe depends heavily on the mainframe environment. It is important to know the release level of the CA IDMS mainframe system to install the mainframe components of CA IDMS Visual DBA Version 18. Knowing the release level determines which version of the IDMSVnnX or IDMSRnnX script you use in the following instructions.
How to Convert to SQL, Create additional SQL Catalogs, Set Up Server and CCI

Contents

- Convert CATSYS (see page 90)
- Create SYSSLQ Catalog (see page 91)
- Create an Updated DMCL Module, Update the DBTABLE, and Format SYSSLQ (see page 91)
- Load the Catalogs with SQL System Definitions (see page 92)
- Set Up CCI (see page 92)
- Set Up CA IDMS Server (see page 93)

In this step, you perform five basic tasks to convert a non-SQL catalog to an SQL catalog, to create an additional SQL catalog, to set up Server and optionally CCI as discussed in the following procedure.

Follow these steps:

1. Convert the system catalog, CATSYS, from a NONSQL to a SQL-type catalog, using OCF.

2. Create a new SQL catalog named SYSSLQ.

3. Create an updated DMCL module and update the DBTABLE to include the new SYSSLQ catalog in each nonsystem dictionary that is accessible by CA IDMS Visual DBA. Format the new SQL catalog SYSSLQ.

4. Load the catalogs with SQL system definitions

5. Set up the mainframe component of CA IDMS Server and optionally CCI.

Note: The catalog entities created for CA IDMS Visual DBA require that each catalog has free space available. For the DDLCAT area, 4 MB of available space is required; for the DDLCATX area 0.5 MB is required. CA IDMS Visual DBA does not use space in the DDLCATLOD area. In most cases, you must expand the system catalog, CATSYS. If expansion is needed for the new SQL catalog, SYSSLQ, you must allocate enough space to accommodate for future versions of CA IDMS Visual DBA and CA IDMS.

Perform the following steps to set up the mainframe environment for CA IDMS Visual DBA.
Convert CATSYS

**Note:** This step is only needed if the target catalog for CA IDMS Visual DBA is a non-SQL catalog. This is typically the case for customers without licenses for CA IDMS SQL and Server who are installing CA IDMS Visual DBA for the first-time and have never installed Visual DB or SQL Web Connect.

Before actually converting the CATSYS system catalog it is advised to take a backup of the CATSYS areas, so that a restore can be done quickly if needed.

**To convert the system catalog, CATSYS, from a NON-SQL to a SQL-type catalog, using OCF:**

1. CONNECT TO SYSTEM
2. DISPLAY SEGMENT CATSYS AS SYNTAX
3. Edit the OCF workspace as follows:
   a. Modify `DISPLAY SEGMENT CATSYS AS SYNTAX;` to `DROP SEGMENT CATSYS`
   b. Modify attribute of segment CATSYS from `FOR NONSQL` to `FOR SQL`.
   c. Add `STAMP BY AREA` for areas DDLCAT and DDLCATLOD.
   d. Add `STAMP BY TABLE` for area DDLCATX.
   e. Apply the syntax.
   f. Clear the OCF workspace.
   g. Include the updated segment, CATSYS, in all the DMCLs that use it. That is, for the DMCL named `cvdmcl` and used by the Central Version:
      ```sql
      ALTER DMCL cvdmcl INCLUDE SEGMENT CATSYS;
      ```
   **Note:** This step is necessary because the `DROP` done in step 3a removed this segment from your DMCL definition.
   h. Generate your DMCL by entering `GENERATE DMCL cvdmcl`
Create SYSSQL Catalog

The source for SYSSQL can be cloned from the system catalog, CATSYS. You can use the following steps to create a SYSSQL segment using OCF.

To create the SYSSQL segment, using OCF

1. CONNECT to SYSTEM
2. DISPLAY SEGMENT CATSYS AS SYNTAX
3. Edit the OCF workspace as follows:
   a. Change all occurrences of CATSYS to SYSSQL.
   b. Change the file names to the new names you have selected in the file and physical area sections.
   c. Modify the physical area definitions by changing the space, starting page information, and page size to the values you have selected for the new segment.

   \[\textbf{Note}: \text{Do not change the area names from DDLCAT, DDLCATX, and DDLCATLOD.}\]

   d. Verify that segment definition SYSSQL has attribute \textit{FOR SQL}.
   e. Verify that areas DDLCAT and DDLCATLOD have attribute \textit{STAMP BY AREA}.
   f. Verify that area DDLCATX has attribute \textit{STAMP BY TABLE}.
   g. Apply the syntax.
   h. Clear the OCF workspace.
   i. Include the new SYSSQL segment in your DMCL by entering \texttt{ALTER DMCL cvdmcl INCLUDE SEGMENT SYSSQL;}
   j. Generate your DMCL by entering \texttt{GENERATE DMCL cvdmcl;}

Create an Updated DMCL Module, Update the DBTABLE, and Format SYSSQL

1. Run a batch job to punch and link the DMCL cvdmcl.
2. Use OCF or IDMSBCF to update the DBTABLE used by your CA IDMS system to include the new SQL catalog, SYSSQL, for each application dictionary by entering the following:

   ALTER DMCL cvdmcl;
   ALTER DBNAME dbname INCLUDE SEGMENT SYSSQL;

3. Run a batch job to punch and link the above DBTABLE.

4. Run a batch job to format the new SYSSQL segment.

Load the Catalogs with SQL System Definitions

1. Run an IDMSBCF batch job, using member TABLEDDL in the IDMS source library, to load the system tables into the CATSYS and SYSSQL catalogs.

   Note: If the IDMSBCF job does not end successfully, rerunning the step can terminate with message DB002028 DDL not allowed in the SYSTEM schema. An attempt has been made to create or modify the definition of a table in the SYSTEM schema. If this message occurs while executing against the CATSYS catalog, the CATSYS catalog must be restored; in case of the new SYSQL catalog, the SYSSQL segment must be reformatted. After the cause of the problems have been identified and resolved, the TABLEDDL must then be reexecuted.

2. Run an IDMSBCF batch job, using member VIEWDDL in the IDMS source library, to load the sysca views into the CATSYS and SYSSQL catalogs.

Set Up CCI

Setting up CCI is only necessary if you want CA IDMS Server to use the CCI communications protocol. ODBC data sources define which communications protocol is used. This protocol can be either 'CCI' or 'IDMS'. CCI is a component of the CA Common Services. CCI supports multiple communication protocols, but for CA IDMS Visual DBA and Server the TCPIP protocol is required. This is accomplished by adding the following line to the CCI initialization parmlib member CCIPARMS:

   PROTOCOL(TCPIP)

To start the CCITCP subtask on the mainframe, the CCITCP proc from the CA Common Services CAIPROC dataset must be copied to a cataloged system procib. After shutting down and restarting CAIENF, CCITCP will be running and accepting CCI/PC connection requests from CA IDMS Visual DBA and Server.

Note: See the CA Common Services documentation for the operating system installation instructions and to the CA IDMS Server Using section for CA IDMS installation.
The CA IDMS installation consists of adding a line of type CCI, with associated PTerm/Lterm pairs to the system sysgen. Provide at least four PTerm/Lterm pairs for each CA IDMS Visual DBA user.

**Set Up CA IDMS Server**

If CCI is not set up for CA IDMS Server, CA IDMS Server on the mainframe must be configured to use TCP/IP.

In case your CA IDMS system does not have the system definitions for the CA IDMS Server component, update your system:

- Run an IDMSDDDL job with the DLODSERV member as input against the system dictionary.
- Run a SYSGEN job (online or batch) with an INCLUDE IDMS-SERVER statement and generate your system.

**Note:** For more information on the configuration and usage of CA IDMS Server, see the **CA IDMS Server Using section**. This section is provided in both PDF and HTML formats with the **IDMS Server Using section** installation of the product.

---

**How to Install the CA IDMS Visual DBA Version 18 SQL Definitions**

**Contents**

- Install CA IDMS Visual DBA SQL Definitions Using IDMSBCF (see page 94)
- Install CA IDMS Visual DBA SQL Definitions Using CA IDMS Visual DBA (see page 95)

CA IDMS Visual DBA uses SQL to access all of the CA IDMS mainframe objects that it manages. This step executes the SQL DDL statements to add the SQL schema, view, function, and table procedure definitions required by CA IDMS Visual DBA Version 18. The CA IDMS Visual DBA definitions must be installed in the SQL catalog for each dictionary that CA IDMS Visual DBA manages.

**Note 1:** Each dictionary to be controlled must have a catalog associated with that dictionary. The catalog component of different dictionaries can be shared. If multiple dictionaries share the same catalog, only one dictionary needs to have the SQL definitions installed.
**Note 2:** You may need to increase the catalog size to accommodate the added views and table procedures. This may be the case for the CATSYS segment files if you used the original installation defaults. You must have at least 1000 pages in your DDLCAT area for all catalogs that are used with CA IDMS Visual DBA.

**Note 3:** CA IDMS Visual DBA Version 18 SQL definitions can coexist with definitions of older CA IDMS Visual DBA releases. There is no need to uninstall older version definitions before installing Version 18 definitions.

**Note:** For more information on instructions on uninstalling prior versions, see the section Uninstall and Reinstall CA IDMS Visual DBA (see page 96).

The following are the two methods of installing the CA IDMS Visual DBA SQL definitions:

- Using the mainframe Batch Command Facility IDMSBCF
- Using CA IDMS Visual DBA

**Install CA IDMS Visual DBA SQL Definitions Using IDMSBCF**

This option submits the SQL DDL statements required by CA IDMS Visual DBA Version 18 directly to CA IDMS for processing.

**To install CA IDMS Visual DBA SQL definitions using IDMSBCF**

1. Locate the SQL script with the definitions needed by CA IDMS Visual DBA for your environment. The script you use is located in the IdmsR16x, IdmsR17x, or IdmsV18x folder of the CA IDMS Visual DBA product folder, depending on the release level of CA IDMS.
   - For CA IDMS r16 the full path of the script file Vdb5R16X.SQL is typically: `C:\Program Files\CA\CA IDMS Visual DBA V18\IdmsR16x\Vdb5R16X.SQL`
   - For CA IDMS r17 the full path of the script file Vdb5R17X.SQL is typically: `C:\Program Files\CA\CA IDMS Visual DBA V18\IdmsR17x\Vdb5R17X.SQL`
   - For CA IDMS Version 18 and 18.5 the full path of the script file Vdb5V18X.SQL is typically: `C:\Program Files\CA\CA IDMS Visual DBA V18\IdmsV18x\Vdb5V18X.SQL`

2. Edit the SQL script as explained in the comments to optionally enable Enhanced Object Security and to define the names of the dictionaries that you want CA IDMS Visual DBA to manage. Optionally, you can also change the name of the **IDMSDIRL** dictionary if it is not **SYSDIRL**. The VDB5R16X, VDB5R17X and VDB5V18X scripts contain three predefined dictionaries: **SYSTEM**, **APPLDICT**, and **SYSDICT** in three separate lines. You can change the predefined names and add or remove lines with dictionary names.

3. Upload the file to the mainframe using a Text File Transfer Protocol.
4. Execute the Batch Command Facility (IDMSBCF), using the uploaded file as input, against all dictionaries that you want CA IDMS Visual DBA to manage.

**Note:** For more information on enabling Object Security, see the section *Enable Enhanced Object Security for an IDMS CVCA IDMS* in the *CA IDMS VDBA Using* section.

## Install CA IDMS Visual DBA SQL Definitions Using CA IDMS Visual DBA

You can use an SQL command console of either CA IDMS Visual DBA Version 18, CA IDMS Visual DBA r17, or CA IDMS Visual DBA r16 to execute the SQL DDL statements.

If Visual DBA Version 18 is used, even if Enhanced Object Security is disabled, a profile for the installing user must exist on the IDMS Central Version and the profile must contain a rule allowing execution of the SQL command processor against the target dictionary in update mode.

As an example, if the target dictionary is SYSTEM, the following rule allows execution of the SQL command processor against it:

```
Cmd Console SQL/SYSTEM(U)
```

### To Install CA IDMS Visual DBA SQL Definitions

The steps to install CA IDMS Visual DBA SQL Definitions are the following:

1. Run CA IDMS Visual DBA Version 18 or r17 on your PC. Make the Node window visible and active. Expand the root node, Node, to display all the available nodes which are those ODBC data sources that use a CA IDMS ODBC driver.

2. Select the Data Source for the target dictionary for the install. If no appropriate node (ODBC data source) to your mainframe CV/Dictionary exists, perform the following steps:
   a. Add a node using the Add option on the Node menu or use the Add button on the Node window toolbar.
   b. Define the ODBC data source as a system or user ODBC data source. The dictionary to be specified in the ODBC Data Source definition is the target dictionary for the installation.

3. Open a Command Console to your Central Version (CV) by selecting the Cmd Console option on the Node menu, or use the Cmd Console button on the Node window toolbar or right-click the selected node and select Cmd Console. A dialog prompts you for a userid and password to connect with the CA IDMS CV.

4. After a successful connection, the command console appears. From the command console, perform the following steps:
a. Select the default dictionary of the node or ODBC data source in the first unlabeled list box on the Command Console window.

b. Check that the second unlabeled list box contains the default processor SQL. Keep this default processor.

5. Use the Open Script option on the Script menu to select the installation SQL script that corresponds to your CA IDMS release. These script files are located in the IdmsR16x, IdmsR17x or IdmsV18x folder of the CA IDMS Visual DBA product folder, depending on the IDMS release.
   For CA IDMS r16 the full path of the script file Vdb5R16x.SQL is typically:  
   C:\Program Files\CA\CA IDMS Visual DBA V18\IdmsR16x\Vdb5R16X.SQL
   For CA IDMS r17 the full path of the script file Vdb5R17x.SQL is typically:
   C:\Program Files\CA\CA IDMS Visual DBA V18\IdmsR17x\Vdb5R17X.SQL
   For CA IDMS Version 18 and 18.5 the full path of the script file Vdb5V18X.SQL is typically:  
   C:\Program Files\CA\CA IDMS Visual DBA V18\IdmsV18x\Vdb5V18X.SQL

4. Edit the SQL script as explained in the comments to optionally enable Enhanced Object Security and to define the names of the dictionaries that you want CA IDMS Visual DBA to manage. Optionally, you can also change the name of the IDMSDIRL dictionary if it is not SYSDIRL. The script contains three predefined dictionaries: SYSTEM, APPLDICT, and SYSDICT in three separate lines. You can change the predefined names and add or remove lines with dictionary names.

6. Click the Trace Tab to display the execution of the script progress.

7. Click the GO button or press F5.

4. Note: A disabled GO button in the command console of CA IDMS Visual DBA Version 18 indicates that either no profile exists for the user or the profile does not allow execution of the SQL command processor against the target dictionary.

The installation is successful if the script terminates without errors. Warnings are acceptable.

Uninstall and Reinstall CA IDMS Visual DBA

Contents
- Uninstall the PC Client Component (see page 97)
  - Uninstall CA IDMS Visual DBA r16 (see page 97)
  - Uninstall CA IDMS Visual DBA r17 (see page 97)
  - Uninstall CA IDMS Visual DBA Version 18 (see page 97)
- Uninstall the Mainframe SQL Definitions (see page 98)
Uninstall the PC Client Component

Use the following procedures to uninstall PC client component.

Uninstall CA IDMS Visual DBA r16

CA IDMS Visual DBA r17 coexists with CA IDMS Visual DBA r16, so there is no need to uninstall CA IDMS Visual DBA r16 prior to installing CA IDMS Visual DBA r17. However, if at any time you want to uninstall Visual DBA r16 on your PC, open the Control Panel, select Add/Remove Programs, select CA IDMS Visual DBA r16, and click Remove.

Uninstall CA IDMS Visual DBA r17

CA IDMS Visual DBA Version 18 coexists with CA IDMS Visual DBA r17 so there is no need to uninstall CA IDMS Visual DBA r17 before installing CA IDMS Visual DBA Version 18. However, if at any time you want to uninstall Visual DBA r17 on your PC, open the Control Panel, select Add/Remove Programs, select CA IDMS Visual DBA r17, and click Remove.

Uninstall CA IDMS Visual DBA Version 18

You can uninstall the PC Client component of CA IDMS Visual DBA Version 18.

To uninstall the PC Client component of CA IDMS Visual DBA Version 18

1. Open the Control Panel and select Add/Remove Programs. The Add/Remove Programs dialog displays.


3. Select Remove and click Next. The Confirm Uninstall dialog displays.
4. Click OK.  
The Setup Status dialog displays showing the progress of the maintenance operation.

5. When the Maintenance Complete dialog displays, click Finish.

Uninstall the Mainframe SQL Definitions

Use the following procedure to uninstall the Mainframe SQL definitions using a command console of either Visual DBA r16, r17 or Version 18.

Uninstall CA IDMS Visual DBA r16

⚠️ You can use CA IDMS Visual DBA Version 18 to uninstall the Visual DBA r16 mainframe SQL definitions.

To uninstall CA IDMS Visual DBA r16 mainframe SQL definitions

1. Open an SQL Command Console session of CA IDMS Visual DBA Version 18 on the node (ODBC data source) that contains the dictionaries you want to uninstall.

2. Select the dictionary that you want to uninstall from the dictionary drop-down menu.

3. Open the appropriate VDB3UNxx.SQL script located in the IDMSR16X, IDMSR17X or IDMSV18X subfolders of the Visual DBA product folder and execute it:

   - VDB3UN16.SQL for CA IDMS r16
   - VDB3UN17.SQL for CA IDMS r17
   - VDB3UN18.SQL for CA IDMS Version 18.0

4. Repeat the previous two steps for each dictionary you want to uninstall.

⚠️ Notes:

- The VDB3UNxx.SQL scripts are found in the appropriate IdmsRxxx or IdmsVxxx folder underneath the CA IDMS Visual DBA Version 18.0 product folder. These folders are created during the installation of CA IDMS Visual DBA Version 18.0 on the PC.

- For more information, see Installing CA IDMS Visual DBA (see page 85).
Uninstall CA IDMS Visual DBA r17

You can use CA IDMS Visual DBA Version 18 to uninstall the Visual DBA r17 mainframe SQL definitions.

To uninstall CA IDMS Visual DBA r17 mainframe SQL definitions

1. Open an SQL Command Console session of CA IDMS Visual DBA Version 18 on the node (ODBC data source) that contains the dictionaries you want to uninstall.

2. Select the dictionary that you want to uninstall from the dictionary drop-down menu.

3. Open the appropriate VDB4UNxx.SQL script located in the IDMSR16X or IDMSR17X subfolders of the Visual DBA product folder and execute it:
   - VDB4UN16.SQL for CA IDMS r16
   - VDB4UN17.SQL for CA IDMS r17
   - VDB4UN18.SQL for CA IDMS Version 18.0

4. Repeat the previous two steps for each dictionary you want to uninstall.

Notes:

- The VDB4UNxx.SQL scripts are found in the appropriate IdmsRxxx or IdmsVxxx folder underneath the CA IDMS Visual DBA Version 18.0 product folder. These folders are created during the installation of CA IDMS Visual DBA Version 18.0 on the PC.

- For more information, see Installing CA IDMS Visual DBA (see page 85).

Alternately, you can upload the VDB4UNxx.SQL file to the mainframe and run an IDMSBCF batch job to execute the script. The IDMSBCF batch job must be run against each dictionary for which CA IDMS Visual DBA r17 SQL definitions are to be uninstalled.
Uninstall CA IDMS Visual DBA Version 18

You can use CA IDMS Visual DBA Version 18 to uninstall the mainframe SQL definitions of an existing Version 18 instance.

To uninstall CA IDMS Visual DBA Version 18

1. Open an SQL Command Console session of CA IDMS Visual DBA Version 18 on the node (ODBC data source) that contains the dictionaries you want to uninstall.

2. Select the dictionary that you want to uninstall from the dictionary drop-down menu.

3. Open the appropriate VDB5UNxx.SQL script and execute it:
   - VDB5UN16.SQL for CA IDMS r16
   - VDB5UN17.SQL for CA IDMS r17
   - VDB5UN18.SQL for CA IDMS Version 18.0 and 18.5

4. Repeat the previous two steps for each dictionary you want to uninstall.

Note: The VDB5UNxx.SQL scripts are found in the appropriate IdmsR16x, IdmsR17x, or IdmsV18x folder underneath the CA IDMS Visual DBA Version 18 product folder.

Alternately, you can upload the VDB5UNxx.SQL file to the mainframe and run an IDMSBCF batch job to execute the script. The IDMSBCF batch job must be run against each dictionary for which CA IDMS Visual DBA Version 18 SQL definitions are to be uninstalled.

CA IDMS Visual DBA Version 18 Reinstallation

To reinstall CA IDMS Visual DBA Version 18 on top of an existing Version 18 installation, you must first uninstall both the PC Client and the mainframe SQL definitions of the existing version.

Note: For more information on installing these components, see the Section Installing CA IDMS Visual DBA (see page 85).

VARBLIST Variables

The VARBLIST variables topics assist you with configuration decisions and provides detailed information for variables that must be specified in the VARBLIST file before running CAISAG.

If this is a complete base configuration of CA IDMS, the default dictionary and database file sizes are sufficient for generating a small system to test the installation. File sizes used in an earlier configuration are a better indication of the sizes needed for your environment.
Member Name

BEGINMEM=member-name

This variable establishes the member names for all the generated configuration jobs. The configuration jobs are created in the SAMPJCL library. The member-name is one to six alphanumeric characters. Two numbers are appended by CAISAG to create unique member names.

This feature allows you to create multiple versions of the configuration jobs while maintaining a record of the original configuration.

Example

After installing CA IDMS, you decide to configure an additional CA IDMS product. By changing the BEGINMEM value, a history is maintained of the original complete base configuration as well as the new add-on configuration.

Products

product-code=YES
NO

This variable specifies the product name of a product to configure. For a listing of the available products, see CA IDMS Product List.

To configure a particular product, change its value in VARBLIST from NO to YES.

Note: To access a DC/UCF system from CICS, install and configure CA IDMS CICS Support and CA IDMS UCF.

Global DMCL

GJGLDMCL=dmcl-name

This variable specifies the name of the global DMCL. If you are performing a CA IDMS complete base configuration, this specifies the new global DMCL; otherwise, specify the name of the current global DMCL.

Upgrade Configuration 1

GJUPGRAD=YES
NO
An upgrade is for sites that are currently running CA IDMS at an earlier release. An upgrade is available for CA IDMS Release 12.0 and later, and may update database areas, but does not allocate or format database areas.

The default is NO, indicating that this is not an upgrade.

If you choose an upgrade, (YES), you must specify the name of the existing global DMCL in the GJGLDMCL variable (see Global DMCL (see page 101)). Upgrades adhere to the following actions:

- CAISAG ignores all parameters for database file allocation.
- Additional products cannot be configured.

**Important!** If you are running CA IDMS Release 10.2 (or earlier), you cannot utilize the upgrade.

### Tape Class

TAPCLASS=T

This variable specifies the job class to be used for jobs requiring a tape mount. For jobs requiring a tape mount, CAISAG automatically substitutes the tape class in the CLASS= parameter on the jobcard.

### Disk VOLSER and Disk Contention

GJxxxxSER=volume

This variable allows you to specify the pack on which to allocate the data set. For every data set created by the configuration process, there is a corresponding variable designating the disk VOLSER. If you want the operating system to choose the pack, specify a null value (two single quotes) for the GJxxxxSER variable. Or you can specify the following:

PACK = ''
GJxxxxSER = @PACK@

The GJxxxxSER variable is useful for reducing or eliminating disk contention issues. Areas such as the DDLDCLOD, DDLDCLOG, and DDLDCMSG areas are used heavily at runtime and should be assigned to separate DASD to reduce disk contention.

Journal file placement is important; for optimum performance allocate four journal files on separate DASD. The optimum allocation when you have two disk drives is as follows:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Disk 1</th>
<th>Disk 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journal 1</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
The optimum allocation when you have three disks is as follows:

<table>
<thead>
<tr>
<th>File Name</th>
<th>Disk 1</th>
<th>Disk 2</th>
<th>Disk 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journal 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Journal 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Journal 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Journal 4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**CV Number**

GJCVNUM=nnn

The CV number identifies the DC/UCF system to the SVC. Each SVC contains 256 slots used for communication between address spaces. The CV number specifies the slot used by a particular CV. Valid values for the CV number are 0 through 255. If two central versions are assigned the same CV number, they cannot execute concurrently.

**DC System Number**

GJDCSYS=nnnn

The DC system number uniquely identifies a DC/UCF system. It identifies the system being generated, modified, copied, or deleted. Valid values are 1 through 9999, and the DC system numbers must be unique. Many sites use the same number for the DC system and the CV number (see CV Number) assigning a value from 1 to 255.

The DC system number can be specified in the S= parameter on the EXEC card in the startup deck (JCL to bring the system up).

**Important!** Do not assign DC system numbers 90 and 99. These system numbers are reserved for use by CA IDMS during the configuration process.

**Free Storage**

GJFRESTG=nnnn (default=1700)
The amount of storage, in kilobytes returned (freed) to the operating system at DC/UCF startup time. The storage is freed for operating system use during DC/UCF startup operations. GJFRESTG must specify a positive integer storage amount.

The free storage amount can be specified by using the FSTG= parameter on the EXEC statement in your CV startup JCL. If you have included an RHDCPARM module with your CV startup module, the free storage value specified using the FSTG= parameter will override the value in the RHDCPARM module. For more information on #DCPARM or FREESTG, see the Administrating section.

Operating system abends due to insufficient memory during startup are likely the result of an inadequate amount of storage specified in the GJFRESTG variable.

The GJFRESTG variable also affects the amount of storage available to the operating system for extending the LSQA at runtime.

**Uppercase Terminal Support**

GJCASE=MIXED
UPPER

CA IDMS products support both uppercase and mixed case installations. If site requirements prohibit displaying mixed-case characters, specify UPPER. This often occurs due to language issues, not hardware limitations.

**Authorized Userid**

GJAUTH=userid

The GJAUTH and GJAUTHPW variables should be left with null values unless you are doing an upgrade configuration or add-on configuration and your dictionaries are secured.

**VTAM ID**

GJVTAMID='' applid

This variable is used only for those sites configuring CA IDMS/DC. If left null, the default, no VTAM line is configured. Otherwise, specify the name of the APPLID.

**CWA Displacement**

GJnga=nn

This variable is for sites configuring CA IDMS CICS support. CA IDMS CV requires exclusive use of a fullword in the CICS CWA. Specify the decimal displacement of this fullword relative to zero from the start of the CWA.
Add-On Variables

GJNUMJRN= ''
DMCLSAVE= ''
DBTBSAVE= ''

When you configure CA IDMS for the first time, CA IDMS/DB is a required product. Subsequent configurations for additional products are known as add-on configurations.

The following variables pertain to manual add-on configurations only:

- GJNUMJRN specifies the number of disk journals defined to the system.

- DMCLSAVE specifies a backup load module name. If you are configuring the SQL option or the ASF option, your current DMCL load module will be renamed to this name, and a new DMCL load module containing the new segments will be created using your current DMCL load module name, taken from the GJGLDMCL= variable. If you are not configuring the SQL option or the ASF option with an add-on configuration, this variable is ignored.

- DBTBSAVE specifies a backup load module name. If you are configuring the SQL option or the ASF option, your current DB name table load module will be renamed to this name and a new DB name table load module will be created using the GJGLDBTB= name.

For a manual add-on configuration, we recommend changing the value of the BEGINMEM variable to avoid overwriting your original configuration jobs.

Page Size

GJxxPSZ=nnnnGJXARENT=nnnn

The default page sizes are based on 3390 disk drives. Specify a page size appropriate for your DASD.

If the XA program reentrant pool is large enough, programs are loaded once per CV cycle. If contention occurs in the XA program pools, you can reduce runtime I/O by increasing the default page size for the dictionary load (DDLDCLOD) area from the default of 5064.

You may also want to consider startup resources. Buffer space is defined in the DMCL; the larger the database page sizes, the larger the buffer size. It is possible to create a DMCL that has millions of bytes in the buffer pool depending on the:

- Number of buffers
- Size of the database pages
- Number of pages allocated in each buffer pool

The larger the buffer pool, the more startup resources CV requires.
CA Common Services for z/OS

GJSTEPL1=dsname

When the GJSTEPL1 variable is coded, a user-defined library is added to the appropriate steps in the generated configuration JCL.

Ensure one of the following conditions is met prior to starting the CA IDMS configuration process:

- The CA Common Services for z/OS load library is in your z/OS system LNKLST concatenation.
- The CA Common Services for z/OS load library is in the STEPLIB concatenation in all database jobs of the CA IDMS configuration process. The CA Common Services for z/OS load library must be placed last in the concatenation.

CVKEY

GJCVKEY=nn

A primary protect key can be specified to restrict use of the SVC. For more information, see Creating a Secured CA IDMS System on z/OS.

Log and Task Analyzer Billing Information

WIGSISVC = YES
NO

WIGSISVC should be set to YES if you are configuring CA IDMS Log Analyzer or CA IDMS Task Analyzer. It modifies the CA IDMS SVC to access job accounting data and copy it into the ERE. If GSISVCX is not invoked by the CA IDMS SVC, the CA IDMS Log Analyzer and CA IDMS Task Analyzer Billing Reports and the CA IDMS Log Analyzer Billing Record File will not contain valid billing data for external run units. The CA IDMS Log Analyzer and CA IDMS Task Analyzer Billing Reports and the CA IDMS Log Analyzer Billing Record File are dependent upon this ERE data.

CA Endevor/DB Message Library

ABMSGDSN = msg. = ' '

If CA Endevor SCM is installed at your site, specify the name of the message library here, otherwise leave the null value. If you specify a library name, messages will be copied from the CAGJMSG library into the library you specify.
Variables for SQL Web Connect

The following sections describe the variables available for base, upgrade and add-on configurations with respect to the SQL Web Connect feature.

- **Base Configuration** (see page 107)
- **Upgrade Configuration** (see page 107)
- **Add-On Configuration** (see page 108)

**Base Configuration**

SYSSQL = YES

NO

The SYSSQL variable governs the creation of System SQL Catalog within the APPLDICT dictionary, on a ‘Base’ installation. The SQL Catalog is a required component for using SQL with SQL WEB Connect. Users who have purchased the CA IDMS SQL Option automatically receive this component.

SQLDEMO = YES

NO

The SQLDEMO variable governs the creation of the SQL version of the Employee Skills Demo Database on a ‘Base’ installation.

**Upgrade Configuration**

UPGSYSQL = YES

NO

The UPGYSQL variable governs the creation of System SQL Catalog within the APPLDICT dictionary, on an ‘Upgrade’ installation. The SQL Catalog is a required component for using SQL with SQL WEB Connect.

Users who purchased the CA IDMS SQL Option normally already have this component, just like Visual DBA users.

The addition of the SQL Catalog requires updates to both the global DMLC and Database name Table of your CV.

UPGQDEMO = YES

NO

The UPGQDEMO variable governs the creation of SQL version of the Employee Skills Demo Database on an ‘Upgrade’ installation.

Specify NO if you have already installed the SQL version of the Employee Skills Demo Database. The Employee Skills database has not changed since Release 12.0.

The addition of the Employee Skills database requires updates to both the global DMLC and Database name Table of your CV.
Add-On Configuration

ADDSYSQL = YES
NO

The ADDYSQL variable governs the creation of System SQL Catalog within the APPLDICT dictionary, on an ‘Add-On’ installation. The SQL Catalog is a required component for using SQL with SQL Web Connect.

The addition of the SQL Catalog requires updates to both the global DMLC and Database name Table of your CV.

ADDQDEMO = YES
NO

The ADDQDEMO variable governs the creation of the SQL version of the Employee Skills Demo Database on an ‘Add-On’ installation.

The addition of the Employee Skills database requires updates to both the global DMLC and Database name Table of your CV.

Installing Your Product from Tape

The following topics cover all aspects of tape installation in the recommended sequence:

- Download the SAMPJCL Library from Tape (see page 108)
- Modify the Receive Job (see page 109)
- Customize the AGJSEDIT Edit Macro (see page 109)
- Make the AGJSEDIT Edit Macro Accessible (see page 110)
- Create Your SMP/E System (see page 110)
- Install Maintenance on Your SMP/E System (see page 111)
- Deploy and Configure Your Product (see page 114)

Download the SAMPJCL Library from Tape

The SAMPJCL library contains all jobs necessary to complete the SMP/E portion of the installation. Customize the following IEBCOPY job to download the SAMPJCL library from the tape:

```plaintext
//DOWNLOAD EXEC PGM=IEBCOPY,REGION=4096K
//SYSPRINT DD SYSOUT=* 
//SYSUT1 DD DSN=CAI.SAMPJCL,DISP=OLD,
//UNIT=tapeunit, 
//VOL=SER=CAGJI5, 
//LABEL=(1,SL)
```
Modify the Receive Job

Change the Receive job (AGJ4RECD) into a tape job.

Follow these steps:

1. Change 'DASD' to 'tape' in line 11 (for future reference).
2. Delete line 31 that contains:
   
   `RFPREFIX(DASDHLQ)`
3. Replace the SMPPTFIN DD statement on line 27 with the following three lines and customize the tape unit:

   ```
   SMPPTFIN DD DISP=SHR,DSN=CAI.SMPMCS,
   //UNIT=(tapeunit,,DEFER),VOL=SER=CAGJI5,
   //LABEL=(2,SL)
   ```

Customize the AGJSEDIT Edit Macro

The AGJSEDIT member in SAMPJCL is an edit macro and needs to be customized.

To customize AGJSEDIT, follow the instructions in the member. The rightmost parameters for each ISREDIT change command are the ones to replace with the values for your site. The DASDHLQ value does not have to match anything because you are using a tape, but it should be a legal high-level-qualifier for your site.
Make the AGJSEDIT Edit Macro Accessible

The AGJSEDIT edit macro is executed to customize each installation job. Before you can execute the macro, it must be made accessible to your TSO session. To do so, copy the member to a library in your SYSPROC concatenation. Use the following command to see the libraries in your SYSPROC concatenation:

```
TSO ISRDDN ONLY SYSPROC
```

**Note:** You must have the update authority for the library in the SYSPROC concatenation to which you copy the AGJSEDIT member from SAMPJCL. If you do not have the update authority to any of the libraries in your SYSPROC concatenation, ask your systems programmer for help.

Create Your SMP/E System

**Contents**

- How to Use an Edit Macro (see page 110)
- Customize and Submit Jobs in SAMPJCL (see page 111)

SAMPJCL contains six jobs to create your SMP/E environment and install the untailored CA IDMS modules. Instead of making global changes in these jobs, customize them using the AGJSEDIT edit macro.

How to Use an Edit Macro

An edit macro is a specialized kind of CLIST that contains edit commands. An edit macro has to be executed from within the member you are editing (and not from ISPF Option 6 as you execute a CLIST). You must be in EDIT mode, not in BROWSE mode.

To execute the customized AGJSEDIT edit macro, type AGJSEDIT on the command line of the member you are editing. AGJSEDIT makes global changes in the member you are editing. If you get the following message, the AGJSEDIT member is not accessible to your TSO session:

```
IKJ56500I COMMAND AGJSEDIT NOT FOUND.
```

After you have used AGJSEDIT to customize an installation job, submit the job, but do not exit the member until the job finishes successfully. If the job fails, CANCEL out of the member, make corrections to the AGJSEDIT member in the SYSPROC concatenation, and try again.
Customize and Submit Jobs in SAMPJCL

Customize (using AGJSEEDIT) and submit the following jobs in SAMPJCL to create the SMP/E environment and install the untailored software. Comment out any FMIDs for products you are not installing in the SMP/E jobs (AGJ4RECD, AGJ5APP, and AGJ6ACC).

1. AGJ1HOLD Downloads external HOLDDATA
2. AGJ2ALL Allocates IDMS and SMP/E datasets
3. AGJ3CSI Defines the SMP/E CSI
4. AGJ4RECD RECEIVE
5. AGJ5APP APPLY
6. AGJ6ACC ACCEPT

⚠️ **Note:** The Receive job (AGJ4RECD) is a tape job. Before submitting it, you can add /*SETUP cards or change the job class.

Install Maintenance on Your SMP/E System

Install maintenance on your SMP/E system using one of the following approaches:

- Follow the directions in the Apply Preventive Maintenance section which follows below.
  or
- Use CA CSM to install maintenance. To do so:

  1. Access CA CSM.
  2. Click the SMP/E Environments tab.
  3. Click the Migrate SMP/E Environment link under Actions on the left side of the screen to bring up the Migrate wizard.
  4. Click NEXT until the dialog ends (unless a prefix value needs to be corrected).
     Now CA CSM knows about your SMP/E environment and you can install maintenance using CA CSM.

⚠️ **Note:** You can also complete the installation (that is, perform deployment and configuration) using CA CSM.
Apply Preventive Maintenance

**Important!** We strongly recommend that you use CA CSM to maintain your CA Technologies z/OS-based products. The procedure that is discussed in this section is fully automated when you use CA CSM.

CA Support Online has maintenance and HOLDDATA published since the installation data was created. After the maintenance process completes, the product is ready to deploy.

Use this procedure during product installation and for ongoing preventive maintenance in non-installation use cases according to your maintenance strategy.

**Note:** To review the CA Technologies mainframe maintenance philosophy, see your Best Practices Guide or visit the CA Next-Generation Mainframe Management page (https://support.ca.com/phpdocs/0/8319/mainframe20_support.html).

This procedure directs you to use the CAUNZIP utility. The CAUNZIP utility processes ZIP packages directly on z/OS without the need for an intermediate platform, such as a Microsoft Windows workstation. If you are not familiar with this utility, see the CA Common Services for z/OS Administration section. This section includes an overview and sample batch jobs. To use this utility, you must be running CA Common Services for z/OS Version 14.0 with PTF RO54887 or CA Common Services for z/OS Release 14.1 with PTF RO54635.

**Follow these steps:**

1. Check the Download Center for PTFs that have been published since this release was created. If the base release was created recently, no PTFs will have been published yet. If PTFs exist, add published solutions for your product to your Download Cart, and click Checkout.

2. Specify that you want a complete package. When processing completes, a link appears on the Review Download Requests page. You also receive an email notification.

3. Click the Alternate FTP link for your order to obtain FTP login information and the ZIP file location. Download the ZIP file into a USS directory on your z/OS system.

4. Run the CAUNZIP utility. CAUNZIP unzips the package of published solutions and creates a SMPNTS file structure that the SMP/E RECEIVE FROMNTS command can process. For sample JCL to run the utility that is located in yourHLQ.CAW0JCL(CAUNZIP), see the CA Common Services for z/OS CAUNZIP Administering section. After execution completes, the ZIPRPT data set contains the summary report. The summary report does the following:

   - Summarizes the content of the product order ZIP file.
Details the content of each data set and the z/OS UNIX files produced.

Provides a sample job to receive the PTFs in your order.

5. Review the sample job that is provided in the CAUNZIP output ZIPRPT file. Cut and paste the JCL into a data set, specify your SMP/E CSI on the SMPCSI DD statement and submit the job to receive the PTFs in your order.

6. Verify that you have the values from the base installation in the AGJSEDIT macro that was customized in the installation steps.

7. Open the SAMPJCL member AGJ1HOLD in an edit session and execute the AGJSEDIT macro from the command line.

⚠️ **Note:** Update AGJ1HOLD SAMPJCL to download the HOLDDATA file.

AGJ1HOLD is customized.

8. Submit AGJ1HOLD.
The job downloads the external HOLDDATA file.

9. Open the SAMPJCL member AGJ7RECH in an edit session and execute the AGJSEDIT macro from the command line.
AGJ7RECH is customized.

10. Submit AGJ7RECH.
The job receives the external HOLDDATA file.

11. *(CA Recommended Service (CA RS)) installation only)* Do the following:

   a. Determine which ASSIGN statements to download.

      - The yearly CA RS ASSIGN statements are stored in the following file:
        ftp.ca.com/pub/ASSIGN/YEARLY/CARyyyy.TXT
        ftp.ca.com/pub/ASSIGN/CARyyymm.TXT

      - The quarterly CA RS ASSIGN statements are stored in the following file:

   b. Open the SAMPJCL member AGJ7CARS in an edit session, update AGJ7CARS SAMPJCL to download ASSIGN statements from CA Support and execute the AGJSEDIT macro from the command line.

AGJ7CARS is customized.

12. *(CA RS installation only)* Submit AGJ7CARS.
The job downloads the CA RS ASSIGN statements.
13. (CA RS installation only) Open the SAMPJCL member AGJ7RECP in an edit session, manually add the data set that contains the ASSIGN statements to the SMPPTFIN DD, and execute the AGJSEDIT macro from the command line. AGJ7RECP is customized.

14. (CA RS installation only) Submit AGJ7RECP. The job receives the external HOLDDATA file and CA RS ASSIGN statements.

15. Open the SAMPJCL member AGJ8APYP in an edit session and execute the AGJSEDIT macro from the command line. AGJ8APYP is customized.

16. Submit AGJ8APYP. The PTFs are applied.

17. (Optional) Open the SAMPJCL member AGJ9ACCP in an edit session and execute the AGJSEDIT macro from the command line. AGJ9ACCP is customized.

18. (Optional) Submit AGJ9ACCP. The PTFs are accepted.

Note: You do not have to submit the job at this time. You can accept the PTFs according to your site policy.

HOLDDATA

When you apply maintenance, you typically encounter SMP/E HOLDDATA. We use HOLDDATA to notify your SMP/E system of SYSMODs that have errors or special conditions. We support system and external HOLDDATA.

Deploy and Configure Your Product

Perform deployment and configuration to complete the installation using one of the following methods:

- Use CA CSM to complete the installation; in this case both deployment and configuration are required. For more information, see the Deploying Products and Configuring Products sections in the CA Chorus Software Manager Using section

- Complete the installation manually; in this case deployment is not required. For more information on configuration, see Starting Your Product (see page 47).