

CA Chorus™

Site Preparation Guide

Version 04.0.00, Sixth 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 © 2015 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 ACF2™ for z/OS (CA ACF2)
- CA Chorus™
- CA Chorus™ for IMS Database Management
- CA Chorus™ for Security and Compliance Management
- CA Chorus™ for Storage Management
- CA Chorus™ Infrastructure Management for Networks and Systems
- CA Chorus™ Software Manager (CA CSM)
- CA Common Services for z/OS (CA Common Services for z/OS)
- CA Datacom®/AD (CA Datacom/AD)
- CA Datacom/DB®
- CA Easytrieve
- CA Top Secret® for z/OS (CA Top Secret)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

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

Documentation Changes

The following documentation updates have been made since the fifth edition of this documentation:

- [Software Requirements](#) (see page 32)
 - Noted that CA Chorus for DB2 Database Management Release 3.0 is not compatible with CA Chorus Release 4.0. Also noted that pop-up blockers must be disabled before you access your CA Chorus instance.
 - Updated that browser pop-up blockers should be disabled before accessing CA Chorus instance.
- [Installer Security Privileges](#) (see page 39)—Chorus Installer can now also have UID=0 to run ETJIO100.

The following documentation updates have been made since the fourth edition of this documentation:

- Global—Updated to clarify the TSF behavior.
- [How to Authorize Users to Work in CA Chorus](#) (see page 46)—Noted that the CAMFC resource class and entries cannot be modified.
- [Software Requirements](#) (see page 32)—Noted a change in Service Release support. Version 4.0 also supports IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 (5655-W44) in addition to the IBM JDK mentioned previously.

The following documentation updates have been made since the third edition of this documentation:

- [CA Chorus Architecture](#) (see page 11)—Updated the diagram and TSF Bridge description to clarify the TSF behavior.
- [Time Series Facility Architecture](#) (see page 13)—Renamed this topic and updated it to clarify the TSF behavior.
- [Pre-Installation Planning](#) (see page 21)—Noted that you should verify that you are using the most current version of the documentation before beginning any site preparation or installation tasks.
- [How to Authorize Users to Work in CA Chorus](#) (see page 46)—Added the security role resource for CA Chorus for IMS Database Management.
- [CA Chorus Server Requirements](#) (see page 34)—Updated to add CA Chorus for DB2 Database Management requirements.
- [Software Requirements](#) (see page 32)—Clarified support for new browsers.
- [Pre-Installation Planning](#) (see page 21) and [Run the CA Chorus Platform Security Job](#) (see page 41)—Added the new ETJ2540T security upgrade job.

- [How the Installation Process Works](#) (see page 15)—Noted that the discipline installation, deployment, and configuration procedures do not apply to CA Chorus for IMS Database Management.

The following documentation updates have been made since the second edition of this documentation:

- [How the Installation Process Works](#) (see page 15)
 - Added a step to activate your discipline using a CFAR.
 - Updated the installation diagram to note the CFAR activation and to note the steps that require the use of CA CSM.
- [Pre-Installation Planning](#) (see page 21) and [Run the CA Chorus Platform Security Job](#) (see page 41):
 - Added links to the ETJI095x security jobs on CA Support Online.
 - Added the new ETJ3040x security upgrade job.
- [CA Chorus Server Requirements](#) (see page 34)—Noted that CA Chorus now automatically configures the heap memory size.
- The following documentation updates have been made since the first edition of this documentation:
- [Software Requirements](#) (see page 32)—Corrected the list of browsers that are supported at the initial release of CA Chorus Platform Version 4.0.

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

- [Data Set and Path Considerations](#) (see page 28)—Added table entry and description for RUNTIME_USER_HLQ.
- [Started Task Considerations](#) (see page 30)—Added the CHORNTSF started task and the CHORTSFB started task.
- [Time Series Facility Considerations](#) (see page 13)—Added a description of the Time Series Facility (TSF) changes.
- [Software Requirements](#) (see page 32)
 - Noted a change in Service Release support. Version 3.0 now supports IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 **Service Release 5 or 7** (5655-W44), including optional JZOS batch launcher. Support for Service Release 7 is new.
 - Noted the backward compatibility PTFs that are required to run Version 3.0 disciplines on the Version 4.0 CA Chorus Platform.
- [System Requirements](#) (see page 35)—Added information about disk space requirements for the CA Chorus installation.

- [Port Requirements](#) (see page 37)—Noted that you can now specify the TSF relay monitor port using the MONPORT parameter in CETJOPTN(TSFRPRMS).
- [Run the CA Chorus Platform Security Job](#) (see page 41)
 - Added the CHORNTSF started task and the CHORTSFB started task.
 - Added a step to restart CA Top Secret.
- [Installer Security Privileges](#) (see page 39)
 - Updated FSACCESS permissions information.
 - Changed BPX.FILEATTR.APF, BPX.FILEATTR.PROGCTL, and BPX.FILEATTR.SHARELIB from optional to required.
- Global
 - Noted the CA Chorus 3.0 to CA Chorus 4.0 migration changes.
 - Removed the manual configuration information.
 - Noted that Recommended Reading is now listed under Content Type on the CA Chorus product page.
 - Renamed the JBoss server to the CA Chorus Application Server.

Contents

Chapter 1: Architecture and Installation Overview 11

CA Chorus Architecture	11
Time Series Facility Architecture	13
How the Installation Process Works.....	15
Installation Methods	18

Chapter 2: Addressing General Prerequisites 21

Pre-Installation Planning	21
Security Administrator and System Programmer Checklists	23
Software Requirements	32
CA Chorus Server Requirements	34
System Requirements	35
CA CSM Dynamic Temporary Storage Requirements (CA Chorus Installation and Deployment)	35
CA CSM Deployment Process Storage Requirement.....	36
Real Storage Recommendations	36
Port Requirements	37
(Optional) SMTP Email Requirements.....	38
USS Parmlib Requirements	38

Chapter 3: Addressing Security Requirements 39

Installer Security Privileges	39
Run the CA Chorus Platform Security Job	41
How to Authorize Users to Work in CA Chorus.....	46
Review User Software Requirements	47
Authorize CA Chorus Users to Access USS Resources	47
Authorize Users to Work in CA Chorus	50
How to Configure CA CSM PassTickets for CA Chorus	56
Sample: Use CA ACF2 to Configure PassTickets for Connecting to CA CSM from CA Chorus	58
Sample: Use CA Top Secret to Configure PassTickets to Connect to CA CSM from CA Chorus	59
Sample: Use IBM RACF to Configure PassTickets to Connect to CA CSM from CA Chorus	61
Update the CA CSM Startup Parameters	64

Chapter 4: Using the Prerequisite Validator 65

How to Use the CA Chorus Prerequisite Validator	65
Install the Prerequisite Validator	66

Run the Prerequisite Validator.....	67
-------------------------------------	----

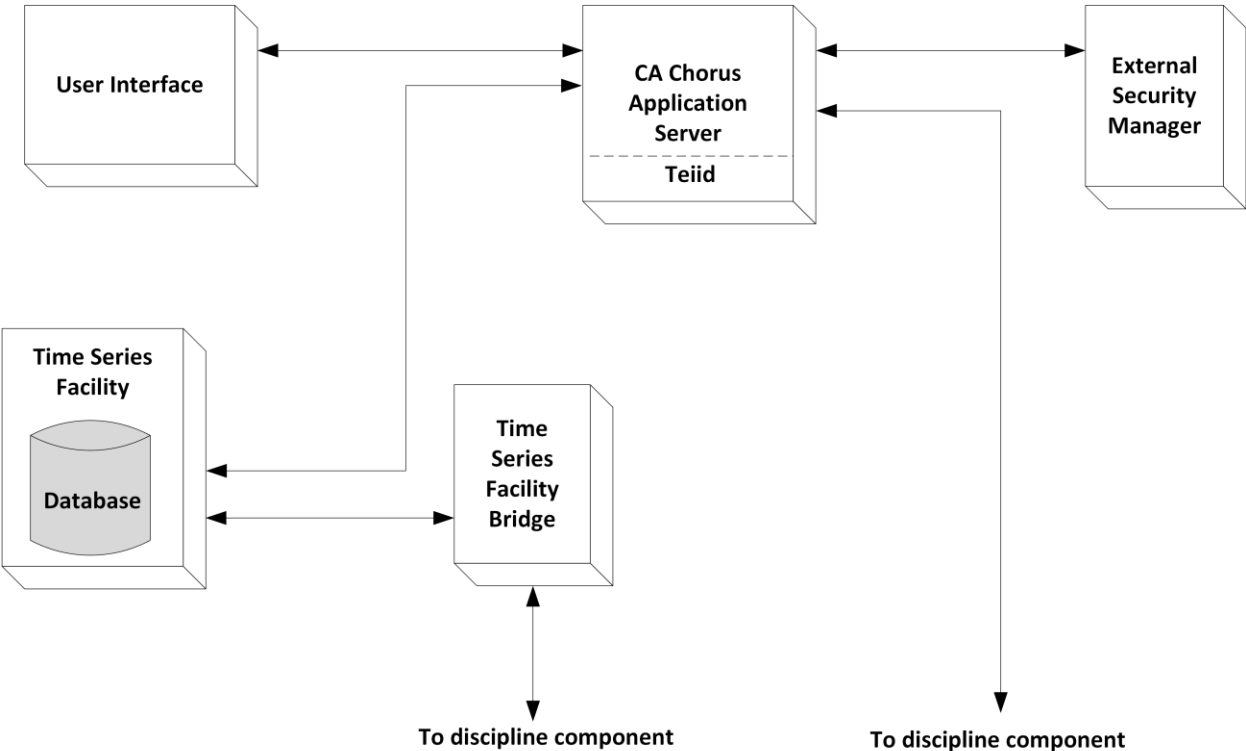
Chapter 1: Architecture and Installation Overview

This section contains the following topics:

- [CA Chorus Architecture](#) (see page 11)
- [How the Installation Process Works](#) (see page 15)
- [Installation Methods](#) (see page 18)

CA Chorus Architecture

The following diagram details the architecture and data flow for CA Chorus components:



The following list details the components and products that you use with CA Chorus:

User Interface

Provides product access using a browser (Firefox or Internet Explorer). The user interface (UI) uses SQL queries to fetch data using [Teiid](#) and different data sources.

CA Chorus Application Server

Hosts the CA Chorus application. This server is a Java-based application server that operates cross-platform.

Teiid

Translates data source content for the CA Chorus Application Server. Teiid is a data virtualization system that lets applications use data from multiple, heterogeneous data stores. Teiid includes tools, components, and services for creating and executing bi-directional data services. Through abstraction and federation, data is accessed and integrated in real time across distributed data sources. This process occurs without copying or otherwise moving data from its system of record.

Time Series Facility (TSF)

Stores data that the CA Chorus products collect and provide. The TSF provides a single point for collection, storage, management, and organization of product performance and other TSF data.

Time Series Facility (TSF) Bridge

Allows TSF client requests to send and store data into the TSF Server.

External Security Manager

Protects resources and access rights to CA Chorus and its disciplines. Each discipline interoperates with CA ACF2, CA Top Secret, and IBM RACF to provide user ID, resource access, and PassTicket security.

Time Series Facility Architecture

The Time Series Facility (TSF) stores the data that the mainframe products collect and provide. The TSF provides a single point for the collection, storage, management, and organization of the product data. You can use the TSF for analyzing your product data, and reporting. TSF data is collected on a periodic basis, which provides useful information about parameters such as performance or usage. Version 4.0 introduces a simplified TSF architecture while maintaining the robust User Interface (UI).

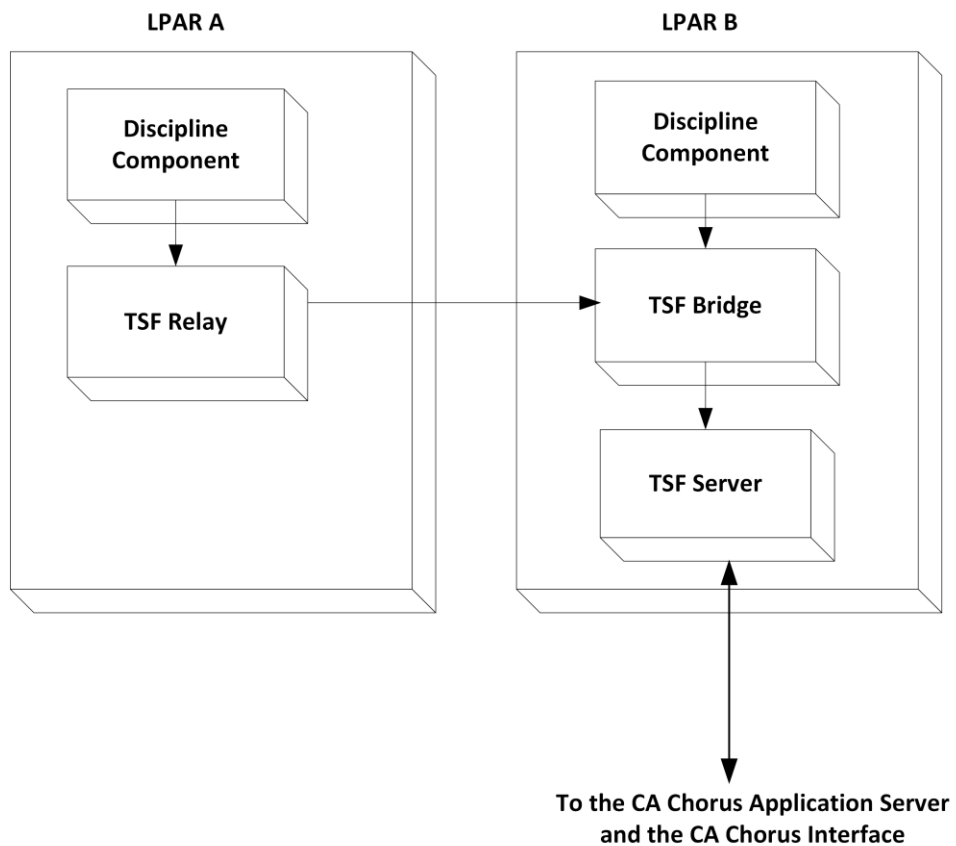
In all releases before Version 4.0, CA Datacom/AD housed the TSF database. The back-end products and CA Chorus then communicated with this database using a TSF Server. Version 4.0 introduces a TSF architecture that eliminates the CA Datacom/AD database, thus simplifying data management and configuration tasks. In this new architecture, the database resides on a file system under the CA Chorus installation. You must route your TSF connections from the CA Chorus disciplines to a TSF Bridge. This bridge then sends your data to the TSF Server. Ultimately, all TSF data reaches the new TSF Server and is housed in its database (not in a CA Datacom/AD database). Therefore, the TSF documentation includes commands and procedures that are related to the TSF Bridge (CHORTSFB) and the new TSF Server (CHORNTSF).

Exceptions

Application developers can push data to the TSF Server using APIs (C or Assembler). If you are a Software Development Kit user, you decide the API to use. This new TSF architecture uses only the CHORNTSF started task. To use the new TSF architecture, configure your application to talk directly to the TSF Server (hostname and port), bypassing the TSF Bridge.

The following diagram shows these TSF configurations:

- LPAR A: Uses the TSF Bridge and TSF Relay on a remote LPAR.
- LPAR B: Uses the TSF Bridge on a local LPAR.



How the Installation Process Works

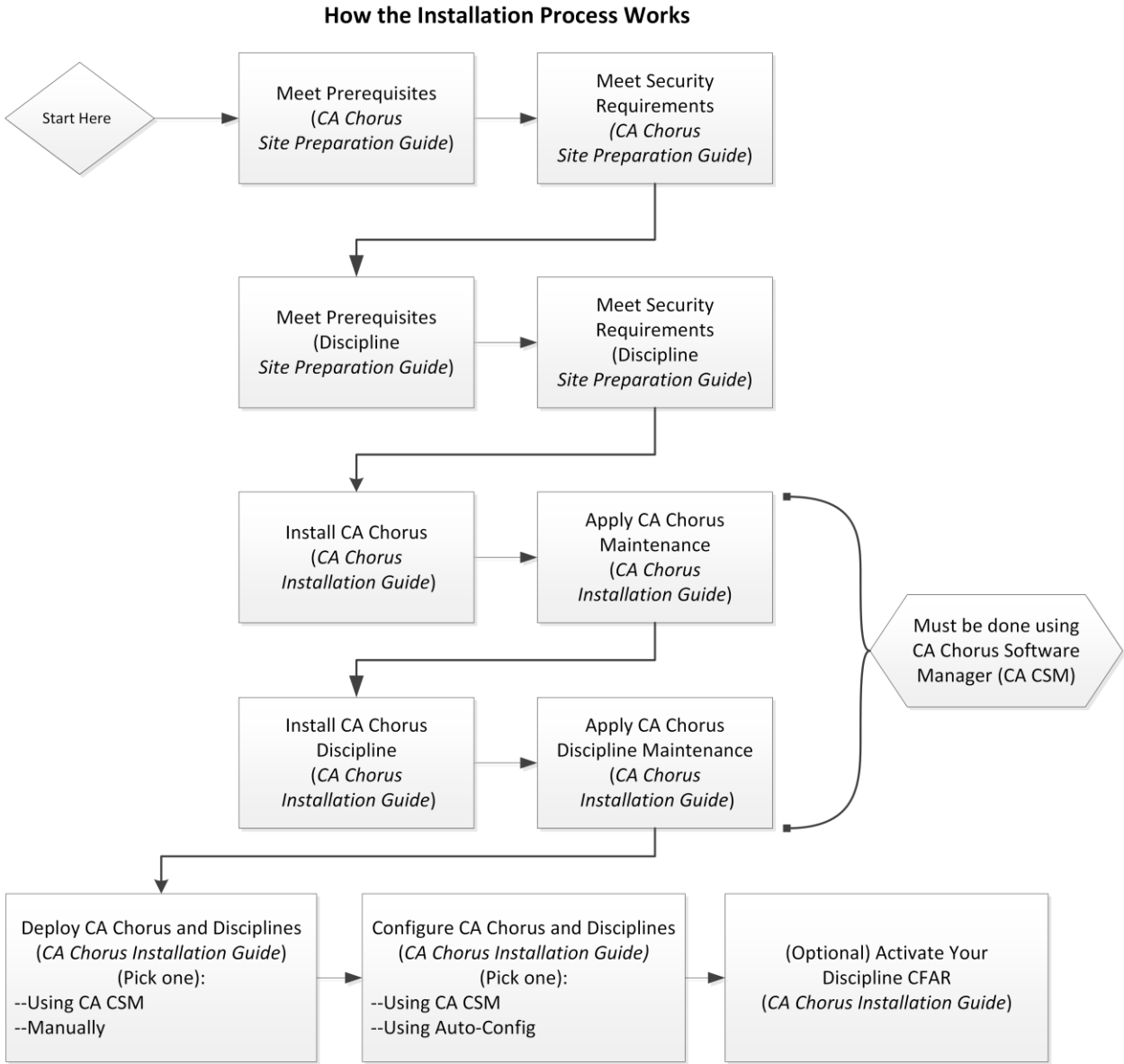
This guide details the tasks that a system programmer and security administrator can complete before starting the installation, deployment, and configuration tasks that are described in the *Installation Guide*. The following diagram provides a high-level overview of the CA Chorus and discipline installation, deployment, and configuration process and the guides that you use.

Important! You must use CA Chorus Software Manager to install CA Chorus and its disciplines.

Important! If you install a discipline, you must deploy and configure it.

Note: For the boxes that indicate work from the discipline *Site Preparation Guide*, repeat this step for each discipline that you are installing.

Important! These discipline installation, deployment, and configuration procedures do not apply to CA Chorus for IMS Database Management. To install this discipline, see the CA Chorus for IMS Database Management *Site Preparation Guide*.



To install, deploy, and configure your CA Chorus and its disciplines, complete the following steps:

1. Meet the software, system, port, and other prerequisites as described in the *CA Chorus Site Preparation Guide*.
2. Meet the security requirements as described in the *CA Chorus Site Preparation Guide*.
3. Meet the software, system, port, and other prerequisites as described in the applicable discipline *Site Preparation Guide*. Repeat this step for each discipline that you are installing.

4. Meet the security requirements as described in the applicable discipline *Site Preparation Guide*. Repeat this step for each discipline that you are installing.
5. Install CA Chorus and the applicable disciplines using CA CSM as described in the *CA Chorus Installation Guide*. This step involves acquiring the CA Chorus software (transporting to your z/OS system) and installing using SMP/E. The installation process creates a CSI environment and runs the RECEIVE, APPLY, and ACCEPT SMP/E steps. The software is untailed.
6. Deploy CA Chorus and the applicable disciplines using CA CSM or a manual process. The *CA Chorus Installation Guide* details both methods.

This step copies the target libraries to another system or LPAR.

Important! For deployments from CA CSM, you must deploy CA Chorus and your disciplines at the same time. For example, installing CA Chorus, Security, and Storage, and then deploying only CA Chorus and Security is not supported.

Important! To use the CA CSM Software Configuration Service, CA CSM deployment is required.

7. Configure CA Chorus and the disciplines. This step creates customized load modules, bringing the CA Chorus software to an executable state. You configure the product using one of the following methods:

CA CSM

This method lets you use the wizard-based CA CSM tools to configure the product. For this configuration method, a deployment using CA CSM is required.

The *Installation Guide* includes the CA Chorus and discipline steps for this method.

Automated Configuration

This method lets you edit one batch job (ETJICUST) and one configuration file. A Java program then propagates your changes to the applicable members. You then manually submit each job. For this option, we recommend that you configure the CA Chorus Platform and disciplines at the same time.

The *Installation Guide* includes the CA Chorus and discipline steps for this method.

8. (Optional) If your discipline uses CA Chorus File Archive (CFAR), activate your discipline CFAR. You must first install, deploy, and configure the CA Chorus Platform and your discipline before you can do so. The *Installation Guide* includes the steps for this activation.

Installation Methods

Before you begin an installation, review each method. Identify the method that applies to your site and then continue to the next topic for an installation overview.

Important! You must use CA Chorus Software Manager to install CA Chorus and its disciplines.

Important! The CA Chorus Platform and each discipline must share the same CSI.

Important! These discipline installation, deployment, and configuration procedures do not apply to CA Chorus for IMS Database Management. To install this discipline, see the CA Chorus for IMS Database Management *Site Preparation Guide*.

CA Chorus Platform + Discipline Installation

You are installing a new instance of the CA Chorus Platform, and you want to install at least one discipline at the same time. Follow the installation instructions and ensure that you install all components into the same CSI name.

New Discipline Installation

You have previously installed the CA Chorus Platform, and possibly one or more disciplines, and you now want to install another discipline.

Note the following rules:

- You must use the same CSI as the existing CA Chorus Platform (and disciplines, if any). You must redeploy and reconfigure this one CSI as one segment.
 - If you use CA CSM to deploy and configure the discipline using CA CSM SCS, redeploy and reconfigure the CA Chorus Platform at the same time using the same CSI.
 - If you use the automatic configuration method, you need only install, deploy, and configure the new discipline.
- After all the discipline configuration steps are completed, run ETJI0150 to enable the new discipline, and restart the CA Chorus Application Server.

Applying Maintenance to existing CA Chorus Platform and Discipline(s)

You have previously installed the CA Chorus Platform, and possibly one or more disciplines, and you now want to apply maintenance to both.

The rules noted in New Discipline Installation apply.

Upgrade CA Chorus

The *Upgrade Guides* explain the steps to upgrade the CA Chorus Platform from Version 3.0 to Version 4.0 or Release 2.5 to Version 4.0. For the upgrade, you must install a new environment, which means you complete the steps in the *Site Preparation Guide* and the *Installation Guide*. You then finalize the configuration and migrate the data based on the steps in the applicable *Upgrade Guide*.

CA Chorus Platform Installation Only - Software Development Kit Implementation

You are installing the CA Chorus Platform to use the Software Development Kit (SDK). This list details the high-level tasks to install the CA Chorus Platform and view sample SDK data in the Investigator.

Important! As you use the guides to install and configure CA Chorus for SDK-only usage, ignore all discipline steps.

- a. Complete all CA Chorus Platform tasks as noted in the *CA Chorus Site Preparation Guide*.
- b. Go to the *CA Chorus Installation Guide*, and complete all CA Chorus Platform installation, deployment, and configuration tasks. Do not start the CA Chorus Application Server yet or attempt to log in to the product.
- c. Go to the *Software Development Kit User Guide* and complete *How to Add Your Data and Metadata to the Investigator*.
- d. Grant access to this SDK using the user authorization steps in the *CA Chorus Site Preparation Guide*.
- e. Start the CA Chorus Application Server (CHORJBOS started task) as noted in the *CA Chorus Installation Guide*.
- f. Complete the Verify the Installation and Configuration steps as noted in the *CA Chorus Installation Guide*.

Chapter 2: Addressing General Prerequisites

This section contains the following topics:

- [Pre-Installation Planning](#) (see page 21)
- [Software Requirements](#) (see page 32)
- [CA Chorus Server Requirements](#) (see page 34)
- [System Requirements](#) (see page 35)
- [Port Requirements](#) (see page 37)
- [\(Optional\) SMTP Email Requirements](#) (see page 38)
- [USS Parmlib Requirements](#) (see page 38)

Pre-Installation Planning

The CA Chorus installation is a detailed process that requires personnel in several areas of expertise. We suggest that you meet with each of the following team members before the installation begins and review the roles of each person:

- Systems programmer for z/OS
- Storage administrator for DASD allocations
- Security administrator for access permissions and security configuration

For this meeting, we recommend that you use the following items:

- [Security Administrator and System Programmer Checklists](#) (see page 23)
- CA Chorus Platform and applicable discipline *Site Preparation Guides*
- *Installation Guide*

- Applicable security job on the [CA Chorus product page](#) under Content Type, Recommended Reading:
 - New installations, or upgrades where you use a unique CA Chorus Administrator ID (CHORADM) for the Version 4.0 region:
 - CA ACF2: [ETJI095A](#)
 - CA Top Secret: [ETJI095T](#)
 - IBM RACF: [ETJI095R](#)
 - Note:** On CA Support Online, the links to the Version 4.0 security jobs are appended with two letters instead of one to differentiate these jobs from the Version 3.0 security jobs: ETJI095AC for CA ACF2, ETJI095TS for CA Top Secret, and ETJI095RA for IBM RACF.
 - Release 2.5 to Version 4.0 upgrades where you use the same CHORADM for the Release 2.5 and Version 4.0 regions and are using CA Top Secret:
 - CA Top Secret: [ETJ2540T](#)
 - If you are using CA ACF2 or IBM RACF, use the ETJI095x security job.
 - Version 3.0 to Version 4.0 upgrades where you use the same CHORADM for the Version 3.0 and Version 4.0 regions:
 - CA ACF2: [ETJ3040A](#)
 - CA Top Secret: [ETJ3040T](#)
 - IBM RACF: [ETJ3040R](#)

Important! Do not begin the installation until all team members have a clear understanding of their installation responsibilities. Failure to do so can impact your ability to complete the installation in a timely manner.

Download the Latest Documentation

We continually update our documentation to provide the most up-to-date information. Verify that you are using the most current documentation, available on CA Support Online, before continuing with your site preparation and installation tasks.

Security Administrator and System Programmer Checklists

Each table in this section outlines high-level installation details. We recommend that the security administrator and the system programmer review each table together. After the review, the administrators must agree to certain details or must be aware of others before either person begins their work in this guide and the *Installation Guide*.

For some entries in the tables, specify the agreed upon value. For other entries, simply coordinate the implementation details.

Important! Do not start any preparation or installation procedures until you have completed the work in these checklists. For example, you need the values in these tables for the security setup and product configuration.

Security Considerations

In the following table, security symbolics lead with & or %. These symbolics appear in the ETJ1095x, ETJ2540x, or ETJ3040x security jobs that the security administrator runs.

%

Indicates a default value.

&

Indicates that you must determine a value.

If a value in the following checklist does not include one of these symbols, you cannot change the value. For example, you must use CAMFC.

Important! For this checklist and the ones in [Data Set and Path Considerations](#) (see page 28) and [Started Task Considerations](#) (see page 30), you can fill in the Value fields in the PDF. To do so, use Adobe Reader. You can also copy each checklist into a single spreadsheet.

ID or Security Entity (Symbolic)	Definition	Value
CHORGRP (%CHORGRP)	CA Chorus Administrative Group Specifies the default group name.	
CHORUGRP (&CHORUGRP)	CA Chorus Users Group (optional) Aids administration by assigning resources to the group rather than to individual users.	

ID or Security Entity (Symbolic)	Definition	Value
CA Chorus Discipline Groups (&CHRDxGRP (where x identifies the discipline))	<p>Aids administration by assigning resources to the group rather than to individual users. (Optional)</p> <p>Users will be connected to the discipline groups which they need for their job function.</p> <p>We recommend using names that follow your site's naming standards and organization.</p>	
CHORADM (%CHORADM)	<p>Administrative (Started Task Owner):</p> <ul style="list-style-type: none"> ■ Owns started tasks. ■ Must have an OMVS segment. ■ Used to generate PassTickets for users. <p>Note: We recommend that the home directory be the same location as the CA Chorus USS installation.</p>	

ID or Security Entity (Symbolic)	Definition	Value
CHORTH (%CHORTH)	<p>Ancillary User:</p> <ul style="list-style-type: none"> ■ Used only as the User ID to access back-end functions when no user is logged in. Primarily used during startup to obtain configuration data. ■ Used in PassTicket generation. The User ID is never used directly for jobs or online access. No one should have access to the password for this user ID. For RACF, a password is required. CA ACF2 or CA Top Secret do not use a password. ■ CHORJBOS must be able to generate PassTickets for CHORTH, and CHORTH must be given access to the appropriate applications (APPLID). ■ Requires the same security permissions as a CA Chorus user, except for the following items: <ul style="list-style-type: none"> -- CAMFC -- CETJOPTV CETJEZTR for CA Easytrieve report execution ■ Some disciplines may need CHORTH authorization for access to back-end products. For details, see the applicable discipline <i>Site Preparation Guide</i>. 	
Installer ID (&INSTALLER)	<p>The user ID of the installer must have update access to the new HLQ and data sets. After installation, update authority can be revoked. For complete details, see Installer Security Privileges (see page 39).</p>	

ID or Security Entity (Symbolic)	Definition	Value
PassTickets	<p>A PassTicket resource is needed by the CA Chorus Platform. The disciplines require additional PassTicket definitions.</p> <p>Will PassTicket access be defined on a group or individual basis?</p> <ul style="list-style-type: none"> ■ Groups are easier to manage and probably permit more decentralization. Group authority remains with central security, but a local (group) administrator controls membership. ■ Some sites may prefer to have the access explicitly shown per user. 	value not required
	<p>The security administrator must select a KEYMASKED or SESSKEY value for each application. However, because it must be protected the values will not be entered here. The same value must be used for the application on all systems.</p> <p>Note: We supply a demo KEYMASKED and SESSKEY value that you can use for the installation; however, we recommend that you use a site-specific value.</p>	value not required
	<p>CHORWEBS (%CHORWEBS): Default application ID for which PassTickets are generated for users. If you intend to use a different APPL, confirm and record that value.</p>	
	<p>CSMAPPLM (&CSMAPPLM): Default application ID for which PassTickets are generated for users launching CA CSM from the Quick Links module. If you intend to use a different APPL, confirm and record that value. These steps do not reside in ETJI095x. See How to Configure CA CSM PassTickets (see page 56).</p> <p>If you are not adding CA CSM as a quick link, ignore this option.</p>	

ID or Security Entity (Symbolic)	Definition	Value
CAMFC	<p>CAMFC is a resource class specifically for CA Chorus. The name of the class and entries are fixed. The CA Chorus Platform has one entry—CHORUS.SETTINGS.KNOWLEDGECENTER: Only users who will update or maintain the user documents in the Knowledge Center need this entry.</p> <p>Each discipline has an entry in this class. The group for the discipline should be permitted read access to the entry for the discipline.</p> <p>Note: CAMFC is a resource class specifically for CA Chorus. The name of the class and entries cannot be modified.</p>	You must use CAMFC.
CAWEBSVR Master Facility	CA Top Secret Only: You must define and add users to this master facility.	CA Top Secret Only: You must use CAWEBSVR
Program Control (APF Authorization)	Data sets named in the steplibs of the started tasks must be under program control (IBM RACF only). For sites using CA ACF2 or CA Top Secret, these libraries must be APF authorized.	n/a
	<p>Libraries with HLQ for Runtime Environment:</p> <ul style="list-style-type: none"> ■ CETJPLD: Includes the CA Chorus library. ■ CC2DPLD: Includes the Time Series Facility (TSF) Bridge product load library. ■ CC2DLOAD: Includes the TSF Bridge library. 	
	<p>(IBM RACF only) Non-CA Chorus Libraries</p> <p>Libraries used by CA Chorus must be in program control even though they are in Linklist and not explicitly named in CA Chorus. These libraries may have been added to program control when their product was installed, but now the system administrator must verify this configuration.</p> <p>The system programmer must supply the site-specific name.</p> <ul style="list-style-type: none"> ■ Java v7 m0 library: &JAVALIB ■ CCS.CAWOLINK: CA CCS library - Release 14.1 (for Version 4.0 CA Chorus) ■ TCPIP.SEZALOAD - ■ SYS1.CSSLIB: A C++ library from IBM 	

Data Set and Path Considerations

In the following table, security symbolics lead with & or %. These symbolics appear in the ETJ1095x, ETJ2540x, or ETJ3040x security jobs that the security administrator runs.

%

Indicates a default value.

&

Indicates that you must determine a value.

If a value in the following checklist does not include one of these symbols, you cannot change the value. For example, you must use CAMFC.

Before completing this checklist, review the following points:

- If data sets have not previously been defined in your security product, a group and profile may also need to be defined, before permitting access by CA Chorus IDs.
- Team must agree to the HLQ for CA Chorus installation. The installation HLQ is different than the runtime environment. Both may need to be defined. No default values are provided for these entries. The sample JCL provides commands for establishing the runtime environment.

Data Sets (Symbolic)	Considerations	Value
TCP (&TCPDATA)	The data set or member of a library as named in the SYSTCPD DD statement of the TCP/IP started task must be available to CHORADM (read only). This data set varies by system.	
Java Library (&JVALIB)	Fully qualified data set name of the PDS/E that contains the JVMLDMnn module installed with JZOS. The Java v7 library must be available to CHORADM and CHORUGRP (read only).	

Data Sets (Symbolic)	Considerations	Value
Java Home (@JAVA_HOME) Note: You do not need this value for security, but you may need the data set which is mounted to it.)	The UNIX System Service (USS) Java Home directory must be read accessible to CHORADM. This may require also read FSACCESS to the mounted filesystem (if FSACCESS is enabled).	
Installation Environment	HLQ: installation environment	
Runtime Environment (\$CAI @RT_HLQ)	HLQ: runtime environment	
RUNTIME_USER_HLQ (%RTUSR_HLQ)	Streamlines identification of key files so you can use a different HLQ for the z/OS files that you create during configuration.	
Time Series Facility Bridge Runtime (\$TSFB)	HLQ for VSAM data sets. If site standards indicate that VSAM files should have particular allocation requirements, a different HLQ can be assigned to VSAM data sets.	
CA Chorus Home Directory Path (&XWORKDIR)	Complete path to the CA Chorus home directory in USS (USS directory where the CA Chorus runtime filesystem will be mounted). The default is /cai/cetjr4m0.	

Data Sets (Symbolic)	Considerations	Value
CA Chorus Java Dump Files	The HLQ used for the JVM SYSDUMP output data set.	

Started Task Considerations

In the following table, security symbolics lead with & or %. These symbolics appear in the ETJI095x, ETJ2540x, or ETJ3040x security jobs that the security administrator runs.

%

Indicates a default value.

&

Indicates that you must determine a value.

If a value in the following checklist does not include one of these symbols, you cannot change the value. For example, you must use CAMFC.

Note: Disciplines may also require jobs or started tasks of their associated products to also be executing. These items are described in the respective product guides.

Important! In the following content, **CHORTSFB** indicates the TSF Bridge started task; **CHORNTSF** indicates the TSF Server started task.

CA Chorus has multiple started tasks and one spawned task. You may name them according to your site standards and preferences. The default names are as follows:

Item (Symbolic)	Definition	Value
CHORJBOS (%CHORJBOS)	CHORJBOS: CA Chorus Application Server Hosts the CA Chorus application.	

Item (Symbolic)	Definition	Value
CHORNTSF (%CHORTNSF)	Time Series Facility (TSF) Server Stores the data that is collected and provided by CA mainframe products. The TSF provides a single point for collection, storage, management, and organization of product performance and other TSF data.	
CHORTSFB (%CHORTSFB)	Time Series Facility (TSF) in a TSF Bridge Configuration Allows TSF client requests to send and store data into the TSF Server.	
CHORTSFR (%CHORTSFR)	Time Series Facility (TSF) Relay Task in a TSF Bridge Configuration A TSF data relay lets you send data collected on a remote LPAR to the TSF. The TSF Relay Task is only used with the TSF Bridge.	
CHORJBOS for DSI	CHORJBOS spawns another task for CA DSI security verification. (Optional) If you want this task to have a different name from the one chosen for CHORJBOS, grant the CA Chorus administrative user ID read access to BPX.SUPERUSER and BPX.DAEMON facilities, and update DSI JOBNAME in CETJOPTN(ENVETJ) after configuration has been run.	

Software Requirements

The following software is required for CA Chorus:

- CA Technologies Software—The following software is required:

Important! The following PTFs are required for backward compatibility. If you do not apply these PTFs, you cannot use Version 3.0 disciplines in CA Chorus Version 4.0.

– For CA Chorus for DB2 Database Management, Version 3.0 is not compatible with CA Chorus Version 4.0.

– For CA Chorus for Security and Compliance Management, apply PTF RO70930.

– For CA Chorus for Storage Management, apply PTF RO71331.

– For CA Chorus Infrastructure Management for Networks and Systems, apply PTF RO70708.

– CA Common Services for z/OS (CCS) Release 14.1 with CAIRIM and CAMASTER service components, and CA Easytrieve Release 11.6.

– Apply all CCS maintenance with the following FIXCAT label: CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.*, where * indicates the version of CA Chorus that you are installing.

CCS: The service components are delivered and installed with CCS. If other CA Technologies products are installed at your site, these services and others may be installed. If these services have not been installed, install them now. For more information about the installation and configuration of these components, see the CCS documentation.

Important! The CAMASTER address space must be running. If it is running, the following message is in the z/OS syslog as part of the IPL portion of messages: CAMS101I CAMASTER INITIALIZATION COMPLETE.

CAMASTER is a noncancelable started task that provides system services and storage resources for various CA products and CCS. CAMASTER uses minimal CPU, and cannot be stopped or restarted.

Note: As part of meeting the CCS prerequisite, the CAWLOAD load library must be APF-authorized.

CA Easytrieve: Before CCS Release 14.1, CA Easytrieve was delivered as the Easytrieve Service CDX8E00. Starting with CCS Release 14.1, CA Easytrieve is delivered as a stand-alone pax installation. A single installation of CA Easytrieve can operate in CCS mode or full functionality mode without requiring multiple installations of CA Easytrieve. CCS 14.1 ships CA Easytrieve Release 11.6 in its package. If you have CA Easytrieve 11.6 installed, you do not need to install the copy that is distributed with CCS 14.1; they are the same. If you do not have CA Easytrieve Release 11.6 installed, follow the instructions that are listed in Appendix B of the *CA Easytrieve Release 11.6 Installation Guide*.

- CA Chorus Software Manager (CA CSM) Release 5.1 and 6.0: You must use CA CSM to install CA Chorus.

Important! With CA CSM Version 6.0, you can now use the Software Configuration Service (SCS) without the requirement to have first used the Software Deployment Service (SDS); however, CA Chorus Version 4.0 does not support this feature. Therefore, if you plan to use SCS for your CA Chorus configuration, you must deploy first using SDS.

- Apply all CA CSM maintenance with the following FIXCAT label: CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.*, where * indicates the version of CA Chorus that you are installing.

Important! Confirm that CA CSM is configured with the system setting to use Product Specific File System. Use the Settings tab in CA CSM to verify this setting. Click Software Installation, scroll to SIS Base Install-File System in the right pane, and verify that the bullet for Product Specific File System is selected.

Important! CA Chorus supports only zFS file systems. HFS file systems are not supported.

- IBM Software—The following software must be available on the systems where you install CA Chorus:
 - IBM z/OS - All supported releases
 - IBM z/OS UNIX System Services (USS) support for zFS file systems
 - IBM z/OS system logger
 - IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 Service Release 5 or 7 (5655-W44), or IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 (5655-W44), including optional JZOS batch launcher.
 - IBM 31-bit SDK for z/OS, Java Technology Edition, Version 7 Release 0 Modification 0 (5655-W43) or IBM 31-bit SDK for z/OS, Java Technology Edition, Version 7 Release 1 (5655-W43), is required to generate batch reports in CA Chorus. This feature uses the CA Easytrieve service component of CCS.

- PC software that is required for each user:
 - Adobe Flash Player 9.0.124 or above
 - At the release of Version 4.0, we have certified CA Chorus for Microsoft Windows Internet Explorer 9 and 11, and Mozilla Firefox 23 through 32. As new browsers are released, we will certify them and post compatibility on the [CA Chorus Browser Compatibility](#).

You can use CA Chorus in new browser releases; however, until each release officially passes our certification test, you may face intermittent issues. If you encounter issues, please contact Support and we will resolve your issue.

Note: Disable pop-up blockers for your browser before accessing your CA Chorus instance. CA Chorus requires a minimum screen resolution of 1024 x 768. If your screen resolution does not meet this requirement, use full screen mode (F11 in most browsers) to include the scroll bar on the display.

CA Chorus Server Requirements

CA Chorus requires 2450 MB of heap memory with the following additional heap requirements for each discipline:

- 200 MB for CA Chorus for DB2 Database Management
- 200 MB for CA Chorus Infrastructure Management for Networks and Systems
- 100 MB for CA Chorus for Security and Compliance Management
- 200 MB for CA Chorus for Storage Management

CA Chorus automatically configures the heap memory size based on the disciplines that you install. This configuration is done during the CA CSM Software Configuration Service (SCS) or in CETJJCL(ETJI0150).

Examples

CA Chorus with all disciplines requires: 2450 MB + 200 MB + 200 MB + 100 MB + 200 MB = 3150 MB.

CA Chorus with the Security discipline and the Storage discipline requires: 2450 MB + 100 MB + 200 MB = 2750 MB.

System Requirements

Confirm that your site addresses the following system requirements:

Processor

CA Chorus uses a JavaVM environment on z/OS. So, we *strongly* recommend that you use a zIIP specialty processor for the best performance and better use of resources.

Disk

Note: All space allocations are approximated values and are described for 3390 DASD and approximated to a near high value.

- For the Installation of CA Chorus Platform: 8000 cylinders.
- For the Deployment of CA Chorus Platform: 5200 cylinders.
- For the Configuration of CA Chorus Platform using Auto-Configuration: 9500 cylinders.
- For the Configuration of CA Chorus Platform using CA CSM Software Configuration Service (SCS): 14000 cylinders.

Note: After you complete the installation, you can delete the pax file to free space.

- Secondary space allocation on the DASD must be available.

Note: For post-installation disk space recommendations for the Time Series Facility, see the *Administration Guide*.

CA CSM Dynamic Temporary Storage Requirements (CA Chorus Installation and Deployment)

During a CA CSM installation and deployment of CA Chorus, approximately 2000 cylinders of CA CSM dynamic temporary file system space is required.

Note: CA CSM allocates temporary file systems as required during product acquisition, installation, deployment, and other tasks. By default, CA CSM keeps a temporary file system for 60 minutes. After the file system has been idle for 60 minutes, CA CSM de-allocates and releases it. By default, the size of the temporary file system is 1000 tracks for primary and secondary. The CA CSM global startup environment variables define the idle time value and allocation settings of the dynamic temporary storage. If the default size values are not sufficient to allow installation or deployment of CA Chorus in your environment, contact CA Support.

A CA CSM user can override where the non-USS storage is allocated by using the CA CSM Software Installation User Settings:

- Approximately 300 cylinders are needed for the data sets that are created using the Temporary Data Set Prefix.
- Approximately 700 cylinders are needed for the data sets that are created using the GIMUNZIP. These cylinders are allocated using the specified GIMUNZIP Data Set Prefix.

CA CSM Deployment Process Storage Requirement

For a CA CSM deployment of CA Chorus, CA CSM requires approximately 2000 cylinders of USS space on the target system to process a deployment.

This storage is not dynamic and must be set up before a CA Chorus deployment. For more information, see the CA CSM product documentation.

Real Storage Recommendations

Implementation of the LFAREA z/OS parameter improves CA Chorus performance. We recommend but do not require its use.

This parameter specifies the amount of real storage to be made available for 1 MB pages. The value that is specified for this parameter indicates the amount of online real storage at IPL to back large pages.

Important! For LFAREA parameter details, see the *IBM z/OS MVS Initialization and Tuning Reference*. If you set or change this value, an IPL is required.

CA Chorus Usage

When using Auto Config, review the instructions about the LFAREA parameter.

```
/*LARGE_PAGE - If LFAREA is enabled for the system, uncomment this
/* option to improve CA Chorus performance. By default the LFAREA
/* for a system is set to NONE. The LFAREA value for the system is
/* specified in the SYS1.PARMLIB(IEASYSxx) member.
/* This option requests the JVM to allocate the Java object heap using
/* large page size of 1M.
/ SET LARGE_PAGE='#IJO="$IJO -Xlp"'
```

When using CA CSM SCS, the CA Chorus large page setting is derived from the CA CSM system registry for LFAREA, and ENVETJ is updated automatically. Therefore, for CA Chorus to use this feature, the LFAREA located in the MVS System profile must be set to a value other than none.

Port Requirements

CA Chorus has the following port requirements for the CA Chorus Application Server and Time Series Facility (TSF) components:

- Thirteen consecutive ports for the CA DSI server and CA Chorus Application server. The CA Chorus Application Server ports consist of one DSI two-way (connecting and listening) port, and 12 server (listening) ports.
- Two ports for the TSF Server. These ports are server (listening) ports similar to the 12 CA Chorus Application Server ports that are noted in the previous bullet.
- One one-way port for the TSF Bridge. (This port does not need to be consecutive with the 13 ports for the CA DSI server and CA Chorus Application Server.) You can specify an actual value (port number), or you can omit the value to let the TSF Bridge dynamically assign a port number.

Note: If the TSF Bridge instances are being used on a remote LPAR, one more one-way port is required to receive data from a relay. You must specify an actual value; dynamic assignment is not supported.

- One one-way port for the TSF Relay. (This port does not need to be consecutive with the 13 ports for the CA DSI server and CA Chorus Application Server.) You can specify an actual value (port number), or you can omit the value to let the TSF Bridge dynamically assign a port number.

Note: The TSF Remote Relay uses an additional port for monitoring the connection from the TSF relay to the TCP/IP stack. By default, this port is dynamically allocated. To specify this port value instead of having it dynamically allocated, edit the MONPORT parameter in the TSFRPRMS member in *your_chorus_hlq*.CETJOPTN.

To confirm that the ports you intend to use are available, consult your network management team.

These ports are configured later in the installation during the CA Chorus Application server and TSF configuration.

(Optional) SMTP Email Requirements

In the Investigator, which resides within the CA Chorus interface, you can specify an email action so that you are notified when a performance policy is met.

For example, you can create a policy in the Investigator to be notified when x number of users unsuccessfully attempt to log into the product in a specified time interval. If you have configured SMTP with the product, you can then receive an email that the policy criteria were met. Doing so automates this type of notification.

If you want your site to use this feature, identify the following information. You use this information later when you configure CA Chorus:

SMTPHOST

Name/IP Address of the SMTP mail server.

SMTPPORT

Port number of the SMTP mail server (1024 through 65535).

USS Parmlib Requirements

In the z/OS parmlib member BPXPRMxx, CA Chorus requires MAXFILEPROC(64000).

To verify the settings, enter the following command from an MVS console:

```
D OMVS,OPTIONS
```

Chapter 3: Addressing Security Requirements

This section contains the following topics:

[Installer Security Privileges](#) (see page 39)

[Run the CA Chorus Platform Security Job](#) (see page 41)

[How to Authorize Users to Work in CA Chorus](#) (see page 46)

[How to Configure CA CSM Passtickets for CA Chorus](#) (see page 56)

Installer Security Privileges

Before you begin the installation process, verify that the CA Chorus installer user ID has the following security privileges defined:

- For UNIX System Services:
 - A valid OMVS definition that includes UID specification for the installer user ID.
 - Superuser authority. You can grant superuser authority for a non-zero UID by assigning BPX.SUPERUSER resource in the FACILITY class with READ access.
Note: Exercise caution while assigning UID(0) to the Installer user IDs. These IDs pass all z/OS UNIX security verifications and can perform any z/OS UNIX function.
 - READ and EXECUTE permissions on the CA Datacom/AD USS directory for CHORADM and CHORGRP. (CA Chorus for Security and Compliance Management only)
 - READ access to the following resources in the FACILITY class:
 - (Optional) BPX.SUPERUSER - only required in case of non-zero UID
 - BPX.FILEATTR.APF
 - BPX.FILEATTR.PROGCTL

- BPX.FILEATTR.SHARELIB

Note: If there is a failure in executing `setuid(0)` while using `UID(0)`, check the `SUPERUSER` parameter in the `BPXPRMxx` member as indicated in [Product Installation Fails for a Product Using a UNIX Directory](#). Also, if you have switched the `UID` from non-zero to zero or vice-versa before commencing the install, ensure to run below commands to avoid issues with `setuid(0)` later when ownership on the file system is incorrectly set. These commands help activate changes to OMVS user profile records.

- For CA ACF2,

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

```
F ACF2,OMVS
```

- For CA Top Secret,

```
TSS MODIFY OMVSTABS
```

- (Optional) BPX.SERVER

- SUPERUSER.FILESYS.PFSCTL profile in UNIXPRIV resource class

(Optional, depending on your site's security configuration) Ability to manipulate zFS data sets. This ability requires `UPDATE` authority to the appropriate entities within the `FSACCESS` class.

Note: Verify with your Security Administrator if `FSACCESS` permissions are needed.

`FSACCESS` lets you secure access to a ZFS file system container (that is, a data set). The resource name is the ZFS file system name.

For example: You defined a ZFS file system that is named `OMVS.ZFS.WEBSRV.TOOLS`, and then you created directories `U1` and `U2` with files in the directories. A resource check for class `FSACCESS` resource `OMVS.ZFS.WEBSRV.TOOLS` occurs when a user tries to access a file in directory `U1` or `U2` in the ZFS file system. For more details, see the applicable security product documentation.

- For z/OS:

- Authority to read, create, update, and execute from the CA Chorus installation data sets and libraries.
- Authority to execute commands to manipulate the external security manager (CA ACF2, CA Top Secret, or IBM RACF) database.

APF authorization and other security requirements that must be performed through an external security product are defined during the CA Chorus configuration process, as described in the *Installation Guide*. You complete those tasks during the installation because you need to access various jobs and members from the installation package.

Run the CA Chorus Platform Security Job

The ETJI095x, ETJ2540T, and ETJ3040x security jobs simplify how you meet many security requirements. You run *one* of these jobs depending on your installation type and external security manager.

Note: In these security jobs, x equals A for CA ACF2, T for CA Top Secret, or R for IBM RACF. These jobs reside on the [CA Chorus product page](#) under Content Type, Recommended Reading.

- ETJI095x for new installations, or for upgrades where you use a unique CA Chorus Administrator ID (CHORADM) for the Version 4.0 region.
- ETJ2540T for upgrades where you use the same CHORADM for the Release 2.5 and Version 4.0 regions and are using CA Top Secret.
- ETJ3040x for upgrades where you use the same CHORADM for the Version 3.0 and Version 4.0 regions.

Important! These jobs and this section apply only to CA Chorus Platform security. The discipline *Site Preparation Guides* address additional security requirements. Before proceeding with this topic, determine if your discipline offers a security job. To do so, check the discipline product page under Content Type, Recommended Reading. To simplify security administration, we recommend that you run these jobs at the same time.

The following list details the security requirements that the job addresses.

Important! Review the following conceptual material before you proceed to the steps at the *end of this topic*.

(CA Top Secret only) Master Facility

If you are using CA Top Secret, define a master facility and associate it with the CA Chorus started task. Use CAWEBSVR as the master facility. The master facility (MASTFAC keyword) lets users access the CAWEBSVR facility. Before you can use the facility as a master facility, define it to CA Top Secret as a user facility in the system facilities matrix.

Important! Perform this task only once. If you have added CAWEBSVR to the facilities matrix and you have activated the definition, do not repeat this task.

You then give permission to the CA Top Secret facility CAWEBSVR for every user ACID accessing CA Chorus.

Administrator User ID and Group ID

You run CA Chorus using one user ID (CHORADM by default), which has a defined UNIX System Services (USS) segment, so that the following conditions are met:

- The user ID has a valid UID that is *not* UID(0).
- The shell is specified as the default shell, typically `/bin/sh`.
- The user ID has a valid OMVS group.

Note: We recommend that the home directory be the same as the CA Chorus installation path.

The following security user IDs are created when you run the ETJI095x job. If the default values are not used, change all occurrences of CHORADM, CHORGRP, and CHORTH D in the security job.

CHORADM

Started task user ID that is used to run CA Chorus.

CHORGRP

Default group name. This group creates a relationship among all relevant security objects.

CHORTH D

User ID for PassTicket requests related to applications.

Note: Unique USS UIDs and GIDs (user ID and group ID numbers) must be used for the CA Chorus started task user IDs. Select a UID and GID that numerically match to track them easier.

Important! All users, including the installer, must have access to the group specified in this member. The default group is CHORGRP.

Started Tasks

The following started tasks are defined when you run the ETJ1095xx job. The default values are shown. If you do not use default names for the started tasks, change the names in the security job.

Note: We recommend that all CA Chorus tasks run as a started task with REGION=0M. If your site restricts the REGION=0M parameter, we recommend that you run with the maximum region size permitted.

Important! In the following content, CHORTSFB indicates the TSF Bridge started task; CHORNTSF indicates the TSF Server started task.

CHORTSFB

Started task name that is associated with the TSF Bridge.

CHORNTSF

Started task name that is associated with the Time Series Facility (TSF) Server.

CHORTSFR

Started task name that is associated with the TSF Relay for a remote TSF configuration. This started task is created only if TSF data relays are defined.

CHORJBOS

Started task name that is associated with the CA Chorus Application Server.

Resource Class

CA Chorus defines security resources in class CAMFC, which you define using your security product. You then assign permissions for users to the discipline-specific resources as applicable. For more information about the required user permissions, see the discipline-specific installation guides.

Note: CAMFC is a resource class specifically for CA Chorus. The name of the class and entries cannot be modified.

PassTickets for General Users

The CA Chorus server generates PassTickets that permit users to access the various back-end products that the CA Chorus disciplines use. As users access components, PassTickets are generated to validate the requests.

The CA Chorus PassTicket configuration includes the following systems:

- One z/OS system running the CA Chorus Application server and the back-end products (like CA Detector, CA Compliance Manager, CA Vantage SRM, and CA NetMaster NM for TCP/IP) that are required for the CA Chorus disciplines on the same system. This type of system is a CA Chorus server system.

- Additional z/OS systems running only the products and components that the CA Chorus disciplines require. This type of system is known as a CA Chorus remote system.

The CA Chorus server system provides the entry point for CA Chorus users. Users can then access all of the CA Chorus remote systems that they have been authorized to use in your network of z/OS systems.

The PassTicket configuration for the security product must be done on each z/OS system that is hosting a component that CA Chorus uses. Configure PassTickets in your z/OS security products to enable the generation and validation of connections that are required for CA Chorus disciplines. If your site meets the following criteria, no additional security setup is required on the remote systems:

- The security products in your z/OS configuration are using a shared security database.
- You want to add one or more remote systems, only the CA Chorus server system setup is required.

If the requisite products and components exist on a remote system that does not share the security database, additional security setup is required on the remote systems.

PassTickets for CA CSM Users

CA Chorus uses PassTicket security to let users launch CA CSM from the Quick Links module without requiring another user login. All systems using PassTickets must have identical application names and session keys for all nodes on the network. Note the following requirements:

- If your CA Chorus instance and CA CSM instance reside on *different* machines, after you run this job, complete the applicable steps in [How to Configure CA CSM PassTickets for CA Chorus](#) (see page 56).
- If your CA Chorus instance and CA CSM instance reside on the *same* machines, after you run this job, CA CSM PassTicket configuration is complete, with one exception. If you are using CA ACF2, complete the one CA Chorus server side and CA CSM side step in [Sample: Use CA ACF2 to Configure PassTickets for Connecting to CA CSM from CA Chorus](#) (see page 58).

Follow these steps:

1. Retrieve the security job that applies to your installation type and external security manager:
 - a. For new installations, or for upgrades where you use a unique CA Chorus Administrator ID (CHORADM) for the Version 4.0 region:
 - CA ACF2: [ETJI095A](#)
 - CA Top Secret: [ETJI095T](#)
 - IBM RACF: [ETJI095R](#)

Note: On CA Support Online, the links to the Version 4.0 security jobs are appended with two letters instead of one to differentiate these jobs from the Version 3.0 security jobs: ETJI095AC for CA ACF2, ETJI095TS for CA Top Secret, and ETJI095RA for IBM RACF.
 - b. For Release 2.5 to Version 4.0 upgrades where you use the same CHORADM for the Release 2.5 and Version 4.0 regions and are using CA Top Secret:
 - CA Top Secret: [ETJ2540T](#)
 - If you are using CA ACF2 or IBM RACF, use the ETJI095x security job.
 - c. For Version 3.0 to Version 4.0 upgrades where you use the same CHORADM for the Version 3.0 and Version 4.0 regions:
 - CA ACF2: [ETJ3040A](#)
 - CA Top Secret: [ETJ3040T](#)
 - IBM RACF: [ETJ3040R](#)

2. Review the entire job.
3. Edit the job according to the comments.
4. Submit the job.

The noted security requirements are met.

5. (CA Top Secret only) Complete the following steps:
 - a. Add the following lines to the applicable CA Top Secret parameter file (PARMFILE):

```
FACILITY (USERxx=NAME=CAWEBSVR)
FACILITY (CAWEBSVR=PGM=***** )
FACILITY (CAWEBSVR=ACTIVE, SHRPRF, MULTIUSER, AUTHINIT)
```

xx

User facility number. Use any available user facility number on your system.

Important! The xx value must match the value that you specified when you ran the security job.

- b. Restart CA Top Secret.

How to Authorize Users to Work in CA Chorus

This scenario shows how a security administrator authorizes users to work in CA Chorus (Platform and disciplines). For CA Chorus, the security administrator must perform the following tasks:

- Authorize and confirm each user UNIX System Services (USS) environment.
- Authorize users to work in CA Chorus and its disciplines using the applicable External Security Manager (ESM).

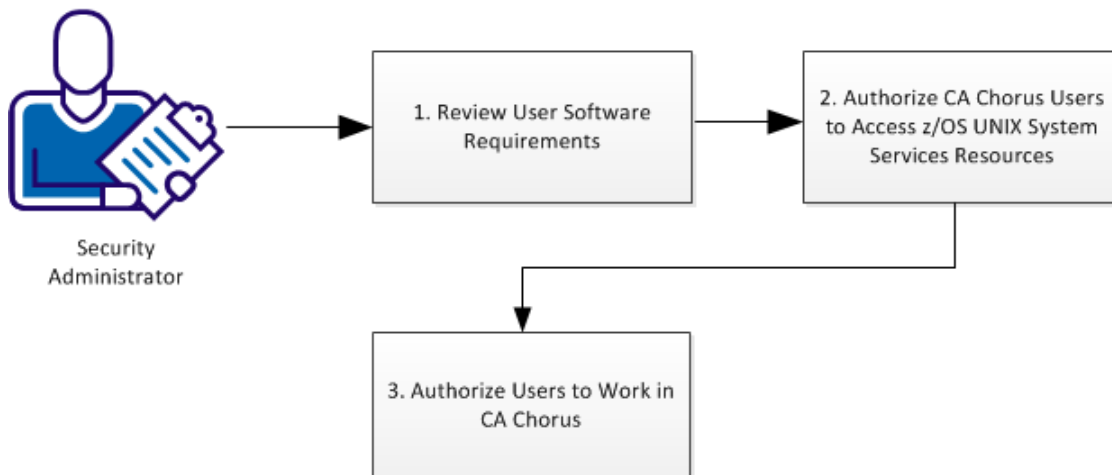
Note: CAMFC is a resource class specifically for CA Chorus. The name of the class and entries cannot be modified.

To perform these authorizations, the security administrator uses CA ACF2, CA Top Secret, or IBM RACF.

The following illustration describes the tasks to authorize users to work in CA Chorus and its supported disciplines:

Note: You can complete the tasks in any order; however, we recommend that you perform the tasks in the order that is shown in this diagram.

How to Authorize Users to Work in CA Chorus



Complete the following tasks to authorize users to work in CA Chorus:

1. [Review User Software Requirements](#) (see page 47).
2. [Authorize CA Chorus Users to Access z/OS UNIX System Services Resources](#). (see page 47)
3. [Authorize Users to Work in CA Chorus](#) (see page 50).

Review User Software Requirements

- PC software that is required for each user:
 - Adobe Flash Player 9.0.124 or above
 - At the release of Version 4.0, we have certified CA Chorus for Microsoft Windows Internet Explorer 9 and 11, and Mozilla Firefox 23 through 32. As new browsers are released, we will certify them and post compatibility on the [CA Chorus Browser Compatibility](#).

You can use CA Chorus in new browser releases; however, until each release officially passes our certification test, you may face intermittent issues. If you encounter issues, please contact Support and we will resolve your issue.

Note: CA Chorus requires a minimum screen resolution of 1024 x 768. If your screen resolution does not meet this requirement, use full screen mode (F11 in most browsers) to include the scroll bar on the display.

Authorize CA Chorus Users to Access USS Resources

The CA Chorus components and disciplines use z/OS TCP/IP communications services and z/OS UNIX System Services (USS). Define an OMVS segment for each user so that they can access z/OS USS resources when working in CA Chorus. Use CA ACF2, CA Top Secret, or IBM RACF to enable this access.

To authorize CA Chorus users to access z/OS USS resources, define an OMVS segment for each user that contains the following options:

- A default shell program specification (PROGRAM or OMVSPGM)
- A numeric z/OS USS user ID (UID)

Note: A policy could exist at your site for assigning OMVS UID numbers. If not, use a unique number.

- A numeric z/OS USS group ID (GID)

Follow these steps:

1. Confirm whether the user has access to the OMVS segment:

- CA ACF2:
LIST *userid* profile(all) section(all)
- CA Top Secret:
TSS LIST(*userid*) DATA(ALL)
- IBM RACF:
LISTUSER *userid* OMVS NORACF

If the user does not have this access, go to the next step.

2. Create a home directory to associate with each user ID (UID).

For example, to set up a directory 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
```

3. Confirm the owner and access to the directory:

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

The following sample results appear:

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

The bold areas show that the correct owner and read/write access exists.

4. Define the OMVS segment using your security product:

Note: A valid group record must exist before executing these commands.

- CA ACF2:
CHANGE *userid* UID(*uid*) HOME(*path_name*) OMVSPGM(/bin/sh)
GROUP(*ggggg*)
- CA Top Secret:
TSS ADD(*userid*) HOME(*path_name*) OMVSPGM(/bin/sh) UID(*uid*)
GROUP(*ggggg*) DFLTGRP(*ggggg*)
- IBM RACF:
ALU *userid* OMVS(UID(*uid*) HOME(*path_name*) PROGRAM(/bin/sh))
GROUP(*ggggg*) DFLTGRP(*ggggg*)

The following syntax variables apply to all three security products:

userid

Identifies the user ID.

path_name

Identifies the home directory to associate with each user ID.

uid

Identifies the user identification (UID) number.

ggggg

Identifies the OMVS group.

5. Confirm the contents of the OMVS segment:

■ CA ACF2:

LIST *userid* profile(all) section(all)

■ CA Top Secret:

TSS LIST(*userid*) DATA(ALL)

■ IBM RACF:

LISTUSER *userid* OMVS NORACF

The user now has a defined OMVS segment and can access USS, which is required for users to work in CA Chorus.

Authorize Users to Work in CA Chorus

You can add or remove access permissions to CA Chorus supported disciplines. These permissions ensure that users have access to the disciplines and functions that they need. CA Chorus uses a resource name high-level qualifier of CHORUS for all the permissions that are required. CA Chorus checks that users have READ access to applicable resources. You can also modify the permissions:

- To manage content in the Knowledge Center. The Knowledge Center is a repository for all the documentation in CA Chorus. Content can include CA product documentation, user-generated documentation, Chicago-Soft MVS/Quick-Ref, websites, and links to third-party documentation.
- To grant access to the web-entitled user interface. This interface includes the Tutorials module, Web Application module, Text module, Quick Links module, and the Knowledge Center. For access to all other modules, the user must have access to the Software Development Kit or a discipline.
- To use the auto-refresh option.
- To use CA Chorus File Archive (CFAR) to package your files and to deploy the package through the ETJICFAR job to the CA Chorus Application Server. After integrating your product, you can add your discipline-specific quick links and the Knowledge Center data sources.

For all permissions, you authorize users with CA ACF2, CA Top Secret, or IBM RACF commands.

- Authorize a User with CA ACF2.
- Authorize a User with CA Top Secret.
- Authorize a User with IBM RACF.

Sample: Authorize a User with CA ACF2

Use this procedure to identify the users that can log in to CA Chorus and can use specific disciplines and tools. The commands in this procedure are samples. For detailed information about using these commands, see the *CA ACF2 Administration Guide*.

To define user access permissions:

```
SET RESOURCE(MFC)
RECKEY CHORUS ADD(resource-name UID(uid-of-userid1) SERVICE(READ)
ALLOW)
RECKEY CHORUS ADD(resource-name UID(uid-of-userid2) SERVICE(READ)
ALLOW)
...
RECKEY CHORUS ADD(resource-name UID(uid-of-useridn) SERVICE(READ)
ALLOW)
```

resource-name

Identifies the CA Chorus resource that the user is permitted to access.

ADMIN.CFAR

Controls access to the CFAR operations of deploy, undeploy, replace, and config.

Note: The CFAR operations fail without this access.

ROLE.IMSTOOLS

Controls access to CA Chorus for IMS Database Management functions.

ROLE.INFRASTRUCTURE

Controls access to CA Chorus Infrastructure Management for Networks and Systems functions.

ROLE.SECURITY

Controls access to CA Chorus for Security and Compliance Management functions (UI and batch).

ROLE.SDK*instance*

Controls access to an SDK. CA Chorus can support multiple SDKs. Work with the system administrator and application developer to define and share this name. We recommend that the application developer use this name to build the files necessary to support the SDK. For more details, see the *Software Development Kit User guide*.

instance

An alphanumeric string to identify this resource for your SDK.

ROLE.STORAGE

Controls access to CA Chorus for Storage Management functions.

SETTINGS.KNOWLEDGECENTER

Indicates that the user can index content in the Knowledge Center.

SETTINGS.AUTOREFRESH

Indicates that the user can use the auto-refresh option.

uid-of-userid1, uid_of_userid2, ..., uid_of_useridn

Identifies the UID of the CA Chorus user requesting access.

READ

Indicates that the user has READ access.

The user has access to the specified resources and can log in and work in CA Chorus.

Example

The following commands grant user ABC1 the following abilities:

- Log in to CA Chorus.
- Modify the documentation in the Knowledge Center.
- Use the auto-refresh option.

```
SET RESOURCE(MFC)
RECKEY CHORUS ADD(SETTINGS.KNOWLEDGECENTER UID(*****ABC1)
SERVICE(READ) ALLOW)
RECKEY CHORUS ADD(SETTINGS.AUTOREFRESH UID(*****ABC1)
SERVICE(READ) ALLOW)
```

Sample: Authorize a User with CA Top Secret

Use this procedure to identify the users that can log in to CA Chorus and can use specific disciplines and tools. The commands in this procedure are samples. For detailed information about using these commands, see the *CA Top Secret Command Functions Guide* and *CA Top Secret Control Options Guide*.

As you set up user authorizations, consider the following points:

- Longer entity names where a single level is longer than 8 bytes do not lend themselves to using an asterisk mask. We recommend a floating point mask.
- Be careful when using prefixed permissions because you can impact multiple calls and not just the discipline login itself.

To define user access permissions:

```
TSS PERMIT(acid1) CAMFC(resource-name) ACCESS(READ)
TSS PERMIT(acid2) CAMFC(resource-name) ACCESS(READ)
...
TSS PERMIT(acidn) CAMFC(resource-name) ACCESS(READ)
```

resource-name

Identifies the CA Chorus resource that the user is permitted to access.

CHORUS.ADMIN.CFAR

Controls access to the CFAR operations of deploy, undeploy, replace, and config.

Note: The CFAR operations fail without this access.

CHORUS.ROLE.IMSTOOLS

Controls access to CA Chorus for IMS Database Management functions.

CHORUS.ROLE.INFRASTRUCTURE

Controls access to CA Chorus Infrastructure Management for Networks and Systems functions.

CHORUS.ROLE.SECURITY

Controls access to CA Chorus for Security and Compliance Management functions (UI and batch).

CHORUS.ROLE.STORAGE

Controls access to CA Chorus for Storage Management functions.

CHORUS.ROLE.SDKinstance

Controls access to an SDK. CA Chorus can support multiple SDKs. Work with the system administrator and application developer to define and share this name. We recommend that the application developer use this name to build the files necessary to support the SDK. For more details, see the *Software Development Kit User Guide*.

instance

An alphanumeric string to identify this resource for your SDK.

Important! Use *unique* names for your SDK instance. Be aware of like-named SDK instances because you can erroneously apply permissions. For example, CHORUS.ROLE.SDKROLE1 and CHORUS.ROLE.SDKROLE123 would have the same permissions. The same masking restrictions apply for letters and numbers.

CHORUS.SETTINGS.KNOWLEDGECENTER

Indicates that the user can index content in the Knowledge Center. Indexing the content lets the user add or remove documentation from this repository.

CHORUS.SETTINGS.AUTOREFRESH

Indicates that the user can use the auto-refresh option. This option refreshes the data that appears in the CA Chorus UI whenever the back-end data changes.

acid1, acid2, ..., acidn

Identifies the ACID of the CA Chorus user requesting access. The ACID can be a user or a profile.

READ

Indicates that the user has READ access.

The user has access to the specified resources and can log in and work in CA Chorus.

Example

The following commands grant user ABC1 the following abilities:

- Log in to CA Chorus.
 - Modify the documentation in the Knowledge Center.
 - Use the auto-refresh option.
- ```
TSS PERMIT(ABC1) CAMFC(CHORUS.SETTINGS.KNOWLEDGECENTER)
ACCESS(READ)
TSS PERMIT(ABC1) CAMFC(CHORUS.SETTINGS.AUTOREFRESH) ACCESS(READ)
```

### Sample: Authorize a User with IBM RACF

Use this procedure to identify the users that can log in to CA Chorus and can use specific disciplines and tools. The following commands are samples. For detailed information about using these commands, see the IBM RACF product documentation.

#### Follow these steps:

1. Add each discipline resource to CAMFC:

**Note:** This step is not required for feature-based resources (for example, auto-refresh). You need only perform this step one time. If you have defined the resource to CAMFC, go to step 2.

```
RDEFINE CAMFC CHORUS.ROLE.discipline UACC(NONE)
```

#### *discipline*

```
IMSTOOLS
INFRASTRUCTURE
SECURITY
STORAGE
```

**Note:** For a detailed explanation of each discipline resource, see step 2.

The applicable discipline resource is assigned to CAMFC. You can now give users access to the discipline.

2. Permit user access to specific resources:

```
PERMIT resource-name ID(uid-of-userid1) AC(READ) CLASS(CAMFC)
PERMIT resource-name ID(uid-of-userid2) AC(READ) CLASS(CAMFC)
...
PERMIT resource-name ID(uid-of-useridn) AC(READ) CLASS(CAMFC)
```

***resource-name***

Identifies the CA Chorus resource the user is permitted to access.

**CHORUS.ADMIN.CFAR**

Controls access to the CFAR operations of deploy, undeploy, replace, and config.

**Note:** The CFAR operations fail without this access.

**CHORUS.ROLE.IMSTOOLS**

Controls access to CA Chorus for IMS Database Management functions.

**CHORUS.ROLE.INFRASTRUCTURE**

Controls access to CA Chorus Infrastructure Management for Networks and Systems functions.

**CHORUS.ROLE.SECURITY**

Controls access to CA Chorus for Security and Compliance Management functions (UI and batch).

**CHORUS.ROLE.STORAGE**

Controls access to CA Chorus for Storage Management functions.

**CHORUS.ROLE.SDK*instance***

Controls access to an SDK discipline. CA Chorus can support multiple SDKs. Work with the system administrator and application developer to define and share this name. We recommend that the application developer use this name to build the files necessary to support the SDK. For more details, see the *Software Development Kit User Guide*.

**Note:** *instance* is an alphanumeric string to identify this resource for your SDK.

**CHORUS.SETTINGS.KNOWLEDGECENTER**

Indicates that the user can index content in the Knowledge Center. Indexing the content lets the user add or remove documentation from this repository.

**CHORUS.SETTINGS.AUTOREFRESH**

Indicates that the user can use the auto-refresh option. This option refreshes the data that appears in the CA Chorus UI whenever the back-end data changes.

***uid-of-userid1, uid\_of\_userid2, ..., uid\_of\_useridn***

Identifies the UID of the CA Chorus user requesting access.

**READ**

Indicates the user has READ access.

3. Activate the changes that are made to the CAMFC resources:

```
SETROPTS RACLIST(CAMFC) REFRESH
```

The changes are activated.

The user has access to the specified resources and can log in and work in CA Chorus.

### Example

The following commands grant user ABC1 the following abilities:

- Log in to CA Chorus.
- Use the functions of CA Chorus for Security and Compliance Management.
- Modify the documentation in the Knowledge Center.
- Use the auto-refresh option.

```
PERMIT CHORUS.ROLE.SECURITY ID(ABC1) AC(READ) CLASS(CAMFC)
```

```
PERMIT CHORUS.SETTINGS.KNOWLEDGECENTER ID(ABC1) AC(READ)
CLASS(CAMFC)
```

```
PERMIT CHORUS.SETTINGS.AUTOREFRESH ID(ABC1) AC(READ) CLASS(CAMFC)
SETROPTS RACLIST(CAMFC) REFRESH
```

## How to Configure CA CSM PassTickets for CA Chorus

CA Chorus uses PassTicket security to let users launch CA CSM from the Quick Links module without requiring an additional user login. All systems using PassTickets must have identical application names and session keys for all nodes on the network.

This scenario shows how a security administrator and system administrator configure PassTickets to let users use CA CSM without requiring an additional user login.

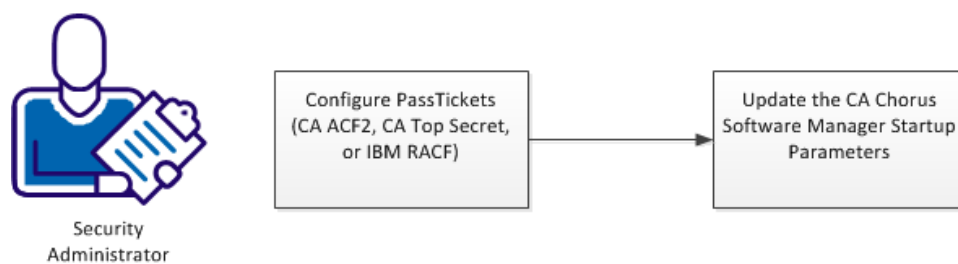
**Important!** The procedures in this scenario assume that you have run the ETJI095x security job. If you have not done so, complete that step first.

A *PassTicket* is a temporary encoded and encrypted substitute for the user password that can be used to access a specific application. The PassTicket must be used within a few minutes of the time it is generated. Using PassTickets enables the z/OS components and products to authenticate a user ID without sending z/OS passwords through the network. Instead, the user is authenticated after they first log in with a valid z/OS user ID and password. The following process occurs when the user selects a function that accesses a z/OS component:

- The CA Chorus web service calls the z/OS security product to generate a PassTicket for access authorization.
- The PassTicket is sent with the user request to the component, possibly on a different z/OS system.
- The component calls the z/OS security product to authenticate the user using the PassTicket as a password substitute before processing the request.

**Note:** Examples are provided for using CA ACF2, CA Top Secret, and IBM RACF to configure PassTickets to connect to CA CSM. These examples are provided as a guideline. For detailed information about using CA ACF2 commands, see the *CA ACF2 Administration Guide*. For detailed information about using CA Top Secret, see the *CA Top Secret Command Functions Guide*. For detailed information about using IBM RACF, see the IBM documentation.

#### How to Configure CSM PassTickets for CA Chorus



To launch and use CA CSM from CA Chorus, complete the following tasks:

1. Configure your security system to use PassTickets. Choose *one* of the following options:
  - [Use CA ACF2 to Configure PassTickets for Connecting to CA CSM from CA Chorus](#) (see page 58)
  - [Use CA Top Secret to Configure PassTickets for Connecting to CA CSM from CA Chorus](#) (see page 59)
  - [Use IBM RACF to Configure PassTickets for Connecting to CA CSM from CA Chorus](#) (see page 61)
2. [Update the CA CSM startup parameters](#) (see page 64).

**Important!** Verify that you use the same CA CSM applid that is used in CA Chorus.

## Sample: Use CA ACF2 to Configure PassTickets for Connecting to CA CSM from CA Chorus

This sample shows how a security administrator configures PassTickets for connecting to CA CSM from CA Chorus after they have run the ETJI095x security job.

**Note:** The commands in this procedure are samples. For detailed information about using these commands, see the *CA ACF2 for z/OS Administration Guide*.

This procedure requires that you set up security on the CA Chorus server and the CA CSM server. The following procedure highlights where you are working and when your focus shifts to a new server. Note the following definitions that apply to both servers:

### ***applid***

Defines the application ID used for PassTicket validation for the CA Chorus Quick Links module. Replace *applid* with your CA CSM applid. For CA CSM configuration details, see [Update the CA CSM Startup Parameters](#) (see page 64).

**Default:** CSMAPPLM

### **MULT-USE**

Lets you reuse the same PassTicket multiple times.

### **SSKEY**

Defines an encryption key for the application in the format of 16 random hexadecimal digits that are different from the values shown in the example.

**Note:** This example demonstrates a complete key SESSKEY value of 16 hexadecimal digits (creating an 8-byte or 64-bit key). Each application key must be the same on all systems in the configuration and the values must be kept secret and secured.

### CA Chorus Server Side Steps

1. Allow individual users to access CA CSM:  
SET RESOURCE(SAF)  
RECKEY *applid* ADD(UID(*chorus\_userid*) SERVICE(READ) ALLOW)  
F ACF2,REBUILD(SAF)

### ***chorus\_userid***

Users who need to access CA CSM through the Quick Links module.

PassTickets are configured on the CA Chorus server side.

### (Optional) CA CSM Server Side Steps

**Note:** If you inserted a GSO CLASMAP record to change the type code for the APPL class to APL, use APL instead of SAF for TYPE in the following commands.

**Important!** If CA Chorus and CA CSM are not on the same machine, steps 1 and 2 are required. Step 3 is required in all situations.

1. Define the CA CSM connection application session key:

```
SET PROFILE(PTKTDATA) DIV(SSIGNON)
INSERT applid SSKEY(0123456789ABCDEF) MULT-USE
F ACF2,REBUILD(PTK),CLASS(P)
```

2. Permit the CA CSM started task user ID to generate and evaluate PassTickets on behalf of CA CSM users:

```
SET RESOURCE(PTK)
RECKEY IRRPTAUTH ADD(applid. - UID(uid-of-csm_stc_userid)
SERVICE(UPDATE,READ) ALLOW)
F ACF2,REBUILD(PTK)
```

***uid\_csm\_stc\_userid***

Specifies the CA CSM application server started task user ID. This ID must be able to generate PassTickets for any user.

**Default:** MSMSERV

3. Allow individual users to access CA CSM:

```
SET RESOURCE(SAF)
RECKEY applid ADD(UID(uid-csm_userid) SERVICE(READ) ALLOW)
F ACF2,REBUILD(SAF)
```

PassTickets are configured on the CA CSM server side.

To complete PassTicket setup, go to [Update the CA CSM Startup Parameters](#) (see page 64).

## Sample: Use CA Top Secret to Configure PassTickets to Connect to CA CSM from CA Chorus

This sample shows how a security administrator configures PassTickets for connecting to CA CSM from CA Chorus after they have run the ETJI095x security job.

**Note:** This procedure assumes that the PTKTDATA class and IRRPTAUTH resource ownership have been defined.

This procedure requires that you set up security on the CA Chorus server and the CA CSM server. The following procedure highlights where you are working and when your focus shifts to a new server. Note the following definitions that apply to both servers:

***applid***

Defines the application ID used for PassTicket validation for the CA Chorus Quick Links module. Replace *applid* with your CA CSM applid. For CA CSM configuration details, see [Update the CA CSM Startup Parameters](#) (see page 64).

**Default:** CSMAPPLM

***department***

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

**SESSKEY**

Defines an encryption key for the application in the format of 16 random hexadecimal digits that are different from the values shown in the example.

**Note:** This example demonstrates a complete key SESSKEY value of 16 hexadecimal digits (creating an 8-byte or 64-bit key). Each application key must be the same on all systems in the configuration and the values must be kept secret and secured.

**SIGNMULTI**

Permits reuse of the same PassTicket multiple times.

### CA Chorus Server Side Steps

When you ran the ETJI095x job, you configured passtickets for this server.

### (Optional) CA CSM Server Side Steps

**Important!** If CA Chorus and CA CSM are not on the same machine, complete this procedure.

1. Define the CA CSM connection application session key:

```
TSS ADDTO(NDT) PSTKAPPL(applid) SESSKEY(0123456789ABCDEF) SIGNMULTI
```

2. Permit the CA CSM started task user ID to generate and evaluate PassTickets on behalf of CA CSM users:

```
TSS PERMIT(esm_stc_userid) PTKTDATA(IRRPTAUTH.applid.) ACCESS(READ,UPDATE)
esm_stc_userid
```

Specifies the CA CSM application server started task user ID. This ID must be able to generate PassTickets for any user.

3. Add the applid to the applicable department:

```
TSS ADDTO(department) APPLICATION(applid)
```

4. Allow individual users to access CA CSM:

```
TSS PERMIT(esm_stc_userid) APPL(applid)
```

PassTickets are configured on the CA CSM server side.

To complete PassTicket setup, go to [Update the CA CSM Startup Parameters](#) (see page 64).

## Sample: Use IBM RACF to Configure PassTickets to Connect to CA CSM from CA Chorus

This sample shows how a security administrator configures PassTickets for connecting to CA CSM from CA Chorus after they have run the ETJI095x security job.

**Note:** Before you begin this procedure, verify that the PTKTDATA class and ownership for the PassTicket resource (IRRPTAUTH) have been defined.

This procedure requires that you set up security on the CA Chorus server and the CA CSM server. The following procedure highlights where you are working and when your focus shifts to a new server. Note the following definitions that apply to both servers:

***applid***

Defines the application ID used for PassTicket validation for the CA Chorus Quick Links module. Replace *applid* with your CA CSM applid. For CA CSM configuration details, see [Update the CA CSM Startup Parameters](#) (see page 64).

**Default:** CSMAPPLM

**KEYMASKED**

Defines an encryption key for the application using values that are different from the values in the sample syntax.

**Note:** The sample syntax demonstrates a complete key value of 16 hexadecimal digits (creating an 8-byte or 64-bit key). Each application key must be the same on all systems in the configuration and the values must be kept secret and secured.

**APPLDATA('NO REPLAY PROTECTION')**

Lets you use the same PassTicket multiple times.

### CA Chorus Server Side Steps

When you ran the ETJ1095x job, you configured passtickets for this server.

### (Optional) CA CSM Server Side Steps

**Important!** If CA Chorus and CA CSM are not on the same machine, complete this procedure.

1. Define the CA CSM connection application session key:

```
SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
RDEFINE PTKTDATA applid SSIGNON(KEYMASKED(FEDCBA9876543210)) APPLDATA('NO
REPLAY PROTECTION')
```

2. Permit the CA CSM started task user ID to generate and evaluate PassTickets on behalf of CA CSM users:

```
SETROPTS GENERIC(PTKTDATA)
RDEFINE PTKTDATA IRRPTAUTH.applid.* CLASS(PTKTDATA) UACC(NONE)
PERMIT IRRPTAUTH.applid.* CLASS(PTKTDATA) ID(csm_stc_userid)
ACCESS(READ,UPDATE)
```

#### ***csm\_stc\_userid***

Specifies the CA CSM application server started task user ID. This ID must be able to generate PassTickets for any user.

**Default:** MSMSERV

3. Allow individual users to access CA CSM:

```
RDEFINE APPL applid UACC(NONE)
PERMIT applid CLASS(APPL) ID(csm_stc_userid) ACCESS(READ)
SETROPTS CLASSACT(APPL)
```

4. Refresh the PTKTDATA class and activate the APPL class:

```
SETROPTS RACLIST(PTKTDATA) REFRESH
SETROPTS CLASSACT(APPL)
```

PassTickets are configured on the CA CSM server side.

To complete PassTicket setup, go to [Update the CA CSM Startup Parameters](#) (see page 64).

## Update the CA CSM Startup Parameters

This procedure shows how the system administrator starts the CA CSM application server with the created CA CSM application ID.

**Follow these steps:**

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

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

***applid***

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

**Default:** CSMAPPLM

2. Restart the CA CSM application server.

The changes take effect.

Users can now access CA CSM from the Quick Links module.

# Chapter 4: Using the Prerequisite Validator

---

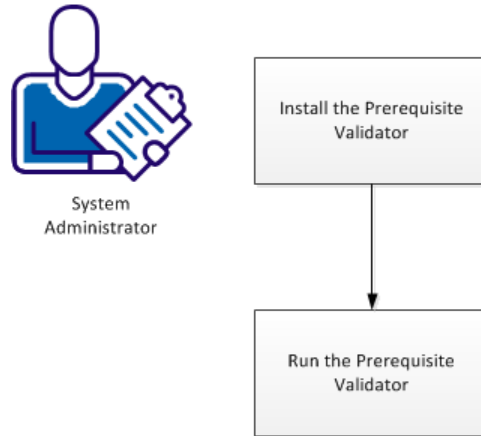
## How to Use the CA Chorus Prerequisite Validator

This scenario shows how a system administrator installs and maintains many products at their site. You want to install products quickly and efficiently. Using the Prerequisite Validator, you can confirm that your site is ready for a CA Chorus installation. If your site fails the validation, you can update your site software before the installation instead of during an installation. The latter can be time consuming and troublesome.

The tool is designed to confirm that you have configured key items correctly, including but not limited to:

- Java version
- z/OS version
- port availability
- SAF resource access
- root access

How to Use the CA Chorus Prerequisite Validator



Complete these steps:

1. [Install the Prerequisite Validator](#) (see page 66)
2. [Run the Prerequisite Validator](#) (see page 67)

## Install the Prerequisite Validator

The packed CA Chorus Prerequisite Validator product package is available on the product page in the Download Center on the CA Support Online website. You can download and unpack it in the same way you download and unpack other mainframe pax files.

### Follow these steps:

1. Log in to CA Support Online, and navigate to the CA Chorus Download Center.  
**Note:** The Prerequisite Validator pax file appears under the CA Chorus Version 4.0 Product list.
2. Download the Prerequisite Validator pax file. You can use a zOS FTP client in batch mode to download the file.
3. Open an OMVS session and change to the directory (using a 'cd' command) where you downloaded the pax file. This directory is the same one that you used in the FTP batch job in the previous step.
4. Unpack ChorusPreValidator.pax.Z using the exact case for the full pax file name:

```
pax -rvf ChorusPreValidator.pax.z
```

### **ChorusPreValidator.pax.z**

Name of the Prerequisite Validator pax file.

**Example:** DVD11094914E.pax.Z

5. Change to the new ChorusPreValidator subdirectory:  

```
cd ChorusPreValidator
```
6. Review the license text file. By running this utility, you accept the license agreement.
7. Review the parameters in the SITE PARAMETERS section in ChrPreval.sh. Change the defaults as is necessary. Use an EBCDIC editor to modify this file.

**Note:** You can use the USS oedit command to start an ISPF edit session. Enter 'oedit ChrPreval.sh' at the OMVS command line.

## Run the Prerequisite Validator

You can execute the Prerequisite Validator utility directly from the native USS command prompt.

### Follow these steps:

1. If your OMVS session is still running, skip this step. Otherwise, open an OMVS session, and change to the ChorusPreValidator subdirectory:

```
cd downloadDir/ChorusPreValidator
```

#### ***downloadDir***

Directory where you downloaded the Prerequisite Validator pax file.

2. Run the utility:

```
sh ChrPreval.sh
```

Upon successful execution, the Prerequisite Verification report appears in browse mode and the following files are generated:

- ChorusValidatorReport.txt
  - ChorusPre-ValidationLogyyyy-mm-dd, hh-mm-ss, ttt.log
3. If the utility output meets all required acceptance criteria, you can now install and configure the product.
  4. Choose one of the following options:
    - If you are only installing the CA Chorus Platform, go to the *Installation Guide*.
    - If you are installing a discipline, go to the applicable *Site Preparation Guide*.