

# CA Chorus™ Software Manager

## Site Preparation Guide

Release 5.1



51000068XPG, Fourth Edition

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

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

## CA Technologies Product References

This document references the following CA Technologies products:

- CA Chorus™ Software Manager (CA CSM)
- CA ACF2™ for z/OS
- CA Chorus™
- CA Common Services for z/OS
- CA Database Management Solutions for DB2 for z/OS
- CA Datacom/MSM
- CA Distributed Security Integration for z/OS (CA DSI Server)
- CA PDSMAN® PDS Library Management (PDSMAN)
- CA Top Secret® for z/OS

## Contact CA Technologies

### Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At <http://ca.com/support>, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

### Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to [techpubs@ca.com](mailto:techpubs@ca.com).

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at <http://ca.com/docs>.



# Contents

---

<b>Chapter 1: Overview</b>	<b>9</b>
Audience .....	9
Required Skills .....	9
How to Prepare for CA CSM Installation .....	10
<b>Chapter 2: Check Requirements and Ports</b>	<b>11</b>
Disk Space Requirements .....	11
Software Requirements .....	12
z/OS Configuration .....	15
CSF Initialization .....	15
Web Access Requirements .....	16
TCP/IP Port Reservation .....	17
<b>Chapter 3: Set Up Security</b>	<b>19</b>
Access Requirements to Download, Install, and Set Up CA CSM .....	19
Access Requirements for User ID Associated with the CA CSM Application Server .....	21
Set Up USS Authorization for Users .....	22
CA CSM Associated Security IDs - OMVS Segment and Home Directory .....	24
SAF Check During SMP/E Processing .....	24
<b>Chapter 4: Use the CA CSM Prerequisite Validator Utility</b>	<b>25</b>
Prepare for Installation .....	25
Verify the Prerequisite Validator Requirements .....	25
Download the Prerequisite Validator Product Package .....	26
Execute from Native USS Command Prompt .....	27
Modify Default Properties .....	28
<b>Chapter 5: Set Up Security for CA CSM with CA ACF2 for z/OS</b>	<b>31</b>
How to Set Up User Security .....	31
Example: Set Up Security for Administrators .....	32
Example: Set Up Security for Users .....	33
Example: Set Up Security for Restricted Users .....	34
How to Set Up SCS Address Space Security .....	36
Set Up SCS Address Space Security .....	37
Configure PassTickets .....	37

---

## **Chapter 6: Set Up Security for CA CSM with CA Top Secret for z/OS** **41**

How to Set Up User Security .....	42
Define the CAMSM Resource Class .....	42
Define Security Profiles .....	43
Attach Security Profiles to Users.....	45
Set Up Started Task Security .....	46
How to Set Up SCS Address Space Security.....	46
Set Up SCS Address Space Security .....	47
Configure Passtickets.....	48

## **Chapter 7: Set Up Security for CA CSM with IBM RACF** **51**

How to Set Up User Security .....	52
Define the CAMSM Resource Class .....	52
Define the Group Profiles.....	53
Connect Users to the Group Profiles.....	55
How to Set Up SCS Address Space Security.....	56
Set Up SCS Address Space Security .....	57
Configure Passtickets.....	57

---

## Documentation Changes

### 4th Edition (May 2014)

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

- Reorganized the chapters
- [Set Up Security](#) (see page 19): added this chapter
- Check Requirements and Ports > [Software Requirements](#) (see page 12): updated the section
- [Required Skills](#) (see page 9): added this section
- [Check Requirements and Ports](#) (see page 11): renamed the chapter





# Chapter 1: Overview

---

This guide describes the preparation that you should do before you install CA CSM Release 5.1 or upgrade CA CSM to the latest version.

This section contains the following topics:

[Audience](#) (see page 9)

[Required Skills](#) (see page 9)

[How to Prepare for CA CSM Installation](#) (see page 10)

## Audience

This guide details the tasks that a system programmer and security administrator can complete before you begin the installation or upgrade tasks that the *Installation Guide* describes. Following this Site Preparation Guide can dramatically simplify your installation experience.

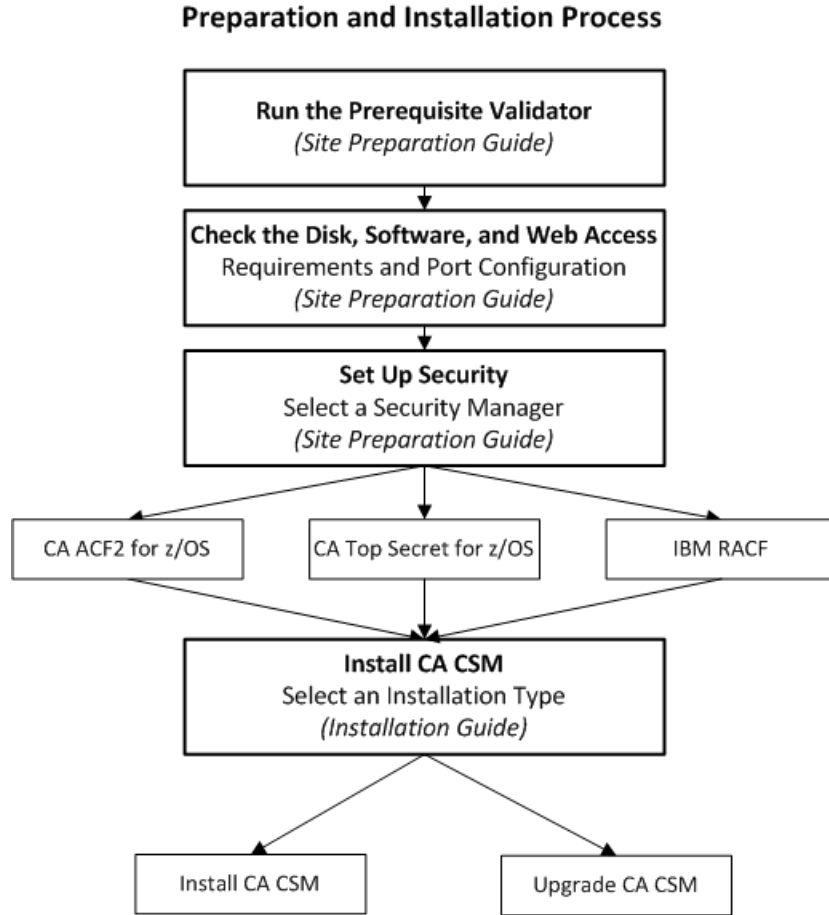
## Required Skills

Performing the tasks that this guide describes is a team effort that requires the following skills:

- z/OS UNIX System Services (USS) and file systems, to set up a functional UNIX and file systems environment
- Security server (for example, CA ACF2 for z/OS, CA Top Secret for z/OS, or IBM RACF) or the security product you use, to authorize access to resources
- Java for z/OS
- CA Common Services for z/OS
- Network administration, to set up access for acquiring and downloading product packages

## How to Prepare for CA CSM Installation

The following diagram provides a high-level overview of the CA CSM preparation and installation process and the guides that you use to complete it.



To prepare for installation and upgrade of CA CSM, complete the following steps:

1. Run the Prerequisite Validator utility as described in the *Site Preparation Guide*.
2. Verify the disk, software, and web access requirements, and port configuration as described in the *Site Preparation Guide*.
3. Set up security requirements as described in the *Site Preparation Guide*.
4. Install CA CSM Release 5.1 or upgrade your existing version of CA CSM to Release 5.1 as described in the *Installation Guide*.

# Chapter 2: Check Requirements and Ports

---

Verify that disk requirements, software requirements, and web access requirements are met, and the TCP/IP ports are configured.

This section contains the following topics:

[Disk Space Requirements](#) (see page 11)

[Software Requirements](#) (see page 12)

[Web Access Requirements](#) (see page 16)

[TCP/IP Port Reservation](#) (see page 17)

## Disk Space Requirements

CA CSM has the following disk space requirements:

**Note:** All space allocations are described for 3390 DASD.

- For the installation and setup of CA CSM:
  - Hierarchical File System (HFS) or zSeries File System (zFS) space = 680 cylinders

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

**Important!** Starting from z/OS V2.1, IBM has changed the way the utility program IOEAGFMT (zFS data set formatter) functions. The utility requires the zFS kernel address space to be active before any execution of IOEAGFMT is allowed. If you use zFS file systems at your site, you must ensure that zFS kernel address space is active. For more information, see the *IBM z/OS Distributed File Services zFS Administration*.

- z/OS space = 678 cylinders  
This space contains the CA Datacom/MSM SMP/E environment and runtime libraries. The SMP/E environment contains the CA Datacom/MSM, [assign the DSV variable value for your book], and CA CSM components.
- A TSO region = 143360 KB (at minimum)
- SDS root space = 100 tracks (approximately)

For the Software Deployment Service (SDS), the aggregated amount of DASD space for the initial DASD setup is 100 tracks. This amount includes CA CSM and SDS space on the CA CSM host only, and does *not* include space for the deployment snapshot file system. Additional space is needed for the SDS target system.

- SDS deployment space = 500 cylinders

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

- For the operation of CA CSM:

After initial setup, CA CSM allocates additional HFS or zFS files depending on the download of products and maintenance. The amount of space that is allocated varies depending on the number of products and maintenance, and the size of any associated files.

## Software Requirements

CA CSM has the following *minimum* software requirements:

### CA Technologies software

Your system must have CA Common Services for z/OS Release 14.1, Version 14, or r12.

- Verify that CETN500 is applied to CA CSM driving system, and all the target systems for the Software Deployment Service (SDS) and the Software Configuration Service (SCS).

When you install CETN500 into CA Common Services for z/OS r12 or Version 14, it replaces CETN300 or CETN400.

**Note:** Apply all published CETN500 maintenance, deploy to all target systems, and verify that HOLDDATA instructions are completed. If you do not apply CETN500, CA CSM is operational; however the Software Configuration Service (SCS) and the Software Deployment Service (SDS) are unavailable.

- Apply PTFs RO17488, RO19624, RO41046, RO42868, and RO43995 to r12.

If you do not plan to use the SDS, you can skip PTFs RO19624 and RO42868.

For passing APPLID on CAICCI authentication calls, apply PTF RO37409. PTF RO18999, which is also required, is automatically applied as part of RO42868.

- Apply PTFs RO40945, RO44235, and RO44412 to Version 14.

If you do not plan to use the SCS, you can skip PTF RO44235.

For passing APPLID on CAICCI authentication calls, apply PTFs RO30506, RO30937 and RO33987.

CA Common Services for z/OS load libraries CAW0LOAD and CAW0PLD (Release 14.1 and Version 14.0) or CAIPLD (r12), must be accessible to CA CSM through the Job Control Language or system LINKLST. The following services are required:

- CAICCI

**Note:** CAICCI must be configured and running on CA CSM driving system and on all the target systems for the SDS and the SCS.

- CAIENF

- CAIRIM

- CA-C Runtime

**Note:** For more information about CA Common Services for z/OS, see the CA Common Services for z/OS user documentation.

If you have other CA Technologies software products, verify that you have installed mandatory maintenance for these products:

- If you use CA ACF2 for z/OS, apply PTF RO31548 to CA ACF2 for z/OS r14. Alternatively, apply PTF RO30898 to CA ACF2 for z/OS r15.
- If you use CA Top Secret for z/OS, apply PTF RO31780 to CA Top Secret for z/OS r14. Alternatively, apply PTF RO30836 to CA Top Secret for z/OS r15.
- If you use CA PDSMAN on your SCS target system, apply PTF RO26804 to CA PDSMAN r7.6. Alternatively, apply PTF RO25866 to CA PDSMAN r7.7.

### IBM software

Your system must satisfy the following requirements:

- Your system has the latest version of z/OS or the last previous version. IBM supports the most currently announced GA version plus the one previous version.
- Your system uses the TCP/IP protocol suite of z/OS Communications Server, with the FTP.DATA data set that is configured with the JESINTERFACELEVEL 2 statement. When installation jobs are submitted through FTP, the CA CSM installation process requires the JESINTERFACELEVEL 2 statement to obtain job status and output. You can return the JESINTERFACELEVEL to its previous value after CA CSM is successfully installed.

Alternatively, you can configure the CA CSM installation process to use TSO for job submission and processing.

- Your system has at least SMP/E V3R5.

- Your system has IBM Java SDK for z/OS:
  - Java 6.0, build 2.4, at maintenance level SR9 (31 bit or 64 bit).
  - Java 6.0, build 2.4, at maintenance level SR10 (31 bit or 64 bit).
  - Java 6.0, build 2.6, base build (31 bit or 64 bit).

**Note:** Java 6.0, build 2.6 is the equivalent of IBM Java 6.0.1. For Java 6.0, install PTF UK56434, APAR PM08437, SDK6 SR8.

  - Java 6.0.1, build 2.6, at maintenance level SR1 (31 bit or 64 bit).
  - Java 7.0, build 2.6 (31 bit or 64 bit).

You can download the software in non-SMP/E installable format. For more information, go to the following website and click the link to the software: <http://www-03.ibm.com/servers/eserver/zseries/software/java/>. This web page lists the available IBM SDK releases. The release link redirects you to a more detailed web page. The detailed page usually has a link in the text for *additional install information*. The page that opens from this link can have helpful information to customize the JZOS Batch Launcher function that CA CSM uses. For example, this information can help you create an alternate JVM loadlib for CA CSM, if that is a preferred configuration at your site.

- Your Language Environment library CEE.SCEERUN2 is APF-authorized.

### PC software

The computer that is used to access CA CSM must have at least one of the following web browsers:

- Mozilla Firefox 13, 14, 15, or 16
- Microsoft Internet Explorer 7, 8, or 9
- Microsoft Internet Explorer 10 (compatibility mode only)

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

We recommend you use Mozilla Firefox.

Verify that your web browser has JavaScript and cookies that are enabled for the server where CA CSM is running.

**Note:** The recommended screen resolution is 1024 x 768 pixels or higher. If you have a lower screen resolution, some elements of the CA CSM web-based interface do not display properly.

## z/OS Configuration

To run the CA CSM installer utility and CA CSM application server successfully, specify the following OMVS limits in SYS1.PARMLIB(BPXPRMxx):

**MAXASSIZE(nnnnn)**

Set to 2147483647.

**MAXCPUIME(nnnnn)**

Set to at least 20000.

**MAXFILEPROC(nnnnn)**

Set to at least 10000.

**MAXTHREADS(nnnnn)**

Set to at least 1000.

**MAXTHREADTASKS(nnnnn)**

Set to at least 1000.

**Note:** To display current settings, issue the following command:

```
DISPLAY OMVS,OPTIONS
```

You can use the SETOMVS operator command to change these values dynamically without performing the IPL of the operating system. To change them dynamically, issue the following operator commands:

```
SETOMVS MAXASSIZE=2147483647
SETOMVS MAXCPUIME=20000
SETOMVS MAXFILEPROC=10000
SETOMVS MAXTHREADS=1000
SETOMVS MAXTHREADTASKS=1000
```

## CSF Initialization

The CA CSM application server (MSMTC) tries to set a random file in use to track its user sessions. If one is created, CA CSM uses it. The creation of this file is performed in the base Apache Tomcat application regardless of the platform. If this file cannot be set, the CA CSM application uses its own logic to track user sessions. In z/OS, the successful creation of the random file requires that your site has an Integrated Cryptographic Services Facility (ICSF) processor that is attached and enabled. If your site does not have the ICSF processor, CA CSM issues messages similar to the following example, and continues to initialize:

```
Aug 5, 2010 4:56:37 PM org.apache.catalina.session.ManagerBase setRandomFile
WARNING: Failed to close randomIS.
```

If an ICSF processor is enabled, initialize the CSF address space completely before starting the CA CSM application server (MSMTC). If you do not initialize the CSF address space, CA CSM fails; and it fails without retrying. Perform a recycle of the MSMTC started task to recover.

If you have an ICSF processor that is attached to your LPAR, we recommend that you use your system automation software to add the CSF started task as a prerequisite to the start of the MSMTC started task.

Ensure that you only start the MSMTC started task after a successful initialization of the CSF address space. Set your system automation software to look for the following CSF initialization messages:

CSFM001I ICSF INITIALIZATION COMPLETE

This message signals that the CSF services have been started but are not available and a cipher key has not yet been loaded.

Or

CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.

This message signals that ICSF services are available and a cipher key has been loaded.

**Note:** For more information, see the *IBM z/OS Cryptographic Services PKI Services Guide and Reference (SA22-7693-12)*.

## Web Access Requirements

Your network administrator must configure access to the following websites and FTP sites:

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

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

- scftpd.ca.com (using FTP Port Number 21)



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

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

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

## TCP/IP Port Reservation

We recommend that you reserve these TCP/IP ports:

- CA CSM application server HTTP port
- CA DSI Server port
- CA CSM application server redirect port
- CA CSM application server shutdown port

To reserve the ports, update the z/OS TCP/IP profile data set.

### Example:

```
PORT      Application ID
22120 TCP MSMTC* ; CA CSM Application Server HTTP port
22130 TCP MSMTC* ; CA DSI server port
22140 TCP MSMTC* ; CA CSM Application server redirect port
22150 TCP MSMTC* ; CA CSM application server shutdown port
```

**Note:** We recommend that for security reasons you use an 8-character-long Application ID instead of using asterisks (\*), as shown in the example in this section. To change **MSMTC** to an 8-character-long job name, edit the CA CSM startup JCL (*RunTimeMVSHLQPrefix.JCL(MSMTCSRVR)*). Then, change **MSMTC\*** to the same 8-character-long job name in the z/OS TCP/IP profile data set.

If you use a 5-character-long name for your CA CSM application server, you must use an asterisk (\*) against the CA DSI Server port number definition because of a unique sequence number that is appended to the Application ID.



# Chapter 3: Set Up Security

---

This section contains the following topics:

- [Access Requirements to Download, Install, and Set Up CA CSM](#) (see page 19)
- [Access Requirements for User ID Associated with the CA CSM Application Server](#) (see page 21)
- [Set Up USS Authorization for Users](#) (see page 22)
- [CA CSM Associated Security IDs - OMVS Segment and Home Directory](#) (see page 24)
- [SAF Check During SMP/E Processing](#) (see page 24)

## Access Requirements to Download, Install, and Set Up CA CSM

To download, install, and to set up CA CSM, your security administrator must configure the following access authorities on your system:

1. Access to UNIX System Services (USS) for downloads and the implementation of CA CSM:

If you decide to create and mount new file systems for CA CSM, you need *one* of the following authorities:

- If your site uses CA SAF HFS security, BPX.CAHFS.CHANGE.FILE.ATTRIBUTES
- If your site does *not* use CA SAF HFS security, UID(0) or BPX.SUPERUSER authority

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

2. UPDATE authority to the following data sets or libraries for the user implementing CA CSM:

- SYSx.PARMLIB
- Procedure library that stores the JCL jobs that are used to start the CA CSM address spaces, for example, SYS3.PROCLIB
- (Optional) The master catalog if you decide to define alias entries for the CA CSM data set prefixes

3. Access for the user ID associated with the CA CSM setup utility:

- Permission to access the following FACILITY class profiles that are related to UNIX:
  - BPX.FILEATTR.APF (READ authority)
  - BPX.FILEATTR.PROGCTL (READ authority)
  - BPX.FILEATTR.SHARELIB (READ authority)

- BPX.DAEMON (READ authority)
- BPX.SERVER (UPDATE authority)
- BPX.CONSOLE (READ authority)
- Permission to access the SERVAUTH class profile, EZB.STACKACCESS (READ authority)
- Permission to access the CSFSERV class profile, CSFOWH (READ authority) providing you want to perform SMP/E GIMUNZIP hash validation
- Permission to create and modify data sets for the qualifiers (CA CSM MVS SMP/E and runtime data sets) specified in the options file.  
**Note:** Your user ID can have BPX.SUPERUSER access and it can switch to SUPERUSER. Then the switched SU ID requires a create and modify access to the MVS data set qualifiers specified in the options file.
- If you are using IBM RACF, access to the following data sets for program control:
  - SYSx.MIGLIB
  - CEE.SCEERUN2
  - Members IEANTCR, IEANTDL, and IEANTRT of SYS1.CSSLIB
  - Member JVMLDM60 (for 31-bit Java 6.0) or JVMLDM66 (for 64-bit Java 6.0) of the data set where Java load modules are installed.  
*Or*
  - Member JVMLDM61 (for 31-bit Java 6.0.1) or JVMLDM67 (for 64-bit Java 6.0.1) of the data set where Java load modules are installed.  
*Or*
  - Member JVMLDM70 (for 31-bit Java 7.0.) or JVMLDM76 (for 64-bit Java 7.0)
  - (Optional) member IDIXCEE of SYS1.IDI.SIDIAUTH, only if you use IDIXCEE as an optional exit.

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

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

```
RDEFINE PROGRAM member ADDMEM('h1q.Libraryname'//NOPADCHK) UACC(READ)
```

For example:

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

If the resources exist, issue the following command:

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

For example:

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

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

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

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

## Access Requirements for User ID Associated with the CA CSM Application Server

For CA CSM to operate successfully, the user ID associated with the CA CSM application server (MSMTC job or started task) requires the following access authorities:

1. Your security administrator must configure access to UNIX System Services (USS) for CA CSM. The CA CSM application server user ID must have an OMVS segment with a valid home directory with RDWR access. The CA CSM application server user ID is expected to have UID(0). If you want to configure CA CSM without UID(0), see the *Administration Guide*.
2. Your security administrator must configure the following access:
  - Permission to access the following FACILITY class profiles that are related UNIX:
    - BPX.FILEATTR.APF (READ authority)
    - BPX.FILEATTR.PROGCTL (READ authority)
    - BPX.FILEATTR.SHARELIB (READ authority)
    - BPX.SERVER (UPDATE authority)
    - BPX.CONSOLE (READ authority)
  - Permission to access the SERVAUTH class profile, EZB.STACKACCESS (READ authority)
  - CA ACF2 for z/OS only: MUSASS permission for users who start CA CSM
  - If your site uses CA SAF HFS security, the following access:
    - BPX.CAHFS.SET.RLIMIT (READ authority)
    - BPX.CAHFS.PTRACE (READ authority)
    - BPX.CAHFS.MOUNT (READ authority)

- BPX.CAHFS.UNMOUNT (READ authority)
- BPX.CAHFS.CHANGE.FILE.MODE (READ authority)

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

**Note:** If you are using SAF security, consider the following options:

- If the CSFSERV class is active, verify that the user ID for this request in the CA CSM application server has READ access to CSFRNG and CSFDSV.
- If the APPL class is active, verify that the user ID for the request in the CA CSM application server has READ access to the OMVSAPPL resource.

**Note:** CA CSM executes GIMUNZIP in the security context of the CA CSM application server ID. If SMP/E security is active, the CA CSM application server ID must have READ access to the GIM.PGM.GIMUNZIP resource in the SAF FACILITY class.

## Set Up USS Authorization for Users

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

**Follow these steps:**

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

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

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

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

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

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

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

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

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

**Note:** The OMVS segment must contain the following components:

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

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

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

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

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

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

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

```
LISTUSER uuuuuu OMVS NORACF
```

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

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

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

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

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

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

The following result appears:

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

## CA CSM Associated Security IDs - OMVS Segment and Home Directory

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

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

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

## SAF Check During SMP/E Processing

All CA CSM features that execute SMP/E commands do it in the security context of the user that is logged in to CA CSM and drives these features. Depending on the CA CSM feature, users must have READ access to different sets of SMP/E SAF facility class resources.

**Note:** CA CSM executes GIMUNZIP in the security context of the CA CSM application server ID. If SMP/E security is active, the CA CSM application server ID must have READ access to the GIM.PGM.GIMUNZIP resource in the SAF FACILITY class.

**Note:** For more information about how to enable SAF check, see the *Administration Guide*.

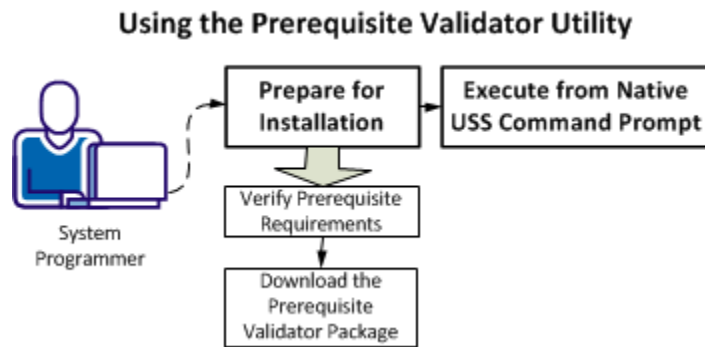


# Chapter 4: Use the CA CSM Prerequisite Validator Utility

---

The Prerequisite Validator utility helps you ensure that all necessary security authorizations are in place before you install CA CSM.

You perform the following tasks to verify that all necessary authorizations are in place before you begin your installation tasks:



1. [Prepare for installation](#) (see page 25).
  - a. [Verify the Prerequisite Validator requirements](#) (see page 25).
  - b. [Download the Prerequisite Validator product package](#) (see page 26).
2. [Execute from native USS command prompt](#) (see page 27).

## Prepare for Installation

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

1. [Verify the Prerequisite Validator requirements](#) (see page 25).
2. [Download the Prerequisite Validator product package](#) (see page 26).

## Verify the Prerequisite Validator Requirements

You must have the following minimum requirements to use this utility:

- The latest version of z/OS or the last previous version
- OMVS segment for the user

- Java

Your system has IBM Java SDK for z/OS:

- Java 6.0, build 2.4, at maintenance level SR9 (31 bit or 64 bit).
- Java 6.0, build 2.4, at maintenance level SR10 (31 bit or 64 bit).
- Java 6.0, build 2.6, base build (31 bit or 64 bit).

**Note:** Java 6.0, build 2.6 is the equivalent of IBM Java 6.0.1. For Java 6.0, install PTF UK56434, APAR PM08437, SDK6 SR8.

- Java 6.0.1, build 2.6, at maintenance level SR1 (31 bit or 64 bit).
- Java 7.0, build 2.6 (31 bit or 64 bit).

- Minimum TSO REGION size 128 MB

- BPX.SERVER READ resource access for verifying SAF resources that are required for CA CSM installation.

**Note:** Prerequisite Validator Utility verifies user access to particular resources and does *not* verify general user access rights (for example, NORESCHK for CA Top Secret for z/OS). The Prerequisite Verification report can indicate that you do not have access to the resources.

## Download the Prerequisite Validator Product Package

The Prerequisite Validator utility is available on [the CA Support Online website](#).

**Follow these steps:**

1. Go to [the CA Support Online website](#), log in, and go to the Download Center.
2. Enter CA Chorus Software Manager in the Select a Product field, select the latest release, and click Go.

**Note:** If you cannot find CA Chorus Software Manager in the product list, click the link *Don't see your product name below?*.

A list of product downloads is displayed.

3. Download the Prerequisite Validator pax file (CA CSM PRE VAL UTIL-ESD ONLY) to a directory in your USS environment.

## Execute from Native USS Command Prompt

Execute the Prerequisite Validator utility using the native USS command prompt in your z/OS system.

**Follow these steps:**

1. Open the native USS command prompt in your z/OS system.
2. Change to the directory where you downloaded the Prerequisite Validator pax file using the following command:

```
cd path_where_Prerequisite_Validator_is_downloaded
```

For example:

```
cd /u/users/MSMpre
```

3. Issue the following command:

```
pax -rvf 51000068XU1.pax.Z
```

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

The Bin folder contents are extracted.

4. Issue the following command:  

```
cd Bin
```
5. (Optional) Modify the [default properties file parameters](#) (see page 28) if necessary.

6. Issue the following command to invoke the utility:

```
./MSMVal.sh JavaHomePath
```

For example:

```
./MSMVal.sh /usr/lpp/java/J6.0
```

The license agreement appears.

7. Review the license agreement, and press F3.

You are prompted to accept the agreement.

Enter **Y** to accept the agreement.

The utility gathers the host name and IP address from the system and attempts an FTP connection to verify the JESINTERFACELEVEL.

- (Optional) If you did not provide a host name when you [modified the default file parameters](#) (see page 28) or the gathered host name fails to connect, provide the host name in response to the prompt. Alternatively, you can provide this value using the default properties file as documented in the subsequent section.

At the end of a successful execution, the Prerequisite Verification report appears in browse mode and the following files are generated:

- MSMPre-RequisiteVerificationReport.txt
- MSMPre-RequisiteLogyyyy-mm-dd,hh-mm-ss,ttt.log

## Modify Default Properties

Some parameters in the Prerequisite Validator utility are populated with default properties.

Modify the default properties file parameters per your site requirements, if necessary.

The following file lets you set default values per your site requirements:

*unpax\_directory/Bin/lib/MSMSetupDefault.properties*

This file contains the following parameters:

### Hostname or IP Address

HOSTNAME=

Specify the host name or IP address of your system. The Prerequisite Validator utility uses the host name or the IP address of your system to test the FTP connection and to verify the JESINTERFACELEVEL value.

### Local Host FTP Port

ftp.port=

Specify the FTP port number for the hostname or IP address you specified. The Prerequisite Validator utility tests the FTP connection and verifies the JESINTERFACELEVEL value.

**Default:** 21

### Authorization for Issuing FTP Command

ftp.stat.check.credential=

Specify ftp.stat.check.credential=y if your site requires authorization to issue FTP quote STAT commands. The command appears in the log as follows:

503 Login required, enter USER

When set to **y**, the utility prompts you for a user ID and password.

**Default:** n

### Proxy Server for FTP Request

The following parameters are related to FTP proxy checks. Set the parameter to **yes** to activate FTP check through the proxy.

```
ftp.proxy.enabled=  
ftp.proxy.host=  
ftp.proxy.port=  
ftp.proxy.credential.check=  
ftp.proxy.fireCmd.proxy_userid=  
ftp.proxy.fireCmd.site=  
ftp.proxy.fireCmd.acct=  
ftp.advanced.session.options=
```

The utility verifies the connection to the external CA Support FTP servers. If your site requires these requests to go through a proxy server, then modify these parameters as shown in the following example:

```
ftp.proxy.enabled=yes  
ftp.proxy.host=hostname_or_IP_address  
ftp.proxy.port=port_number  
ftp.proxy.credential.check=n_or_y
```

When `ftp.proxy.credential.check=y`, change the following parameters:

```
ftp.proxy.fireCmd.proxy_userid=proxy_userid
```

You can change the following parameters based on your proxy requirements:

```
ftp.proxy.fireCmd.site=  
ftp.proxy.fireCmd.acct=  
ftp.advanced.session.options=
```

### Proxy Server for HTTP Request

The following parameters are related to HTTP proxy checks. Set the following parameter to **yes** to activate HTTP check through the proxy.

```
http.proxy.enabled=  
http.proxy.host=  
http.proxy.port=80  
http.proxy.credential.check=  
http.proxy.type=  
http.domain=
```

The utility verifies the connection to the external CA Support HTTP servers. If your site requires these requests to go through a proxy server, then modify these parameters as shown in the following example:

```
http.proxy.enabled=yes  
http.proxy.host=company_proxy_name  
http.proxy.port=80  
http.proxy.credential.check=y_or_n  
http.proxy.type=NTLM  
http.domain=company_domain_name
```

### **SAF Resource Access Check**

SafSecurityResourceAccess=

The utility verifies user access for the following resources:

BPX.SERVER(UPDATE)  
BPX.FILEATTR.SHARELIB(READ)  
BPX.FILEATTR.PROGCTL(READ)  
BPX.FILEATTR.APF(READ)

Specify SafSecurityResourceAccess=n to turn off the resource access check.

**Default:** y

### **MSMServerPortNo**

MSMServerPortNo=

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

**Default:** 22120

### **MSMDSIPORTNO**

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

**Default:** 22130

### **MSMConnectorRedirectPortNo**

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

**Default:** 22140

### **MSMTomcatServerShutdownPortNo**

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

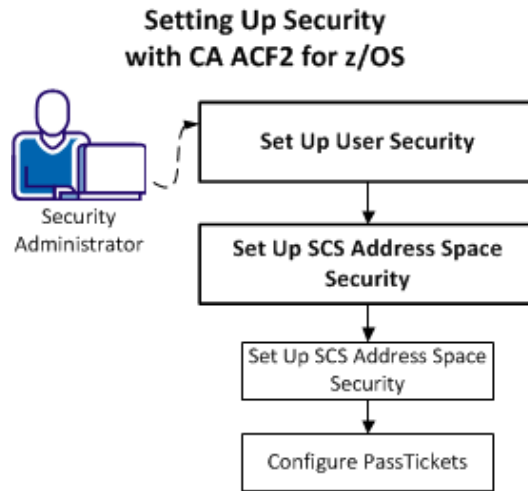
**Default:** 22150

You completed using the Prerequisite Validator utility. You can now start installing CA CSM.

# Chapter 5: Set Up Security for CA CSM with CA ACF2 for z/OS

---

You perform the following tasks to set up security for CA CSM with CA ACF2 for z/OS:



1. [Set up user security](#) (see page 31):
2. [Set up Software Configuration Service \(SCS\) address space security](#) (see page 36):
  - a. [Set up SCS address space security](#) (see page 37).
  - b. [Configure PassTickets](#) (see page 37).

## How to Set Up User Security

To set up user security, you create a global system options (GSO) CLASMAP record using the CAMSM resource class and grant user permission to appropriate CA CSM resource profiles.

**Note:** CAMSM is the default name of the SAF resource class. Your system may use a different name depending on your CA CSM installation.

To define the CLASMAP record, issue the following CA ACF2 for z/OS commands:

```
SET C(GSO)
INSERT CLASMAP.MSM ENTITYLN(246) MUSID() RESOURCE(CAMSM) RSRCTYPE(MSM)
```

To refresh the CLASMAP record, issue the following command:

```
F ACF2,REFRESH(CLASMAP),TYPE(GSO)
```

To grant user permission to appropriate CA CSM resource profiles, use the commands in the following examples for various roles:

- [Administrators](#) (see page 32)
- [Users](#) (see page 33)
- [Restricted Users](#) (see page 34)

## Example: Set Up Security for Administrators

You want to grant the user, MSMUSR1, access to all actions. The actions include the management of system settings, system registry, methodologies, deployments, configurations, and of user settings.

Issue the following CA ACF2 for z/OS commands:

```
SET R(MSM)
COMPILE STORE
$KEY(LOGON) TYPE(MSM)
UID(****MSMUSR1)          SERVICE(READ)    ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(ADMIN) TYPE(MSM)
SETTINGS. - UID(****MSMUSR1)  SERVICE(READ)    ALLOW
LMPKEY. -   UID(****MSMUSR1)  SERVICE(READ)    ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(SC) TYPE(MSM)
@ACTION. - UID(****MSMUSR1)  SERVICE(READ)    ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(SMPE) TYPE(MSM)
@ACTION. - UID(****MSMUSR1)  SERVICE(READ)    ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(SYSREG) TYPE(MSM)
UID(****MSMUSR1)  SERVICE(READ)    ALLOW
```



```

SET R(MSM)
COMPILE STORE
$KEY(DEPLOY) TYPE(MSM)
UID(*****MSMUSR1) SERVICE(READ) ALLOW

```

```

SET R(MSM)
COMPILE STORE
$KEY(METHOD) TYPE(MSM)
UID(*****MSMUSR1) SERVICE(READ) ALLOW

```

```

SET R(MSM)
COMPILE STORE
$KEY(CONFIG) TYPE(MSM)
UID(*****MSMUSR1) SERVICE(READ) ALLOW

```

```

SET R(MSM)
COMPILE STORE
$KEY(TM) TYPE(MSM)
UID(*****MSMUSR1) SERVICE(READ) ALLOW

```

## Example: Set Up Security for Users

You want to grant the user, MSMUSR2, access to all user actions, but the user can only access the SANDBOX system within the environment. A user with this setup cannot manage system or other users' settings, modify the system registry, nor create methodologies. The user can create deployments that are targeted for the SANDBOX system and can use methodologies that other CA CSM users defined. The user can create configurations that are targeted for the SANDBOX remote system using system profile values already defined, but cannot implement those configurations.

Issue the following CA ACF2 for z/OS commands:

```

SET R(MSM)
COMPILE STORE
$KEY(LOGON) TYPE(MSM)
UID(*****MSMUSR2) SERVICE(READ) ALLOW

```

```

SET R(MSM)
COMPILE STORE
$KEY(ADMIN) TYPE(MSM)
SETTINGS.USER. - UID(*****MSMUSR2) SERVICE(READ) ALLOW
LMPKEY. - UID(*****MSMUSR2) SERVICE(READ) ALLOW

```

```
SET R(MSM)
COMPILE STORE
$KEY(SC) TYPE(MSM)
@ACTION. -          UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(SMPE) TYPE(MSM)
@ACTION. -          UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(SYSREG) TYPE(MSM)
@DISPLAY. -         UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
@PROFILE.DISPLAY   UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
@SYSTEM.SANDBOX    UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(METHOD) TYPE(MSM)
@DISPLAY. -         UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(DEPLOY) TYPE(MSM)
@DISPLAY. -         UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
@BUILD. -           UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
@EXECUTE. -         UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(CONFIG) TYPE(MSM)
@DISPLAY. -         UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
@ACTION.CREATE     UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
@ACTION.REMOVE     UID(*****MSMUSR2)  SERVICE(READ)  ALLOW
```

## Example: Set Up Security for Restricted Users

You want to grant the user, MSMUSR3, access to the following actions only:

- Download product packages.
- Install product packages that are downloaded outside of CA CSM.
- Migrate an existing SMP/E environment to CA CSM.

- Remove knowledge of an SMP/E environment from CA CSM.
- Create and deploy their own deployments.
- Create and maintain remote systems within the system registry, including profile information.
- Implement prepared configurations on remote systems.

Issue the following CA ACF2 for z/OS commands:

```
SET R(MSM)
COMPILE STORE
$KEY(LOGON) TYPE(MSM)
UID(*****MSMUSR3)          SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(ADMIN) TYPE(MSM)
SETTINGS.USER. -          UID(*****MSMUSR3)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(SC) TYPE(MSM)
@ACTION.INSTPKG. -        UID(*****MSMUSR3)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(SMPE) TYPE(MSM)
@ACTION.MIGRATE. -        UID(*****MSMUSR3)  SERVICE(READ)  ALLOW
@ACTION.REMOVECSI. -      UID(*****MSMUSR3)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(SYSREG) TYPE(MSM)
                                UID(*****MSMUSR3)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(METHOD) TYPE(MSM)
@DISPLAY. -                UID(*****MSMUSR3)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(DEPLOY) TYPE(MSM)
@SELF. -          UID(****MSMUSR3)  SERVICE(READ)  ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(CONFIG) TYPE(MSM)
@ACTION.IMPL     UID(****MSMUSR3)  SERVICE(READ)  ALLOW
```

## How to Set Up SCS Address Space Security

The SCS address space verifies the user ID assigned to the requesting started task or initiated job and authorizes it to connect.

The security setup that is required for CA CSM is only set up on the driving system. To set up the SCS address space security, do so on every target system, which can include the CA CSM driving system.

**Note:** An unauthorized CA CSM user ID is denied access to the selected target system.

If security profiles are not defined, CA CSM cannot connect to the SCS address space, including from within the address space.

Configure permission to access the entity SCSAS.CONNECT (READ authority) of the class CAMSM. The permission allows connections to the SCS address space through the CA CSM application server and the SCS address space.

PassTickets are used to verify the started task ID of the CA CSM application server. Verifying the started task ID allows secure connections from a remote system to the address space.

To set up SCS address space security:

1. [Set up SCS address space security](#) (see page 37).
2. [Configure PassTickets](#) (see page 37).

## Set Up SCS Address Space Security

Define the global systems options (GSO) record and define the rule to permit access to a user ID on every target system.

### Follow these steps:

1. Define the GSO record:

```
SET C(GSO)
INSERT CLASMAP.MSM ENTITYLN(246) MUSID() RESOURCE(CAMSM) RSRCTYPE(MSM)
```

2. Define the rule to permit access to a user ID:

```
SET R(MSM)
COMPILE STORE
$KEY(SCSAS) TYPE(MSM)
CONNECT.-      UID(****userid)                SERVICE(READ)    ALLOW
CONNECT.-      UID(****userid2)              SERVICE(READ)    ALLOW
```

#### *userid*

Specifies the user ID assigned to the SCS address space.

#### *userid2*

Specifies the user ID assigned to the CA CSM application server driving system.

## Configure PassTickets

Set up PassTickets on the system where the CA CSM application server is executing and on each system where the SCS address space is running.

**Note:** To generate a valid PassTicket, use the values for the remote SCS address space on the system where the CA CSM application server is running.

To set up PassTickets, use the commands in the following examples on both the server and remote target systems.

**Note:** These examples are provided as a guideline and are intended for security administrators familiar with PassTicket configuration.

- [Example: Configure PassTickets for CA CSM Application Server](#) (see page 38)
- [Example: Configure PassTickets for SCS Address Space on Remote Systems](#) (see page 39)

After you finish configuring PassTickets on both the server and remote target systems, you have completed security setup for CA CSM with CA ACF2 for z/OS.

## Example: Configure PassTickets for CA CSM Application Server

You can use CA ACF2 for z/OS to configure PassTickets on the system where the CA CSM application server is executing.

### Follow these steps:

1. Define the session key for the CA CSM application server:

```
SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
INSERT MSMCAPPL SSKEY(0123456789ABCDEF) NOMULT-USE
```

#### **MSMCAPPL**

Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

**Note:** This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

2. Enable READ access to the MSMCAPPL PassTicket key value:

```
SET RESOURCE(PTK)
RECKEY IRRPTAUTH ADD(MSMCAPPL.stc-userid UID(uid-of-stc-userid))
SERVICE(READ,UPDATE) ALLOW
```

#### **stc-userid and uid-of-stc-userid**

Specifies the user ID and UID associated with the CA CSM application server started task.

**Note:** You can also use the ACFNRULE utility program to add rule lines to an existing rule. For more information about this option, see the *CA ACF2 for z/OS Administration Guide*.

3. Complete the PassTicket setup:

```
F ACF2,REBUILD(PTK),CLASS(P)
F ACF2,REBUILD(PTK)
```

## Example: Configure PassTickets for SCS Address Space on Remote Systems

You can use CA ACF2 for z/OS to configure PassTickets on the remote systems where the SCS address space is running.

### Follow these steps:

1. Define the MSMCAPPL session keys:

```
SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
INSERT MSMCAPPL SSKEY(0123456789ABCDEF) NOMULT-USE
```

#### **MSMCAPPL**

Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

**Note:** This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

2. Enable READ access to the MSMCAPPL PassTicket key value:

```
SET RESOURCE(PTK)
RECKEY IRRPTAUTH ADD(MSMCAPPL.stc-userid UID(uid-of-stc-userid))
SERVICE(READ,UPDATE) ALLOW
```

#### **stc-userid and uid-of-stc-userid**

Specifies the user ID and UID associated with the SCS address space.

**Note:** You can also use the ACFNRULE utility program to add rule lines to an existing rule. For more information about this option, see the *CA ACF2 for z/OS Administration Guide*.

3. Complete the PassTicket setup on the remote systems:

```
F ACF2,REBUILD(PTK),CLASS(P)
F ACF2,REBUILD(PTK)
```

You completed site preparation. Your system is ready to install CA CSM.



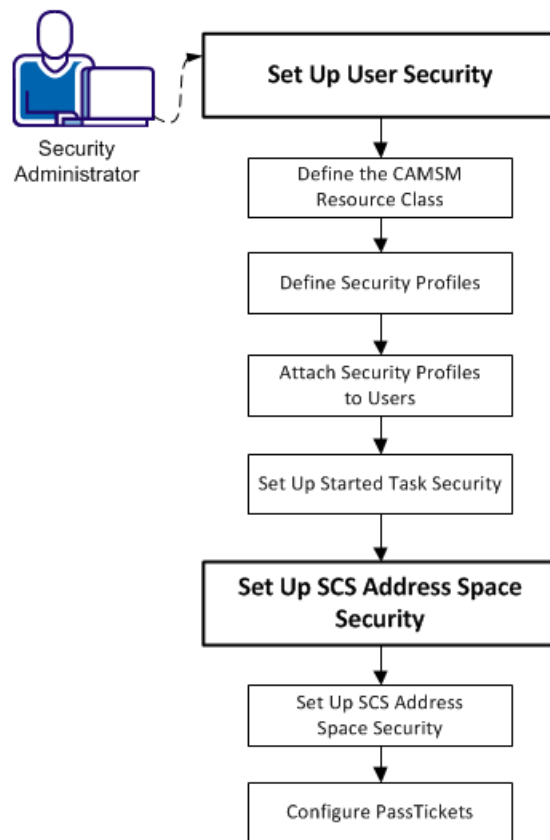


# Chapter 6: Set Up Security for CA CSM with CA Top Secret for z/OS

---

You perform the following tasks to set up security for CA CSM with CA Top Secret for z/OS:

## Setting Up Security with CA Top Secret for z/OS



1. [Set up user security](#) (see page 42):
  - a. [Define the CAMSM resource class](#) (see page 42).
  - b. [Define security profiles](#) (see page 43).
  - c. [Attach security profiles to users](#) (see page 45).
  - d. [Set up started task security](#) (see page 46).

2. [Set up Software Configuration Service \(SCS\) address space security](#) (see page 36):
  - a. [Set up SCS address space Security](#) (see page 47).
  - b. [Configure PassTickets](#) (see page 48).

## How to Set Up User Security

CA CSM uses resource profiles to grant access to resources on the web-based interface. The resource class is CAMSM. In CA Top Secret for z/OS, you can define security profiles that include the appropriate resource profiles for various roles and can attach the security profiles to users.

**Note:** CAMSM is the default name of the SAF resource class. Your system may use a different name depending on your CA CSM installation.

To set up user security:

1. [Define the CAMSM resource class](#) (see page 42).
2. [Define the security profiles to configure the roles](#) (see page 43).
3. [Attach the profiles to users](#) (see page 45).
4. [Set up started task security](#) (see page 46).

## Define the CAMSM Resource Class

Before you can use the CA CSM resource profiles, you define the CAMSM class that contains the profiles to CA Top Secret for z/OS.

**Note:** CAMSM is the default name of the SAF resource class. Your system may use a different name depending on your CA CSM installation.

**Follow these steps:**

1. Issue the following commands:

```
TSS ADDTO(RDT) RESCLASS(CAMSM)
      ATTR(MASK) MAXLEN(246)
TSS REPL(RDT) RESCLASS(CAMSM)
      ACLST(READ=4000,UPDATE=8000,CONTROL=0400,NONE=0000)
      DEFACC(READ)
```

2. Define resource profiles within the CAMSM class:

```
TSS ADDTO(MSMDPT) CAMSM(LOGON)
TSS ADDTO(MSMDPT) CAMSM(ADMIN.)
TSS ADDTO(MSMDPT) CAMSM(SC.)
TSS ADDTO(MSMDPT) CAMSM(SMPE.)
TSS ADDTO(MSMDPT) CAMSM(SYSREG.)
TSS ADDTO(MSMDPT) CAMSM(METHOD.)
TSS ADDTO(MSMDPT) CAMSM(DEPLOY.)
TSS ADDTO(MSMDPT) CAMSM(CONFIG.)
TSS ADDTO(MSMDPT) CAMSM(TM.)
```

**Note:** You deny or grant access to CA CSM using resource profiles.

## Define Security Profiles

You can define security profiles for various roles and attach the profiles to users. Use the commands in the following examples for various roles:

- [Administrators](#) (see page 44)
- [Users](#) (see page 44)
- [Restricted Users](#) (see page 45)

## Example: Set Up Security for Administrators

You want to define a profile, MSMPRF1, that grants access to all actions. The actions include the management of system settings, system registry, methodologies, deployments, configurations, and of user settings.

Issue the following CA Top Secret for z/OS commands:

```
TSS CREATE(MSMPRF1) NAME('CA CSM ADMIN PROFILE') DEPT(MSMDPT) TYPE(PROFILE)
TSS PERMIT(MSMPRF1) CAMSM(LOGON) ACCESS(READ)
TSS PERMIT(MSMPRF1) CAMSM(ADMIN.) ACCESS(READ)
TSS PERMIT(MSMPRF1) CAMSM(SC.) ACCESS(READ)
TSS PERMIT(MSMPRF1) CAMSM(SMPE.) ACCESS(READ)
TSS PERMIT(MSMPRF1) CAMSM(SYSREG.) ACCESS(READ)
TSS PERMIT(MSMPRF1) CAMSM(METHOD.) ACCESS(READ)
TSS PERMIT(MSMPRF1) CAMSM(DEPLOY.) ACCESS(READ)
TSS PERMIT(MSMPRF1) CAMSM(CONFIG.) ACCESS(READ)
TSS PERMIT(MSMPRF1) CAMSM(TM.) ACCESS(READ)
```

## Example: Set Up Security for Users

You want to define a profile, MSMPRF2, that grants access to all user actions, but the user can only access the SANDBOX system within the environment. A user with this setup cannot manage system or other users' settings, modify the system registry, nor create methodologies. The user can create deployments that are targeted for the SANDBOX system and can use methodologies that other CA CSM users defined. The user can create configurations that are targeted for the SANDBOX remote system using system profile values already defined, but cannot implement those configurations.

Issue the following CA Top Secret for z/OS commands:

```
TSS CREATE(MSMPRF2) NAME('CA CSM USER PROFILE') DEPT(MSMDPT) TYPE(PROFILE)
TSS PERMIT(MSMPRF2) CAMSM(ADMIN.SETTINGS.USER) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(ADMIN.LMPKEY) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(SC.@ACTION) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(SMPE.@ACTION) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(SYSREG.@DISPLAY) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(SYSREG.@PROFILE.DISPLAY) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(SYSREG.@SYSTEM.SANDBOX) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(METHOD.@DISPLAY) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(DEPLOY.) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(CONFIG.@DISPLAY) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(CONFIG.@ACTION.CREATE) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(CONFIG.@ACTION.REMOVE) ACCESS(READ)
```

## Example: Set Up Security for Restricted Users

You want to define a profile, MSMPRF3, that grants access to the following actions only:

- Download product packages.
- Install product packages that are downloaded outside of CA CSM.
- Migrate an existing SMP/E environment to CA CSM.
- Remove knowledge of an SMP/E environment from CA CSM.
- Create deployments and deploy them (if they are the owner).
- Create and maintain remote systems within the system registry, including profile information.
- Implement prepared configurations on remote systems.

Issue the following CA Top Secret for z/OS commands:

```
TSS CREATE(MSMPRF3) NAME('CA CSM SMPE USER PROFILE') DEPT(MSMDPT) TYPE(PROFILE)
TSS PERMIT(MSMPRF3) CAMSM(ADMIN.SETTINGS.USER) ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(SC.@ACTION.INSTPKG) ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(SMPE.@ACTION.MIGRATE) ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(SMPE.@ACTION.REMOVECSI) ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(SYSREG) ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(METHOD.@DISPLAY) ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(DEPLOY.@SELF) ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(CONFIG.@ACTION.IMPL) ACCESS(READ)
```

## Attach Security Profiles to Users

You attach security profiles to users to grant the users access to CA CSM actions in various roles.

To attach security profiles to users, issue CA Top Secret for z/OS commands in TSO, for example:

```
TSS ADDTO(MSMUSR1) PROFILE(MSMPRF1)
TSS ADDTO(MSMUSR2) PROFILE(MSMPRF2)
TSS ADDTO(MSMUSR3) PROFILE(MSMPRF3)
```

The example sets up the following configuration:

- The MSMPRF1 profile permits access to the user MSMUSR1.
- The MSMPRF2 profile permits access to the user MSMUSR2.
- The MSMPRF3 profile permits access to the user MSMUSR3.

## Set Up Started Task Security

If you plan to run the CA CSM application server (MSMTC) as a started task under CA Top Secret for z/OS, accomplish relevant configuration settings.

### Follow these steps:

1. Define a facility for the started task:

```
TSS MODIFY FACILITY (USERxx=NAME=MSM)
TSS MODIFY FACILITY (MSM=MULTIUSER, SIGN(M))
```

The facility is used to control who can log in to the server.

**Note:** For more information, see the *CA Top Secret for z/OS Control Options Guide*.

2. Create an ACID (user ID) to control the server.

**Note:** For more information, see the *CA Top Secret for z/OS Command Functions Guide*.

3. Define the server region to the STC table.

The STC entry contains the server procedure name and ACID.

**Note:** For more information, see the *CA Top Secret for z/OS Command Functions Guide*.

4. Add the facility that you defined in Step 1 to the server ACID, using the MASTFAC keyword.

**Note:** For more information, see the *CA Top Secret for z/OS Command Functions Guide*.

5. Add the facility that you defined in Step 1 to each user who requires logon to the server, using the FACILITY keyword.

**Note:** For more information, see the *CA Top Secret for z/OS Command Functions Guide*.

## How to Set Up SCS Address Space Security

The SCS address space verifies the user ID assigned to the requesting started task or initiated job and authorizes it to connect.

The security setup that is required for CA CSM is only set up on the driving system. To set up the SCS address space security, do so on every target system, which can include the CA CSM driving system.

**Note:** An unauthorized CA CSM user ID is denied access to the selected target system.

If security profiles are not defined, CA CSM cannot connect to the SCS address space, including from within the address space.

Configure permission to access the entity SCSAS.CONNECT (READ authority) of the class CAMSM. The permission allows connections to the SCS address space through the CA CSM application server and the SCS address space.

PassTickets are used to verify the started task ID of the CA CSM application server. Verifying the started task ID allows secure connections from a remote system to the address space.

To set up SCS address space security:

1. [Set up SCS address space security](#) (see page 47).
2. [Configure PassTickets](#) (see page 48).

## Set Up SCS Address Space Security

Set up security for the SCS address space in CA Top Secret for z/OS.

### Follow these steps:

1. Add the resource class to the RDT:

```
TSS ADDTO(RDT) RESCLASS(CAMSM) ATTR(MASK) MAXLEN(246)
TSS REPL(RDT) RESCLASS(CAMSM)
          ACLST(READ=4000,UPDATE=8000,CONTROL=0400,NONE=0000)
          DEFACC(READ)
```

2. Create a CA CSM departmental ACID:

```
TSS CREATE(MSMDPT) NAME('CA CSM Department') TYPE(USER)
```

3. Define the resource profiles within the CAMSM class:

```
TSS ADDTO(MSMDPT) CAMSM(SCSAS.CONNECT)
```

4. Create a CA Top Secret for z/OS profile.

```
TSS CREATE(SCSPRF1) NAME('CA CSM SCS AS PROFILE')
DEPT(MSMDPT) TYPE(PROFILE)
```

5. Permit the resource to access the profile:

```
TSS PERMIT(SCSPRF1) CAMSM(SCSAS.CONNECT) ACCESS(READ)
```

6. Assign the profile to the ACID:

```
TSS ADDTO(userid) PROFILE(SCSPRF1)
```

### *userid*

Specifies the user ID assigned to the SCS address space.

## Configure PassTickets

Set up PassTickets on the system where the CA CSM application server is executing and on each system where the SCS address space is running.

**Note:** To generate a valid PassTicket, use the values for the remote SCS address space on the system where the CA CSM application server is running.

To set up PassTickets, use the commands in the following examples on both the server and remote target systems.

**Note:** These examples are provided as a guideline and are intended for security administrators familiar with PassTicket configuration.

- [Example: Configure PassTickets for CA CSM Application Server](#) (see page 48)
- [Example: Configure PassTickets for SCS Address Space on Remote Systems](#) (see page 49)

After you finish configuring PassTickets on both the server and remote target systems, you have completed security setup for CA CSM with CA Top Secret for z/OS.

### Example: Configure PassTickets for CA CSM Application Server

You can use CA Top Secret for z/OS to configure PassTickets on the system where the CA CSM application server is executing.

#### Follow these steps:

1. Update the resource descriptor table (RDT) to define the PTKTDATA class (which is not a predefined class):

```
TSS ADDTO(RDT) RESCLASS(PTKTDATA) RESCODE(n) ACLIST(ALL,READ,UPDATE) MAXLEN(37)
```

**Note:** Include RESCODE(*n*) in the range of 101 to 13F to make PTKTDATA a prefixed resource class.

2. Assign ownership to a department for the PassTicket session key (SESSKEY) resource:

```
TSS ADDTO(department) PTKTDATA(IRRPTAUTH)
```

#### ***department***

Specifies a preexisting department. The ownership of the application is defined to this department. This ownership lets the department administrator (or higher) define permissions for PassTicket generation and validation.



- Define the CA CSM application server PassTicket session key:

```
TSS ADDTO(NDT) PSTKAPPL(MSMCAPPL) SESSKEY(0123456789ABCDEF)
```

**MSMCAPPL**

Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

**Note:** This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

- Permit access to the CA CSM application server PassTicket session key value for the Started Task User for the CA CSM application server:

```
TSS PERMIT(stc-userid) PTKTDATA(IRRPTAUTH.MSMCAPPL.) ACCESS(READ,UPDATE)
```

**stc-userid**

Specifies the ACID that you defined the access requirements for user ID associated with the CA CSM application server.

## Example: Configure PassTickets for SCS Address Space on Remote Systems

You can use CA Top Secret for z/OS to configure PassTickets on the remote systems where the SCS address space is running.

**Follow these steps:**

- Define the SCS address space PassTicket session key:

```
TSS ADDTO(NDT) PSTKAPPL(MSMCAPPL) SESSKEY(0123456789ABCDEF)
```

**MSMCAPPL**

Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

**Note:** This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

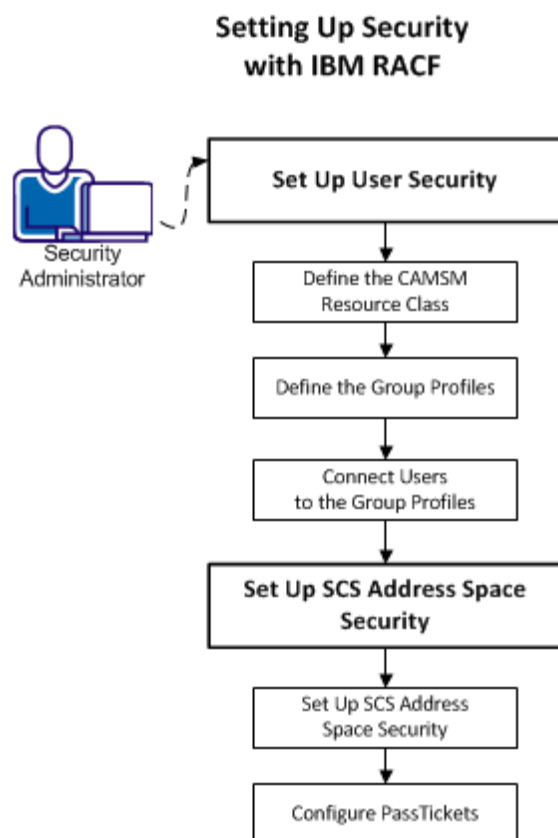
You completed site preparation. Your system is ready to install CA CSM.



# Chapter 7: Set Up Security for CA CSM with IBM RACF

---

You perform the following tasks to set up security for CA CSM with IBM RACF:



1. [Set up user security](#) (see page 52):
  - a. [Define the CAMSM resource class](#) (see page 52).
  - b. [Define the group profiles](#) (see page 53).
  - c. [Connect users to the group profiles](#) (see page 55).
2. [Set up Software Configuration Service \(SCS\) address space security](#) (see page 36):
  - a. [Set up SCS address space security](#) (see page 57).
  - b. [Configure PassTickets](#) (see page 57).

## How to Set Up User Security

CA CSM uses resource profiles to grant access to resources on the web-based interface. The resource class is CAMSM. In IBM RACF, you can define group profiles that include the appropriate resource profiles for various roles and connect the users to the group profiles.

**Note:** CAMSM is the default name of the SAF resource class. Your system may use a different name depending on your CA CSM installation.

To set up user security:

1. [Define the CAMSM resource class](#) (see page 52).
2. [Define the group profiles](#) (see page 53).
3. [Connect users to the group profiles](#) (see page 55).

### Define the CAMSM Resource Class

Before you can use the CA CSM resource profiles, you define the CAMSM class that contains the profiles to IBM RACF.

**Note:** CAMSM is the default name of the SAF resource class. Your system may use a different name depending on your CA CSM installation.

**Follow these steps:**

1. Issue the SETROPTS LIST command to verify that the CDT resource appears within both the CLASSACT and RACLIST list of entries.
2. Define the generic profile:

```
RDEFINE CDT CAMSM UACC(NONE) CDTINFO(GENERIC,MAXLENGTH(246) POSIT(nnn)  
OTHER(ALPHA,NATIONAL,NUMERIC,SPECIAL) RACLIST(ALLOWED))
```

***nnn***

Defines a posit number that does not conflict with IBM reserved values.

**Note:** For more information about posit numbers, see the *IBM Server RACF Command Language Reference*.

The generic profile is defined.

3. Finalize the changes:

```
SETROPTS RACLIST(CDT) REFRESH  
SETROPTS GENERIC(CAMSM) RACLIST(CAMSM) CLASSACT(CAMSM)
```

The changes take effect and the CAMSM resource class is defined to IBM RACF.

**Note:** You deny or grant access to CA CSM using resource profiles.

## Define the Group Profiles

You can define group profiles that include the appropriate resource profiles for various roles. You can connect the users to the group profiles.

**Note:** You deny or grant access to CA CSM using resource profiles.

The following examples define group profiles for various roles.

- [Administrators](#) (see page 53)
- [Users](#) (see page 54)
- [Restricted Users](#) (see page 54)

### Example: Set Up Security for Administrators

You want to define a profile, MSMPRF1, that grants access to all actions. The actions include the management of system settings, system registry, methodologies, deployments, configurations, and of user settings.

Issue the following IBM RACF commands:

```
ADDGROUP MSMPRF1 DATA('CA CSM ADMIN')
```

```
RDEFINE CAMSM LOGON UACC(NONE)
RDEFINE CAMSM ADMIN.* UACC(NONE)
RDEFINE CAMSM SC.* UACC(NONE)
RDEFINE CAMSM SMPE.* UACC(NONE)
RDEFINE CAMSM SYSREG.* UACC(NONE)
RDEFINE CAMSM METHOD.* UACC(NONE)
RDEFINE CAMSM DEPLOY.* UACC(NONE)
RDEFINE CAMSM CONFIG.* UACC(NONE)
RDEFINE CAMSM TM.* UACC(NONE)
```

```
PERMIT LOGON CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT ADMIN.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT SC.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT SMPE.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT SYSREG.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT METHOD.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT DEPLOY.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT CONFIG.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT TM.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
```

## Example: Set Up Security for Users

You want to define a profile, MSMPRF2, that grants access to all user actions, but the user can only access the SANDBOX system within the environment. A user with this profile cannot manage system or other users' settings, modify the system registry, nor create methodologies. The user can create deployments that are targeted for the SANDBOX system and can use methodologies that other CA CSM users defined. The user can create configurations that are targeted for the SANDBOX remote system using system profile values already defined, but cannot implement those configurations.

Issue the following IBM RACF commands:

```
ADDGROUP MSMPRF2 DATA('CA CSM USER')

RDEFINE CAMSM LOGON UACC(NONE)
RDEFINE CAMSM ADMIN.SETTINGS.USER.* UACC(NONE)
RDEFINE CAMSM ADMIN.LMPKEY.* UACC(NONE)
RDEFINE CAMSM SC.@ACTION.* UACC(NONE)
RDEFINE CAMSM SMPE.@ACTION.* UACC(NONE)
RDEFINE CAMSM SYSREG.@DISPLAY UACC(NONE)
RDEFINE CAMSM SYSREG.@PROFILE.DISPLAY UACC(NONE)
RDEFINE CAMSM SYSREG.@SYSTEM.SANDBOX UACC(NONE)
RDEFINE CAMSM METHOD.@DISPLAY UACC(NONE)
RDEFINE CAMSM DEPLOY.* UACC(NONE)
RDEFINE CAMSM CONFIG.@DISPLAY UACC(NONE)
RDEFINE CAMSM CONFIG.@ACTION.CREATE UACC(NONE)
RDEFINE CAMSM CONFIG.@ACTION.REMOVE UACC(NONE)

PERMIT LOGON CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT ADMIN.SETTINGS.USER.* CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT ADMIN.LMPKEY.* CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT SC.@ACTION.* CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT SMPE.@ACTION.* CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT SYSREG.@DISPLAY CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT SYSREG.@PROFILE.DISPLAY CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT METHOD.@DISPLAY CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT DEPLOY.* CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT CONFIG.@DISPLAY CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT CONFIG.@ACTION.CREATE CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT CONFIG.@ACTION.REMOVE CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
```

## Example: Set Up Security for Restricted Users

You want to define a profile, MSMPRF3, that grants access to the following actions only:

- Download product packages.
- Install product packages that are downloaded outside of CA CSM.
- Migrate an existing SMP/E environment to CA CSM.

- Remove knowledge of an SMP/E environment from CA CSM.
- Create deployments and deploy them (if they are the owner).
- Create and maintain remote systems within the system registry, including profile information.
- Implement prepared configurations on remote systems.

Issue the following IBM RACF commands:

```
ADDGROUP MSMPRF3 DATA('CA CSM SMPE')
```

```
RDEFINE CAMSM LOGON UACC(NONE)
RDEFINE CAMSM ADMIN.SETTINGS.USER.* UACC(NONE)
RDEFINE CAMSM SC.@ACTION.INSTPKG UACC(NONE)
RDEFINE CAMSM SMPE.@ACTION.MIGRATE UACC(NONE)
RDEFINE CAMSM SMPE.@ACTION.REMOVECSI UACC(NONE)
RDEFINE CAMSM DEPLOY.@SELF UACC(NONE)
RDEFINE CAMSM SYSREG.* UACC(NONE)
RDEFINE CAMSM METHOD.@DISPLAY UACC(NONE)
RDEFINE CAMSM CONFIG.@ACTION.IMPL UACC(NONE)
```

```
PERMIT LOGON CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT ADMIN.SETTINGS.USER.* CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT SC.@ACTION.INSTPKG CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT SMPE.@ACTION.MIGRATE CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT SMPE.@ACTION.REMOVECSI CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT DEPLOY.@SELF CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT SYSREG.* CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT METHOD.@DISPLAY CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT CONFIG.@ACTION.IMPL CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
```

## Connect Users to the Group Profiles

You connect users to group profiles to grant the users access to CA CSM actions in various roles.

To connect users to group profiles, issue IBM RACF commands in TSO, for example:

```
CONNECT MSMUSR1 GROUP(MSMPRF1)
CONNECT MSMUSR2 GROUP(MSMPRF2)
CONNECT MSMUSR3 GROUP(MSMPRF3)
```

The example sets up the following configuration:

- The MSMPRF1 profile permits access to the user MSMUSR1.
- The MSMPRF2 profile permits access to the user MSMUSR2.
- The MSMPRF3 profile permits access to the user MSMUSR3.

## How to Set Up SCS Address Space Security

The SCS address space verifies the user ID assigned to the requesting started task or initiated job and authorizes it to connect.

The security setup that is required for CA CSM is only set up on the driving system. To set up the SCS address space security, do so on every target system, which can include the CA CSM driving system.

**Note:** An unauthorized CA CSM user ID is denied access to the selected target system.

If security profiles are not defined, CA CSM cannot connect to the SCS address space, including from within the address space.

Configure permission to access the entity SCSAS.CONNECT (READ authority) of the class CAMSM. The permission allows connections to the SCS address space through the CA CSM application server and the SCS address space.

PassTickets are used to verify the started task ID of the CA CSM application server. Verifying the started task ID allows secure connections from a remote system to the address space.

To set up SCS address space security:

1. [Set up SCS address space security](#) (see page 57).
2. [Configure PassTickets](#) (see page 57).



## Set Up SCS Address Space Security

Set up security for the SCS address space in IBM RACF.

**Note:** If you have already [defined and activated the CAMSM resource class in IBM RACF](#) (see page 52), you can skip steps 1 through 4.

### Follow these steps:

1. Issue the SETROPTS LIST command to verify that the CDT resource appears within both the CLASSACT and RACLIST list of entries.

2. Define the generic profile:

```
RDEFINE CDT CAMSM UACC(NONE) CDTINFO(GENERIC,MAXLENGTH(246) POSIT(nnn)
OTHER(ALPHA,NATIONAL,NUMERIC,SPECIAL) RACLIST(ALLOWED))
```

***nnn***

Defines a posit number that does not conflict with IBM reserved values.

**Note:** For more information about posit numbers, see the *IBM Server RACF Command Language Reference*.

The generic profile is defined.

3. Make the generic profile changes take effect:

```
SETROPTS RACLIST(CDT) REFRESH
```

4. Activate the CAMSM class:

```
SETROPTS RACLIST(CAMSM) CLASSACT(CAMSM)
```

5. Define the resource profiles within the CAMSM class:

```
RDEFINE CAMSM SCSAS.CONNECT UACC(NONE)
```

6. Permit the resource to a user:

```
PERMIT SCSAS.CONNECT CLASS(CAMSM) ID(userid) ACCESS(READ)
```

***userid***

Specifies the user ID assigned to the SCS address space.

7. (Optional) If the CAMSM class is RACLISTed, refresh the class:

```
SETROPTS RACLIST(CAMSM) REFRESH
```

## Configure PassTickets

Set up PassTickets on the system where the CA CSM application server is executing and on each system where the SCS address space is running.

**Note:** To generate a valid PassTicket, use the values for the remote SCS address space on the system where the CA CSM application server is running.

To set up PassTickets, use the commands in the following examples on both the server and remote target systems.

**Note:** These examples are provided as a guideline and are intended for security administrators familiar with PassTicket configuration.

- [Example: Configure PassTickets for CA CSM Application Server](#) (see page 58)
- [Example: Configure PassTickets for SCS Address Space on Remote Systems](#) (see page 59)

After you finish configuring PassTickets on both the server and remote target systems, you have completed security setup for CA CSM with IBM RACF.

### Example: Configure PassTickets for CA CSM Application Server

You can use IBM RACF to configure PassTickets on the system where the CA CSM application server is executing.

#### Follow these steps:

1. Activate the PassTicket class:

```
SETROPTS CLASSACT(PTKTDATA)
SETROPTS RACLIST(PTKTDATA)
SETROPTS GENERIC(PTKTDATA)
```

2. Define a profile for the application and specify the session key:

```
RDEFINE PTKTDATA MSMCAPPL SSIGNON(KEYMASKED(0123456789ABCDEF)) UACC(NONE)
```

#### **MSMCAPPL**

Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

**Note:** This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

3. Define a profile and permit access to the MSMCAPPL PassTicket session key value for the Started Task user ID so that it can access the SCS address space:

```
RDEFINE PTKTDATA IRRPTAUTH.MSMCAPPL.stc-userid UACC(NONE)
```

#### **stc-userid**

Specifies the user ID associated with the CA CSM application server started task. This user ID only needs the ability to generate a PassTicket for itself.

4. Permit access to the MSMCAPPL PassTicket session key value for the CA CSM application server:

```
PERMIT IRRPTAUTH.MSMCAPPL.stc-userid CLASS(PTKTDATA) ID(stc-userid)
ACCESS(READ,UPDATE)
```

5. Refresh the PTKTDATA class:

```
SETROPTS RACLIST(PTKTDATA) REFRESH
```

## Example: Configure PassTickets for SCS Address Space on Remote Systems

You can use IBM RACF to configure PassTickets on the remote systems where the SCS address space is running.

### Follow these steps:

1. Activate the PassTicket class:

```
SETROPTS CLASSACT(PTKTDATA)
SETROPTS RACLIST(PTKTDATA)
```

2. Define a profile for the application and specify the session key:

```
RDEFINE PTKTDATA MSMCAPPL SSIGNON(KEYMASKED(0123456789ABCDEF)) UACC(NONE)
```

#### ***MSMCAPPL***

Defines the session key for the SCS address space ID used during CA CSM Configuration processing. This name may have been overridden when you installed CA CSM, so it should reflect the real application name.

**Note:** This example demonstrates a complete session key value of 16 hex digits (creating an 8-byte or 64-bit key). Change your key so that it consists of 16 random hex digits, and is different from the values in this example. Each application key must be the same on all systems in the configuration, and the values must be kept secret and secured.

3. Permit access to the MSMCAPPL PassTicket session key value for the SCS address space Started Task user ID:

```
RDEFINE IRRPTAUTH.MSMCAPPL.stc-userid CLASS(PTKTDATA) UACC(NONE)
```

#### ***stc-userid***

Specifies the SCS address space Started Task user ID.

4. Refresh the PTKTDATA class:

```
SETROPTS RACLIST(PTKTDATA) REFRESH
```

You completed site preparation. Your system is ready to install CA CSM.