CA XCOM™ Data Transport® Management Center

Product Guide

r11.5

ca technologies

2nd Edition

Contact CA Technologies

Contact CA Support

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

- 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

Provide Feedback

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

If you would like 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.

CA Technologies Product References

This document references the following CA Technologies products:

- CA XCOM™ Data Transport® (CA XCOM Data Transport)
- CA XCOM™ Data Transport® Gateway (CA XCOM Gateway)
- CA XCOM™ Data Transport® Management Center (CA XCOM Management Center)

Contents

Chapter 6: Using CA XCOM Management Center Through the Internet   109

Glossary   243

Index   245

Chapter 1: Introduction

This section contains the following topics:

CA XCOM Data Transport Management Center

The CA XCOM Data Transport Management Center (CA XCOM Management Center) is a platform-independent application. It enables users to use web browsers to schedule data transfers between local and remote CA XCOM Data Transport servers, and it gives them access to history records and to the status of previously scheduled transfers.

CA XCOM Management Center uses Transmission Control Protocol/Internet Protocol (TCP/IP) to communicate with a CA XCOM Data Transport server.

Communication and Management

Users can communicate with CA XCOM Management Center by using its website, to schedule data transfers and access to history records.

The CA XCOM Management Center server contains and communicates with the following parts:

■ Relational database tables

■ HTTP server

■ CA XCOM Interface Server
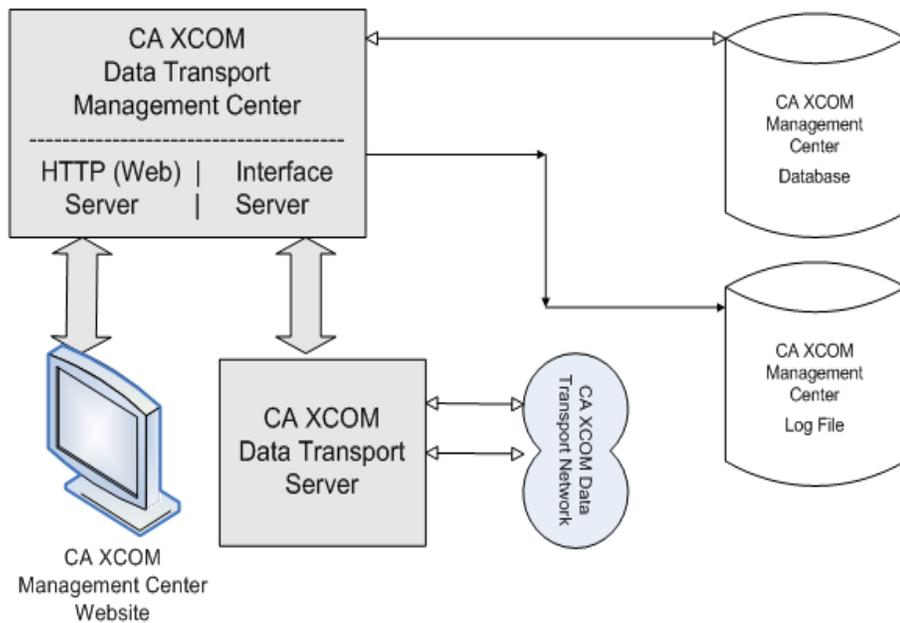
Relational Database Tables

The CA XCOM Management Center uses a set of relational database tables to save and handle the data related to the operation of the interface. Through these database tables, the users and servers defined to the system are grouped and the user's authorization for different functions is defined.

The following database tables are used internally by CA XCOM Management Center:

- Users

- Groups

- User-Group-Subscription

- Servers

- Server-Group-Subscription

- Servers

- Configuration

HTTP Server Component

The HTTP Server also hosts the CA XCOM Management Center website, which provides the ability to perform functions such as schedule transfer access to history records and CA XCOM Management Center administration.

CA XCOM Interface Server

The CA XCOM Interface Server performs the following services:

- Schedules a set of transfers for processing by CA XCOM Data Transport.

- Acts as a bridge, providing communication and connectivity between CA XCOM Management Center and a local CA XCOM Data Transport server.

CA XCOM Data Transport Server

Performs the transfer of requests and responses between the CA XCOM Management Center server and other servers in the CA XCOM Data Transport network.

CA XCOM Management Center Terms

Client Connection and Authentication

Client users identify themselves by user ID and password; these are authenticated credentials.

Authorization

The user ID is authenticated during the logon process. The user's level of authorization is ascertained by referencing a local database.

User authorizations are customer configurable and control both of the following:

- Administrative capabilities
- Configuration file processing capabilities

Transfer Protocol

CA XCOM Management Center acts as a server and supports the Hypertext Transfer Protocol (HTTP) using a web browser.

CA XCOM Management Center also accepts HTTPS client connection, to permit encryption of data.

Global Parameters File

This file is in XML format. It stores parameters required for CA XCOM Management Center processing. CA XCOM Management Center accesses this file to get parameters required to process different functions. The file is accessible and can be modified by the Super Admin user.

Export and Import Process

CA XCOM Management Center users with proper authority can export configuration files and server information and save the exported data as an XML file on the web server. These exported files can later be imported and their content can be processed by CA XCOM Management Center.

Chapter 2: System Requirements and Setup

This section contains the following topics:

System Requirements

The system requirements for CA XCOM Management Center are as follows:

- CA XCOM Data Transport r11.5

- Java JDK 6

- JBoss Application Server 4.0.5GA

- MySQL® version 5 or DB2 UDB version 9

- IE 7.0 or 8.0, or Firefox 3.5

Note: With the CA XCOM Management Center software, CA Technologies provides a separate CD containing the JBoss Application Server 4.0.5GA. This CD is called JBoss Application Server 4.0.5GA – CD.

Operating Systems

CA XCOM Management Center runs on the following operating systems.

- All versions of Windows that are supported by CA XCOM Data Transport r11.5

- SuSE Linux Enterprise (X86 and X86-64)

- Redhat Enterprise Linux (X86 and X86-64)

- Oracle Linux (X86 and X86-64)

Software

The following software is required.

- CA XCOM Data Transport r11.5 server

- Java JDK version 6

- JBoss Application Server 4.0.5GA

Note: With the CA XCOM Management Center software, CA Technologies provides a separate CD containing the JBoss Application Server 4.0.5GA. This CD is called JBoss Application Server 4.0.5GA – CD.

Databases

The following databases are supported by CA XCOM Management Center:

- MySQL version 5
- DB2 UDB version 9

Browsers

The following browsers are supported by CA XCOM Management Center:

- IE 7.0 and 8.0
- Firefox 3.5

Hardware Requirements

The hardware requirements for CA XCOM Management Center are in line with vendor-recommended hardware to support platforms as defined in Software above.

Pre-Installation Considerations

Relational Database Tables

CA XCOM Management Center uses a set of relational database tables for its operation. These database tables must be defined at the time of installation.

Super and Group Administrator Users

The Super Administration attribute is used to identify which of the users defined to CA XCOM Management Center should be granted the authority to change the CA XCOM Management Center configuration.

The Group Administration attribute is used to identify which of the users defined to CA XCOM Management Center should be granted the authority to change the group configuration for CA XCOM Management Center.

Users who do not possess these attributes are entitled to use non-administrative facilities (for example, schedule transfer or request history records), but cannot make configuration changes. These users may need proper authority to process some of the schedule transfer functions.

The Super and Group Administration attributes can be set for individual users by using the functions under the Admin tab of CA XCOM Management Center.

Note: The functions under the Admin tab can be accessed only by existing Super and/or Group Administration users.

Important! When CA XCOM Management Center is initially installed and no authorized users have been defined for this CA XCOM Management Center, the first user who successfully logs in is automatically defined as a Super Administrator user for this CA XCOM Management Center.

Installation Prerequisites

Before you install the product, check the following prerequisites:

■ Privileges required

In order to install CA XCOM Management Center on Microsoft Windows Vista, Microsoft Windows XP, Microsoft Windows 2003, or Microsoft Windows 2008, you must log on to Microsoft Windows as a user with administrator privileges. On UNIX or Linux, you must log on as a user with root privileges if installing into the /opt/CA system directory.

■ System Libraries for Linux

The CA Embedded Entitlements Manager (EEM) installation requires library libstdc++.so.6 to exist in the usr/lib directory. This library can be installed from rpm libstdc++ if it has not been previously installed as part of your operating system.

■ JBoss installation

CA XCOM Management Center requires that a copy of the JBoss Application Server must be installed. Additionally, even though the JBOSS_HOME environment variable is recommended but not mandated by JBoss, it is always required by CA XCOM Management Center. Before installing CA XCOM Management Center, verify that this environment variable is defined and correctly set to indicate the path for the JBoss installation directory.

For Windows, environment variables can be accessed in either of the following ways:

– By right clicking Computer or My Computer within Windows Explorer

– By right clicking the Start Menu, then selecting Properties, Advanced Settings, Environment Variables

For Linux, set environment variables as follows:

1. Open the /etc/profile file in the vi editor.

2. Move to the end.

3. Add the following lines:

```
JAVA_HOME=<JDK Installation Directory Path>
export JAVA_HOME
JBOSS_HOME=<JBOSS Installation Directory Path>
export JBOSS_HOME
```

Note: Use this procedure to set the environment variables permanently on any of the supported Linux platforms.

■ Database preparation

CA XCOM Management Center needs access to a DB2 or MySQL database server; the product installer automatically creates the required database tables within a designated database.

Notes:

– For MySQL, the installer can either create a new database or use an existing one.

– For DB2, the installer is unable to create a new database and this must be done using DB2 administration tools before installing CA XCOM Management Center.

To enable creation of tables (and optionally, for MySQL only, the creation of a database), the installer requests the following:

– The user ID and related password for a database administration user account that has the necessary create and drop structure privileges.

– The user ID and related password for a database user account that is to be used subsequently by CA XCOM Management Center whenever it needs to access or update its database tables.

  This second account requires read and update privileges for all tables within the CA XCOM Management Center database, but does not need any structure or administration privileges or access to any other database.

– To enable database access by CA XCOM Management Center, the installer also requires a copy of the JDBC connector/driver for the appropriate database system. In the case of DB2 only, a copy of the JDBC Driver License is also needed.

■ Free disk space

Approximately 40 MB of disk space is required for the software files created by a full product installation of CA XCOM Management Center. In addition, disk space is required for the CA XCOM Management Center database, logs, and trace files. The amount of space needed varies, depending on the size of the database.

■ CA XCOM Data Transport r11.5 server

Your CA XCOM Data Transport r11.5 server must be installed before you can install CA XCOM Management Center.

Note: Your CA XCOM Data Transport r11.5 server does not need to be on the same system as where you are installing CA XCOM Management Center.

Compatibility Issues

CA XCOM Management Center requires the environment variable JAVA_HOME to be set to the JDK (Java Development Kit) directory. If JAVA_HOME is set to the JRE (Java Runtime Environment) directory or to a private third-party JVM, JBOSS will not start and EEM will not install as part of CA XCOM Management Center.

To find out which directory JAVA_HOME is set to

1. Navigate to the bin directory immediately beneath the directory set in JAVA_HOME.

2. Look for a member called javac.exe.

    This file exists only in the JDK bin directory. If the file is not there then your JAVA_HOME environment variable is set to the JRE directory.

If the JAVA_HOME variable is set to a JRE directory or a private JVM and it cannot be changed, then use the following procedure:

To install CA XCOM Management Center

1. Open a Windows command line window.

2. Navigate to where the CA XCOM Management Center install.exe file is located.

3. To set the local JAVA_HOME variable to the Java JDK location, execute the following command:

    SET JAVA_HOME=<JDK location>

    Example:

    SET JAVA_HOME=C:\Program Files\Java\jdk1.6.0_11

4. To execute the installer, type install and press Enter.

Chapter 3: Installing and Uninstalling

This section contains the following topics:

Install Product

The installation procedure provided for CA XCOM Management Center r11.5 can be used to install any combination of the following components:

- CA XCOM Management Center

- CA XCOM Interface Server—a required component that enables CA XCOM Management Center to interact with CA XCOM Data Transport

- CA Embedded Entitlements Manager (EEM)—a required component that enables CA XCOM Management Center to perform user authentication during user logon processing

To install CA XCOM Management Center

1. Ensure that you have a copy of the appropriate JDBC connector driver according to whether you want the installed product components to use a DB2 or MySQL database.

   Note: For MySQL, you require MySQL Connector/J, the official JDBC driver for MySQL. You can download this .jar file from the MySQL website at www.MySQL.com.

2. Stop your JBoss server.

   Note: If CA XCOM Management Center is already installed in JBoss, it is recommended that you delete the tmp, log, and work folders from the configuration (where the product is installed) before proceeding with the installation.

3. Ensure that you have administrator privileges on your computer.

4. Depending on the operating system, take *one* of the following actions to launch the installer:

   a. (Windows) Double-click the Install.exe file.

      This file is contained on the product CD or can be downloaded from the CA Support website.

   b. (UNIX and Linux) Issue the command **sh install.bin**.

5. Follow the dialogs referencing additional information and complete the installation process.

   The product is installed.

6. Restart JBoss.

7. Access the CA XCOM Management Center website and review the global parameters. If necessary, update the values.

   Note: Although the installer has initialized many parameters, several others need to be set manually after installation.

Installer Dialogs

The installer presents a series of dialogs that prompt you for information. These dialogs are described in the following section.

Note: You must stop your JBoss server before initiating the install process. We also recommend that you close down other programs running on your computer before initiating the install.

Step 1: Accept License Agreement

The installer starts with an Introduction dialog followed by a License Agreement dialog.

To accept the license agreement

1. Launch the installer.

    The Introduction dialog opens:
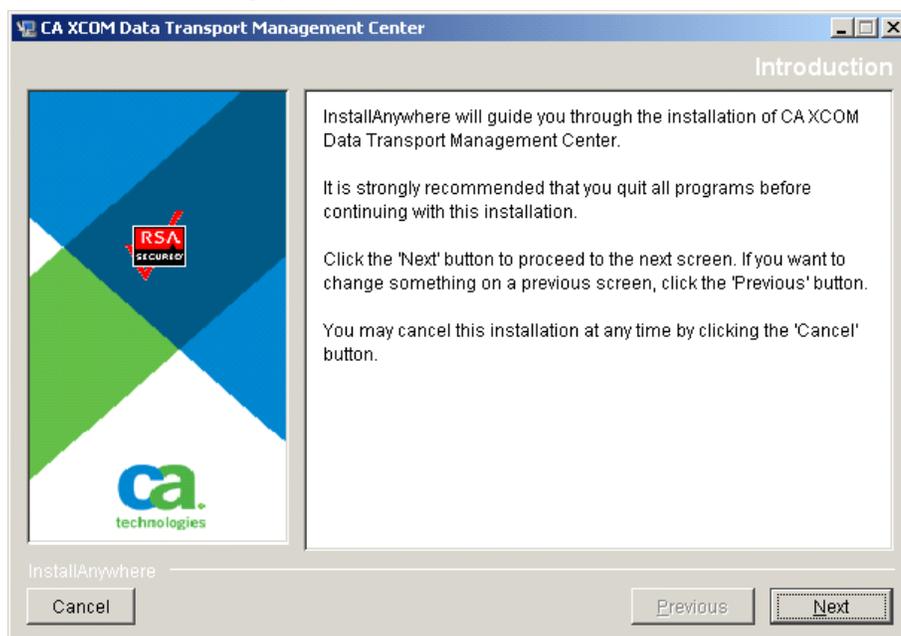
Before you proceed beyond this point, we recommend that you close down other programs running on your computer. Additionally, your JBoss server should have already stopped.

2. Read the introductory text, and click Next.

   The License Agreement dialog opens:
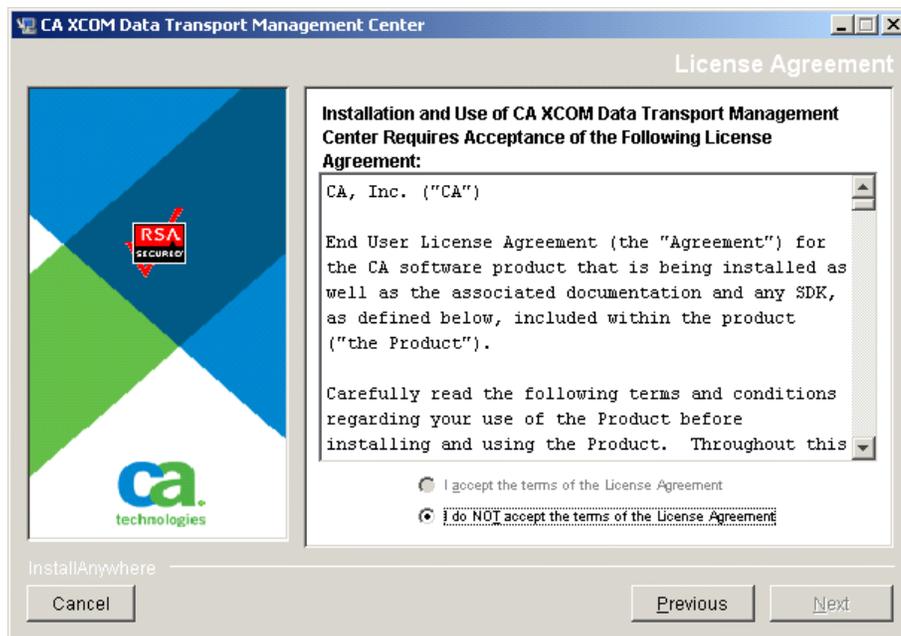
3. Read the license agreement in full.

   When you scroll to the end of the agreement, you can specify whether you want to accept the agreement.

4. Click I accept the terms of the License Agreement and then Next.

   The Choose Install Set dialog opens.

Step 2: Select the Components to Install

After you accepted the license agreement, you are prompted to select the type of installation:

Typical

Installs all components.

Custom

Enables you to select which components to install.

You select a custom installation under certain circumstances, for example:

■ You have already installed the Interface Server, for example:

– You have installed CA XCOM Gateway previously.

– You have installed and uninstalled CA XCOM Management Center previously, but did not uninstall the Interface Server.

■ You do not want to install the CA Embedded Entitlements Manager (EEM) component because you would prefer CA XCOM Management Center to use an EEM server that is installed on a different machine.

To select the components to install

1. On the Choose Install Set dialog, click either Typical or Custom, and then Next.
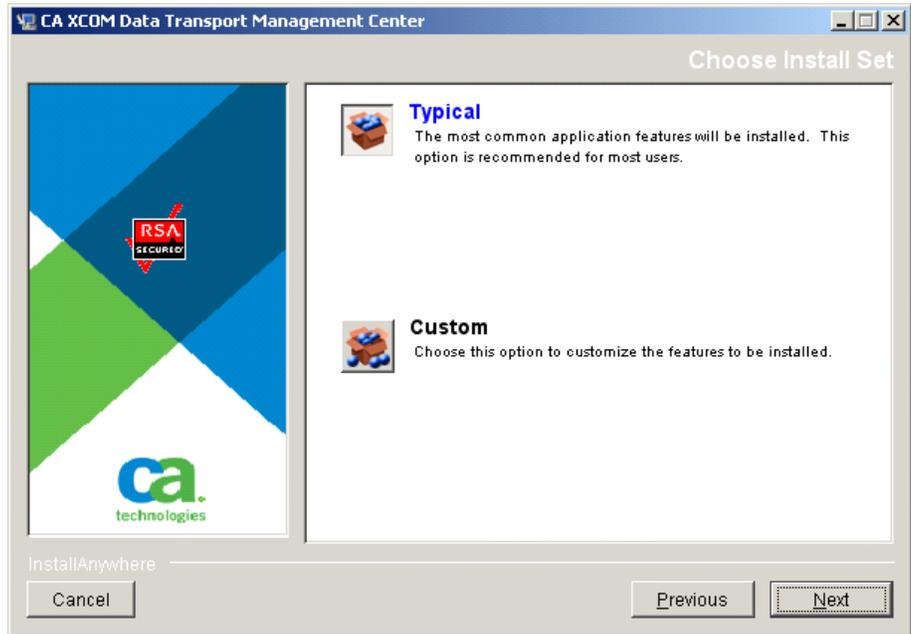
   - If you selected Typical, the Choose Install Folder dialog (see page 27) for the Interface Server opens.

   - If you selected Custom, you are prompted to select the components to install:
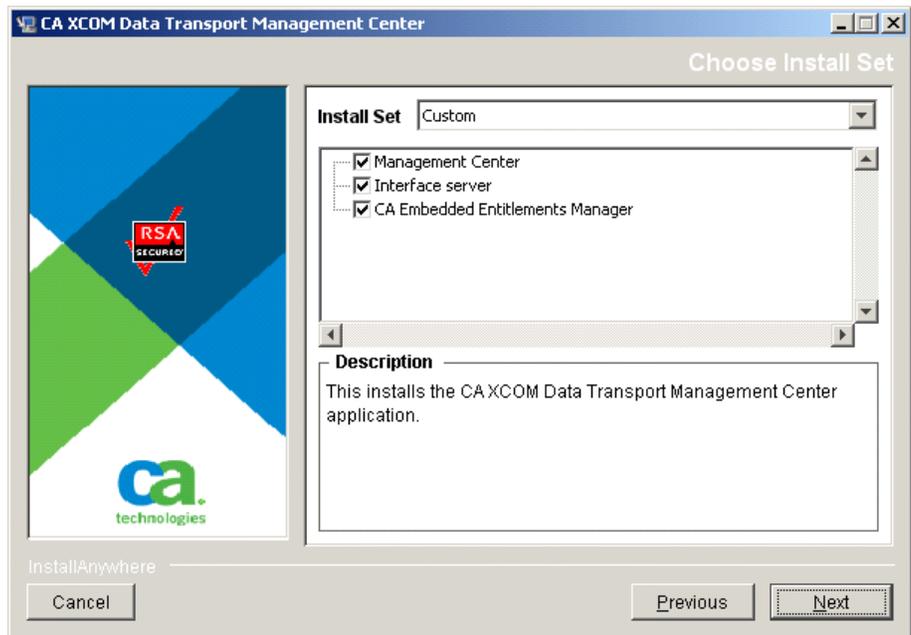
   Continue with the next step.

2. (Optional) Select the components you want to install, and click Next.

If you selected to install the Management Center but not the Interface Server, the Interface Server Configuration dialog (see page 35) opens.

Otherwise, dialogs for the selected components open in the following sequence: Interface Server and then Management Center.

Step 3: (Interface Server) Specify Destination Folder

The dialogs described in this step and the next two steps relate to the installation of the CA XCOM Interface Server, which is typically the first component for which the installer requests detailed information. The first dialog, Choose Install Folder, prompts you to specify a destination folder for the installation.

To specify a destination folder for the installation of the CA XCOM Interface Server

1. On the Choose Install Folder dialog, accept the default folder or select an alternative location for product installation.

   Note: The default folder is C:\Program Files\CA\XCOMIF. If the folder does not exist, the installer creates the folder during installation.
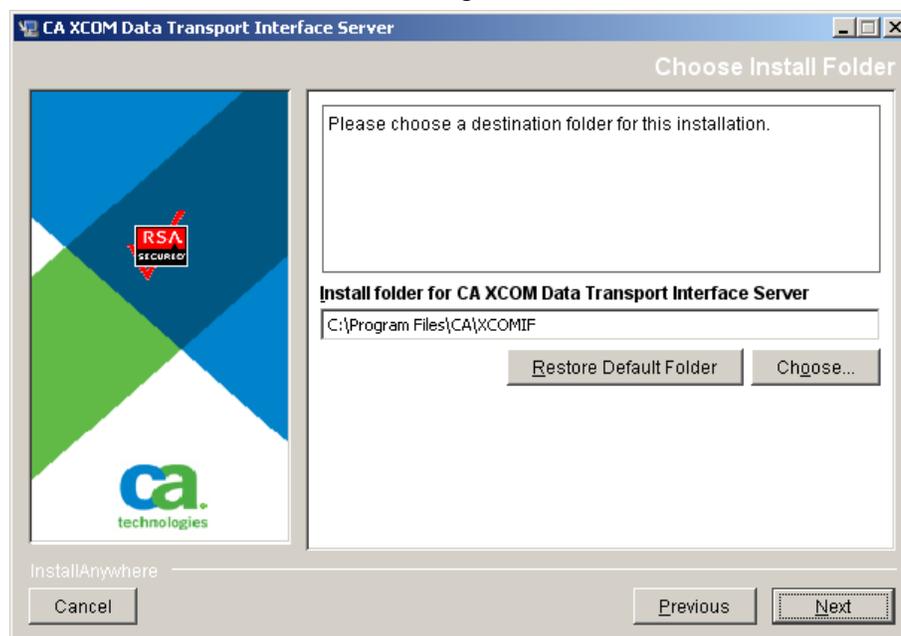
2. Click Next.

   The folder information is saved, and the first of two Database Information dialogs opens.

Step 4: (Interface Server) Define Database User and Database

The Database Information dialogs define a database user and the database for the CA XCOM Interface Server to store status information. The database can be DB2 or MySQL.

For MySQL, the installer can be requested to either create a new database or use an existing one. However, for DB2, the installer is unable to create databases and so the database must be predefined using DB2 administration tools.

A database user account is required by the CA XCOM Interface Server to enable it to access and update its database tables. This account needs read and update privileges for all tables in the designated database, but does not need any structure or administration privileges or any access privileges for any other database.

The installer also requests user ID and password credentials for an admin user database account. These will be used only during product installation, to create tables within the database. The admin user account needs to have table create and drop structure privileges for the designated database, to enable it to create tables. For MySQL only, the admin user account also needs database creation privilege, if the installer is to be requested to create a new database.

The database table names used by CA XCOM Data Transport are unique to each product. Consequently, you can share the same database between CA XCOM Interface Server, CA XCOM Gateway, and CA XCOM Management Center, or you can use separate databases for each component.

Depending on whether you use a DB2 or MySQL database, the procedure differs.

To define the DB2 user and database

1. On the first Database Information dialog, select DB2 from the Database drop-down list.

    The dialog displays the DB2 information fields:
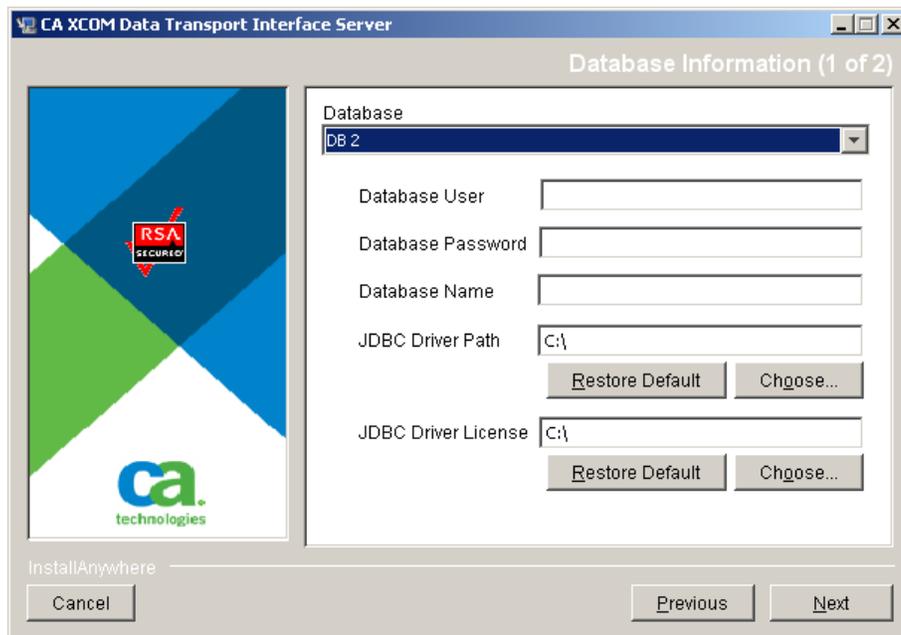
2. Complete the fields:

    ■   Specify the ID and password of a previously defined DB2 user, together with the name of an existing database.

        If a suitable user does not exist, you can use your operating system tools to create a user account for connection and access to the database tables.

    ■   Specify the file folder locations at which the installer can locate the DB2 JDBC Connector and its license.

3.   Click Next.

The second Database Information dialog opens:
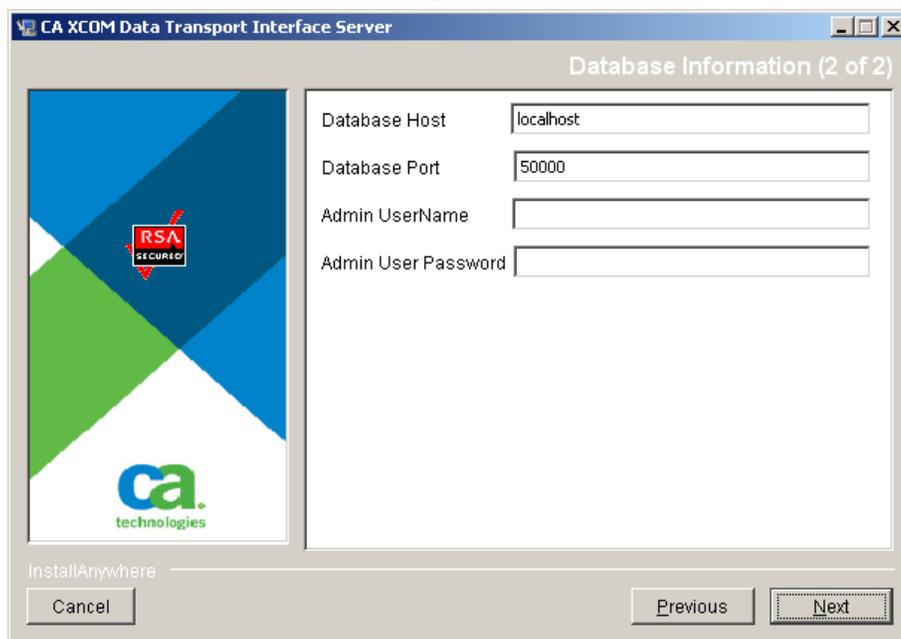
4.   Complete the fields:

■   Specify the host name and port information that the CA XCOM Interface Server requires to connect to the DB2 database server (local or remote).

The port number is set initially to the default value of 50000 for DB2.

■   Specify the ID and password for an administrative user account which has been granted the ability to create database tables.

During installation, the installer connects to the database server as this user to create the required database tables.

5.   Click Next.

The installer connects to the specified database server to verify the validity of the specified information. The Application Server Information dialog opens.

Note: Tables are not created at this stage. They are created later after you review your installation choices and request the installation to proceed.

To define the MySQL user and database

1. On the first Database Information dialog, select MySQL from the Database drop-down list.

   The dialog displays the MySQL information fields:

2. Complete the fields:

   ■ Specify the ID and password of a user, and the name of a database.

   You can specify an existing user and database, or you can ask the installer to create the user and database.

   The indicated user account will be used by the CA XCOM Interface Server, on an ongoing basis, to access and update database tables. Therefore, if you specify an existing user, this user account must have all data privileges (that is, select, insert, update, and delete) at either database or global level, but does not require structure or administrative privileges.

   Notes:

   – If you are using a database user that was created outside of the CA XCOM Management Center installer, you need to ensure that the database user already exists with the required access.

   – If the database server is in the local machine, user@localhost must exist

   – If the database server is in a remote machine, user@remote must exist.

   – If the database is in a remote machine and user@localhost exists but user@remote does not exist, the installer will not create user@remote, even if the Create User option is checked. The installer will produce an error.

–   Similarly, if the database is in the local machine and user@remote exists but user@localhost does not exist, the installer will not create user@localhost, even if the Create User option is checked. The installer will produce an error.

–   During installation, if there are any database errors, installation will not stop, but the database errors will be logged to "%INSTALL_DIR%\installlogs\CA XCOM Data Transport Management Center_install.log" for CA XCOM Management Center and to "%INSTALL_DIR%\installlogs\CA XCOM Data Transport Interface Server_install.log" for the CA XCOM Interface Server.

■   If you want to create a new database user, check the Create User option.

Note: The installer will create the database user only if both of the following apply:

–   The Create User option is checked.

–   The user does not already exist as either user@localhost or user@remote.

■   Specify the file folder location at which the installer can locate MySQL Connector/J, the official JDBC driver for MySQL.

3. Click Next.

The second Database Information dialog opens:
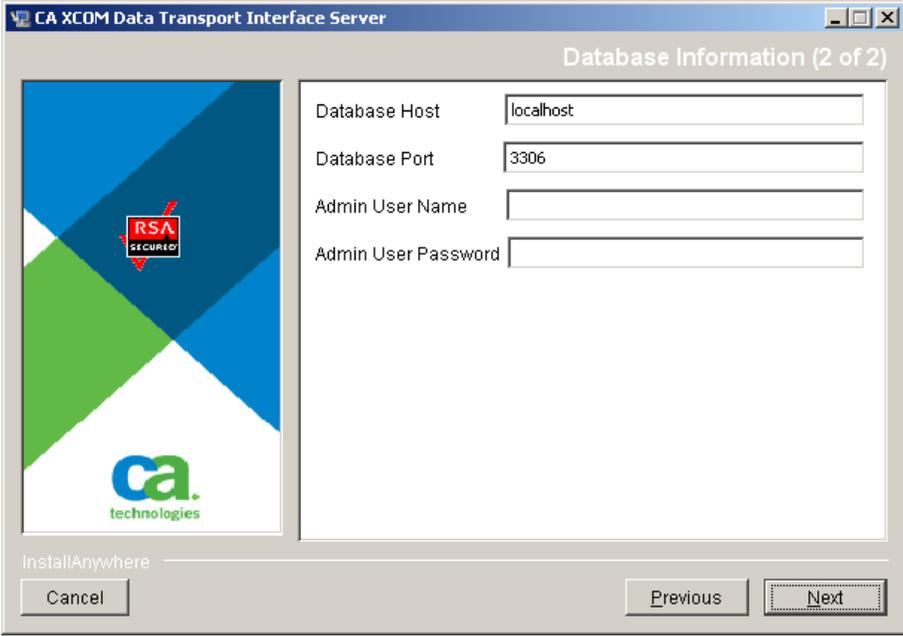
4. Complete the fields:

■ Specify the host name and port information that the CA XCOM Interface Server requires to connect to the MySQL database server.

The port number is set initially to the default value of 3306, the standard MySQL server port number.

■ Specify the ID and password for an administrative user who has been granted the ability to create database tables, and when specified, a new user or database.

Notes:

– For MySQL, the administrative user must have all privileges. If the database server is in a remote machine, then the administrative user with remote access (%) must have all privileges.

– During installation, the installer connects to the database server as this user to create the required database tables, and when specified, a new user or database.

5. Click Next.

The installer connects to the specified database server to verify the validity of the specified information. The Application Server Information dialog opens.

Note: Tables are not created at this stage. They are created later after you review your installation choices and request the installation to proceed.

Step 5: (Interface Server) Specify JBoss Configuration Information

The Application Server Information dialog gathers information required to configure the CA XCOM Interface Server parameters related to JBoss.

To specify the JBoss configuration information

1. On the Application Server Information dialog, specify the following information:

    ■   JBoss configuration path, which points to a folder that is a subdirectory of the JBOSS_HOME\server directory, for example, C:\Program Files\JBoss\server\default.

        Click the Choose button to navigate to the appropriate folder in your file system, or type the folder path in the JBoss Configuration field.

    ■   Port number

        Specify the HTTP port number for JBoss in the HTTP Port field.

    Note: These settings affect the communication of both CA XCOM Gateway and CA XCOM Management Center with the CA XCOM Interface Server.
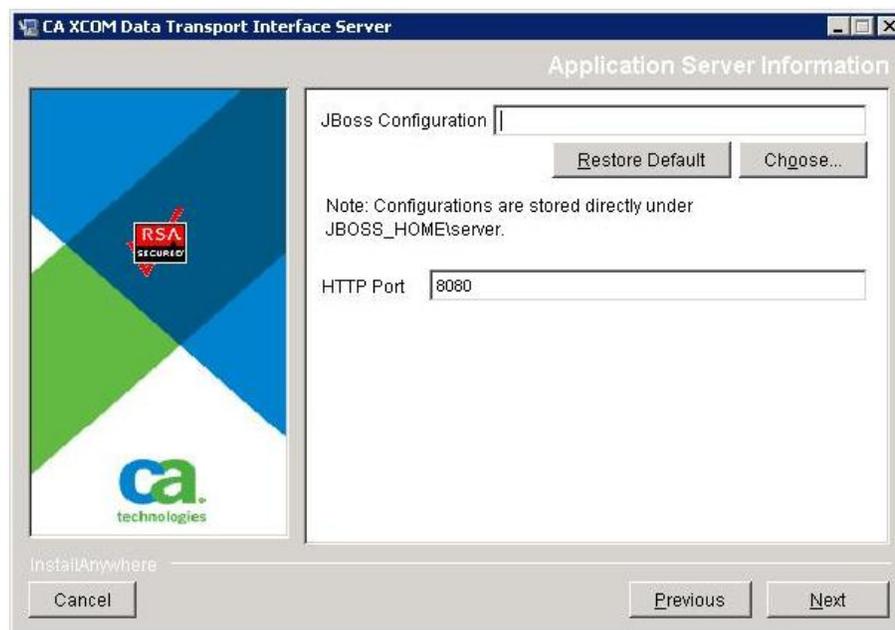
2. Click Next.

Step 6: Supply Configuration Information of Existing CA XCOM Interface Server (MC)

If you selected Custom installation, and selected to install the CA XCOM Management Center but not the CA XCOM Interface Server, the installer requires information about the existing CA XCOM Interface Server that you want the CA XCOM Management Center to use.

To supply configuration information of an existing CA XCOM Interface Server

1. On the CA XCOM Interface Server Configuration dialog, specify the following information:

   ■ Host name for the computer on which the CA XCOM Interface Server is running

   If the CA XCOM Interface Server is running on the same computer, specify **localhost** (the default) for the host name.

   ■ The port number that was specified when this CA XCOM Interface Server was installed.
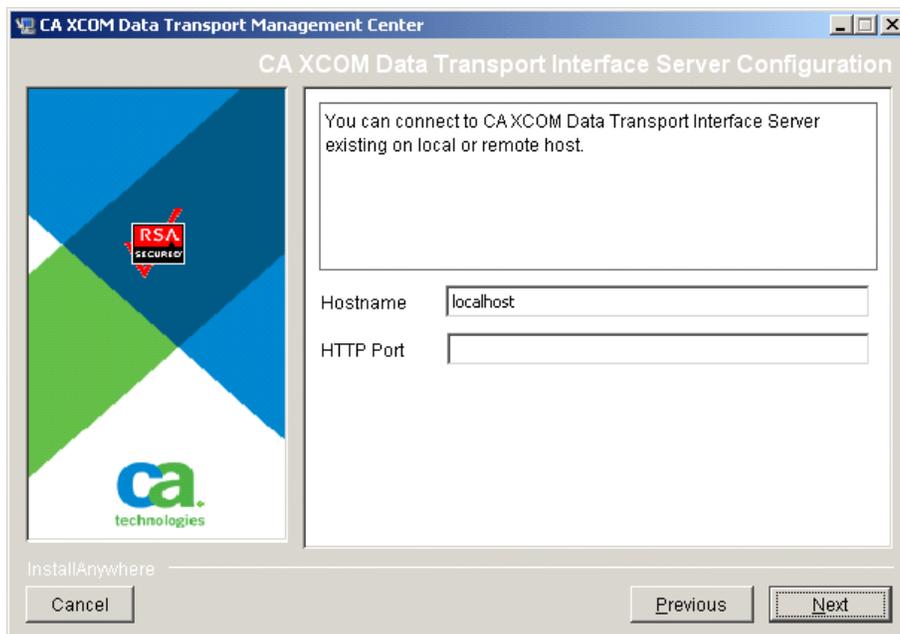
2. Click Next.

   The Choose Install Folder dialog for the CA XCOM Management Center opens.

Step 7: (Management Center) Specify Destination Folder

The dialogs described in this step and the next four steps relate to the installation of CA XCOM Management Center, which is typically the second component for which the installer requests detailed information. The first dialog, Choose Install Folder, prompts you to specify a destination folder for the installation.

To specify a destination folder for the installation of CA XCOM Management Center

1. On the Choose Install Folder dialog, accept the default folder or select an alternative location for product installation

    Note: The default folder is C:\Program Files\CA\XCOMMC. If the folder does not exist, the installer creates the folder during installation.
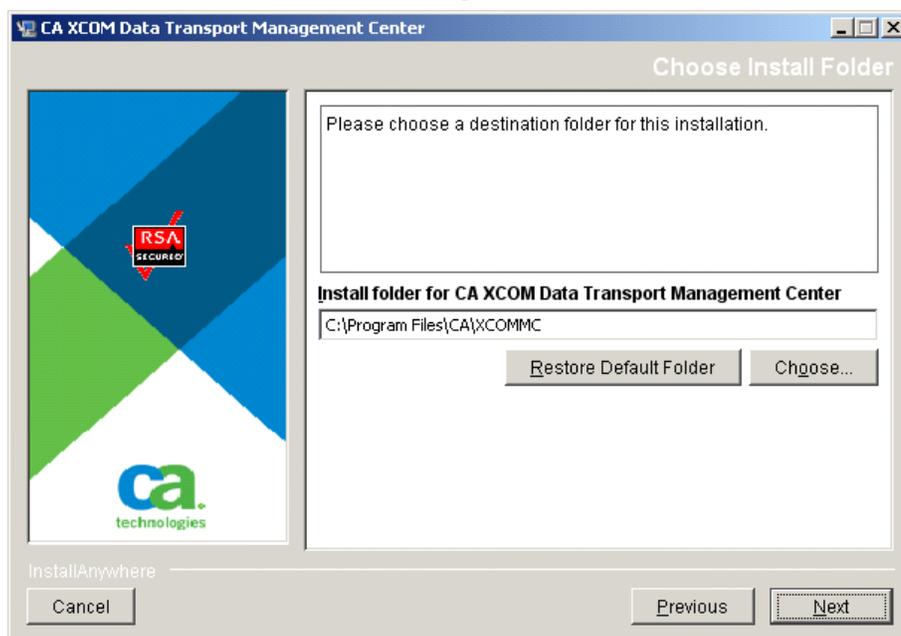
2. Click Next.

    The folder information is saved, and the first of two Database Information dialogs opens.

Step 8: (Management Center) Define Database User and Database

The Database Information dialog defines a database user and the database for CA XCOM Management Center to store configuration and status information. The database can be DB2 or MySQL.

The procedure is similar to the corresponding procedure for the Interface Server. If you have already entered database information for the CA XCOM Interface Server, that information provides initial values for the CA XCOM Management Center dialogs. You can accept those values. The procedure is described briefly here. For details, see the procedure for the CA XCOM Interface Server.

To define the database user and database

1. On the first Database Information dialog, select the type of database from the Database drop-down list.

   The dialog displays the information fields for the selected type of database.

2. Complete the fields, and click Next.

   The second Database Information dialog opens.

3. Complete the fields, and click Next.

   The Application Server Information dialog opens.

Step 9: (Management Center) Specify JBoss Configuration Information

The Application Server Information dialog gathers information required to configure the CA XCOM Management Center parameters related to JBoss.

The procedure is similar to the corresponding procedure for the Interface Server (see page 34). If you have already entered JBoss configuration information for the CA XCOM Interface Server, that information provides initial values for the CA XCOM Management Center dialog. You can accept those values.

To specify the JBoss configuration information

1. On the Application Server Information dialog, specify the following information:

    ■   JBoss configuration path, which points to a folder that is a subdirectory of the JBOSS_HOME\server directory, for example, C:\Program Files\JBoss\server\default

        Click the Choose button to navigate to the appropriate folder in your file system, or type the folder path in the JBoss Configuration field.

    ■   Port number

        Specify the HTTP port number for JBoss in the HTTP Port field.

    Note: These settings affect the communication of both CA XCOM Gateway and CA XCOM Management Center with the CA XCOM Interface Server.

2. Click Next.

    The EEM Information dialog opens.

Step 10: (Management Center) Specify Information for CA EEM

CA XCOM Management Center requires access to a CA Embedded Entitlements Manager (EEM) server to authenticate users when they sign in to the CA XCOM Management Center website.

The CA EEM Authentication dialog requests information that enables CA XCOM Management Center to connect to the CA EEM server to access the directory information that it needs to authenticate users.

To specify the CA EEM information

1. On the CA EEM Authentication dialog, specify the following information:

   EEM Server Hostname

   Defines the host name (or IP address) of the machine that will be used to run the CA EEM server with which CA XCOM Management Center must communicate.

   If CA EEM has been selected for installation, this field is preset to **localhost** and cannot be changed.

   If CA EEM has not been selected for installation and if it is already installed on the local machine, you can use the default value of **localhost** to select this CA EEM server. Alternatively, you can specify a host name (or IP address) that refers to a different machine on which CA EEM has already been installed.

   Note: The CA EEM server always uses port 5250. So you cannot specify another port.

   Admin User Name

   Defines the user ID that is used to perform administrative functions on the CA EEM user interface.

   The current release of CA EEM only supports an administrator user account with the user ID **EiamAdmin**. For this reason, the user ID field is preset to this value and cannot be changed.

   If CA EEM has been selected for installation on the local machine, the **EiamAdmin** user ID will be used to create an administrator account for the new CA EEM server.

   Admin Password

   Provides the password associated with the CA EEM administrative user account.

   If the host name refers to an existing CA EEM server (that is, CA EEM has not been selected for local installation), the current administrator password for that server must be entered.

Alternatively, if CA EEM has been selected for installation on the local machine, the specified password will be assigned to the EEM administrator account created when that component is installed. Subsequently, this password will need to be used to gain access to the CA EEM User Interface to perform administrative functions.

Confirm Password

When CA EEM has been selected for installation on the local machine, this prompt will appear, requesting you to re-enter the password specified in the preceding password field. This is to ensure that the password has been correctly typed, so that the new EEM administrator account can be created correctly with the intended password.

Note: If the host name refers to an existing EEM server (that is, CA EEM has not been selected for local installation), the Confirm Password prompt will not appear.

2. Click Next.

If EEM has not been selected for installation, the installer will check that it can successfully communicate with an EEM server on the specified host machine, using the supplied administrator user ID and password.
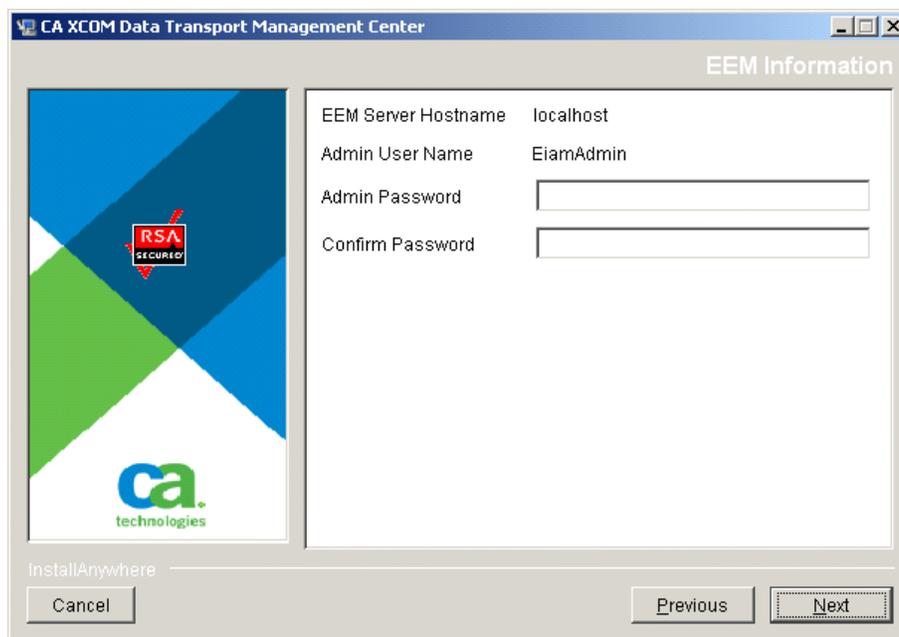
If verification is successful, the Keystore information dialog opens.

If verification fails, an error dialog opens. Click OK on the error dialog to return to the EEM Information dialog. You can then correct the specified information.

Step 11: Review Specified Installation Options

Before you invoke the installation process, review the specified installation options. If a specified option is not correct, you can correct the error before installation.

To review the specified installation options

1. On the Pre-installation Summary dialog, review the installation options.

Note: For security reasons, specified passwords are not included.

If you want to change an option, use the Previous button to return to the corresponding dialog to modify the specified information.

2. When you are satisfied that all options are correct, click Install.

   The installation process starts.

   When installation is complete, the Install Complete dialog opens:
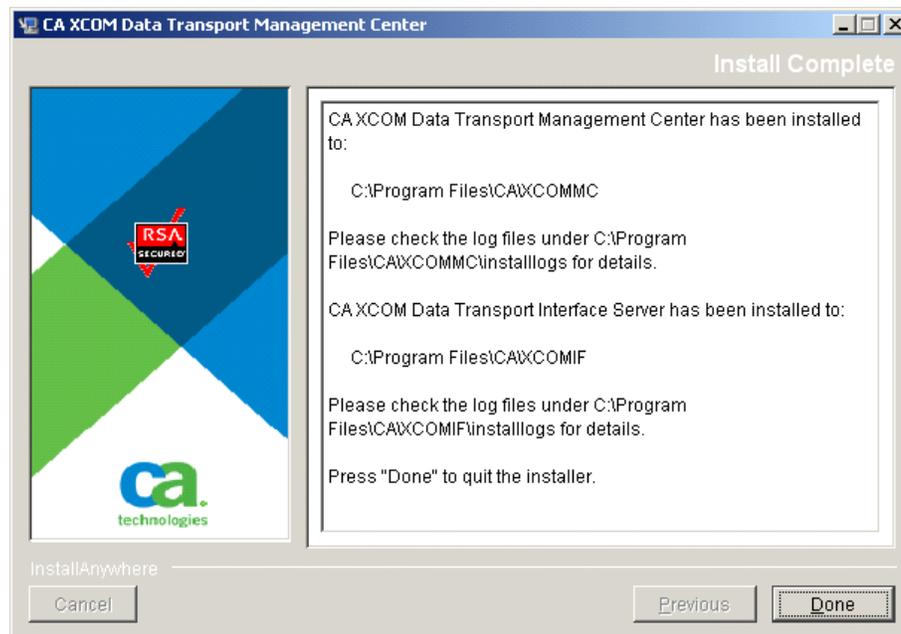
3. After completing the installation, you need to start JBoss and configure the CA EEM server. You should then access the CA XCOM Management Center website, as described in the following chapter, to review the global parameters and update them, if necessary.

   Note: Although the installer has initialized many parameters, several others need to be set manually after installation.

Install the Product in Console Mode

For Linux only, you can also choose to install the product in console mode.

To install CA XCOM Management Center in console mode

1. Enter the following command at the command prompt:

   sh %FilePath_where_installer_is_saved% -i console

   The command launches the installer and the introduction dialog opens.

2. Press Enter.

   The EULA dialog opens.

   Note: Because there is no scroll option on the console, you need to press Enter to scroll to the end of this page.

3. To accept the terms of the license agreement, type **Y** and press Enter.

   As each page of the dialog appears, the console prompts you for the following details:

   ■ Install set

   ■ Install path for the CA XCOM Interface Server

   ■ Database details

   ■ Database user details

   ■ Database administrator details

   ■ JBoss configuration path

   ■ JBoss HTTP port number

   ■ Directory path for CA XCOM Management Center

   ■ Further database details for CA XCOM Management Center

   ■ JBoss details for CA XCOM Management Center

   ■ CA EEM details

   ■ Keystore information

   ■ Certificate information

   ■ FTP information

4. Complete the required information on each page and then press Enter to move to the next page.

   When you have finished, the console displays the information that you have entered.

   Review this information and edit if required.

5. To confirm the displayed information, press Enter.

   The Install Complete console appears, displaying details of the installation.

   Note: To navigate in console mode screens, do the following:

   ■ To go to the next input screen, press Enter.

   ■ To go to the previous input screen, type **back** and press Enter.

   ■ To quit or cancel the installation, type **quit** and press Enter.

6. Press Enter to close the installation process.

Silent Installation

In silent mode, the installer has no end-user interaction, and runs by providing a response file from which the installer retrieves the values for various installer variables used to control the install.

Important! Before you run the installer in silent mode, you need to manually create the response file (with .properties as the extension) for the installer to use. For more information, see Variables Used in the Installer Response File.

To run the installer in silent mode

Important! The installer cannot be executed in silent mode from a mapped network drive; the command has to be run on your local machine.

1. Open the command prompt.

2. Navigate to the directory containing install.exe.

3. Enter the following command at the command prompt:

    For Windows

    `install.exe -i silent -f <<`*`fully qualified path of response file`*`>>`

    For Linux

    `sh install.bin -i silent -f <<`*`fully qualified path of response file`*`>>`

    Note: The words 'install' and 'silent' must be in lowercase.

    The response to this command varies, depending on your operating system, as follows:

    On Windows

    ■ The command runs immediately. It does not show progress or a completion message.

    ■ Check the Processes tab in the Task Manager for install.exe, because this process represents the silent installer. When this process is removed from Processes tab, installation is complete.

    On Linux

    The silent installer shows installer progress and a completion message.

Check the Log Files

After installation is complete, you need to check the log files for any error or warning messages.

To check the log files

1. Open the temporary directory for your system, as follows:

   ■ On Windows, run the following command:

     `%temp%`

   ■ On Linux, use the following path:

     `/tmp`

2. Check the following files in the temporary directory:

   ■ CA XCOM Data Transport Interface Server_preinstall.log (for CA XCOM Interface Server)

   ■ CA XCOM Data Transport ManagementCenter_preinstall.log (for CA XCOM Management Center)

3. Check the log files in USER_INSTALL_DIR\installlogs, which is the installation directory for both the CA XCOM Interface Server and CA XCOM Management Center.

Features To Be Installed

The CHOSEN_INSTALL_FEATURE_LIST defines the list of short names of features to be installed. The names do not contain any spaces and are separated by commas.

The features that can be installed are as follows:

Feature	Short Name
CA XCOM Interface Server	IServer
CA XCOM Management Center	MC
CA Embedded Entitlements Manager	EEM

Important! You can request installation of CA Embedded Entitlements Manager (EEM) only if you also request installation of CA XCOM Management Center.

Example:

`CHOSEN_INSTALL_FEATURE_LIST=IServer,MC,EEM`

This list installs all three features.

Variables Used in the Installer Response File

You need to define variables in your installer response file. There are different sets of variables required, depending on which features you are installing.

The prefixes of the variables are as follows:

IS_

Settings for the CA XCOM Interface Server

MC_

Settings for CA XCOM Management Center

Notes:

■ For Windows, specify two backslashes (\\) in the path values; for example:

C:\\Program Files\\CA\\XCOMIF

■ For Linux, specify a single forward slash (/) in the path values; for example:

/opt/CA/XCOMIF

Variables to Install CA XCOM Management Center Without the CA XCOM Interface Server

The following variables are required if you choose to install CA XCOM Management Center and *not* to install the CA XCOM Interface Server. These variables are used to configure an existing CA XCOM Interface Server.

Important! If you select the CA XCOM Interface Server for installation, do not use these variables.

IS_HOST_NAME

The host name where the CA XCOM Interface Server is running (either local or remote host)

IS_HTTP_PORT

The HTTP port where the JBoss is running with which the CA XCOM Interface Server is configured.

Variables to Install the CA XCOM Interface Server

The following variables are required if you choose to install the CA XCOM Interface Server.

Important! If you do not select the CA XCOM Interface Server for installation, do not use these variables.

IS_USER_INSTALL_DIR

The installation directory for the CA XCOM Interface Server.

IS_DB_DBTYPE

The database type DB2 or MYSQL.

IS_DB_DBNAME

The database name.

IS_DB_CREATE_DB

1 to create a new database; 0 to use an existing database.

It cannot be 1 if IS_DB_DBTYPE is DB2.

IS_DB_XCOM_USER

The database user name

IS_DB_XCOM_PWD

The database user's password

IS_DB_CREATE_USER

1 to create a new user; 0 to use an existing user.

It cannot be 1 if IS_DB_DBTYPE is DB2.

IS_DB_XCOM_CONFIRM_PWD

Confirm the database user's password.

This is required if IS_DB_CREATE_USER is 1.

IS_DB_DRIVER_PATH1

The fully qualified path of the database driver file for MYSQL or DB2.

IS_DB_DRIVER_PATH2

The fully qualified path of the database driver license file for DB2.

Not required if IS_DB_DBTYPE is MYSQL.

IS_DB_HOST_NAME

The host where the database server (MYSQL or DB2) is installed.

IS_DB_PORT_NO

The port of the database server.

IS_DB_ADMIN_USER

The user with administrative credentials for the database server.

IS_DB_ADMIN_PWD

The administrative user's password.

IS_JBOSS_CONFIG

The fully qualified path of the JBoss configuration directory.

IS_HTTP_PORT

The HTTP port where JBoss is running on the local host.

Variables to Install CA XCOM Management Center

The following variables are required if you choose to install CA XCOM Management Center:

MC_USER_INSTALL_DIR

The installation directory for CA XCOM Management Center.

MC_DB_DBTYPE

The database type: DB2 or MYSQL.

MC_DB_DBNAME

The database name.

MC_DB_CREATE_DB

1 to create a new database; 0 to use an existing database.

Note: It cannot be 1 if GW_DB_DBTYPE is DB2.

MC_DB_XCOM_USER

The database user name.

MC_DB_XCOM_PWD

The database user password.

MC_DB_CREATE_USER

1 to create a new user; 0 to use an existing user.

Note: It cannot be 1 if GW_DB_DBTYPE is DB2.

MC_DB_XCOM_CONFIRM_PWD

Confirm the database user password.

Note: This is required if GW_DB_CREATE_USER is 1.

MC_DB_DRIVER_PATH1

The fully qualified path of the database driver file for MYSQL or DB2.

MC_DB_DRIVER_PATH2

The fully qualified path of the database driver license file for DB2.

Note: Not required if GW_DB_DBTYPE is MYSQL.

MC_DB_HOST_NAME

The host where the database server (MYSQL or DB2) is installed.

MC_DB_PORT_NO

The port of the database server.

MC_DB_ADMIN_USER

The user with administrative credentials to the database server.

MC_DB_ADMIN_PWD

The administrative user's password.

MC_JBOSS_CONFIG

The fully qualified path of the JBoss configuration directory.

MC_HTTP_PORT

The HTTP port where JBoss is running on the local host.

MC_EEM_HOSTNAME

The host name (or IP address) of the CA EEM server to be used by CA XCOM Management Center.

Notes:

- This host name cannot be suffixed by a port number, because the CA EEM server always uses port 5250 and this cannot be overridden.

- This variable is required only if CA EEM is not selected for installation. If CA EEM is selected for installation, this variable is preset to localhost and its value will be discarded if specified.

MC_EEM_ADMIN_PASSWORD

The password for CA EEM's EiamAdmin administrator account. If you are installing CA EEM, the password provided will be used to set the administrator password for the new server. Alternatively, if the host name (above) references an existing, previously installed EEM server, this variable must provide the current administrator password for that server.

MC_EEM_ADMIN_CONFIRM_PASSWORD

This variable must be set to the same value as GW_EEM_ADMIN_PASSWORD.

Sample Response File

The following is a sample response file to install all features.

```
#Choose Install Set
#------------------
CHOSEN_INSTALL_FEATURE_LIST=MC,IServer,EEM

#Choose Install Folder
#---------------------
IS_USER_INSTALL_DIR=C:\\Program Files\\CA\\XCOMIF

#Database Information (1 of 2)
#----------------------------
IS_DB_DBNAME=db_iserver2
IS_DB_DBTYPE=MYSQL
IS_DB_XCOM_USER=user01
IS_DB_XCOM_PWD=user01
IS_DB_XCOM_CONFIRM_PWD=user01
IS_DB_DRIVER_PATH1=C:\\My
Documents\\XCom\\Management\\Prototype\\mysql-connector-java-5.0.6-bin.jar
IS_DB_CREATE_DB=1
IS_DB_CREATE_USER=1

#Database Information (2 of 2)
#----------------------------
IS_DB_HOST_NAME=DBHOSTNAME
IS_DB_PORT_NO=3306
IS_DB_ADMIN_USER=root
IS_DB_ADMIN_PWD=adminadmin

#Application Server Information
#----------------------------
IS_JBOSS_CONFIG=C:\\JBoss\\jboss-4.0.5.GA\\server\\default
IS_HTTP_PORT=8080

#Choose Install Folder
#---------------------
MC_USER_INSTALL_DIR=C:\\Program Files\\CA\\XCOMGW

#Database Information (1 of 2)
#----------------------------
MC_DB_DBNAME=db_gateway2
MC_DB_DBTYPE=MYSQL
MC_DB_XCOM_USER=user01
MC_DB_XCOM_PWD=user01
MC_DB_XCOM_CONFIRM_PWD=user01
MC_DB_DRIVER_PATH1=C:\\My
Documents\\XCom\\Management\\Prototype\\mysql-connector-java-5.0.6-bin.jar
MC_DB_CREATE_DB=1
MC_DB_CREATE_USER=1
```

```
#Database Information (2 of 2)
#----------------------------
MC_DB_HOST_NAME=DBHOSTNAME
MC_DB_PORT_NO=3306
MC_DB_ADMIN_USER=root
MC_DB_ADMIN_PWD=adminadmin

#Application Server Information
#------------------------------
MC_JBOSS_CONFIG=C:\\JBoss\\jboss-4.0.5.GA\\server\\default
MC_HTTP_PORT=8080

#CA Embedded Entitlements Manager (EEM) Server Information
#--------------------------------------------------------
MC_EEM_ADMIN_PASSWORD=adminpassword
MC_EEM_ADMIN_CONFIRM_PASSWORD=adminpassword
```

Uninstall the Product

For Windows

The programs can be uninstalled component-by-component by using Control Panel, Add or Remove Programs.

For Linux

Enter the following command:

`sh %INSTALLDIR%/Uninstall_XCOMMC/Uninstall\ XCOMMC`

Note: After you uninstall the components, you can remove the database objects.

Uninstall Modes

By default, the uninstall mode is the same the install mode. For example, if CA XCOM Management Center was installed in silent mode, it is uninstalled in silent mode by default. To set uninstall mode explicitly, run the uninstaller with the –i switch.

Examples for Windows:

■ To uninstall CA XCOM Management Center in GUI mode, open the command prompt and navigate to Uninstall_XCOMGW inside the XCOMGW directory. Then run the following command:

```
"Uninstall XCOMMC.exe" -i swing
```

■ To uninstall the CA XCOM Interface Server in GUI mode, open the command prompt and navigate to Uninstall_XCOMIF inside the XCOMIF directory. Then run the following command:

```
"Uninstall XCOMIF.exe" -i swing
```

Similarly, you can use -i console to uninstall in console mode.

Examples for Linux:

■ To uninstall CA XCOM Management Center in GUI mode, enter the following command:

```
sh %INSTALLDIR%/Uninstall_XCOMMC/Uninstall\ XCOMMC -i swing
```

■ To uninstall CA XCOM Management Center in console mode, enter the following command:

```
sh %INSTALLDIR%/Uninstall_XCOMMC/Uninstall\ XCOMMC -i console
```

■ To uninstall CA XCOM Management Center in silent mode, enter the following command:

```
sh %INSTALLDIR%/Uninstall_XCOMMC/Uninstall\ XCOMMC -i silent
```

■ To uninstall CA XCOM Interface Server in silent mode, enter the following command:

```
sh %INSTALLDIR%/Uninstall_XCOMIF/Uninstall\ XCOMIF -i silent
```

Uninstall CA XCOM Management Center

Before you uninstall CA XCOM Management Center, stop JBoss.

To uninstall CA XCOM Management Center from Windows

1. Stop JBoss.

2. Open the Control Panel, Add or Remove Programs window, and select CA XCOM Data Transport Management Center.

3. Click Change/Remove, and follow the prompts to uninstall CA XCOM Management Center.

Uninstall the CA XCOM Interface Server

Before you uninstall the CA XCOM Interface Server, stop JBoss.

To uninstall the CA XCOM Interface Server

1. Ensure that JBoss has stopped.

2. In Windows, do the following:

    a. Open the Control Panel, Add or Remove Programs window, and select CA XCOM Data Transport Interface Server.

    b. Click Change/Remove, and follow the prompts to uninstall the CA XCOM Interface Server.
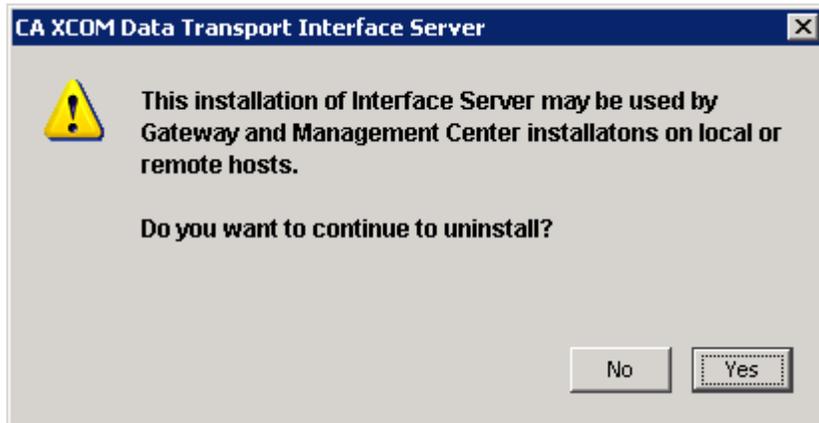
Important! If a CA XCOM Gateway or CA XCOM Management Center is configured to use the CA XCOM Interface Server on this computer, those products cannot operate if the CA XCOM Interface Server is uninstalled. Do not proceed unless you are confident that no instances of those products are using this CA XCOM Interface Server actively.

Remove Database Objects

Uninstalling the components does not remove the databases and their content.

To remove database objects, use the configuration and administration tools of your database server:

- If the database is shared and you want to remove database objects for a single product only, drop those objects selectively based on their names.

- If the databases are not shared, drop the databases that you created for CA XCOM Management Center.

  All schemas, tables, and indexes in the databases are removed.

Chapter 4: Post-Installation and Startup

This section contains the following topics:

Configure CA Embedded Entitlements Manager (EEM)

If, during installation, you installed CA Embedded Entitlements Manager (EEM) and indicated that CA XCOM Management Center is to use this newly installed CA EEM server on the same machine, you need to use the CA EEM User Interface to configure CA EEM before its first use.

Note: The installation of CA EEM automatically creates a start menu item, which you can use to access the user interface. To locate this start menu item, select Programs, CA, Embedded Entitlements Manager, EEM UI.

To configure CA EEM

1. On the CA EEM login screen, select the application '<global>' and enter the EEM administrator user ID and password that were provided during the installation (see Step 10: (Management Center) Specify Information for CA EEM).

   The CA EEM user interface appears.

2. Select the Configure tab, then the 'EEM Server' link beneath the tab bar, and finally the 'Global Users/Global Groups' item from the menu pane on the left of the screen.

3. Use the displayed screen to configure CA EEM to identify how your directory of users is to be stored and accessed:

   ■ Stored internally by CA EEM

   ■ Accessible using LDAP as an external directory

   ■ Accessible using CA Site Minder

For more information about configuring CA EEM, see the online help screens of the CA EEM User Interface, together with the CA EEM documentation that can be found, after install, in the following directory:

```
C:\Program Files\CA\SharedComponents\Embedded IAM\Doc
```

Check Library Path Before Starting JBoss

Note: This applies to Linux only.

Before you start JBoss, ensure that $JBOSS_HOME/bin is included in the system library path environment variable LD_LIBRARY_PATH.

If it is not included, append it to LD_LIBRARY_PATH by executing the following command:

```
LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$JBOSS_HOME/bin; export LD_LIBRARY_PATH
```

Start CA XCOM Management Center

To start CA XCOM Management Center, you need to ensure that all of the following are running:

- The CA XCOM Data Transport server
- EEM
- JBoss

To start CA XCOM Management Center on Windows

1. To start the CA XCOM Data Transport server, enter the following command:

   ```
   net start xcomdsrv
   ```

2. To start EEM, enter the following command:

   ```
   net start iGateway
   ```

3. To start JBoss 4.0.5, enter the following command:

   ```
   %JBOSS_HOME%\bin\run.bat
   ```

Note: xcomd and iGateway are installed as services. They can be started from the services window.

To start CA XCOM Management Center on Linux

1. To start the CA XCOM Data Transport server, enter the following command:

   ```
   $XCOM_HOME/sbin/xcomd
   ```

2. To start EEM, enter the following command:

   ```
   $IGW_LOC/S99igateway start
   ```

3. To start JBoss 4.0.5, enter the following command:

   ```
   $JBOSS_HOME/bin/sh run.sh &
   ```

Stop CA XCOM Management Center

To stop CA XCOM Management Center, you need to stop all of the following:

■ The CA XCOM Data Transport server

■ EEM

■ JBoss

To stop CA XCOM Management Center on Windows

1. To stop the CA XCOM Data Transport server, enter the following command:

    `net stop xcomdsrv`

2. To stop EEM, enter the following command:

    `net stop iGateway`

3. To stop JBoss 4.0.5, enter the following command:

    `%JBOSS_HOME%\bin\shutdown.bat -s`

Note: xcomd and iGateway are installed as services. They can be stopped from the services window.

To stop CA XCOM Management Center on Linux

1. To stop the CA XCOM Data Transport server, enter the following command:

    `$XCOM_HOME/sbin/xcomd —s`

2. To stop EEM, enter the following command:

    `$IGW_LOC/S99igateway stop`

3. To stop JBoss 4.0.5, enter the following command:

    `$JBOSS_HOME/bin/sh shutdown.sh -s`

Chapter 5: Configuring and Administering CA XCOM Management Center

This section contains the following topics:

Access the CA XCOM Management Center Website

Initial Login

When CA XCOM Management Center is initially installed and no authorized users have been defined for this CA XCOM Management Center, the first user to successfully log in is automatically added as a Super Administrator user to the CA XCOM Management Center configuration.

Login

Each user ID must be defined in the CA Embedded Entitlements Manager (EEM) global directory, because CA XCOM Management Center always authenticates specified login credentials through CA EEM. Except for the case of an initial login, described above, users whose credentials are authenticated through CA EEM, but are not defined in the CA XCOM Management Center configuration, are automatically added as regular users to the CA XCOM Management Center configuration in the Users database table.

To log in to CA XCOM Management Center

1. Use your web browser to access the CA XCOM Management Center website, as follows:

    `http://<servername>:CA Portal/xcom-mc`

    <servername>

    The host name or IP address of the machine on which the CA XCOM Management Center Server has been installed.

    CA Portal

    The JBoss http port number (default 8080).

    Example:

    `http://myserver:8080/xcom-mc`

    Note: If https has been configured, replace http with https and specify the JBoss https port number.

    The CA XCOM Management Center login screen appears.

2. Enter your user ID and password and click Log In.

3. The Home page appears.

Configure CA XCOM Management Center

Super Admin authority is required for all high-level administration tasks to configure and manage CA XCOM Management Center. With Super Admin credentials, the bar at the top of each page includes an Admin tab and you can click this to perform the following tasks:

- Configure users

- Configure groups

- Configure servers

- Update global parameters

Group Admin authority is required for all administration tasks related to the CA XCOM Management Center groups. With Group Admin credentials, the bar at the top of each page includes an Admin tab and you can click this to perform the following tasks:

- Configure groups

- Configure users in a group

- Configure servers in a group

Note: If there is no Admin tab at the top of the page after you have logged in to CA XCOM Management Center, it is because the user ID with which you logged in does not have Super or Group Admin authority.

Super Admin Process Users

The CA XCOM Management Center configuration should include details for all users who are to be allowed to log in to the CA XCOM Management Center website and use its functions.

You can use the Process Users page on the website to manage your user configuration in the following ways:

- Display users

- Add users

- Delete users

- Update users

- Assign Group Admin to users

Important! You must have Super Admin authority to perform these actions.

Display Users

You can use the Process Users page to display configured users of CA XCOM Management Center.

To display configured users

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Users under Super Admin Functions.

   The Process Users page appears.

Notes:

■ Users can use the filter section on the top of the Process Users page to filter the list of users based on the group they belong to, starting character of the user name, and/or the user name conflicts between users with the same name, but in different combinations of lower/upper case characters.

■ When information for all configured users cannot be accommodated on a single screen, table rows are normally displayed one page at a time. Page information is shown at the top right of the table, indicating the rows presently displayed and the total number of rows. You can click the paging links in this area to display different pages.

Add Users

You can use the Process Users page to add new users to the Users database and optionally assign Super Admin authority to the new users.

To add new users

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Users under Super Admin Functions.

   The Process Users page appears.

4. Click Add New Users.

   The Add New Users page appears.

5. Enter details for a new user.

   Note: If the check box under the Super Admin column is checked for a new user, the user is given Super Admin authority.

6. To add more than one user at a time, either click New to display another empty row or select a row and click copy to copy the row information to a new row.

7. To remove users from the table displayed on the screen, select the rows to be removed and click Remove.

8. Repeat Steps 5 and 6 for each new user.

9. Select the users that you want to be added and click Save.

   The new user(s) are added to the Users database and a confirmation message is displayed.

   Note: If the user(s) already exist in the Users database, an error message is displayed.

The Add New Users page also lets you use the following options:

- Click SaveAll to save all information you entered on this page in the Users database.

- Click Cancel to cancel the current action and return to the previous page.

Delete Users

You can use the Process Users page to delete users from the Users database.

To delete a user

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Users under Super Admin Functions.

   The Process Users page appears.

4. Select users for deletion.

   Note: You can delete one or more users at a time.

5. Click Delete.

   A Delete Users confirmation dialog opens.

6. Click OK.

   The selected users are deleted from the Users database.

Note: If a Super Admin user attempts to delete their own name from the Users database, an error message is displayed and the delete action is canceled.

Update Users

You can use the Process Users page to update attributes of existing users.

To update a user

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Users under Super Admin Functions.

   The Process Users page appears.

4. Select users to update.

   Note: You can update one or more users at a time.

5. Update the user's Super Admin attribute by checking or unchecking the check box.

6. Click Update.

   The attributes of the selected users are updated in the Users database.

Assign/Revoke Group Admin Authority to Users

You can use the Process Users page to assign or revoke Group Admin authority to an existing user.

To assign group admin authority to a user

1. Log in to CA XCOM Management Center.

    The Home page appears.

2. Click Admin.

    The Admin page appears.

3. Click Process Users under Super Admin Functions.

    The Process Users page appears.

4. Click the Group Admin button under Action column for the desired user (row).

    The Assign/Unassign Group Admin page appears. It lists the groups that the selected user is assigned to.

5. Select the group(s) for which you want to update the user's authority.

6. Assign or revoke Group Admin authority for the selected groups by checking or unchecking the check box under the Group Admin column.

    Note: A Super Admin user cannot revoke their own group admin authority.

7. Click Update.

    A confirmation message is displayed on the main Process Users screen.

    Note: You can click on the Cancel button instead to cancel the current operation and return to the previous screen.

Super Admin Process Groups

The CA XCOM Management Center configuration must include details for all the groups that are used to group users and servers defined to CA XCOM Management Center.

You can use the Process Groups page on the website to manage your group configuration in the following ways:

- Display groups
- Add groups
- Delete groups
- Update groups
- Assign Group Admin to users

Important! You must have Super Admin authority to perform these actions.

Display Groups

You can use the Process Groups page to display configured groups of CA XCOM Management Center.

To display configured groups

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Super Admin Functions.

   The Process Groups page appears.

   Process Groups

Select	Group Name	Group Description	Action
☐	Group1		Group Admin
☐	Group2		Group Admin
☐	HR	Human Resources	Group Admin
☐	Marketing	Marketing Department	Group Admin
☐	Payroll	Payroll Department	Group Admin
☐	Sales	Sales Group	Group Admin

Add Groups

You can use the Process Groups page to add new groups to the Groups database.

To add new groups

1. Log in to CA XCOM Management Center.

    The Home page appears.

2. Click Admin.

    The Admin page appears.

3. Click Process Groups under Super Admin Functions.

    The Process Groups page appears.

4. Click Add New Groups.

    The Add New Groups page appears.

5. Enter details for a new group.

6. To add more than one group at a time, either click New to display another empty row or select a row and click copy to copy the row information to a new row.

7. To remove groups from the table displayed on the screen, select the rows to be removed and click Remove.

8. Repeat Steps 5 and 6 for each new group.

9. Select the groups that you want to be added and click Save.

    The new groups are added to the Groups database and a confirmation message is displayed.

    Notes:

    ■   The group name must be a combination of alphanumeric and special characters @ # $ _ starting with an alphabetic character.

    ■   If the groups already exist in the Groups database, an error message is displayed.

The Add New Groups page also lets you use the following options:

■   Click SaveAll to save all information you entered on this page in the Groups database.

■ Click Cancel to cancel the current action and return to the previous page.

Delete Groups

You can use the Process Groups page to delete groups from the Groups database.

To delete a group

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Super Admin Functions.

   The Process Groups page appears.

4. Select groups for deletion.

   Note: You can delete one or more groups at a time.

5. Click Delete.

   A Delete Groups confirmation dialog opens.

6. Click OK.

   The selected groups are deleted from the Groups database.

Update Groups

You can use the Process Groups page to update the attributes of existing groups.

To update a group

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Super Admin Functions.

   The Process Groups page appears.

4. Select group(s) for update.

5. Update the group(s)' description.

6. Click Update.

   The page is redisplayed, showing the updated group(s) description.

Assign/Revoke Group Admin Authority to Users

You can use the Process Groups page to assign or revoke Group Admin authority to an existing user in a group.

To assign/revoke group admin authority to a user

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Super Admin Functions.

   The Process Groups page appears.

4. Click the Group Admin button under Action column for the desired group (row).

   The Assign/Unassign Group Admin page appears. It lists the users assigned to the selected group.

5. Select the users that you want to update their user's authority for the group.

6. Assign or revoke group admin authority for the selected users by checking or unchecking the check box under the Group Admin column.

   Note: A Super Admin user cannot revoke their own group admin authority.

7. Click Update.

   A confirmation message is displayed on the main Process Users screen.

   Note: You can click on the Cancel button instead to cancel the current operation and return to the previous screen.

Super Admin Process Servers

The CA XCOM Management Center configuration must include details for all the servers defined to CA XCOM Management Center and used for schedule transfer and get history record functions.

You can use the Process Servers page on the website to manage your server configuration in the following ways:

- Display servers

- Add servers

- Delete servers

- Update servers

- Export servers

- Download already exported servers

- Import already exported servers

- Upload already downloaded servers

- Import servers from history records

Important! You must have Super Admin authority to perform these actions.

Display Servers

You can use the Process Servers page to display configured servers of CA XCOM Management Center.

To display configured servers

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Servers under Super Admin Functions.

   The Process Servers page appears.

Configure Servers

You can use the Process Servers page to add new servers to the Servers database.

To add new servers

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Servers under Super Admin Functions.

   The Process Servers page appears.

4. Click Add New Servers.

   The Add New Servers page appears.

5. Enter details for a new server.

6. To add more than one server at a time, either click New to display another empty row or select a row and click copy to copy the row information to a new row.

7. To remove servers from the table displayed on the screen, select the rows to be removed and click Remove.

8. Repeat Steps 5 and 6 for each new server.

9. Select the servers that you want to be added and click Save.

   The new servers are added to the Servers database and a confirmation message is displayed.

   Notes:

   ■ The group name must be a combination of alphanumeric and special characters @ # $ _ starting with an alphabetic character.

   ■ If the servers already exist in the Servers database, an error message is displayed.

- You can use the Hide/Show icon on the second column to hide/show the extra information for a row. You can also use the Hide All Details or Show All Details link to hide or show the details for all the rows respectively.

The Add New Servers page also lets you use the following options:

- Click SaveAll to save all information you entered on this page in the Servers database.

- Click Cancel to cancel the current action and return to the previous page.

Delete Servers

You can use the Process Servers page to delete servers from the Servers database.

To delete a server

1. Log in to CA XCOM Management Center.

    The Home page appears.

2. Click Admin.

    The Admin page appears.

3. Click Process Servers under Super Admin Functions.

    The Process Servers page appears.

4. Select servers for deletion.

    Note: You can delete one or more servers at a time.

5. Click Delete.

    A Delete Servers confirmation dialog opens.

6. Click OK.

    The selected servers are deleted from the Servers database.

Update Servers

You can use the Process Servers page to update the attributes of existing servers.

To update a server

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Servers under Super Admin Functions.

   The Process Servers page appears.

4. Select servers for update.

5. Click the Edit link.

   The Update Servers page appears.

6. Select the servers that you want to be updated.

7. Update the server information and click Update.

   The servers are updated in the Servers database and a confirmation message is displayed.

   Note: You can use the Hide/Show icon on the second column to hide/show the extra information for a row. You can also use the Hide All Details or Show All Details link to hide or show the details for all the rows respectively.

The Update Servers page also lets you use the following options:

- Click UpdateAll to update all information you entered on this page in the Servers database.

- Click Cancel to cancel the current action and return to the previous page.

Export Servers

You can use the Process Servers page to export and save server information as an xml file on the web server.

To export servers

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Servers under Super Admin Functions.

   The Process Servers page appears.

4. Select the servers that you want to export.

5. Click Export.

   The Export Servers page appears.

6. Enter the exported file name and optionally the description.

7. Click Save.

   The information is saved in the exported file on the web server and a confirmation message is displayed.

   Notes:

   ■ If the exported file name already exists on the web server, a dialog opens and allows you to append the information to the existing file, to replace the file, or cancel the process.

   ■ Exported server files are stored in the following directory on the web server:

      xxxxx/loginuserid/ExportedServers

xxxxx

> The value of the HOMEDIRECTORY parameter of the EXPORT element in the Global Parameters file.

loginuserid

> The ID of the logged in user (or the first 60 characters of the logged in user ID if the user ID is more than 60 characters long).

The Export Servers page also lets you use the following options:

- Click Download button for an exported file to download the information to your local workstation and save it as an xml file. A dialog opens to specify the path and file name of the downloaded file.

- Click Cancel to cancel the current action and return to the previous page.

Import Servers from Export File

You can use the Process Servers page to import already exported servers file and display the server information on the screen.

To import servers from export file

1. Log in to CA XCOM Management Center

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Servers under Super Admin Functions.

   The Process Servers page appears.

4. Click the Import from Export button.

   The Import Servers page appears.

5. Click the icon under the Import column for an Exported file.

   The information for the servers in the selected Exported file is displayed on the Add New Servers page. You can check the information, update it, and save the servers in the Servers database as described in the Add New Servers section.

   The Import Servers page also lets you use the following options:

   ■ Click Browse button to select a downloaded server xml file from your workstation. Enter the name for the uploaded file. Click the Upload button to upload and save the information on the web server. The uploaded file is saved in the following directory on the web server:

   xxxxx/*loginuserid*/ExportedServers

   xxxxx

      The value of the HOMEDIRECTORY parameter of the EXPORT element in the Global Parameters file.

loginuserid

> The ID of the logged in user (or the first 60 characters of the logged in user ID if the user ID is more than 60 characters long).

- Select one or more exported files from the list and click the Delete link to delete the files from the web server. A dialog opens to confirm or cancel the process. A confirmation message is displayed after deletion.

- Click Cancel to cancel the current action and return to the previous page.

Import Servers from History

You can use the Process Servers page to import servers from history records and display the server information on the screen.

To import servers from history

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Servers under Super Admin Functions.

   The Process Servers page appears.

4. Click the icon under Import From History column for a server.

   Note: The Import From History icon is only available for servers with a valid IP Address.

   The History Parameters page appears.

   The parameters displayed on this page are used to limit the history records to be searched for the servers. See below for the description of the parameters.

5. Enter the desired parameters and click Submit.

   Note: Click Cancel on this page to cancel the import process and return to the Process Servers page.

   The information for the servers found in the searched history records is displayed on the Add New Servers page.

   You can check the information, and then update the servers and save them in the Servers database. (See Add New Servers in this chapter.)

History Parameters

This section describes the history parameters used to import servers from history or to get history records from a server.

Note: These history parameters are not case-sensitive. So filtering history records based on these parameters returns case-insensitive results. For example, specifying **USER01** as the Requesting User ID returns the same results as specifying **user01**.

Selected Server Information

The first line contains information about the server whose history record is to be searched.

If both SSL and non-SSL ports are specified for the server, you can check the **Use SSL** box on this line and the SSL port will be used to connect to the server; otherwise, the non-SSL port will be used.

Start Date and Time

Limits the history request to only those file transfers that were scheduled or completed on or after the start date and time.

End Date and Time

Limits the history request to only those file transfers that were scheduled or completed on or before the end date and time.

Completed, Inactive, and/or Active check box

Specifies if the history request should include inactive transfer requests, active transfer requests, and/or completed transfers.

Limit records to

Limits the records to those file transfers in the queue, in the database, or both.

Requesting User ID

Limits the history request to only those file transfers submitted by a specific user.

Requesting Number

Limits the history request to only those file transfers that contain this specific request number.

Transfer ID

Limits the history request to only those file transfers with a specific transfer ID. The transfer ID is a user-defined identifier for file transfer requests.

Local or Remote

Limits the history request to locally initiated transfers only, remotely initiated transfers only, or both.

File Type

Limits the history request to those transfers with the specified File Type (File, Job, or Report) or All file types.

Transfer Type

Limits the history request to only send transfers, only receive transfers, or both transfer types.

Remote System TCP/IP

Limits the history request by the remote system protocol.

History System ID

Limits the history request by the system ID.

History System Name

Limits the history request by the system name.

Remote System ID

Limits the history request to only those file transfers with a specific remote TCP/IP name or TCP/IP address.

Last Message

Limits the history request by the transfer's last message.

Maximum Entries

Limits the number of history records to be searched.

Minimum File Size

Limits the history request to only those file transfers where the number of bytes transferred is equal to or greater than the value specified.

This value can be a 1- to 10-digit number, where the last digit can be either another numeric digit or a 1-character qualifier, in the form *nnnnnnnnn*(*n*|*x*), where *x* can be one of the following qualifiers:

- B = Bytes
- K = Kilobytes
- M = Megabytes
- G = Gigabytes
- T = Terabytes
- P = Petabytes
- E = Exabytes

Maximum File Size

Limits the history request to only those file transfers where the number of bytes transferred is equal to or less than the value specified. This value can be a 1- to 10-digit number, where the last digit can be either another numeric digit or a 1-character qualifier, in the form $nnnnnnnnn(n|x)$, where x can be one of the following qualifiers:

- B = Bytes
- K = Kilobytes
- M = Megabytes
- G = Gigabytes
- T = Terabytes
- P = Petabytes
- E = Exabytes

Group Admin Process Groups

You can use the Process Groups page on the website under Group Admin functions of the Admin tab to manage groups assigned to you in the following ways:

- Display groups
- Update groups
- Update user authorities in a group
- Remove users from a group
- Assign users to a group
- Assign servers to a group
- Remove servers from a group

Important! You must have Group Admin authority for the group to perform these actions on that group.

Display Groups

You can use the Process Groups page to display groups of CA XCOM Management Center that are assigned to you.

To display assigned groups

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Group Admin Functions.

   The Process Groups page appears.

Update Groups

You can use the Process Groups page to update the attributes of existing groups.

To update a group

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Group Admin Functions.

   The Process Groups page appears.

4. Select groups for update.

5. Update the group descriptions.

6. Click Update.

   The page is redisplayed, showing the updated group descriptions.

Update User Authorities in a Group

You can use the Process Groups page to update the group admin and configuration authorities for the existing users in a group.

To update user authorities in a group

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Group Admin Functions.

   The Process Groups page appears.

4. Click Process Users from the Actions drop-down menu.

   The list of users assigned to the selected group is displayed.

5. Select the users whose authorities you want to update.

6. Assign or revoke group admin authority for the selected users by checking or unchecking the check box under the Group Admin column.

   Note: A Group Admin user cannot revoke their own group admin authority.

7. Select the configuration authority for the selected users from the drop-down menu under Configuration Authority column.

   The configuration authority determines the user's level of authorization to process public configuration files. The levels from low to high are defined as follows:

   1. None

   No configuration file processing allowed.

   The actions not allowed by the user for a configuration file in the group with the authorization level of **none** are as follows:

   ■   Load (the configuration files for the group are not displayed for the load action)

   ■   Edit (Display) transfer records

- Edit (Display) and append transfer records

- Submit

- Export

- Save

- Delete

2. **Submit**

 Users can submit the configuration file, but no access to transfer records inside the file is allowed.

 The actions not allowed by the user for a configuration file in the group with the authorization level of **submit** are as follows:

- Edit (Display) transfer records

- Edit (Display) and append transfer records

- Export

- Save

- Delete

3. **Read**

Users can read the transfer records in a configuration file (using the load button) and submit them for processing.

The actions not allowed by the user for a configuration file in the group with the authorization level of **read** are as follows:

- Save

- Delete

- Edit (Display) transfer records

- Edit (Display) and append transfer records

4. **Edit**

Users can build and save transfer records in a configuration file as well as having Submit and Read authorities.

The only action not allowed by the user for a configuration file in the group with the authorization level of **edit** is as follows:

- Delete

5. **Control**

Means all of the above authorities as well as deleting configuration files.

Users are allowed all the actions described for the **none** authority.

8. Click Update.

   A confirmation message is displayed on the main Process Users screen.

   Note: Click Cancel on this page to cancel the process and return to the previous page.

Remove Users from a Group

You can use the Process Groups page to remove existing users assigned to a group.

To remove users from a group

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Group Admin Functions.

   The Process Groups page appears.

4. Click Process Users from the Actions drop-down menu.

   The list of users assigned to the selected group is displayed.

5. Select the users that you want to remove.

6. Click Remove.

   A Remove Users confirmation dialog opens.

   Note: Click Cancel on this page to cancel the process and return to the previous page.

7. Click OK.

   The selected users are removed from the selected group.

   Note: You can click on Cancel instead to cancel the remove process.

Assign Users to a Group

You can use the Process Groups page to assign new users to a group.

To assign users to a group

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Group Admin Functions.

   The Process Groups page appears.

4. Click Process Users from the Actions drop-down menu.

   The list of users assigned to the selected group is displayed.

   Note: Click Cancel on this page to cancel the process and return to the previous page.

5. Click Add New Users.

   The Add Users page appears.

6. Select the users that you want to add to the group.

7. Optionally, update the group admin and configuration authorities for the selected users, as explained in Update User Authorities in a Group.

8. Click Save.

   The selected users are added to the group. A confirmation message is displayed.

The Add Users page also lets you use the following option:

- Click SaveAll to save all the users listed to the group.

- Click Cancel to cancel the current action and return to the previous page.

Remove Servers from a Group

You can use the Process Groups page to remove existing servers assigned to a group.

To remove servers from a group

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Group Admin Functions.

   The Process Groups page appears.

4. Click Process Servers from the Actions drop-down menu.

   The list of servers assigned to the selected group is displayed.

5. Select the servers that you want to remove.

6. Click Remove.

   A Remove Servers confirmation dialog opens.

   Note: Click Cancel on this page to cancel the process and return to the previous page.

7. Click OK.

   The selected servers are removed from the selected group.

   Note: You can click Cancel instead to cancel the remove process.

Assign Servers to a Group

You can use the Process Groups page to assign new servers to a group.

To assign servers to a group

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Admin.

   The Admin page appears.

3. Click Process Groups under Group Admin Functions.

   The Process Groups page appears.

4. Click Process Servers from the Actions drop-down menu.

   The list of servers assigned to the selected group is displayed.

   Note: Click Cancel on this page to cancel the process and return to the previous page.

5. Click Add New Servers.

   The Add Servers page appears.

6. Select the servers that you want to add to the group.

7. Click Save.

   The selected servers are added to the group. A confirmation message is displayed.

The Add Servers page also lets you use the following option:

■ Click SaveAll to save all the listed servers to the group.

■ Click Cancel to cancel the current action and return to the previous page.

Update the Global Parameters File

CA XCOM Management Center administrators with Super Admin authority can use the Global Parameters page to display or change the values of global parameters. However, the changes made to the global parameters take effect only when CA XCOM Management Center is restarted.

Note: Following the installation of CA XCOM Management Center, the following global parameters may need to be changed, if the installer sets them to fixed values that may not be appropriate:

Log and Trace Parameters

These parameters may need to be changed. They control the destination, format, and reporting level for log messages and trace information generated by CA XCOM Management Center.

General Parameters

These parameters may need to be changed. They specify parameters such as the default home directory for exported server and/or configuration items and default and maximum rows/page for tabular data.

Global parameters are stored in an xml file called xcom-globals.xml within the JBoss conf folder. This file is updated whenever parameters are changed using the Global Parameters page of CA XCOM Management Center. For more information about the format of the xcom-globals.xml file, see the appendix "Configuration XML Formats."

Important! Because incorrect global parameter changes can render CA XCOM Management Center inoperable and the CA XCOM Management Center website inaccessible, we strongly recommend that you save a copy of xcom-globals.xml before making online changes to the global parameters. Problematic changes can then be reversed by restarting CA XCOM Management Center after reinstating the saved file.

To update global parameters

1. Log in to CA XCOM Management Center.

    The Home page appears.

2. Click Admin.

    The Admin page appears.

    Note: If there is no Admin tab on the web page, it means that your login ID does not have Super Admin authority.

3. Click Global Parameters.

    The Global Parameters page appears, displaying the current global parameter values. The parameters are divided into groups and each group can be hidden or revealed by clicking the icon to the left of the group's heading bar. The following sections describe the parameters in each group.

4. Edit the parameter values as required. For a description of each parameter, see the following section.

5. Click Save.

    The changes made to global parameters are saved.

Notes:

■   If an optional parameter value is erased, the default value is saved for the parameter in the Global Parameters file.

■   You can click Reset to reset the values on the page to the ones already stored in the Global Parameters file.

CA EEM Parameter

CA XCOM Management Center requires access to the CA Embedded Entitlements Manager (EEM) server to authenticate users when they log in to the CA XCOM Management Center website. The CAEEM element specifies the attribute related to the EEM server instance that CA XCOM Management Center is to use for the purposes of user authentication.

The CA XCOM Management Center installer sets the CA EEM parameter initially, according to the value entered during product installation. The installer can (optionally) also verify the parameter by ensuring the ability to connect to the designated server.

Important! This parameter can be changed later, but changes cannot be verified by attempting to connect to the specified server. Therefore it is particularly important to save a copy of the xcom-globals.xml file from the JBoss conf folder before changing the CA EEM parameter.

CA EEM Server Host

Identifies the host name of the CA EEM server that is to be used by CA XCOM Management Center for the purposes of user authentication.

Note: The EEM server always uses port 5250. So you cannot specify an alternate port.

Web Interface Parameter

Web Interface URL

Identifies the URL for the host on which the Interface Server war file is located and the port number on which it accepts requests from CA XCOM Management Center. The CA XCOM Interface Server is used to pass the CA XCOM Management Center requests to the base CA XCOM Data Transport product and returns the response back to CA XCOM Management Center.

Default: The same as the host name and port number where the CA XCOM Management Center war file resides.

Database Parameters

The CA XCOM Management Center server needs access to a DB2 or MySQL database, in which it stores configuration information. The database parameters are used to define the database server information needed by CA XCOM Management Center to access this database.

The CA XCOM Management Center installer sets the database parameters initially, according to values entered during product installation. The installer also verifies the parameters by ensuring the ability to connect to the designated server. These parameters can be changed later, and changes are accepted only if CA XCOM Management Center retains its ability to connect to the database server and access its database.

Datasource name

Identifies the JDBC data source, which defines the database server to be used.

User ID and Password

Used by CA XCOM Management Center to access and update its database tables. The specified user must have full access rights to all objects in CA XCOM Management Center's database, including the tables and indexes.

DataBase Creator

The database schema name for DB2 database.

Default: The same as User Name (if not specified)

Important! The DataBase Creator parameter must not be coded for MySQL databases.

Log and Trace Parameters

Log Path

Specifies the destination path for the log file to be created by CA XCOM Management Center. The log file is a text document file with the name mc-log.txt. If the path location is not specified, the default is /tmp/CA_XCOM/. The information in the mc-log.txt file is moved to a new file with the name of mc-log.txt.*yyyy-mm-dd* at the end of the day.

Log Level

Specifies the level of information that CA XCOM Management Center is to record in the log file. Initially this parameter is set to the default value of Informational.

Valid values are as follows:

Informational

Log messages will be recorded for all categories, that is, informational, warning, and error messages.

Warning

Warning and error messages will be written to the log file, but informational messages will not.

Error

Only error messages will be recorded in the log.

Log Date Format

Determines the format of the date that is included as the start of each message written to the log file. This parameter is set initially to the default value of US.

Valid values are as follows:

US

Log messages start with the date in *mm/dd/yyyy* format.

European

Log messages start with the date in *dd/mm/yyyy* format.

Trace File

Specifies the destination path name of the trace file to be created by CA XCOM Management Center. The trace file is used primarily for debugging purposes. It is a txt type file with the name of mc-trace.txt. The default is /tmp/CA_XCOM/. The information in the mc-trace.txt file is moved to a new file with the name mc-trace.txt.*yyyy-mm-dd* at the end of the day.

Trace Level

Specifies the required level of tracing. As the trace level number increases, more detailed trace records are written in the trace file. By default, the trace level is set to zero, which inhibits all tracing.

Note: When responding to customer issues, CA Technical Support may request tracing as an aid to problem source identification and will provide guidance on the setting of these parameters. At all other times, to optimize product performance, tracing should be switched off by setting the trace level to 0.

Export Home Directory Parameter

Export Home Directory

Identifies the default destination folder for exported server and configuration files.

Default: /XCOMGUI/

Exported server files are stored in the following directory:

homedirectory/loginuserid/ExportedServers

Example:

C:\XCOMGUI\USER1\ExportedServers

Exported configuration files are stored in the following directory:

homedirectory/loginuserid/ExportedConfigurations

Example:

C:\XCOMGUI\USER1\ExportedConfigurations

homedirectory

The value of the HOMEDIRECTORY parameter of the EXPORT element in the Global Parameters file.

loginuserid

The ID of the logged in user (or the first 60 characters of the logged in user ID if the user id length is more than 60 characters).

User Name caseInsensitive Parameter

User Name caseInsensitive

Specifies whether the entered user name at login time is case-sensitive, as follows:

- If the parameter is omitted or set to YES (the check box is checked), then the entered user name is treated as case-insensitive and matches with a user name in the Users Database ignoring the case. The user name with the lowest user_row ID in the Users Database is used as the login user.

- If the parameter is set to NO (the check box is cleared), then the entered user name is treated as it is and with no upper/lower case conversion.

Rows/Page Parameters

Default Rows/Page

Identifies the default value (which applies when a user has made no alternative selection at the time of login on the CA XCOM Management Center Home page) specifying the effective Rows/Page value.

The effective Rows/Page value controls the number of data rows to be displayed on any GUI screen (that is, a single page) showing tabular data. When the number of data rows to be presented exceeds the effective Rows/Page value, data rows are displayed over a number of screens (that is, pages), with links enabling navigation between pages.

Range: 1 to 9999

Default: 20

Maximum Rows/Page

Identifies the highest permitted value that can be adopted as the effective Rows/Page value, which controls the number of data rows to be displayed on any GUI screen (that is, a single page) showing tabular data. If a user attempts to select an alternate Rows/Page value at the time of login on the CA XCOM Management Center Home page, they will not be permitted to select any value that is higher than MAXPAGEROWS.

Range: 1 to 9999

Default: 9999

Note: The Default Rows/Page value cannot be greater than the Maximum Rows/Page value.

Configure Global Parameters Offline

Global parameters are stored externally in a file called xcom-globals.xml within the JBoss conf folder. This file is updated whenever parameters are changed using the Global Parameters page of the CA XCOM Management Center website. It is read when CA XCOM Management Center is started and its content at that time dictates the global parameters that are used. Therefore, when the file is updated, parameter changes do not take effect until the next time that CA XCOM Management Center is started.

As an alternative to updating the xcom-globals.xml file by using the website facilities, it is also possible to edit this file by using any suitable text editor. This method of changing global parameters can be used, for example, to correct parameter settings that prevent CA XCOM Management Center from starting.

The same xcom-globals.xml contains global parameters not only for CA XCOM Management Center, but also for the CA XCOM Interface Server and CA XCOM Gateway (if installed). Within the file, each product has its own section, which takes the form of a parent xml element embodying all of the attributes related to that product. When editing the file, it is important to ensure that only the correct section is modified and that sections relating to other products are left unchanged.

Important! We strongly recommend that a copy of the xcom-globals.xml file should always be saved before making any changes to the global parameters. Problematic changes can then be reversed by restarting CA XCOM Management Center after reinstating the saved file.

For more information about the format of the xcom-globals.xml file, see the appendix "XML Formats."

Change Passwords

Both database and keystore passwords within the xcom-globals.xml file are represented in encrypted form, using PASSWORD and KEY attributes within appropriate xml elements.

After installing CA XCOM Management Center, it may become necessary to update the xcom-globals.xml file when these passwords change. The XcomConfiguration.jar utility program is provided to facilitate this.

XcomConfiguration.jar can be located in the 'lib' subdirectory of the JBOSS_HOME\server directory; for example, C:\Program Files\JBoss\server\default\lib.

To execute this program

1. At the command prompt enter the following command line:

    ```
    java –jar "{libdirectory}\XcomConfiguration.jar"
    ```

2. When prompted, enter the path of the folder that contains the xcom-globals.xml file that is to be updated by the utility program.

    Subsequently, you are prompted to enter new passwords for the following:

    ■   The CA XCOM Interface Server keystore

    ■   The CA XCOM Interface Server's database user

    ■   The CA XCOM Gateway keystore (if that product has been installed)

    ■   The CA XCOM Gateway database user (if that product has been installed)

    ■   The CA XCOM Management Center database user

3. At each prompt, do *one* of the following:

    ■   Type the new password, if that particular password has changed.

    ■   Press Enter to leave the existing password unchanged.

On completion of the utility program, the appropriate PASSWORD and KEY attributes within the xcom-globals.xml file are updated to reflect the new passwords that have been entered.

You then need to restart the associated products in order to make the changes effective.

Export and Import Process

Users with proper authority can export server information and configuration files and save them as an xml files on the web server.

The Administration page of the website provides a facility to enable server information to be exported to an xml file by the Super Admin. The Super Admin can then use the import function to import the server information, with the possibility of adding the servers to the CA XCOM Management Center configuration.

Exported server files are stored in the following directory on the web server:

xxxxx/*loginuserid*/ExportedServers

xxxxx

> Tthe value of the HOMEDIRECTORY parameter of the EXPORT element in the Global Parameters file.

loginuserid

> The ID of the logged in user (or the first 60 characters of the logged in user ID if the user ID length is more than 60 characters).

Users with proper authority can also export configuration files as an xml file and save them on the web server. The users can then use the import function to import the transfer records in the exported configuration file and display them on the CA XCOM Management Center Schedule Transfer main page for further processing.

Exported configuration files are stored in the following directory on the web server:

xxxxx/*loginuserid*/ExportedConfigurations

xxxxx

> Tthe value of the HOMEDIRECTORY parameter of the EXPORT element in the Global Parameters file.

loginuserid

> The ID of the logged in user (or the first 60 characters of the logged in user ID if the user ID length is more than 60 characters).

For more information about exporting and importing configuration files, see the chapter "Using CA XCOM Management Center through the Internet."

As with global parameters, this makes it possible to edit exported files using a suitable text editor. It is also possible to programmatically generate server and configuration file information, in xml form, and then import them into CA XCOM Management Center.

For more information about the format of the xml files, see the appendix "XML Formats."

Configure SSL Communication

Data exchanged between CA XCOM Management Center users, CA XCOM Management Center's software components, and CA XCOM Data Transport servers can be transmitted securely, in encrypted form, by means of secure sockets layer (SSL) communication. This can be selected individually for each of the following forms of communication:

- Internet connections to CA XCOM Management Center

- Communication between the CA XCOM Management Center Server and the CA XCOM Interface Server

- Communication between the CA XCOM Interface Server and CA XCOM Data Transport servers

Internet Connections to CA XCOM Management Center

CA XCOM Management Center users can request secure communication with CA XCOM Management Center by using a modified internet address to access the CA XCOM Management Center web site. This address must commence with https, in place of http, and specify the appropriate https port number, as outlined in the chapter "Using CA XCOM Management Center through the Internet."

To enable the use of the https protocol for communication with the CA XCOM Management Center server

1. Configure JBoss to support SSL.

   Internally, JBoss uses Apache Tomcat Server, which handles SSL communication through the https protocol. Enabling support for SSL by the Tomcat server requires the following:

   - Installation of an X509 certificate within a keystore

   - Revision of the Tomcat configuration to turn on SSL, referencing the related keystore and certificate.

   Detailed information can be found on the http://tomcat.apache.org website and by searching the internet using the keywords "tomcat SSL configuration."

Communication Between the CA XCOM Management Center Server and the CA XCOM Interface Server

The CA XCOM Management Center server uses web services to communicate with the CA XCOM Interface Server and can be configured to use the secure https protocol for this communication.

To enable the use of the https protocol for communication with the CA XCOM Interface Server

1. Configure JBoss to support SSL.

   Internally, JBoss uses Apache Tomcat Server, which handles SSL communication through the https protocol. Enabling support for SSL by the Tomcat server requires the following:

   - Installation of an X509 certificate within a keystore

   - Revision of the Tomcat configuration to turn on SSL, referencing the related keystore and certificate

   Detailed information can be found on the http://tomcat.apache.org website and by searching the internet using the keywords "tomcat SSL configuration."

2. Configure the CA XCOM Interface Server to use SSL.

   After installation of CA XCOM Management Center, the https protocol can be configured by updating the Global Parameters offline, to change the INTERFACEURL attribute within the WEBSERVICES xml element, so that it specifies the https protocol with the appropriate port number.

3. Using the keytool utility on the CA XCOM Management Center machine, create a new truststore to be used by CA XCOM Management Center and import into it a copy of the JBOSS SSL certificate, created in step 1. To find and import the necessary certificate, execute the following commands against the JBoss keystore (keystore passwords will be needed):

   Note: Replace the "<...>" in these examples with the actual values.

   a. To list the certificates in the JBoss keystore on the Interface Server machine, execute the following command:

   ```
   "%JAVA_HOME%\\bin\\keytool.exe" —list —keystore <jboss keystore file>
   ```

   Example output:

   ```
   Your keystore contains 1 entries

   authoritycertificate, May 19, 2010, trustedCertEntry,

   Certificate fingerprint (MD5):
   5B:68:BE:49:4B:56:F5:74:84:EB:C2:C4:BD:D7:05:61
   ```

   b. To export the trustedcertentry from the JBoss keystore on the Interface Server machine, execute the following command:

```
"%JAVA_HOME%\\bin\\keytool.exe" -export -alias authoritycertificate -file
cert.cer -keystore <jboss keystore file>
```

c. To create a Management Center truststore and import the cert into it, execute the following command (and reply yes to trusting certificates) on the Management Center machine:

```
"%JAVA_HOME%\\bin\\keytool.exe" -import -alias authoritycertificate -file
cert.cer -keystore <management center truststore file> -storepass <password>
```

4. On the Management Center machine, set the location of the client truststore using two JVM properties; javax.net.ssl.truststore and javax.net.ssl.trustStorePassword. To do this, edit the JBoss /server/default /deploy/properties-service.xml file and add the following to the 'jboss:type=Service,name=SystemProperties' MBean:

```
<attribute name="Properties">
    javax.net.ssl.trustStore= <full path for the Management Center truststore
    file >
    javax.net.ssl.trustStorePassword= < Management Center truststore password>
</attribute>
```

Communication Between the CA XCOM Interface Server and CA XCOM Data Transport Servers

CA XCOM Interface Server communicates with the local CA XCOM Data Transport Server, using web services, to schedule transfers on behalf of CA XCOM Management Center and to monitor their progress. For enhanced security, the SSL (Secure Sockets Layer) protocol can be requested for this control communication between the two server components.

When SSL communication is required, it can be requested by means of the SSL=YES attribute within the TRANSFERCONTAINER xml. Usually the CA XCOM Interface Server and its allied CA XCOM Data Transport Server are installed on the same machine and secure communication between these servers might not be deemed necessary. However, secure SSL communication is always recommended if the CA XCOM Interface Server and its local CA XCOM Data Transport Server are to reside on separate server machines.

To employ SSL communication between the CA XCOM Interface Server and local CA XCOM Data Transport Server, it is first necessary to configure the CA XCOM Interface Server to give it access to the client certificate of the local CA XCOM Data Transport Server.

To configure the CA XCOM Interface Server

1. Generate an SSL client certificate for the CA XCOM Data Transport Server, as described in the *CA XCOM Data Transport Administration Guide*.

2. Using the following steps, create a keystore for the CA XCOM Interface Server to use on the same machine where this server is located.

3. Import the SSL client certificate into the designated keystore, using the keytool utility.

    Note: The facilities offered by the keytool utility program are fully documented on the http://java.sun.com web site (http://java.sun.com/docs/books/tutorial/security/toolsign/step3.html).

    To run the keytool utility, open the command prompt (Start->run->cmd), and execute the keytool utility by entering a command in the following format:

    ```
    "{InterfaceServerInstallDirectory}\jre\bin\keytool.exe" -import -trustcacerts
    -alias {alias id} -keystore "{keystore path/file}" —storepass "{keystore
    password}" -file "{certificate path/file}"
    ```

    {InterfaceServerInstallDirectory}

    The path for the folder into which the CA XCOM Interface Server was installed, for example, c:\Program Files\CA\XCOMIF.

{alias id}

> A unique alias ID that you want to assign to the SSL certificate. This can be any ID that is different from that of any existing certificate within the same keystore.

{keystore path/file}

> The directory path for the keystore location and keystore file name.

> You can specify the path and name of a file that does not presently exist, in which case keytool creates the new keystore.

{keystore password}

> The current password of the existing keystore, or the password to be assigned to a new keystore.

{certificate path/file}

> The directory path and file name of the CA XCOM Data Transport client certificate that you want to import; for example, "C:\Program Files\CA\XCOM\Ssl\cassl.pem".

4. Lastly, the xcom-globals.xml file must be updated to specify the location of the keystore to be used by CA XCOM Interface Server.

    a. Add a <KEYSTORE> element to the <INTERFACESERVER> section of the xcom-globals.xml file and within this element include only a PATH= attribute identifying the location of the new keystore, for example:

    Before:

    ```
    <GLOBALPARAMETERS>
    . . .
        <INTERFACESERVER QUERYCOUNT="9999">
            <LOG LEVEL="INFO"
                PATH="C:\Program Files\CA\XCOMIF/Logs"/>
    . . .
        </INTERFACESERVER>
    </GLOBALPARAMETERS>
    ```

    After:

    ```
    <GLOBALPARAMETERS>
    . . .
        <INTERFACESERVER QUERYCOUNT="9999">
            <KEYSTORE
                PATH="C:\Program Files\CA\Webserver.keystore"/>
            <LOG LEVEL="INFO"
                PATH="C:\Program Files\CA\XCOMIF/Logs"/>
    . . .
        </INTERFACESERVER>
    </GLOBALPARAMETERS>
    ```

b. Save the updated xcom-globals.xml file.

c. Use the XcomConfiguration.jar program to add the PASSWORD= and KEY= attributes.

XcomConfiguration.jar can be located in the 'lib' subdirectory of the JBOSS_HOME\server directory, for example, C:\Program Files\JBoss\server\default\lib.

- To execute this program, at the command prompt enter the command line:

  ```
  java –jar "{libdirectory}\XcomConfiguration.jar"
  ```

- When prompted, enter the path of the folder that contains the xcom-globals.xml file that is to be updated by the utility program.

- When prompted to enter the password for Interface Keystore, type the password for the new keystore and press enter.

- At all of the other prompts, press enter in order to leave all other passwords unchanged.

- Review the updated xcom-globals.xml file, in which the <KEYSTORE> element that was added above, should now include a PASSWORD and a KEY attribute, inserted by the utility program.

Important! After saving the updated xcom-globals.xml file, you need to restart CA XCOM Interface Server for the changes to become effective.

Chapter 6: Using CA XCOM Management Center Through the Internet

You can access the CA XCOM Management Center website through the Internet by using either HTTP or HTTPS. HTTPS allows data to be transferred in encrypted form.

This section contains the following topics:

Log In

User IDs can be defined in the CA XCOM Management Center configuration and the specified credentials must be authenticated through through the CA Embedded Entitlements Manager (EEM). See your CA XCOM Management Center administrator for user ID definition and configuration.

Users whose credentials are authenticated successfully, but are not defined in the CA XCOM Management Center configuration, are automatically added as regular users to the CA XCOM Management Center configuration.

To log in to CA XCOM Management Center

1. Use your web browser to access the CA XCOM Management Center website, by entering the website address supplied by your CA XCOM Management Center administrator.

    Note: For more information about the website address, see Log In in the chapter "Configuring and Administering CA XCOM Management Center."

    The CA XCOM Management Center login screen appears.

2. Enter your user ID and password and click Log In.

    If you do not enter user ID and/or password, an error message is displayed, advising you to enter the missing value.
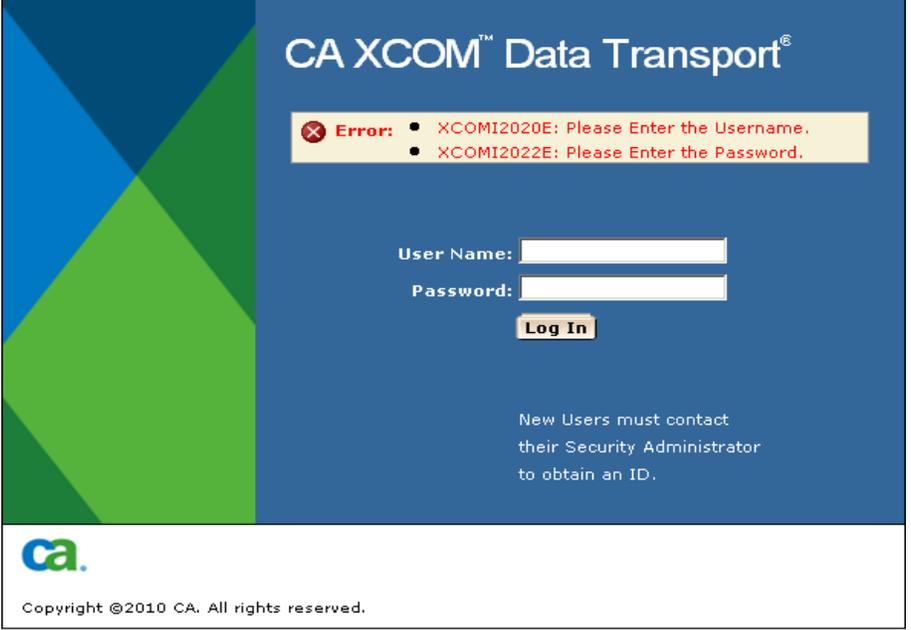
If the authentication by the CA EEM server fails, an error message is displayed and allows the user to re-enter the information. Clicking on the moreInfo button gives more information about the cause of the failure on the error page as shown below.

The output for the MoreInfo button is as follows:

Click the Login button on this page to return to the login page.

Notes:

- The Log In page also appears when your current session has timed out and you request another CA XCOM Management Center function. If your password expires or you do not have a valid login credentials, contact your security administrator.

- The user ID can be up to 255 characters. An error message is issued for user IDs longer than 255 characters.

CA XCOM Management Center Website

The CA XCOM Management Center website consists of the following:

Home tab

Clicking this tab returns you to the initial menu page (shown below) from any page on the website.
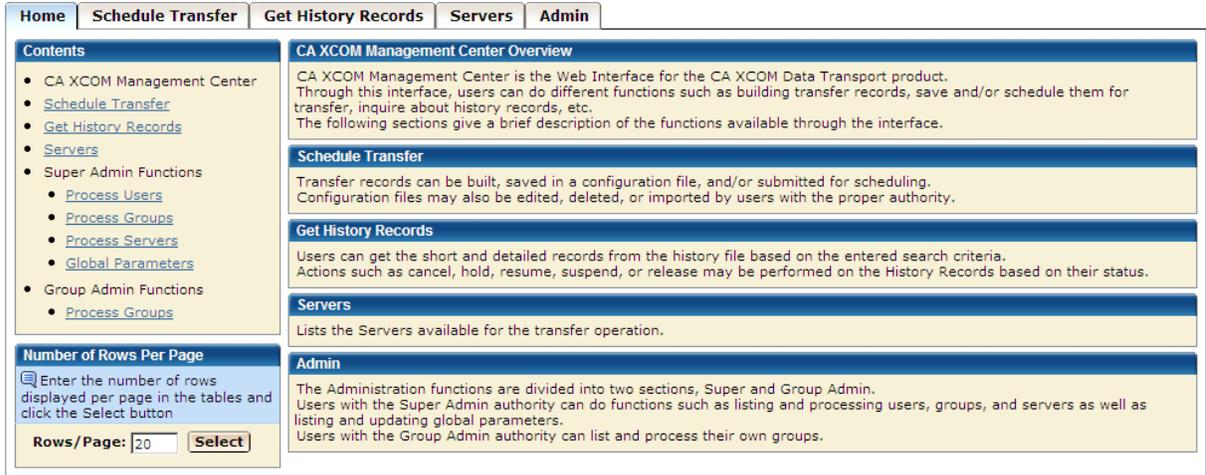
Schedule Transfer tab

Clicking this tab navigates to the schedule transfer section of the website, which permits functions such as building transfer records, saving transfer records as configuration files, and submitting records for schedule.

Get History Records tab

Clicking this tab navigates to the get history records section of the website, which permits users to get the history record information for a server. Users can also update the priority and start data and time of an inactive transfer or change the status of active and/or inactive transfer.

Servers tab

Clicking this tab navigates to the servers record section of the website, which lists all the available servers to the user and their associated attributes.

Admin tab

Clicking this tab navigates to the CA XCOM Management Center configuration facilities (see the chapter "Configuring and Administering CA XCOM Management Center"). The Admin tab appears only if you have logged in to CA XCOM Management Center using a Super and/or Group Administrator user ID.

Filters for Tabular Data

The tabular screens in the following sections provide a leading filter section to enable users to specify wildcard filter values for key columns in the table. When any filters are set, the only rows presented should be those for which the value of each filtered column conforms to the specified filter. A value of * or null for any filter value should be treated equally, as an indication that no filtering should occur for the related data column. When all filter values are either * or null, the presented data should include all table rows, without any filtering.

When a user logs in and gets to a screen with tabular data for the first time, if the total number of data rows is less than or equal to the effective Rows/Page value (that is, the number of rows that can be accommodated on a single page), the screen is displayed showing all of the data rows as a single page, and with the leading filter section hidden (collapsed). However, if the total number of data rows is greater than the effective Rows/Page value, the initially displayed screen shows only an open filter section but without any data rows. The user must then enter and submit a filter selection, and then data rows are displayed according to the submitted filters.

The effective Rows/Page value is displayed and can be changed by the user on the left pane of the Home page. The maximum and default Rows/Page values are specified in the Global Parameters file by the Super Admin.

The filter section can be expanded/collapsed at any time by clicking the arrow on the top left of the section. The example below shows the filter section for the Servers table. The user can specify the filter criteria for System Type, Group, and starting characters of the Server name in the filter section and then click Go to filter the data in the table. Leaving the fields blank, lists all the available servers.

Sortable Columns in Tabular Data

The data on the key columns of the tabular screens on the following sections can be sorted by clicking the column header. A sortable column has an icon on its column heading, as shown in the following figure, where the Server Name and System Type columns are sortable.

Servers						
Show: Hide All Details | Show All Details						
						1-5 of 5
Show Details	**⇕ Server Name**	**⇕ System Type**	**Server Description**	**System ID**	**System Name**	**Groups**
▼ Show	MyLaptop	Windows				Group1
▼ Show	WinServer	Windows				Group2 ▲ Payroll Sales ▼
▼ Show	xcomdmpcc11	z/OS				Group1
▼ Show	xcomdmpcc31	z/OS				Group1 ▲ Group2 Payroll Sales ▼
▼ Show	XCOMLV	z/OS	Lee Server on CC31			Group1

The direction of the sort is indicated by the following icon.

⇕ Ascending

⇕ Descending

Home

The Home page is displayed when you log in to CA XCOM Management Center successfully. You can also return to the Home page at any time after log in by clicking the Home tab.

You can also go to the different tabs, and to the different functions of the Admin tab, by using the links on the left pane.

Rows/Page

This editable field indicates the number of rows per page displayed for tabular data on each screen.

When you enter a value here and click Select, this value is saved as a cookie and then used for all tabular screens of CA XCOM Management Center.

Range: The entered value must be numeric and less than the MAXPAGEROWS attribute value specified in the Global Parameters file. Otherwise, a warning message is issued and the value is set to the maximum.

If no value is saved in the cookie, the field is set to the DEFAULTPAGEROWS value specified in the Global Parameters file.

Schedule Transfer

The Schedule Transfer tab allows you to perform the following functions related to transfer records and configuration files:

- Build transfer records

- Submit transfer records for scheduling

- Save transfer records in a configuration file.

- Display, edit, delete, and submit configuration files.

- Export a configuration file.

- Download an exported configuration file.

- Import an exported configuration file.

- Upload a downloaded exported file.

Build Transfer Records

You can build transfer records using any of the following functions under the Schedule Transfer tab:

Quick Transfer button

You can build a single transfer record quickly by using the Quick Transfer function.

Edit link

You can build one or more transfer records at a time by using the Edit link.

Wizard link

You can build one or more transfer records at a time, in a step-by-step process, by using the Wizard link.

To display the main Schedule Transfer page

1. Log in to CA XCOM Management Center.

   The Home page appears.

2. Click Schedule Transfer.

   The main Schedule Transfer page appears.

Actions on the Main Schedule Transfer Page

The following action links are available for the transfer record table:

Add

Adds an empty transfer record to the transfer record table.

Delete

Deletes selected transfer records from the transfer record table.

Copy

Copies selected transfer records and adds them to the transfer record table.

Submit

Submits selected transfer records for scheduling.

Save

Saves selected transfer records in a configuration database as a configuration file.

Quick Transfer

To build a transfer record by using Quick Transfer

1. Click Schedule Transfer.

    The main Schedule Transfer page appears.

2. Click the Quick Transfer button.

3. The Quick Transfer page appears. It contains a set of collapsible sections.

4. Enter or select the transfer record parameters.

    Notes:

    ■   For a brief description of the parameters on this page, see the appendix "XML Formats."

    ■   You can either type in the information for the local and remote servers or use the Select buttons to select local and remote server information from the list of available servers.

    ■   You can also either type in the local and remote file names or use the Browse buttons to find and select the files from your local workstation.

5. Click the Submit button.

    Quick Transfer builds the transfer record, submits it for scheduling, and returns to the main Schedule Transfer page, displaying the built record in the transfer record table for further processing.

    A confirmation message is also displayed.

    Note: You can click the Cancel button to cancel the process and return to the previous page.

Edit Link

To build a transfer record using the Edit link

1. Click Schedule Transfer.

   The main Schedule Transfer page appears.

2. Click Add link.

   An empty transfer record is added to the table.

   The local server section is also displayed at the top of the page.

3. Either enter the information for the local server or click the Select button to select the local server from the list of available servers.

4. Click Edit link from the Actions drop-down for the empty transfer record.

   The Edit Transfer Record page appears. It contains a set of collapsible sections.

5. Enter or select the transfer record parameters.

   Notes:

   ■ For a brief description of the parameters on this page, see the appendix "XML Formats."

   ■ You can either type in the information for the local and remote servers or use the Select buttons to select local and remote server information from the list of available servers.

   ■ By using the Select button for the remote server, you can select more than one server from the list and build multiple transfer records.

   ■ You can also either type in the local and remote file names or use the Browse buttons to find and select the files from your local workstation.

6. Click the Update button.

7.   CA XCOM Management Center builds the transfer record and returns to the main Schedule Transfer page, displaying the built record in the transfer record table for further processing.

     Note: You can click Cancel to cancel the process and return to the previous page.

Wizard Link

To build a transfer record using the Wizard link

1. Click Schedule Transfer.

    The main Schedule Transfer page appears.

2. Click the Add link.

    An empty transfer record is added to the table.

    The local server section is also displayed at the top of the page.

3. Either enter the information for the local server or click the Select button to select the local server from the list of available servers.

4. Click the Wizard link from the Actions drop-down for the empty transfer record.

5. The Wizard starts.

To use the Wizard

1. On the Local Server Parameters page (Step 1) (with a set of collapsible sections), enter or select local server parameters.

    Click Next or the arrow for Step 2.

    The Select Remote Server page (Step 2) appears.

2. Use the Filter section to get the list of the servers with the desired system type, and select one or more servers from the list.

    Click Next or the arrow for Step 3.

    The Remote Server Parameters page (Step 3) appears. It contains a collapsible section.

3. Enter or select remote server parameters.

    Click Next or the arrow for step 4.

    The Select Options and XTC Parameters page (Step 4) appears. It contains a set of collapsible sections.

4. Enter or select the parameters.

5. Click Finish.

6. The Edit Transfer Record appears, with the entered parameters, on Wizard screens.

7. Review the entered parameters and continue with the steps defined previously in the Edit Link above.

Notes:

■   You can click Cancel on the Wizard screens to cancel the process and return to the main Schedule Transfer page.

■ You can click the Back button to go back to the previous Wizard screens when you are in Step 2 through Step 4.

■ For a brief description of parameters on the Wizard screens, see the appendix "XML Formats."

Submit Transfer Records for Scheduling

After building transfer records, you can submit them for scheduling and get the statistics of the scheduled records.

To submit transfer records

1. Click Schedule Transfer.

   The main Schedule Transfer page appears.

2. For the Quick Transfer function, click the Submit button after building the transfer record on the Quick Transfer screen (see Quick Transfer above).

3. For the Edit function, build the transfer record (see Edit Link above).

4. For the Wizard function, build the transfer record (see Wizard Link above).

5. Enter the information for the local server on the main transfer screen (if it has not been already entered).

6. Select the built transfer records from the Transfer Record table on the main Schedule Transfer screen.

7. Click Submit.

   The records are submitted and a confirmation message is displayed at the top.

   Note: If you want to submit all of the records in the table, you can click the SubmitAll button instead of performing Step 5 and Step 6.

8. Click the Refresh button to display the status of the transfer records in the status column of the submitted records in the table.

9. Click the Refresh action link for a submitted transfer record to get the record's status in the status column of the record.

   Note: The request number of the submitted transfer record is also returned in the status. If you click the Refresh button before the request number is returned from the CA XCOM Data Transport base server, then a "schedule in progress" message is displayed in the Schedule Status column and you must click the Refresh button or link again until the request number is returned from the server.

Save Transfer Records in a Configuration File

After building transfer records, you can save one or more transfer records as a configuration file in the Configuration database. The configuration files can then be:

- Loaded to display and edit transfer records

- Submitted for scheduling

- Exported to an XML file on the web server for later import

To save transfer records

1. Click Schedule Transfer.

   The main Schedule Transfer page appears.

2. Build the transfer records (see Build Transfer Records).

3. Enter the information for the local server on the main Schedule Transfer page (if it has not already been entered).

4. Select the built transfer records from the Transfer Record table on the main Schedule Transfer page.

5. Click Save.

   The Save Transfer Record(s) in Configuration File page appears.

Notes:

- If you want to save all the records in a configuration file, you can click the SaveAll button instead of performing Step 4 and Step 5.

- If you click the Cancel button on this page the save process is canceled and the main Schedule Transfer page appears.

6. From the drop-down menu, select *one* of the following:

   - The Group that you want the file to be saved under

- Private

Note: The Private configuration file is accessible only by the user who has saved the file. If configuration files are saved under a group name, they can be accessed by the users in that group if they have proper authority.

7. Enter the name for the saved configuration file.

8. Click the Save button.

   The configuration file is saved.

   Note: If the file already exists, a dialog opens to replace the file or cancel the process.

The following actions are also available on the Save Transfer Record(s) in Configuration File page.

- Select one or more configuration files listed in a table on this page and click the Delete link to delete them from the Configuration database.

  A dialog opens, allowing you to confirm or cancel the delete process.

- Use the Export link under the Actions column of a configuration file listed in a table to export the selected configuration file as an XML file on the web server.

  For more information, see Export a Configuration File in this chapter.

Display, Edit, Delete, or Submit a Configuration File

You can display and optionally edit the transfer records saved in a configuration file.

You can also delete one or more configuration files from the Configuration database or submit a configuration file for scheduling.

Display and Edit a Configuration File

To display and edit a configuration file

1. Click Schedule Transfer.

    The main Schedule Transfer page appears.

2. Click the Load button.

    The Save Configuration Files page appears.
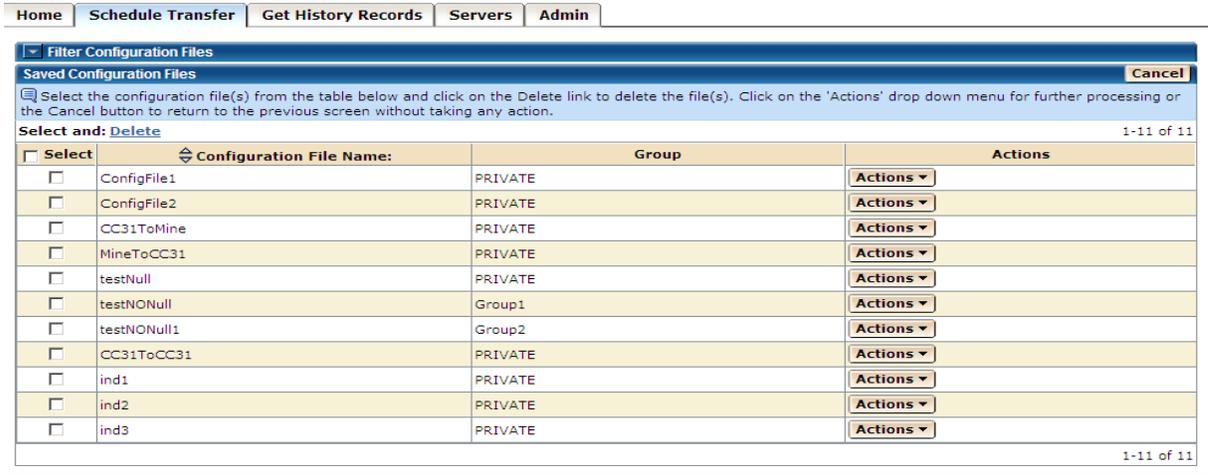
3. Click the Display action link from the Actions drop-down list for a listed configuration file.

    The transfer records for the selected configuration file are displayed in a table on the main Schedule Transfer page.

    Notes:

    ■   You can click the Display & Append action instead and the transfer records for the selected configuration file are appended to the transfer records already listed in the table, but the local server information on the screen remains unchanged.

    ■   If you click the Cancel button on this page, the process is canceled and the system returns to the previous page.

4. You can then edit and/or submit the transfer records as described earlier in this chapter. When you edit a transfer record using the Edit or Wizard action link, the local user password will be cleared if the local user ID is not the same as the ID of the logged in user,

Delete or Submit a Configuration File

To delete or submit a configuration file

1. Click Schedule Transfer.

   The main Schedule Transfer page appears.

2. Click Load button.

   The Save Configuration Files page appears.

| Home | Schedule Transfer | Get History Records | Servers | Admin |

Filter Configuration Files

Saved Configuration Files　　　　　　　　　　　　　　　　　　　　Cancel

Select the configuration file(s) from the table below and click on the Delete link to delete the file(s). Click on the 'Actions' drop down menu for further processing or the Cancel button to return to the previous screen without taking any action.

Select and: Delete　　　　　　　　　　　　　　　　　　　　　　1-11 of 11

☐ Select	⇕ Configuration File Name:	Group	Actions
☐	ConfigFile1	PRIVATE	Actions ▼
☐	ConfigFile2	PRIVATE	Actions ▼
☐	CC31ToMine	PRIVATE	Actions ▼
☐	MineToCC31	PRIVATE	Actions ▼
☐	testNull	PRIVATE	Actions ▼
☐	testNONull	Group1	Actions ▼
☐	testNONull1	Group2	Actions ▼
☐	CC31ToCC31	PRIVATE	Actions ▼
☐	ind1	PRIVATE	Actions ▼
☐	ind2	PRIVATE	Actions ▼
☐	ind3	PRIVATE	Actions ▼

1-11 of 11

3. To delete, select one or more configuration files listed in a table on this page and click the Delete link to delete them from the Configuration database.

   A dialog opens, allowing you to confirm or cancel the delete process.

4. To submit, click the Submit action from the Action drop-down list for a configuration file.

   The transfer records in the file are submitted for scheduling.

Note: If you click the Cancel button on this page, the process is canceled and the system returns to the previous page.

Export a Configuration File

You can export a configuration file as an XML file and save it in a directory on a web server. The transfer records in the exported XML file can then be imported for further processing, such as scheduling.

To export a configuration file

1. Click Schedule Transfer.

   The main Schedule Transfer page appears.

2. Click the Load button.

   The Save Configuration Files page appears.

3. Click the Export action link from the Actions drop-down list for a listed configuration file.

   A dialog opens and allows you to either keep or clear the local user password(s) in the exported configuration file.
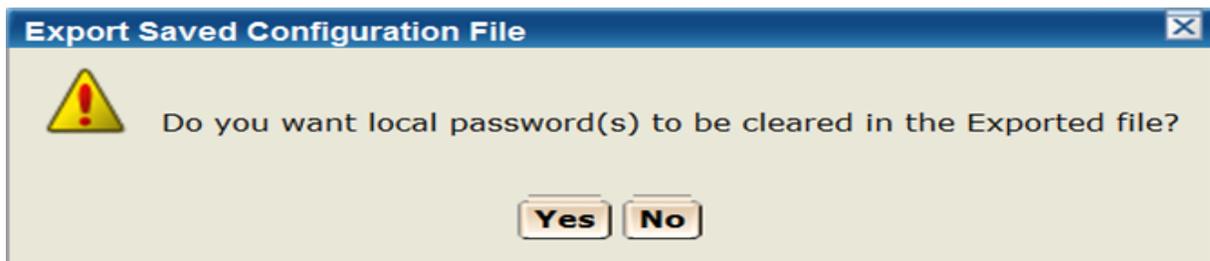
4. Click Yes to clear the password(s) or No to keep them in the exported file.

   The Export and Save Selected Configuration(s) in an XML File page appears.
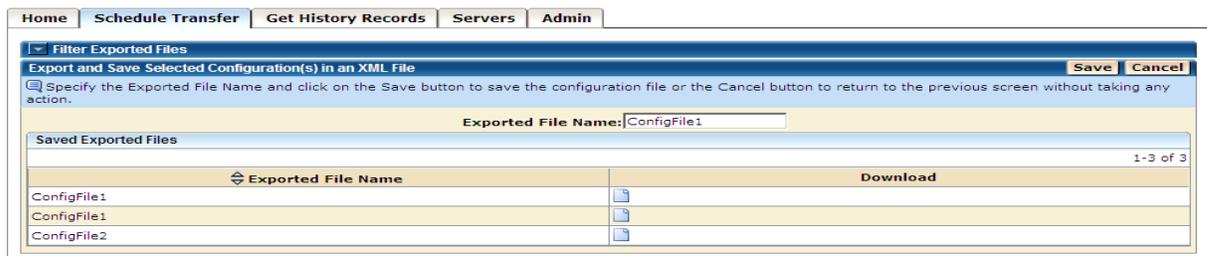
5. Enter the exported file name.

6. Click Save.

   The configuration file, with its transfer records, is saved in an XML file on the web server. The directory path for the exported files is specified in the Global Parameters file by the Super Admin.

Notes:

■ If the exported file name already exists on the web server, a dialog opens and allows you to append the information to the existing file, to replace the file, or to cancel the process.

■ Exported configuration files are stored in the following directory on the web server:

   xxxxx/*loginuserid*/ExportedConfigurations

   xxxxx

      The value of the HOMEDIRECTORY parameter of the EXPORT element in the Global Parameters file.

   loginuserid

      The ID of the logged in user (or the first 60 characters of the logged in user ID if the user ID length is more than 60 characters).

■ If you click the Cancel button on this page, the process is canceled and the system returns to the previous page.

Download an Exported Configuration File

You can download an already exported configuration file from the web server to your workstation. The file can then be uploaded to the web server for further processing.

To download an exported configuration file

1. Navigate to the Export and Save Selected Configuration(s) in an XML File page (see Export a Configuration File).

2. Use the listed exported files and click the icon under the Download column for an exported file.

    A dialog opens and gives you the option of opening, saving, or canceling the process.

3. Click the Save button.

    A dialog opens to select the path and the file name for the downloaded file on your workstation.

4. Select the path and file name and click Save button to save the file.

    Note: If you click Cancel, the process is canceled.

Import an Exported Configuration File

You can import an already exported configuration file from the web server and display its transfer records on the main Schedule Transfer page. The records can then be processed; for example, edited, saved, or submitted for scheduling, as described in the previous sections.

To import an exported configuration file

1. Click Schedule Transfer.

   The main schedule transfer page appears.

2. Click the Import button.

3. The Save Exported Files page appears.

4. Click the Import icon under the Import column for an exported file in the list.

   The transfer records saved in the selected exported file are listed on the main Schedule Transfer page.

   You can process the records as explained above in this section.

   Note: On this page, you may also select one or more records from the exported file list on this page and click Delete link to delete the files. A dialog opens to confirm the delete process or cancel the process.

Upload a Downloaded Exported File

You can upload a downloaded exported file from your local workstation and save it on the web server directory. The directory path for the exported files is specified in the Global Parameters file by the Super Admin.

To upload a downloaded exported file

1. Click Schedule Transfer.

   The main schedule transfer page appears.

2. Click Import button.

   The Save Exported Files page appears.
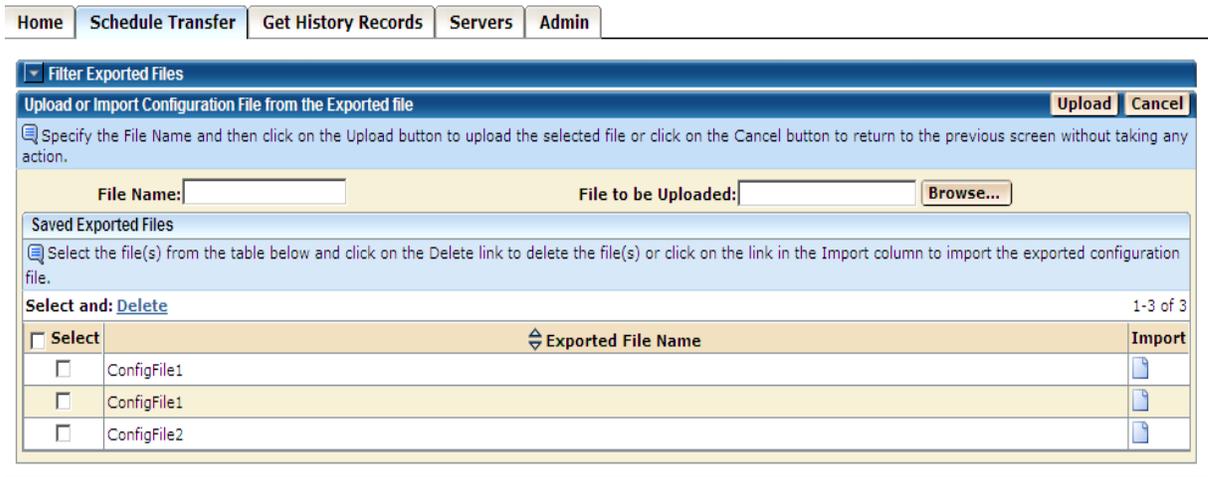
3. Enter the file name for the file to be uploaded.

4. Click the Browse button to find and select the downloaded file from your local workstation.

   A dialog opens to select the drectory and file name of the downloaded file.

5. Click the Upload button.

   The file is uploaded and saved on the web server as an export file for further processing.

   Notes:

   ■ If you click Cancel on this page, the upload process is canceled and the system returns to the previous page.

   ■ If the specified file name for the uploaded file already exists, a dialog opens to replace the file or cancel the process.

Get History Records

The Get History Records tab allows users to get the history record information for a server.

To get history records for a server, click the Get History Records tab.

This tab displays the servers available to you, with the following information:

The Servers page has two sections.

- A collapsible Filter section, where you can specify search criteria to limit the server information in the next section.

- Server information section, which consists of a table. Each row of the table represents information about a server available to you.

Notes:

- If the number of available servers to be listed in the table is more than the number of rows/page specified on the Home page, then the Filter section is the only section displayed when you first get to this tab. You can then enter the filter criteria and display the server information section.

- If the number of available servers is less than the rows/page value, then the filter section is shown collapsed, followed by the table of available servers. You can use the arrow on the left corner of each section to expand and collapse the collapsible sections.

Search Criteria for the Servers Page

The filter section consists of three fields:

System Type

A drop-down list showing the system types

Group

A drop-down list showing the groups assigned to you

Server Name

The input text box (case-sensitive) to enter the starting letters for the servers

After you enter or select the criteria and click the Go button of the filter section, the server list table shows the information for the servers that match the filter criteria.

Note: Selecting blank for any of the above fields removes that criterion from the search. For example, selecting blank for System Type means servers with any system type.

Information in the Available Servers Table

The server information in the table consists of the following:

- Server Name
- System Type
- Server Description
- System ID
- System Name
- Get Record Button

You can sort the entries in the Server Name and System Type columns by clicking the column heading.

Note: The Get Record button under Action column is available only for servers with a valid IP name. You cannot get history records for servers with no IP name.

To display the History Parameters Page, click the Get Record button for the local server that you want to get the history records from.

History Parameters Page

When you click the Get Record button for the local server that you want to get the history records from, the History Parameters Page appears.

Enter or select the parameters on the page to limit the number of records retrieved and returned.

History Parameters

This section describes the history parameters used to import servers from history or to get history records from a server.

Note: These history parameters are not case-sensitive. So filtering history records based on these parameters returns case-insensitive results. For example, specifying **USER01** as the Requesting User ID returns the same results as specifying **user01**.

Selected Server Information

The first line contains information about the server whose history record is to be searched.

If both SSL and non-SSL ports are specified for the server, you can check the **Use SSL** box on this line and the SSL port will be used to connect to the server; otherwise, the non-SSL port will be used.

Start Date and Time

Limits the history request to only those file transfers that were scheduled or completed on or after the start date and time.

End Date and Time

Limits the history request to only those file transfers that were scheduled or completed on or before the end date and time.

Completed, Inactive, and/or Active check box

Specifies if the history request should include inactive transfer requests, active transfer requests, and/or completed transfers.

Limit records to

Limits the records to those file transfers in the queue, in the database, or both.

Requesting User ID

Limits the history request to only those file transfers submitted by a specific user.

Requesting Number

Limits the history request to only those file transfers that contain this specific request number.

Transfer ID

Limits the history request to only those file transfers with a specific transfer ID. The transfer ID is a user-defined identifier for file transfer requests.

Local or Remote

Limits the history request to locally initiated transfers only, remotely initiated transfers only, or both.

File Type

Limits the history request to those transfers with the specified File Type (File, Job, or Report) or All file types.

Transfer Type

Limits the history request to only send transfers, only receive transfers, or both transfer types.

Remote System TCP/IP

Limits the history request by the remote system protocol.

History System ID

Limits the history request by the system ID.

History System Name

Limits the history request by the system name.

Remote System ID

Limits the history request to only those file transfers with a specific remote TCP/IP name or TCP/IP address.

Last Message

Limits the history request by the transfer's last message.

Maximum Entries

Limits the number of history records to be searched.

Minimum File Size

Limits the history request to only those file transfers where the number of bytes transferred is equal to or greater than the value specified.

This value can be a 1- to 10-digit number, where the last digit can be either another numeric digit or a 1-character qualifier, in the form *nnnnnnnnn*(*n*|*x*), where *x* can be one of the following qualifiers:

- B = Bytes

- K = Kilobytes

- M = Megabytes

- G = Gigabytes

- T = Terabytes

- P = Petabytes

- E = Exabytes

Maximum File Size

Limits the history request to only those file transfers where the number of bytes transferred is equal to or less than the value specified. This value can be a 1- to 10-digit number, where the last digit can be either another numeric digit or a 1-character qualifier, in the form *nnnnnnnnn*(*n*|*x*), where *x* can be one of the following qualifiers:

- B = Bytes

- K = Kilobytes

- M = Megabytes

- G = Gigabytes

- T = Terabytes

- P = Petabytes

- E = Exabytes

Display History Records

When you have entered or selected the required history parameters, you can display history records for the server.

To display short history records

1. Click Submit to build the HistoryFilter record and submit a request to get the history records.

   The list of brief (short) history records based on the entered history parameters is displayed on the same page, under the history parameters section.

   Notes:

   ■ If you click Cancel instead, the process is terminated and the previous screen is displayed.

   ■ The QUERYCOUNT parameter in the INTERFACESERVER entity of the Global Parameters file limits the maximum number of records returned in the table. If the actual number of records is more than the value specified in the QUERYCOUNT parameter, a warning message is issued at the top of the page.

| Home | Schedule Transfer | Get History Records | Servers | Admin |

History Parameters for xcomdmpcc31 Server Submit Cancel

Enter values for the history parameters and click on the Submit button. Cancel button returns to the previous screen with no action taken.

| Local Server Information: | IP Name: 123.123.12.31 | Port: 8059 | Use SSL: ☐ | SSL Port: 8069 |

Start Date and Time: Jul 28, 2010 12:00:00 AM   End Date and Time: Jul 28, 2010 11:59:59 PM

Completed: ☑   Inactive: ☐   Active: ☐

Limit records to: All

Requesting User ID: Request Number: Transfer ID:

Local or Remote: All   File Type: All   Transfer Type: All

Remote System TCP/IP: History System ID: History System Name:

Remote System ID: Last Message:

Maximum Entries: 0   Minimum File Size: Maximum File Size:

Short History Record Information

Click on the desired action under the Actions column for a history record or click on the link under Req. No. column to get detail history record.

Show: Hide All Details | Show All Details

1-11 of 11

Show Details	Req. No.	Transfer Type	Transfer ID	EPRTY	SPRTY	User ID	Where Started	Start Date	Start Time	Status	Location	Actions
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	0906	LOGICERROR	DATABASE	
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	0908	LOGICERROR	DATABASE	
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	0910	LOGICERROR	DATABASE	
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	0942	LOGICERROR	DATABASE	
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	0951	COMPLETE	DATABASE	
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	0952	LOGICERROR	DATABASE	
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	0957	LOGICERROR	DATABASE	
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	1345	LOGICERROR	DATABASE	
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	1402	COMPLETE	DATABASE	
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	1403	LOGICERROR	DATABASE	
Show	002000	SENDFILE	TESTB001	10	0	STMMI03	REMOTE	20100728	1403	COMPLETE	DATABASE	

2. To expand a row, click the Show icon in the Show Details column.

   Additional information for the corresponding server is displayed.

   The Show icon is changed to Hide. Click the icon again to hide the extra information.

3. To expand all rows, click the Show All Details link above the table.

   Additional information for all listed servers is displayed.

   The Show All Details link is changed to Hide All Details. Click the link again to hide the extra information.

4. To update the information in the table, click the Submit button.

   Note: The last column in the table is the Action column. Depending on the status of each record, the list of actions displayed may vary, or no actions may be listed. For more information, see Actions on History Records.

5. Click on the Request No. link for a short history record information in the table.

   The Detail History Record page appears in a new window, displaying the following sections:

   ■ General Information

   ■ Notification

   ■ Misc Information

   All fields on this page are display-only.

   Depending on the status of the record, a Refresh button may also be displayed on the top right of the window. Clicking on the Refresh button will refresh the information on the Detailed History Record screen.

Actions on History Records

The following actions are available for history records, depending on the status of each record:

Cancel

Cancels a queued or active transfer.

Hold

Holds a queued transfer.

Release

Releases a held transfer.

Suspend

Suspends an active transfer.

Resume

Resumes a suspended transfer.

Update

Changes execution priority, scheduling priority, or scheduled start date and time for a queued transfer.

When you click the Update action, a new window opens, with the current values for priorities and start date and time.

You can change the values and click the Update button to update the values, or click the Cancel button to cancel the process.
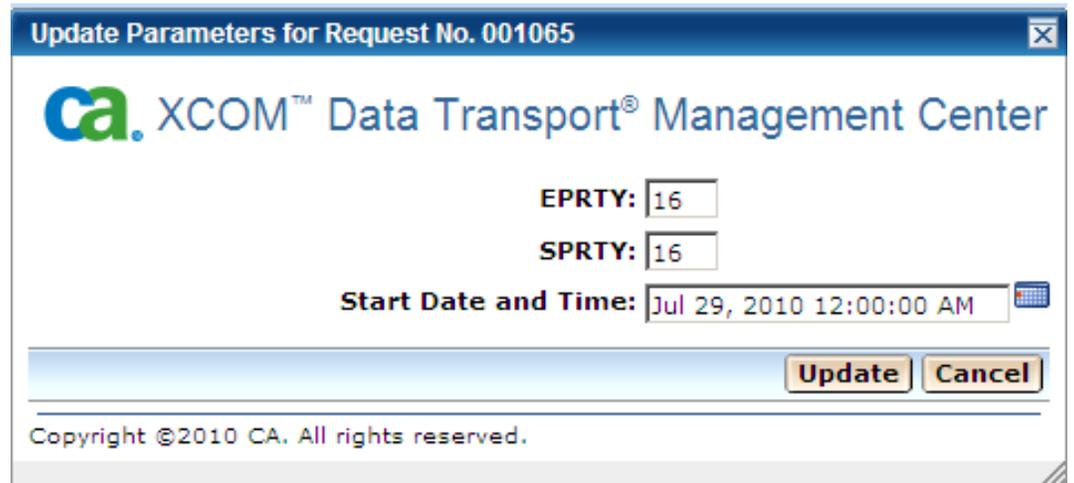
Delete

Removes a queued transfer from the queue.

Servers

The Servers page displays information about the available CA XCOM Data Transport servers for the logged in user. The page consists of two sections:

- A collapsible Filter section, where you can specify search criteria to limit the server information in the next section.

- Server information section, which consists of a table. Each row of the table represents information about a server available to you.

Notes:

- If the number of available servers to be listed in the table is more than the number of rows/page specified on the Home page, then the Filter section is the only section displayed when you first get to this tab. You can then enter the filter criteria and display the server information section.

- If the number of available servers is less than the rows/page value, then the filter section is shown collapsed, followed by the table of available servers. You can use the arrow on the left corner of each section to expand and collapse the collapsible sections.

| Home | Schedule Transfer | Get History Records | Servers | Admin |

Filter Servers

Enter a system type, a group, and/or the starting letters for the server name then click the Go button to filter the servers list in the table. Clear the system type, group, and the server name fields then click the Go button to list all the servers in all the groups.

System Type: [▼]   **Group:** [▼]   **Server Name:** [   ] [Go]

Servers

Show: Hide All Details | Show All Details

1-5 of 5

Show Details	⬍ Server Name	⬍ System Type	Server Description	System ID	System Name	Groups
▼ Show	MyLaptop	Windows				Group1
▼ Show	WinServer	Windows				Group2 Payroll Sales
▼ Show	xcomdmpcc11	z/OS				Group1
▼ Show	xcomdmpcc31	z/OS				Group1 Group2 Payroll Sales
▼ Show	XCOMLV	z/OS	Lee Server on CC31			Group1

Search Criteria for the Servers Page

The filter section consists of three fields:

System Type

A drop-down list showing the system types

Group

A drop-down list showing the groups assigned to you

Server Name

The input text box (case-sensitive) to enter the starting letters for the servers

After you enter or select the criteria and click the Go button of the filter section, the server list table shows the information for the servers that match the filter criteria.

Note: Selecting blank for any of the above fields removes that criterion from the search. For example, selecting blank for System Type means servers with any system type.

Information in the Available Servers Table

The server information in the table consists of the following:

- Server Name
- System Type
- Server Description
- System ID
- System Name
- Get Record Button

You can sort the entries in the Server Name and System Type columns by clicking the column heading.

Note: The Get Record button under Action column is available only for servers with a valid IP name. You cannot get history records for servers with no IP name.

To display the History Parameters Page, click the Get Record button for the local server that you want to get the history records from.

Global Parameters on the CA XCOM Management Center Website

Various types of global parameters are required by the CA XCOM Management Center server, as follows:

- CA EEM parameter

- Web Interface parameter

- JDBC (database) parameters

- Log and trace parameters

- General parameters

CA EEM Parameter

The CA Embedded Entitlements Manager (EEM) parameter sets the hostname for the EEM server to be used by CA XCOM Management Center.

EEM Server Host

The host name or IP address of the machine on which the CA EEM server is located.

Attribute Name: HOST

Default: localhost

Web Interface Parameter

The Web Interface parameter is used to set the URL for the CA XCOM Interface Server.

The attribute for the WEBSERVICES structure is as follows:

Web Interface URL

The URL for the Interface server.

Attribute Name: INTERFACEURL

Default: The same as the host name and port number for the CA XCOM Management Center server

JDBC Parameters

The JDBC parameters are used to define the database server information.

The attributes for the JDBC structure are as follows:

DataBase Creator

The database schema name for DB2 UDB.

Important! This parameter must not be coded for MySQL databases.

Attribute Name: DBCREATOR

Default: The same as User Name.

DataSource Name

The JDBC datasource to be used.

Attribute Name: DATASOURCE

Default: This is a required field and has no default.

User Name

The user ID to be used when connecting to the datasource.

Attribute Name: USER

Default: This is a required field and has no default.

PASSWORD

The password to be used when connecting to the datasource.

Attribute Name: PASSWORD

Default: This is a required field and has no default.

Log and Trace Parameters

We recommend using the trace file primarily for debugging. It is a text file and its location and name are specified in the Global Parameter XML structure in the TRACE structure.

Note: The trace records are free format.

The attributes for the LOG structure are as follows:

Log Path

The path for the log output file.

Attribute Name: PATH

Default: /tmp/CA_XCOM/

Log Level

The log message level.

I

Informational warnings and error messages

E

Error messages

W

Warning and error messages

Attribute Name: LEVEL

Default: I

Log Date Format

The log date format.

US

mm/dd/yyyy

European

yyyy/mm/dd

Attribute Name: DATEFORMAT

Default: *mm/dd/yyyy*

The attributes for the TRACE structure are as follows:

Trace Path

The path of the trace output file.

Attribute Name: PATH

Default: /tmp/CA_XCOM/

Trace Level

The trace level.

Range: 0 through 10, where 0 does not write any trace. As the trace level number increase, more detailed information is written to the trace file.

Attribute Name: LEVEL

Default: 0

General Parameters

The General parameters are the other parameters used in CA XCOM Management Center.

The attribute for the EXPORT structure is as follows:

Export Home Directory

Home directory path for the exported server and configuration files, as follows:

■ Exported server files are stored in the following directory:

xxxxx/*loginuserid*/ExportedServers

■ Exported configuration files are stored in the following directory:

xxxxx/*loginuserid*/ExportedConfigurations

xxxxx

The value of the Export Home Directory parameter.

loginuserid

The ID of the logged in user (or the first 60 characters of the logged in user ID if the user ID length is more than 60 characters).

Attribute Name: HOMEDIRECTORY

Default: /XCOMGUI/

The attribute for the USERNAME structure is as follows:

User Name caseInsensitive

Specifies the user name entered at login time is case-sensitive or not.

Attribute Name: CASEINSENSITIVE

Default: YES

The attributes for the MANAGEMENTCENTERSERVER structure are as follows:

Default Rows/Page

Default number of data rows that will be displayed on a single page of any GUI screen showing tabular data.

Attribute Name: DEFAULTPAGEROWS

Default: 20

Maximum Rows/Page

Maximum number of data rows that will be displayed on a single page of any GUI screen showing tabular data.

Attribute Name: MAXPAGEROWS

Default: 9999

Appendix A: CA XCOM Management Center Messages

This section contains the following topics:

Notational Conventions

Each message has a unique message ID. The message ID consists of the following:

- Product code (XCOMI)

- A unique number

- A severity code (suffixed to the message ID)

The severity code can have one of the following values:

- E—Indicates an error message

- I—Indicates an informational message

- W—Indicates a warning

List of Messages

The following pages list messages that CA XCOM Management Center can return in response to job requests, with reasons and recommended user actions, where appropriate. The messages are listed in numerical order.

XCOMI2001E

FileNotFoundException occurred during Global Parameters XML file processing.

Reason:

Exception occurred during processing of the Global Parameters XML file.

Action:

Check for the existence of the Global Parameters file.

XCOMI2003E

Exception occurred while saving Global Parameters file. Exception message: [*exception-message*].

Reason:

Exception occurred during processing of the Global Parameters XML file.

Action:

Check the *exception message* in the message text and correct the problem.

XCOMI2004E

Unable to get InitialContext. Exception message: [*exception-message*].

Reason:

An exception occurred either during the construction of an initial context for naming operation or during the retrieval of the context's environment.

Action:

Check the *exception-message* content in the message text for more information. Correct the problem and rerun the process.

XCOMI2005E

Problem accessing the Global Parameters File: [*exception-message*].

Reason:

Exception occurred while obtaining the Global Parameters XML file. Check the exception message in the message text.

Action:

Correct the problem and restart the application server.

XCOMI2006E

Error while parsing the file: [*exception-message*].

Reason:

Error occurred while parsing the Global Parameters XML file. Check the exception message in the message text. Check the Global Parameters file for valid attribute names and values.

Action:

If the attribute names and/or values are not valid, correct them and restart the application server.

XCOMI2008W

Parameter Name and/or Value Not Found for Parameter: [*parameter-name*].

Reason:

The parameter for *parameter-name* and/or its value cannot be found in the Global Parameters file.

Action:

Application assigns the default value to the parameter. Add the specified parameter and its value in the Global Parameter file if the default value is not the desired value.

XCOMI2010E

Problem writing to a log/trace file: [*file-name*]. Exception message: [*exception-message*].

Reason:

Exception occurred writing to a log or trace file. The file name is *file-name*.

Action:

Check the *exception-message* for more information about the cause of the problem. Verify that the *file-name* is a valid file.

XCOMI2011E

Directory cannot be created for directory: [*directory-name*]. Default log/trace directory will be used.

Reason:

There is a problem in creating the directory for log or trace file. The directory name is *directory-name*. The directory name is not a valid name.

Action:

The default directory and file name will be used for log or trace.

XCOMI2020E

Please Enter the Username.

Reason:

User name has not been entered on the login page.

Action:

Enter a valid user name and password on the login page and click the Log In button.

XCOMI2021E

Username cannot be more than 255 characters.

Reason:

The maximum length for the user name is 255 characters. The length of the entered user name is more than 255 characters.

Action:

Enter a valid user name, with length no more than the maximum, on the login page along with its password and click the Log In button.

XCOMI2022E

Please Enter the Password.

Reason:

Password has not been entered on the login page.

Action:

Enter a valid user name and password on the login page and click the Log In button.

XCOMI2024E

Authentication failed for User [*user-name*].

Reason:

User authentication failed for the *user-name* during login. The user name and/or password may not be valid. The trace file and log file have more information about the cause of the problem.

Action:

Click the MoreInfo button to see more information about the cause of the problem. Check the trace and log files for XCOMI2026E, XCOMI2028E, XCOMI2029E, or XCOMI2030E messages related to this failure. Correct the problem and try login again.

XCOMI2025I

Check the log and/or trace file for more information.

Reason:

More information about the problem can be found in the log and/or trace files.

Action:

None

XCOMI2026E

Exception occurred during authentication for User: [*user-name*]. Exception message: [*exception-message*].

Reason:

Exception has occurred in authentication of the user during login. The *exception-message* has more information about the cause of the problem.

Action:

Check the *exception-message* related to this exception in the message text. Correct the problem and try login again.

XCOMI2027E

The Sponsor Error related to the exception is: [error-message]

Reason:

User authentication through EEM Server failed.

Action:

This message is preceded by the XCOMI2026E message. Check the exception and error messages in both message texts. If the error message is "EEM Host name is not found", verify that the HOST attribute of the CAEEM structure in the global parameters file is valid. Correct the problem and repeat the process.

XCOMI2032I

Start of user authentication for User: [*user-name*].

Reason:

This is an informational message in the log file. It indicates the start of authentication for the user with the name *user-name*.

Action:

None

XCOMI2033I

User authentication succeeded for User: [*user-name*].

Reason:

This is an informational message. The indicated *user-name* authentication completed successfully.

Action:

None

XCOMI2035E

SQLException occurred while obtaining the database connection. Exception message: [*exception-message*].

Reason:

Connection to an internal database failed. The *exception-message* in the message text contains more information about the connection failure.

Action:

Check the *exception-message* in the message text and correct the problem.

XCOMI2036E

Connection object is null.

Reason:

Connection to an internal database failed. The message preceding this message contains more information about the connection failure.

Action:

Check the preceding messages in the log and/or trace file and correct the problem.

XCOMI2037E

Unable to find DataSource: [*data-source-name*].

Reason:

The connection manager routine tried to find the specified DataSource in the application, but was unsuccessful.

Action:

Check the XCOMI2041 messages in the log and trace files for the cause of the problem. Correct the problem and resubmit the process.

XCOMI2038I

Found DataSource: [*data-source-name*].

Reason:

This is an informational message. The indicated *data-source-name* was successfully found in the system.

Action:

None

XCOMI2039E

Exception occurred in ConnectionManager. Exception message: [*exception-message*].

Reason:

Connection to an internal database failed. The *exception-message* in the message text contains more information about the failure.

Action:

Check the exception-message in the message text and correct the problem.

XCOMI2040E

initCnt value is greater than or equal to *n*.

Reason:

The DataSource cannot be found after trying all the prefixes.

Action:

Make sure that the JDBC DataSource exists in the application server.

XCOMI2041W

DataSource not found. Exception message: [*exception-message*].

Reason:

This warning message is issued when the DataSource cannot be found in the system. The application tries other prefixes to find the DataSource.

Action:

Process continues with the next prefix. No action is required.

XCOMI2042E

Unable to get database connection from DataSource.

Reason:

The DataSource connection failed due to a critical error and an SQLException was raised.

Action:

Check the trace file to get the exception message and to find the cause of the problem. Correct the problem and resubmit the process.

XCOMI2043W

Warning: Less than 3 Super Administrators are defined in the system.

Reason:

This warning message is issued every time a user tries to log in to the application and the number of Super Administrators in the Users database is less than 3.

Action:

None

XCOMI2080E

Unable to access the database SQLException: [*exception-message*].

Reason:

A critical error has occurred accessing the internal database.

Action:

The *exception-message* gives the details of the cause of the error. Correct the error and resubmit.

XCOMI2081I

Selected User(s) deleted from the database.

Reason:

Selected user(s) deleted from the Users database successfully.

Action:

None

XCOMI2082E

Cannot delete logon userId from the database.

Reason:

You cannot delete your own user information from the Users database.

Action:

None.

XCOMI2083W

Selected user(s) deleted from the database, except logon userId. Cannot delete logon userId from the database.

Reason:

You cannot delete your own user information from the Users database. The other selected users' information has been deleted from the Users database successfully.

Action:

None

XCOMI2084W

No row selected. Select one or more rows from the table below.

Reason:

The process failed because no rows were selected from the list.

Action:

Select one or more rows from the list before activating the desired function.

XCOMI2085I

All the Users are already added to this Group.

Reason:

You have selected to add new users to a group, but all the existing users in the Users database have already been added to the group.

Action:

None

XCOMI2086I

Selected User(s) updated in the database.

Reason:

The information for the selected user(s) was updated in the Users database successfully.

Action:

None

XCOMI2087I

Selected Groups updated in the Groups database.

Reason:

The information for the selected group(s) was updated in the Groups database successfully.

Action:

None

XCOMI2088W

No Group selected. Select one or more Group(s) from the table below.

Reason:

The process failed because no groups were selected from the list.

Action:

Select one or more groups from the list before activating the desired function.

XCOMI2089I

Selected Group(s) deleted from the Groups database.

Reason:

Selected group(s) were deleted from the Groups database successfully.

Action:

None

XCOMI2090I

All the Servers are already added to this Group.

Reason:

You have selected to add new servers to a group, but all the existing servers in the Servers database have already been added to the group.

Action:

None

XCOMI2091I

Selected Server(s) deleted from the Servers database.

Reason:

Selected server(s) were deleted from the related groups and Servers database successfully.

Action:

None

XCOMI2092I

Selected Server(s) updated in the database.

Reason:

The update process for the selected server(s) completed successfully in the Servers database.

Action:

None

XCOMI2095E

Exception in closing connection. Exception message: [*exception-message*].

Reason:

An SQLException has occurred during closing a JDBC connection. The *exception-message* has more information about the problem.

Action:

Check the *exception-message*, correct the problem, and resubmit the function.

XCOMI2201I

User(s) information added to the Group: [*group-name*].

Reason:

Selected user(s) were added to the selected group as regular users.

Action:

None

XCOMI2202I

User information added to the Users database.

Reason:

Entered user names were added to the Users database.

Action:

None

XCOMI2203E

Invalid User name(s). The name is either a duplicate or blank.

Reason:

Either the user name(s) entered exists in the Users database or no user name was entered in the input text field.

Action:

Correct the name(s) and resubmit the function.

XCOMI2204W

User information added to the Users database except for the following Users. The name is either a duplicate or blank.

Reason:

Valid user names were added to the Users database, except for the listed users. The error may occur if either of the following conditions is true:

- The listed users already exist in the Users database

- The user name input field was blank.

Action:

Check whether the listed users already exist in the Users database or the user name entry field was blank. Correct the problem and resubmit the function.

XCOMI2206I

Group(s) information added to the Groups database.

Reason:

The add group function was completed successfully and the group(s) added to the Groups database.

Action:

None

XCOMI2207E

Invalid Group name(s). The name is either a duplicate or blank.

Reason:

Either the group name(s) entered exists in the Groups dtabase or no group name was entered in the input text field.

Action:

Correct the name(s) and resubmit the function.

XCOMI2208W

Group(s) information added to the Groups database except for the following group(s). The group name is either a duplicate or blank.

Reason:

Valid group names were added to the Groups database. The listed groups either already exist in the Groups database or no group name was entered in their respective input text fields.

Action:

Correct the problem and resubmit the function.

XCOMI2209I

Parameters updated in the Global Parameters file.

Reason:

The values in the Global Parameters file were updated successfully.

Action:

None

XCOMI2210I

Group Admin assignment/unassignment completed successfully.

Reason:

The Group Admin authority was assigned to /revoked from the specified users successfully.

Action:

None

XCOMI2211I

Server(s) information added to the group: [*group-name*].

Reason:

The selected server(s) were added to the *group-name* group successfully.

Action:

None

XCOMI2212I

Selected server(s) deleted from the group: [*group-name*].

Reason:

The selected server(s) were deleted from the *group-name* group successfully.

Action:

None

XCOMI2213I

Server(s) information added to the Servers database.

Reason:

The new servers information entered was added to the Servers database successfully.

Action:

None

XCOMI2214E

Invalid Server name(s). The name is either a duplicate or blank.

Reason:

The error occurred during addition of new server(s) by Super Admin. The cause of the error is either the entered server name already exists in the Servers database or no server name was entered in the input text field.

Action:

Correct the server name(s).Resubmit the request to add new server(s).

XCOMI2215W

Server(s) information added to the Servers database except for the following Server(s). The server name is either a duplicate or blank.

Reason:

Server information added to the Servers database. The remaining listed servers in the table have either the server name already exists in the Servers database or no server name is entered in their respective input text fields.

Action:

Correct the server name(s) and repeat the process to add a new server(s).

XCOMI2216W

Default rows/page parameter value is greater than the maximum rows/page value. Default is set to the maximum value of @@@@maximumrowvalue##:

Reason:

The specified value for the default rows/page parameter, DEFAULTPAGEROWS, is greater than the value of the maximum rows/page parameter, MAXPAGEROWS, in the Global Parameters file. The default rows/page parameter value is set to the maximum rows/page value.

Action:

Correct the values in the Global Parameters file.

XCOMI2217W

Number of rows exceeds maximum of @@@@maximumrowvalue##, defaulted to the maximum value of @@@@maximumrowvalue##:

Reason:

The number rows/page value specified on the home page by the user is greater than the maximum row/page value specified in the Global Parameters file.

Action:

None. The value is defaulted to the maximum value.

XCOMI2218W

No groups found in the Groups database, process terminated:

Reason:

There is no group in the Groups database. The process to the group(s) is terminated.

Action:

Add group(s) to the database before initiating the process.

XCOMI2300E

Processing failed for obtaining the attributes from the servers XML record.

Reason:

Processing to get the XML attributes for the selected server failed.

Action:

Check the log and trace files for more information and the cause of the failure. Correct the problem and re-run the process.

XCOMI2301E

Processing failed for obtaining the text content for an element in the servers XML record. The element name is: [*element-name*].

Reason:

The process for retrieving the server information for the specified XML element in the server record failed.

Action:

Check the log and trace files for more information and the cause of the failure. Correct the problem and re-run the process.

XCOMI2302E

Building the DOM object failed for the server XML record.

Reason:

Building of the Document Object Model for XML processing of a machineItem or machineContainer record failed.

Action:

Check the log and trace files for more information and the cause of the failure. Correct the problem and re-run the process.

XCOMI2303E

MachineContainer schema file name not found.

Reason:

The schema file cannot be located inside the deployed CA XCOM Management Center Web Application Archive (war) file.

Action:

Contact Technical Support.

XCOMI2304E

Building server XML record failed.

Reason:

The process failed.

Action:

Check the log and trace files for more information about the exception and the cause of the failure. Correct the problem and re-run the process.

XCOMI2305E

Processing attributes for the server XML record failed.

Reason:

Trying to get the attributes from a machineItem record failed.

Action:

Check the log and trace files for more information. Message XCOMI2300E precedes this message in the log file and has more information about the cause of the failure. Correct the problem and re-run the process.

XCOMI2306E

Problem with the Export Server Directory: [*export-directory*].

Reason:

The Server Export function failed due to a problem with the specified directory. The directory cannot be created or is write-protected.

Action:

Check your Global Parameters file for the correct export home directory for the export function. If the directory name is correct, make sure the export directory specified in the message exists and is not a read-only directory.

XCOMI2307E

Parsing the Exported Server File failed. Exception message: [*exception-message*].

Reason:

An exception has occurred during the process of XML parsing of a machineItem record.

Action:

The *exception-message* in the message text contains more information about the cause of the problem. Correct the problem and re-run the process.

XCOMI2308I

Exported server file processed successfully.

Reason:

The process of adding or appending server information to an export file as an XML record completed successfully.

Action:

None

XCOMI2309E

Problem writing into the server export file: [*export-filename*].

Reason:

An exception has occurred when writing into the server export file. The process failed.

Action:

Check the log and trace files for more information about the exception and the cause of the failure. Correct the problem and re-run the process.

XCOMI2310I

Exported server file(s) deleted successfully.

Reason:

Selected exported server file(s) deleted successfully for the file directory.

Action:

None

XCOMI2311E

Obtaining server item information from the Exported Server File failed.

Reason:

An exception has occurred while reading a machineItem record from the export XML file. The process failed.

Action:

Check the log and trace files for more information about the exception and the cause of the failure. Correct the problem and re-run the process.

XCOMI2312I

Upload to the exported server file completed successfully.

Reason:

The upload process of the exported server file from the local server to the server completed successfully.

Action:

None.

XCOMI2313E

Exception occurred while validating XML record.

Reason:

An exception has occurred during XML validation against a schema file. The process failed.

Action:

Check the log and trace files for more information about the XML record, the schema file, and the exception. Correct the problem and re-run the process.

XCOMI2314E

Exception occurred while downloading exported XML server file: [*download-filename*]. Exception message: [*exception-message*].

Reason:

An exception has occurred while downloading an exported server file to a file on the local server. The process failed.

Action:

Check that the specified file name in the message text is valid and that this is not a read-only file. Check the *exception-message* in the message text for more information about the exception. Correct the problem and re-run the download process.

XCOMI2315E

Parameter start date is later than end date.

Reason:

The history parameter start date and time cannot be later (more recent) than the history parameter end date.

Action:

Verify that the date and time entries are correct.

XCOMI2316E

Remote System ID length cannot be more than 8 for 'Remote SYSTEM TCP/IP=NO'.

Reason:

The Remote System TCP/IP value is selected as NO and the entered value for the Remote System ID has an invalid length (more than 8) in the History Parameters page section.

Action:

Either set the TCP/IP to YES or change the ID value to be less than or equal to eight.

XCOMI2317E

Minimum file size exceeds the allowable value of 2 to the power of 63 minus 1.

Reason:

The entered value for the minimum file size value is greater than the allowable value.

Action:

Enter a value less than the specified value.

XCOMI2318E

Maximum file size exceeds the allowable value of 2 to the power of 63 minus 1.

Reason:

The entered value for the maximum file size is greater than the allowable value.

Action:

Enter a value less than the specified value.

XCOMI2319E

Exception occurred while building the History Filter XML record.

Reason:

A critical error occurred while building the History Filter record. The process failed to complete.

Action:

Check the log and trace files for more information and the cause of the failure. Correct the problem and re-run the process.

XCOMI2320E

Problem with the Export Server Directory.

Reason:

This problem occurs when the user does not have write rights on the export home directory.

Action:

Verify that the user has rights on the export directory.

XCOMI2321E

Exception occurred while uploading file to the server. Exception message: [*exception-messag*e].

 Reason:

An exception has occurred while writing the uploaded file to the export directory on the server.

Action:

Check the *exception-message* in the error text. Possible causes are invalid file or directory name. Correct the error and resubmit the import function.

XCOMI2322E

Exception occurred while retrieving the HistoryContainer XML record from XCOM webService Interface. Exception message: [*exception-message*].

Reason:

Some communication-related error has happened while retrieving the HistoryContainer record. The process failed to complete.

Action:

Check the log and trace files for more information and the cause of the failure. Check the status of your CA XCOM Data Transport server. Correct the problem and re-run the process.

XCOMI2323E

JAXBException occurred while retrieving the HistoryContainer XML record from XCOM webService Interface. Exception message: [*exception-message*].

Reason:

Some XML processing-related error has happened retrieving the HistoryContainer record. The process failed to complete.

Action:

Check the *exception-message* and the log and trace files for more information and the cause of the failure. Correct the problem and re-run the process.

XCOMI2324E

Exception occurred while retrieving the HistoryContainer XML record from XCOM webService Interface. Exception message*: [*exception-message*].

Reason:

A critical error occurred while retrieving the HistoryContainer record. The process failed to complete.

Action:

Check the *exception-message* and the log and trace files for more information and the cause of the failure. Correct the problem and re-run the process.

XCOMI2325E

User is not authorized to get history record:

Reason:

The user specified in the history parameters is not authorized to get the history records.

Action:

Check the user ID in the Requesting User ID field of the history parameters and correct it. If the user ID is correct, the user is not authorized to get the history records.

XCOMI2326E

Specified maximum file size value is less than the minimum file size value.

Reason:

The maximum file size value specified on the history parameters screen is less than the minimum file size value.

Action:

Correct the file size values and resubmit the history parameters.

XCOMI2400I

Status changed successfully for the transfer record.

Reason:

The process of changing the status of the selected transfer record completed successfully.

Action:

None

XCOMI2401E

Change Status process failed for the transfer record.

Reason:

The process of changing the status of the selected transfer record failed.

Action:

Contact Technical Support.

XCOMI2402E

RemoteException occurred while changing transfer record status.

Reason:

Some communication-related error occurred during the transfer status change process. The status has not been changed.

Action:

Check the log and trace files for more information and the cause of the failure. Correct the problem and re-run the change transfer status process.

XCOMI2403E

JAXBException occurred while changing transfer record status.

Reason:

Some XML processing-related error occurred during the transfer status change process. The status has not been changed.

Action:

Check the log and trace file for more information and the cause of the failure. Correct the problem and re-run the change transfer status process.

XCOMI2404E

Exception occurred while changing transfer record status.

Reason:

A critical error occurred during the transfer status change process. The status has not been changed.

Action:

Check the log and trace files for more information and the cause of the failure. Correct the problem and re-run the change transfer status process.

XCOMI2405E

JAXBException occurred while building the History Filter XML record.

Reason:

Some XML processing-related error has happened while building the History Filter XML record. The process failed to complete.

Action:

Check the log and trace files for more information and the cause of the failure. Correct the problem and re-run the process.

XCOMI2406E

Exception occurred while building the History Filter XML record.

Reason:

A critical error occurred while building the History Filter XML record. The process failed to complete.

Action:

Check the log and trace files for more information and the cause of the failure. Correct the problem and re-run the process.

XCOMI2407I

No parameters updated. The parameters either are null or have not been changed.

Reason:

The process of updating parameter(s) for the selected transfer record did not succeed. The parameter values were not changed or the values were set to null.

Action:

Change the parameter values as needed and resubmit the update process.

XCOMI2408E

Update failed for parameter(s): *parameter-name*, *parameter-name*. Please check the log for more information.

Reason:

The process of updating parameter(s) for the selected transfer record failed. The failed parameter name(s) are specified in the message.

Action:

Check the log file for more information and the cause of the failure. Correct the problem and re-run the update process.

XCOMI2409I

Update succeeded for parameter(s): *parameter-name, parameter-name.*

Reason:

The process of updating parameter(s) for the selected transfer record completed successfully. The updated parameter(s) are specified in the message.

Action:

None

XCOMI2410W

Update succeeded for parameter(s): *parameter-name, parameter-name,* **but failed for** *parameter-name, parameter-name.* **Please check the log for more information.**

Reason:

The process of updating parameters for the selected transfer record partially completed. The names of the parameters updated and failed are specified in the message.

Action:

Check the log file for more information and the cause of the failure. Correct the problem and re-run the update process for the failed parameters.

XCOMI2411W

The list is not complete. Limit for displayed Short History Records exceeded.

Reason:

The number of listed short history records that can be displayed has reached the maximum limit specified in the Global Parameters XML file of the XCOM webService Interface. There are more records matching the specified History Parameters criteria that could not be displayed.

Action:

Check the count parameter in the XCOM webService Interface Global Parameters XML file. Increase the count value if you want more records to be listed.

XCOMI2500I

User data updated:

Reason:

The rows/page value is updated in the cookie.

Action:

None

XCOMI2501W

Number of rows exceeds maximum of @@@@maximumrowvalue##. Rows set to maximum:

Reason:

The rows/page value specified by the user exceeds the maximum rows/page value specified in the Global Parameters file. The value is set to the maximum.

Action:

If you need to set a larger value for the rows/page parameter, ask the super admin to increase the maximum rows/page parameter value in the Global Parameters file.

XCOMI2502W

Number of rows null or blank, defaulted to @@@@defaultrowvalue##:

Reason:

The rows/page value is either null or blank.

Action:

Specify a numeric value or it defaults to the default rows/page value specified in the Global Parameters file.

XCOMI3013I

Configuration information added to the Configurations database.

Reason:

The addition of configuration files completed successfully.

Action:

Verify that the records have been added to the configuration database.

XCOMI3063I

Upload to the Exported Configuration File completed successfully.

Reason:

The upload operation completed successfully.

Action:

Verify that the imported file is a valid configuration file.

XCOMI3064E

Obtaining configuration item information from the imported configurations failed.

Reason:

Problem obtaining the configuration information from the imported configuration file.

Action:

Verify that the imported file is a valid configuration file.

XCOMI3065E

Obtaining configuration item information from the exported file failed

Reason:

TransferContainer or the TransferItem could not be generated from the exported file because the exported XML is not properly formed.

Action:

Verify that the exported XML file is well formed and has all the required attributes and elements. Try exporting the file again.

XCOMI3066E

Building Transfer Container XML record failed.

Reason:

The XML generated cannot be validated against the XSD. There can be some elements missing in the generated XML or the XSD cannot be found in the export home directory.

Action:

Verify that the XSD exists in the export home directory and see if some value for some required element is missing in the generated XML.

XCOMI3067E

Invalid configuration name. The values are either duplicate or blank.

Reason:

Either the configuration name entered exists in the Configuration database or no configuration name was entered in the input text field.

Action:

Correct the name and resubmit the function.

XCOMI3068E

Building the DOM object failed for the Transfer Container XML record.

Reason:

The building up of the DOM (XML Document Object) object for the passed XML record could not be completed successfully.

Action:

Verify that the data passed for the building of the DOM object is correct.

XCOMI3069I

Selected configuration(s) deleted from the Configurations database

Reason:

The deletion of selected files completed successfully.

Action:

Verify that the records have been deleted from the Configurations database.

XCOMI3070E

Problem writing into the Configuration Export file.

Reason:

The file cannot be written with the configuration info.

Action:

Verify that the user has appropriate rights on the server where the file is being written.

XCOMI3073E

Exception occurred while downloading Exported XML Configurations file.

Reason:

The file cannot be properly downloaded to the user server.

Action:

Verify that the given file is valid and try refreshing the page to check if the file has not been deleted by another user. Check to ensure that the network is up and running.

XCOMI3074E

User has insufficient rights to delete the Configuration file(s)

Reason:

A user with insufficient rights should not be able to delete the configuration files.

Action:

If the user is supposed to have delete authority, verify and give sufficient authority to the user to be able to delete.

XCOMI3075E

Insufficient rights for the selected operation on the Configuration file.

Reason:

User does not have sufficient rights for the current operation.

Action:

Verify the rights of the logged in user and check whether the operation being performed falls under those rights.

XCOMI3076E

Local Server name either does not exist or does not belong to the user or does not match the defined attributes.

Reason:

The given server name in the configuration info does not exist or does not belong to the user.

Action:

Verify that the server name is correct and that the logged in user has rights on that server. Also, try selecting the server from the link instead of manually entering the name.

XCOMI3077I

Exported Configuration File processed successfully.

Reason:

The export of configuration files completed successfully.

Action:

Verify that the records have been exported successfully.

XCOMI3078E

Filename to be exported does not exist.

Reason:

The file to be exported does not exist.

Action:

Verify if the exported file exists.

XCOMI3079W

There cannot be more than eight dependencies for one Transfer Item.

Reason:

There are more than eight dependencies.

Action:

Verify that the number of dependencies does not exceed eight.

XCOMI3080E

Problem found in following entries:

Reason:

A problem occurred while updating a transfer record.

Action:

Verify that the entries present in the transfer record are valid.

XCOMI3081E

Problem with the Export Configuration Directory.

Reason:

This problem occurs when a user does not have write rights on the export home directory.

Action:

Verify that the user has rights on the export directory.

XCOMI3082I

Exported Configuration File(s) deleted successfully.

Reason:

The deletion of selected exported files completed successfully.

Action:

Verify that the records have been deleted from the exported files directory.

XCOMI3083E

The Transfer Records have not been submitted.

Reason:

A refresh action was performed before submitting the transfer records.

Action:

Ensure that the refresh does not occur before the transfer records are submitted.

XCOMI3084W

Transfer Record(s) found which have not been submitted and therefore have not been refreshed.

Reason:

A refresh action was performed for a blank transfer record before submission.

Action:

Ensure that the refresh does not occur before the transfer records are submitted.

XCOMI3085W

Following rows not submitted successfully due to some error:

Reason:

An invalid transfer record was submitted.

Action:

Verify that the submitted records are valid.

XCOMI3086W

Request for Submit Transfer not completed due to the error: [*ERROR_STRING*].

Reason:

The submit operation could not be completed successfully.

Action:

Verify that the web interface server is running and that the supplied credentials in XCOMParameters.xml for the Web Interface server are valid. Also check for the network connection between the CA XCOM Management Center server and the Web Interface server.

XCOMI3087I

Record(s) submitted successfully

Reason:

The submission of transfer records completed successfully.

Action:

Verify that the records have been submitted successfully.

XCOMI3088I

Record(s) refreshed successfully.

Reason:

The refreshing of transfer records completed successfully.

Action:

Verify that the records have been refreshed successfully.

XCOMI3089E

Request for refresh not completed due to the error: [*ERROR_STRING*].

Reason:

The refresh operation could not be completed successfully.

Action:

Verify that the web interface server is running and that the supplied credentials in XCOMParameters.xml for the Web Interface server are valid. Also check for the network connection between the CA XCOM Management Center server and the Web Interface server.

XCOMI3090E

Remote Server with name=[*SERVER_NAME*] does not exist or does not belong to the User for Transfer Item Record #: [*NUMBER*].

Reason:

The specified remote server name does not exist or that server does not belong to the user.

Action:

Verify that the server name is correct and that the logged in user has appropriate rights on that server. Also, try selecting the server from the link instead of manually entering the name.

XCOMI3091E

Remote Server with name=\"@@@@machinename##\" either does not exist or does not belong to the user or does not match the defined attributes in the selected Transfer Item Record.

Reason:

User tried to select a server that does not exist.

Action:

Check whether the selected server exists or not.

XCOMI3092W

No row selected. Select a row from the table below.

Reason:

User tried to perform an action without selecting any row from a table.

Action:

Verify that rows are selected before performing any operation.

XCOMI3093E

Problem in obtaining the details for the selected configuration.

Reason:

The transfer record or export file has no data.

Action:

Verify that the exported data is valid.

XCOMI3095E

Problem in saving the file. The length of file name exceeds the maximum limit of @@@@filelimit@@@@ characters.

Reason:

The length of the user-entered file name, including file path and extension, exceeds 255 characters.

Action:

The file name, including file path and extension, should not exceed the maximum length of 255 characters.

XCOMI3096E

Problem in executing the database query.

Reason:

A critical error has occurred while accessing the internal database.

Action:

Check for the SQLException message in the log and trace files to get the details of the cause of this error. Correct the error and resubmit.

XCOMI3097E

Exception occurred while getting the XTRACE value. Exception message: [*exception-message*].

Reason:

XTRACE is not included in the XML.

Action:

Contact Technical Support.

XCOMI3098E

Schedule in progress.

Reason:

The Refresh button/link has been clicked for one or more submitted transfer records and the response has not yet been received from the CA XCOM Data Transport base server.

Action:

Click the Refresh button/link again to get the status of the transfer records submitted for scheduling.

Appendix B: XML Formats

CA XCOM Management Center saves the information for configuration files, servers, and global parameters in XML format. The structures for these XML files are shown in this appendix.

This section contains the following topics:

Server Information Structure

The XML record for the server information is called the machineContainer record. A machineContainer record consists of one or more machineItem records. The attributes of the machineContainer and the machineItem record are listed in the following sections.

The machineContainer XML Record

The attributes for the machineContainer record are as follows:

<machineContainer>

Specifies the opening tag for a machineContainer record.

name

(Required) Specifies the user-provided name for the list of servers.

Limits: 0 to 12 characters

Default: None

<description>

Specifies the opening tag for the description.

xx...xx

Specifies the user-provided description for the machineContainer record.

Limits: 0 to 32 characters

Default: Null.

</description>

Specifies the closing tag for description.

<machineItem>

Specifies the opening tag for the machineItem record. There will be one machineItem record for each server. The attributes for this record is listed later in this section.

</machineItem>

Specifies the closing tag for a machineItem record.

</machineContainer>

Specifies the closing tag for a machineContainer record.

The machineItem XML Record

The attributes for the machineItem record are as follows:

<machineItem>

Specifies the opening tag for a machineItem record.

domain

The Windows server domain name.

Range: 0 to 15 characters

Default: Null

ipaddress

Specifies the IPname or IPaddress of the server.

Range: 0 to 63 characters

Default: Null

luname

Specifies the LU name on a SNA network.

Range: 0 to 8 characters

Default: Null

machineType

Indicates the type of server. Valid values are as follows:

- AS400
- DEC
- PC
- STRATUS
- TANDEM
- UNIX
- WINDOWSNT
- VM
- ZOS
- ZVM
- ZVSE
- OTHER

Default: None

name

Specifies the user-provided name for the server.

Range: 0 to 12 characters

Default: Null

SystemID

Specifies the unique system identifier for the system.

Range: 0 to 4 characters

Default: Null

SystemName

Specifies the unique system name.

Range: 1 to 8 characters

Default: Null

port

Indicates the specified server port number.

Range: 0 to 65535 characters

Default: Null

sslPort

Specifies the TCP/IP port number that accepts SSL connection requests.

Range: 0 to 65535 characters

Default: Null

<description>

Specifies the opening tag for the description.

xx...xx

Specifies the user-provided description for the server.

Range: 0 to 32 characters

Default: Null

</description>

Specifies the closing tag for description.

</machineItem>

Specifies the closing tag for a machineItem record.

Configuration File Structure

The XML record for the configuration file information is called the TRANSFERCONTAINER record. A TRANSFERCONTAINER record consists of one or more TRANSFERITEM records. The attributes of the TRANSFERCONTAINER record and the TRANSFERITEM record are listed in the following sections.

The TRANSFERCONTAINER XML Record

The attributes for the machineContainer record are as follows:

<TRANSFERCONTAINER>

Specifies the opening tag for a TRANSFERCONTAINER record.

NAME

(Required) Specifies the user-provided name for a configuration file.

Range: 0 to 12 characters

Default: None

<DESCRIPTION>

Specifies the opening tag for the description.

xx...xx

Specifies the user-provided description for the TRANSFERCONTAINER record.

Range: 0 to 32 characters

Default: Null

</ DESCRIPTION>

Specifies the closing tag for description.

<LOCAL>

Specifies the opening tag for the local server.

CPUTYPE

Indicates the type of local server. Valid values are as follows:

- AS400
- DEC
- PC
- STRATUS
- TANDEM
- UNIX
- WINDOWSNT
- VM
- ZOS
- ZVM
- ZVSE
- OTHER

Default: Null

IPADDRESS

Specifies the required IPname or IPaddress of the local server.

Range: 0 to 63 characters

Default: None

MACHINENAME

Indicates the user's name for the local server.

Default: None

PORT

Indicates the specified local server port number.

Range: 0 to 65535 characters

Default: 8044

SSL

Indicates whether the Interface Server should use secure connection to the local server.

Range: YES | NO

Default: NO

</LOCAL>

Specifies the closing tag for local server.

<TRANSFERITEM>

Specifies the opening tag for the TRANSFERITEM record. There is one TRANSFERITEM record for each transfer record in the configuration file.

For the attributes of,this record, see The TRANSFERITEM XML Record following.

</TRANSFERITEM>

Specifies the closing tag for a TRANSFERITEM record.

</TRANSFERCONTAINER>

Specifies the closing tag for a TRANSFERCONTAINER record.

The TRANSFERITEM XML Record

The TRANSFERITEM XML record is built when you build a transfer record through the different functions of the Schedule Transfer tab in CA XCOM Management Center, such as the Edit and Wizard actions.

The following is a sample TRANSFERITEM XML record:

```
<TRANSFERITEM
    CARRIAGEFLAG="NO"
    ENCODING="EBCDIC"
    NAME=""
    START="10172100044"
    >
    <LOCAL>
        <FILE
            NAME="FILETEST1"
            >
            <DCB />
            <ENCRYPTION
                CIPHER="NONE"
                HASH="NONE"
                />
        </FILE>
        <LOGON USER="amame02" />
    </LOCAL>
    <REMOTE
        CPUTYPE="ZOS"
        IPADDRESS="10.22.30.458"
        MACHINENAME="xcomdmpca11"
        PORT="8056"
        >
        <FILE
            NAME="FILETEST2"
            >
            <DCB />
            <ENCRYPTION
                CIPHER="NONE"
                HASH="NONE" />
        </FILE>
        <LOGON
            KEY="66C98D72"

            PASSWORD="CF2FF9CDC0289F796BECAF987ADCA4846DCEB0948CDDA08978D0929588EFA1"
                USER="amame02"
                />
    </REMOTE>
    <XTC>
        <DEPENDENT
```

```
                              ACTION="DECREMENT"
                              COND="SUCCESS"
                              JOB=""
                              />
                    </XTC>
          </TRANSFERITEM>
```

Transfer Record Parameters

The parameters in the following sections are the parameters used on the Edit Transfer Record and Quick Transfer screens of the Schedule Transfer tab in CA XCOM Management Center. Similar parameters are used in the Wizard screens. The parameters correspond to the attributes in the TRANSFERITEM XML record.

Local System Parameters

This section describes the parameters shown on the Local System Parameters section of the Edit Transfer Record or Quick Transfer Record page.

Credentials
User

Defines the user name for the local server whose session is to be used for the transfer. The initial character must be alphabetic.

Password

Defines the password associated with the user name whose session is to be used for the transfer.

Domain

The Windows domain name for use in authenticating the user ID and password.

Range: 1 to 15

Default: None

Note: The local domain field in Quick Transfer Record, Edit Transfer Record, and Wizard pages is handled as follows:

- When the Quick Transfer button is clicked on the main Schedule Transfer page, the local domain field in the credential section is updated with the selected local server domain value if both of the following apply:

  - The local domain field is blank.

  - The CPU type is Windows.

- When the Edit or Wizard action link is clicked on the main Schedule Transfer page, one of the following happens:

  For a new (empty) record:

  The local domain field in the credentials section is updated with the selected local server domain value from the main Schedule Transfer page if the CPU type is Windows.

  If no local server is selected, then the local domain field is not updated and it remains blank.

  Note: The record is considered new (empty) if either the Quick Transfer button is clicked or it is just created by using the Add link on the main Schedule Transfer page.

  For an existing record:

  The local domain field in the credentials section remains unchanged no matter what is selected as the local server.

  Note: The record is considered existing (not empty) if the user has already entered values for the parameters and clicked on either the Update button on the Edit Transfer Record page or the Submit button on the Quick Transfer page.

File Name

Specifies the local path and the name of the file.

File Access Section

User

The name of the user accessing local files. Used for locally initiated transfers only.

Range: 0 to 20

Default: None

Password

The password for access to local files. Used for locally initiated transfers only.

Range: 0 to 14

Default: None

Unit Name

The unit where the file resides.

Range: 0 to 10

Default: None

Unit Count

The number of units for a tape data set.

Range: 1 to 59

Default: 1

Volume Count

The maximum number of volumes for a tape data set.

Range: 1 to 255

Default: 1

Volume Sequence

The sequence number of the first volume of a multivolume tape data set.

Range: 1 to 255

Default: 1

Volume Serial

The volume serial number where the file resides.

Range: 0 to 6

Default: None

SMS Section

DATACLAS

Specifies the name of the data class for the SMS-managed file.

Range: 1 to 8

Default: None

MGMTCLAS

Specifies the name of the management class for the SMS-managed file.

Range: 1 to 8

Default: None

STORCLAS

Specifies the name of the storage class for the local SMS-managed file.

Range: 1 to 8

Default: None

DSNTYPE

The data set definition for the SMS-managed file.

LIBRARY

Defines a PDSE.

PDS

Defines a partitioned data set.

GATEWAYGUID

Defines the unique instance (GUID) for a file that resides in CA XCOM Gateway.

Range: 0 to 36

Default: Null

DCB Section

RECFM

Defines the record format of the local data set.

F

Fixed unblocked.

FA

Fixed unblocked ANSI. Contains ISO/ANSI/FIPS control characters.

FB

Fixed blocked with multiple records per block.

FBA

Fixed blocked ANSI with multiple records per block. Contains ISO/ANSI/FIPS control characters.

FBM

Fixed blocked machine with multiple records per block. Contains machine code control characters.

FBS

Fixed blocked spanned. Multiple records per block written as standard blocks.

FM

Fixed unblocked machine. Contains machine code control characters.

V

Variable unblocked.

VA

Variable unblocked ANSI. Contains ISO/ANSI/FIPS control characters.

VBA

Variable blocked ANSI with multiple records per block. Contains ISO/ANSI/FIPS control characters.

VBM

Variable blocked machine with multiple records per block. Contains machine code control characters.

VBS

Variable blocked spanned. Multiple records per block where the records can span more than one block.

VM

Variable unblocked machine. Contains machine code control characters

VS

Variable unblocked spanned. A record can span more than one block.

U

Undefined.

Default: Null

LRECL

Specifies the actual or maximum length, in bytes, of a logical record.

Range: 0 to 32767

Default: 160

BLKSIZE

Specifies the block size of the data set.

Space DIRBLK

Specifies the number of directory blocks for the data set.

Range: 0 to 99999

Default: 0

Space Primary

Identifies primary storage allocation for the data set.

Range: 0 to 99999

Default: 1

Space RLSE

Specifies whether the unused space for the data set is to be released.

Default: No

Space Secondary

Identifies secondary storage allocation for the data set.

Range: 0 to 99999

Default: 1

Space Unit

Indicates the unit of storage allocation for the data set.

TRK

Tracks

CYL

Cylinders

BLK

Blocks

Default: None

Tape

Specifies whether the data set resides on the tape.

Default: No

DEN

Specifies the density for the tape data set.

Range: 1 to 4

Default: None

Label EXPDT

Specifies the expiration date for the tape data set, in the form *yyddd* or *yyyy/ddd*.

Default: None

Note: Label RETPD and Label EXPDT are mutually exclusive.

Label RETPD

Specifies the retention period for the tape data set, in number of days.

Range: 1 to 9999

Default: No

Note: Label RETPD and Label EXPDT are mutually exclusive.

Label Sequence

Specifies the sequence number of the data set on the tape.

Range: 1 to 9999

Default: 1

Label Type

Specifies the type of label associated with the tape data set. The label type can be AL, AUL, BLP, LTM, NL, NSL, SL, or SUL.

Default: SL

FILEDATA

Indicates how a local USS file is to be allocated:

- Binary
- Text

Default: None

UMASK

Sets the permissions assigned to a file when the file is being created and received on the system for the first time. The value is expressed as an octal number (base 8). The octal number has the same meaning as in the standard UNIX umask command.

Range: 000 to 777

Default: 666 (rw-rw-rw) for files and 777(rwxrwxrwx) for directories

Notify Section

Level

Specifies the local notification level for transfers initiated from the local server.

All

Notifies after transfer completion.

Warn

Notifies only when the transfer received a warning or an error.

Error

Notifies only when the transfer received an error.

Default: ALL

Method

Specifies the method for notifying the transfer completion:

LOG

Causes the CA XCOM Data Transport transfer log to be written.

TSO

Identifies the TSO user who is sent a broadcast message when the file transfer completes.

CICS

Causes CA XCOM Data Transport to begin an LU 6.2 process to CICS when the file transfer concludes.

LU

Defines the local system's LU name and associated VTAM logical unit name.

ROSCOE

Sends notification messages to users of the CA Roscoe timesharing product when a file transfer begins, ends, or fails.

ALL

A notification message is displayed on the local Windows system console.

MAIL

Sends a mail notification message to the local user.

WRITE

A notification message is displayed on the screen.

NONE

No notification is sent.

Default: None

User

The user on the local system who is to be notified when the transfer is complete.

Range: 0 to 12

Default: None

SNA Section

LUNAME

The local system's LU name.

Range: 0 to 17

Default: None

Modename

The mode name.

Range: 0 to 8

Default: None

XNODESPEC

The node specification for the SNA Gateway node.

Range: 0 to 64

Default: None

Encryption At Rest Section

Cipher

Specifies the encryption algorithm used for encrypting data on the local server.

Cipher Key

Specifies the key used to encrypt or decrypt data.

Hash

Specifies the hash algorithm to calculate the digest on the local server.

Digest

Specifies a hash-value that determines the integrity of the data.

Options Parameters

This section describes the parameters shown in the Options section of the Edit Transfer Record or Quick Transfer Record page.

File Options

Create

CA XCOM Management Center attempts to create (allocate) a new file on the remote system.

Append

CA XCOM Management Center adds the records being transferred to the end of an existing file on the remote system.

For an indexed file, the keys must not match those in the file on the remote system or CA XCOM Data Transport terminates the transfer with an error.

Replace

CA XCOM Management Center replaces the contents of a file on the remote system with the data being transferred.

If the file is indexed, the records with matching keys are replaced and those with non matching keys are added.

Notes:

- When transferring a partitioned data set, specify Create only if the PDS itself is being created. If a new member is being sent to an existing PDS, specify Replace.

- If you do not override the default value and the file already exists on the target system, the transfer terminates with an error.

Default: Create

Encoding

Specifies the format of the data being transferred. The system from which the data is retrieved is responsible for performing any necessary conversion.

BINARY

Indicates binary data.

EBCDIC

Indicates that the data is in EBCDIC code.

ASCII

Indicates that the data is in ASCII code.

Default: EBCDIC

Codetable

Specifies the translation table to be used by the remote partner for data conversion. This is indicated by a one- to three-character prefix to the file names, atoe.tab and etoa.tab, that contain the external ASCII-to-EBCDIC and EBCDIC-to-ASCII custom character conversion tables on the CA XCOM Data Transport for Windows and the CA XCOM Data Transport for UNIX platforms.

Range: 1 to 3 alphanumeric characters.

Default: None

Truncate

Specifies how records exceeding the maximum logical record length (LRECL) are to be handled.

Yes

Specifies that records larger than the maximum LRECL are to be truncated to the maximum record length.

No

Specifies that CA XCOM Data Transport is to terminate the file transfer upon receiving a record larger than the maximum LRECL.

Default: No

Notes:

■ This field is supported only by the CA XCOM Data Transport mainframe products: CA XCOM Data Transport for z/OS, CA XCOM Data Transport for z/VSE, and CA XCOM Data Transport for z/VM.

■ When a record is truncated, the data not within the LRECL limit is lost.

Remove Trailing Blanks

Indicates whether the blank spaces at the end of the transfer records are removed:

■ No

■ Yes

Default: No

Compress

Specifies whether CA XCOM Data Transport compresses the data being transferred and decompresses it on the remote system. Compressing the data decreases the transmission time on lower speed lines.

YES

Provides Run Length Encoding (RLE) for blanks and binary zeros only.

NO

No data compression.

RLE

Provides complete Run Length Encoding for all characters.

COMPACT

Provides full RLE (as in RLE above) plus a byte compaction scheme that is suitable for uppercase English text.

COMPACTL

Same as COMPACT above, only the compaction scheme is most beneficial for lowercase English text.

LZSMALL

Lempel Ziv 77 compression with a small memory allocation scheme.

LZMEDIUM

Lempel Ziv 77 compression with a medium memory allocation scheme.

LZLARGE

Lempel Ziv 77 compression with a large memory allocation scheme.

LZRW3

General purpose algorithm that runs fast and gives reasonable compression.

ZLIB(*n*)

Greater compression than LZRW3 but less than LZSMALL, LZMEDIUM, and LZLARGE. The *n* value can be 0 through 3.

Note: Not all compression modes are supported on all platforms.

Default: YES

Checkpoint Count

Specifies the interval at which CA XCOM Data Transport takes a checkpoint (to be used to restart a suspended or failed file transfer). The length of the checkpoint interval is measured in terms of a number of blocks.

0

Specifies that CA XCOM Data Transport is to take no checkpoints.

1 to 9999

Specifies the number of blocks that form a checkpoint interval. A checkpoint is taken whenever the specified number of blocks has been transferred.

Note: If record packing is not used, 1 record = 1 block.

Each time a checkpoint is taken, the output buffers on the receiving system are written to the disk. Making the checkpoint interval too short slows down file transfers; making it too long increases the risk of data loss. It is recommended that the Checkpoint Count be set to at least 1000. On Token Ring, Ethernet and other high-speed networks, the Checkpoint Count should be set to the highest allowable value.

If the receiving system is z/OS or z/VSE, the Checkpoint Count should be a multiple of the blocking factor. For example, if the DCB attributes are RECFM=FB LRECL=80 BLKSIZE=8000, the Checkpoint Count should be a multiple of 100.

Number of Retries

Specifies the number of times a failed attempt to contact the local CA XCOM Data Transport server should be retried.

Default: 1

Retry Interval

Specifies the period of time (in seconds) after which a failed attempt to contact the local CA XCOM Data Transport server should be retried. If this parameter is omitted, a system default value of 1second is used.

Transfer Comment

Transfer description.

Max Record Length

Specifies the maximum logical record length for the transfer records.

Default: 1024

Remote System Identification and Parameters

This section describes the parameters shown on the Remote System Identification and Parameters pane of the Edit Transfer Record or Quick Transfer Record page.

Credentials (Remote)

User ID

Specifies the user ID under whose set of resource access privileges the transfer is to execute on the remote system.

Password

Identifies the password associated with the remote user ID.

Domain

The Windows domain name for use in authenticating the user ID and password.

Range: 1 to 15.

Default: None

Note: The remote domain field in Quick Transfer Record, Edit Transfer Record, and Wizard pages is handled as follows:

- When the Quick Transfer button is clicked on the main Schedule Transfer page, the remote domain field in the credential section is updated with the selected remote server domain value if both of the following apply:

  - The remote domain field is blank.

  - The CPU type is Windows.

- When the Edit or Wizard action link is clicked on the main Schedule Transfer page, one of the following happens:

  For a new (empty) record:

  The remote domain field in the credentials section is updated with the selected remote server domain value from the main Schedule Transfer page if the CPU type is Windows.

  If no remote server is selected, then the local domain field is not updated and it remains blank.

  Note: The record is considered new (empty) if either the Quick Transfer button is clicked or it is just created by using the Add link on the main Schedule Transfer page.

  For an existing record:

  The remote domain field in the credentials section remains unchanged no matter what is selected as the remote server.

  Note: The record is considered existing (not empty) if the user has already entered values for the parameters and clicked on either the Update button on the Edit Transfer Record page or the Submit button on the Quick Transfer page.

Trusted

Allows the user to request a trusted transfer.

Default: No

File Name

The path and name of the remote file.

Unit Name

The unit where the remote file resides.

Range: 0 to 10

Default: None

Unit Count

The number of units for a tape data set.

Range: 1 to 59

Default: 1

Volume Count

The maximum number of volumes for a tape data set.

Range: 1 to 255

Default: 1

Volume Sequence

The sequence number of the first volume of a multivolume tape data set.

Range: 1 to 255

Default: 1

Volume Serial

The volume serial number where the remote file resides.

Range: 0 to 6

Default: None

SMS Section

DATACLAS

Specifies the name of the data class for the remote SMS-managed file.

Range: 1 to 8

Default: None

MGMTCLAS

Specifies the name of the management class for the remote SMS-managed file.

Range: 1 to 8

Default: None

STORCLAS

Specifies the name of the storage class for the remote SMS-managed file.

Range: 1 to 8

Default: None

DSNTYPE

The data set definition for the remote SMS-managed file.

LIBRARY

Defines a PDSE.

PDS

Defines a partitioned data set.

GATEWAYGUID

Defines the unique instance (GUID) for a remote file that resides in CA XCOM Gateway.

Range: 0 to 36

Default: Null

DCB Section

RECFM

Defines the record format of the remote data set.

F

Fixed unblocked.

FA

Fixed unblocked ANSI. Contains ISO/ANSI/FIPS control characters.

FB

Fixed blocked with multiple records per block.

FBA

Fixed blocked ANSI with multiple records per block. Contains ISO/ANSI/FIPS control characters.

FBM

Fixed blocked machine with multiple records per block. Contains machine code control characters.

FBS

Fixed blocked spanned. Multiple records per block written as standard blocks.

FM

Fixed unblocked machine. Contains machine code control characters.

V

Variable unblocked.

VA

Variable unblocked ANSI. Contains ISO/ANSI/FIPS control characters.

VBA

Variable blocked ANSI with multiple records per block. Contains ISO/ANSI/FIPS control characters.

VBM

Variable blocked machine with multiple records per block. Contains machine code control characters.

VBS

Variable blocked spanned. Multiple records per block where the records can span more than one block.

VM

Variable unblocked machine. Contains machine code control characters

VS

Variable unblocked spanned. A record can span more than one block.

U

Undefined.

Default: Null

LRECL

Specifies the actual or maximum length, in bytes, of a logical record.

Range: 0 to 32767

Default: 160

BLKSIZE

Specifies the block size of the remote data set.

Space DIRBLK

Specifies the number of directory blocks for the remote data set.

Range: 0 to 99999

Default: 0

Space Primary

Identifies primary storage allocation for the remote data set.

Range: 0 to 99999

Default: 1

Space RLSE

Specifies whether the unused space for the remote data set is to be released.

Default: No

Space Secondary

Identifies secondary storage allocation for the remote data set.

Range: 0 to 99999

Default: 1

Space Unit

Indicates the unit of storage allocation for the remote data set.

TRK

Tracks

CYL

Cylinders

BLK

Blocks

Default: None

Tape

Specifies whether the remote data set resides on the tape.

Default: No

DEN

Specifies the density for the remote tape data set.

Range: 1 to 4

Default: None

Label EXPDT

Specifies the expiration date for the remote tape data set, in the form *yyddd* or *yyyy/ddd*.

Default: None

Note: Label RETPD and Label EXPDT are mutually exclusive.

Label RETPD

Specifies the retention period for the remote tape data set, in number of days.

Range: 1 to 9999

Default: No

Note: Label RETPD and Label EXPDT are mutually exclusive.

Label Sequence

Specifies the sequence number of the remote data set on the tape.

Range: 1 to 9999

Default: 1

Label Type

Specifies the type of label associated with the remote tape data set. The label type can be AL, AUL, BLP, LTM, NL, NSL, SL, or SUL.

Default: SL

FILEDATA

Indicates how a remote USS file is to be allocated:

- Binary
- Text

Default: None

UMASK

Sets the permissions assigned to a file when the file is being created and received on the system for the first time. The value is expressed as an octal number (base 8). The octal number has the same meaning as in the standard UNIX umask command.

Range: 000 to 777

Default: 666 (rw-rw-rw) for files and 777(rwxrwxrwx) for directories

Report Section

This section describes the fields in the Report section pane of the Edit Transfer Record or Quick Transfer Record page.

Note: This section is displayed only for the Send Report action.

Class

The print class assigned to a report transferred to a remote system.

Range: 1 character

Default: A

Chars

Indicates the character set used when the report is sent to a remote system.

Range: 0 to 4 characters

Default: None

Control

Indicates the type of printer carriage-control codes, if any, that are included in the report file.

ASA

ASA control codes in column 1.

MACHINE

IBM Machine Characters (valid only for IBM mainframes).

BYPASS

If data is already in ASA format, bypass conversion.

NONE

No carriage-control codes are used.

Default: NONE

Copies

The number of copies to be sent. If this parameter is not specified, the remote system queues one copy of the report to the system's default printer.

Range: 1 to 999

Default: 1

Destination

Identifies the printer or other device on the remote system where the report is to be sent. If this parameter is not specified, the remote system sends the report to the system's default printer.

0 to 16 characters

For indirect transfers and for Version 1.

0 to 21 characters

For transfers that are not indirect and for Version 2.

Default: None

Disposition

Indicates what the remote system does with the report file after the report has been printed.

Note: This field is not used when the remote system is an IBM mainframe.

DELETE

After printing the report is deleted.

KEEP

After printing the report is kept.

HOLD

After printing the report is held.

Default: DELETE

FCB

Identifies the FCB JCL parameter when sending the report file to an IBM mainframe, defining print density and lines per page.

Range: Zero to four characters

Default: None

Form

The type of form that should be used to print the report. Because CA XCOM Data Transport places the print job in the remote system's print queue, the print control functions depend on the remote system. The user must verify beforehand that the requested form is available at the remote site.

Note: When sending a report to a VAX system, leave this parameter blank unless you are certain that this is a valid form type. VMS interprets this to mean that no special form is being requested.

Range: 0 to 10 characters

Default: None

Hold

Indicates whether a transferred report file is to be placed on HOLD on the remote system or is to be printed immediately.

Range: YES or NO

Default: NO

Name

Indicates the title of the report.

Range: 0 to 21 characters

Default: None

Spool

Indicates whether the report is to be spooled to disk or printed immediately.

Note: If the remote system is an IBM mainframe, this parameter has no effect on the transfer.

Range: YES or NO

Default: YES

Writer

Specifies the name of the external writer that is to process the report on the

remote system.

Note: This parameter cannot be specified with Version 1 transfers.

Range: 0 to 8 characters

Default: None

Notify Section

Level

Specifies the local notification level for transfers initiated from the remote server.

All

Notifies after transfer completion.

Warn

Notifies only when the transfer received a warning or an error.

Error

Notifies only when the transfer received an error.

Default: ALL

Method

Specifies the method for notifying the transfer completion:

LOG

Causes the CA XCOM Data Transport transfer log to be written.

TSO

Identifies the TSO user who is sent a broadcast message when the file transfer completes.

CICS

Causes CA XCOM Data Transport to begin an LU 6.2 process to CICS when the file transfer concludes.

LU

Defines the local system's LU name and associated VTAM logical unit name.

ROSCOE

Sends notification messages to users of the CA Roscoe timesharing product when a file transfer begins, ends, or fails.

ALL

A notification message is displayed on the local Windows system console.

MAIL

Sends a mail notification message to the local user.

WRITE

A notification message is displayed on the screen.

NONE

No notification is sent.

Default: None

User

The user on the remote system who is to be notified when the transfer is complete.

Range: 0 to 12

Default: None

Encryption At Rest Section

Cipher

Specifies the encryption algorithm used for encrypting data on the remote server.

Cipher Key

Specifies the key used to encrypt or decrypt data.

Hash

Specifies the hash algorithm to calculate the digest on the remote server.

Digest

Specifies a hash-value that determines the integrity of the data.

Misc Options

This section describes the parameters on the Misc Options section of the Edit Transfer Record or Quick Transfer Record page.

Age

Denotes the queue-purging interval in number of days for the transfer requests initiated locally.

Transfer User Data

Specifies the transfer-dependent user data. This data is available to user exits in the RRDXUSER field of the RRDS data area (mapped by the RRDDSECT macro) while the transfer is pending or active. The RRDXUSER field is defined by HDRDSECT within RRDDSECT.

System UserData

Specifies the transfer-dependent user data. This data is available to user exits in the RRDSUSER field of the RRDS data area (mapped by the RRDDSECT macro) while the transfer is pending or active. The RRDSUSER field is defined by HDRDSECT within RRDDSECT.

START

Specifies the start date and time of the transfer.

SPRTY

Indicates the scheduling priority of this metatransfer request. The lowest priority is 1.

Note: This feature has no effect once the transfer begins executing.

Range: 1 to 255

Default: 16

EPRTY

Indicates the execution priority of this metatransfer request. The lowest priority is 1.

Range: 1 to 255

Default: 16

DROPSESS

Indicates whether CA XCOM Data Transport drops an LU-to-LU session at the conclusion of a scheduled file transfer.

YES

Indicates that CA XCOM Data Transport drops the session.

NO

Indicates that CA XCOM Data Transport does not drop the session.

QEMPTY

Indicates that CA XCOM Data Transport is to process all the transfers to a particular LU in the request queue before dropping the session.

Default: NO

SSLConfiguration File Name

Specifies the configssl.cnf file path and file name.

Range: 0 to 256 characters

Default: Null

Transfer ID

Allows the user to enter information to identify the file transfer request.

Note: This is equivalent to the IDENT field on UNIX and Linux.

Range: 0 to 10 characters

Default: Null

JPNCNTL

Indicates whether the header file contains Katakana characters.

K or KATAKANA

The control information (header fields) being transferred contains Katakana character

E or ENGLISH

The control information does not contain Katakana characters.

Default: E (ENGLISH)

JPNDATA

Indicates whether the data file contains Katakana characters.

K or KATAKANA

The data file being transferred contains Katakana characters.

E or ENGLISH

The data file does not contain Katakana characters.

Default: E (ENGLISH)

JPNSHFT

Specifies whether DBCS shift-out and shift-in characters are removed or converted to spaces.

C or CONVERT

The DBCS shift-out/shift-in characters are converted to spaces.

D or DELETE

The DBCS shift-out/shift-in characters are removed.

Default: D (DELETE)

PDSEPGMLIB

Specifies whether the transfer is a z/OS transfer of a PDSE program library.

YES

Indicates a z/OS transfer of a PDSE program library.

NO

Indicates that the transfer is not of a PDSE program library.

Default: No

XCOM Header Version

Indicates the version of the CA XCOM Data Transport protocol to be used for this transfer. For using TCP/IP, only a value of 2 is valid.

Range: 1 or 2

Default: 2

Write EOF

When receiving a text file, set Write EOF to YES to have the end of file character (CTRL + Z) written at the end of the file.

Range: YES or NO

Default: NO

Log File Name

The name of the file where CA XCOM Data Transport logs activity.

XTRACE

Indicates the level of desired execution tracing by CA XCOM Data Transport.

0

No tracing.

1 to 8

Levels of tracing from 1 (lowest) to 8 (highest).

9

Show the contents of the data buffers.

10

Includes levels 1 through 9, plus some additional detailed technical information.

Default: 0

Note: Turning on the trace can seriously degrade performance.

CA XCOM Transfer Control (XTC) Parameters

This section describes the parameters shown in the CA XCOM Transfer Control (XTC) Parameters section of the Edit Transfer Record or Quick Transfer Record page.

Network

Specifies representing the name of the XTC network (XTCNET) running this transfer.

Range: Up to eight alphanumeric characters.

Job

Specifies the name of a transfer request (XTCJOB) in a group of interrelated transfer requests.

Hold

Prevents a schedule transfer from starting until explicitly released.

Yes

Indicates that the transfer is not initiated until it is released.

No

Indicates that the transfer is not held.

Default: No

Hold Count

Specifies a value that controls the holding/releasing of a transfer request. The transfer is released when the value of the parameter

reaches 0.

Range: 0 to 255

Default: 0

Define Global Parameters

A global parameter XML file is set up during installation of CA XCOM Management Center. It is named xcom-globals.xml and is located in the JBoss conf folder.

The CA XCOM Management Center server requires this global parameters .xml file. The CA XCOM Management Center server uses this file to set up and direct CA XCOM Management Center services.

Global parameters are read into memory during CA XCOM Management Center server initialization. Subsequently, most of the parameters can be modified by using the online configuration facilities (see the chapter "Configuring and Administering CA XCOM Management Center").

It is also possible to change global parameters by editing the xcom-globals.xml file. However, when changes are made by this method, CA XCOM Management Center needs to be restarted to make the changes effective.

Important! Because incorrect global parameter changes can render CA XCOM Management Center inoperable and the CA XCOM Management Center website inaccessible, we strongly recommend that you save a copy of xcom-globals.xml before making online changes to the global parameters. Problematic changes can then be reversed by restarting CA XCOM Management Center after reinstating the saved file.

XCOM Global Parameters Structure

The XML Global Parameter structure is as follows:

```
<XCOMCONFIGURATION>
    <MANAGEMENTCENTERSERVER
        MAXPAGEROWS="nnnn"
        DEFAULTPAGEROWS="nnnn"
        >
        <JDBC KEY="encryptionkey"
            PASSWORD="password"
            USER="userid"
            DBCREATOR="schema"
            DATASOURCE="datasource"
            />
        <CAEEM
            HOST="hostname"
            />
        <LOG
            LEVEL="INFO|ERROR|WARN"
            PATH="xxxx"
            DATEFORMAT="xxxxx"
            />
        <TRACE
            LEVEL="nn"
            PATH="xxxxx"
            />
        <WEBSERVICES
            INTERFACEURL="url"
            />
        <EXPORT
            HOMEDIRECTORY="xxxxx"
            />
        <USERNAME
            CASEINSENSITIVE="YES|NO"
            />
    </MANAGEMENTCENTERSERVER>

    <INTERFACESERVER
        QUERYCOUNT="n"
        >
        <JDBC
            DATASOURCE="datasource"
            PASSWORD="passsword"
            KEY="encryptionkey"
            USER="userid"
            />
        <KEYSTORE
            PATH="path"
```

```
                    PASSWORD="password"
                    KEY="encryptionkey"
                    />
              <LOG
                    PATH="xxxx"
                    LEVEL="INFO|ERROR|WARN"
                    />
        </INTERFACESERVER>
</XCOMCONFIGURATION>
```

Attributes

The global parameter attributes are defined by the following structure:

<XCOMCONFIGURATION>

This is the global parameter structure container. This container has two main structures embedded in it, as follows:

- MANAGEMENTCENTERSERVER

- INTERFACESERVER

MANAGEMENTCENTERSERVER Structure

The MANAGEMENTCENTERSERVER structure contains the EXPORT, WEBSERVICES, JDBC, CAEEM, LOG, TRACE, and USERNAME structures.

The attributes for the MANAGEMENTCENTERSERVER structure are as follows:

DEFAULTPAGEROWS="nnnn"

The default value (which will apply when a user has made no alternative selection) specifying the effective Page Rows value. The effective Page Rows value controls the number of data rows to be displayed on any CA XCOM Management Center screen (that is, a single page) showing tabular data. When the number of data rows to be presented exceeds the effective Page Rows value, data rows are displayed over a number of screens (that is, pages), with links enabling navigation between pages.

Range: 1 to 9999

Default: 20

MAXPAGEROWS="nnnn"

The highest permitted value that can be adopted as the effective Page Rows value, which controls the number of data rows to be displayed on a CA XCOM Management Center screen (that is, a single page) showing tabular data. When a user attempts to select a Page Rows value, they cannot select any value higher than MAXPAGEROWS.

Range: 1 to 9999

Default: 9999

EXPORT Structure

The attribute for the EXPORT structure is as follows:

HOMEDIRECTORY="xxxxx"

The home directory path for the exported server and configuration files:

- Exported server files are stored in the following directory:

  xxxxx/*loginuserid*/ExportedServers

- Exported configuration files are stored in the following directory:

  xxxxx/*loginuserid*/ExportedConfigurations

xxxxx

Tthe value of the HOMEDIRECTORY parameter.

loginuserid

The ID of the logged in user (or the first 60 characters of the logged in user ID if the user ID length is more than 60 characters).

Range: 1 to 120 characters

Default: "/XCOMGUI/"

WEBSERVICES Structure

The attribute for the WEBSERVICES structure is as follows:

INTERFACEURL="url"

The Interface Server URL.

Default: The same as the CA XCOM Management Center server URL.

JDBC Structure

Note: This JDBC structure is for the MANAGEMENTCENTERSERVER structure only.

The attributes for the JDBC structure are as follows:

DATASOURCE="datasource"

The JDBC datasource to be used.

Default: None

PASSWORD="password"

The password to be used when connecting to the datasource.

If KEY is specified, the password is represented in encrypted form, otherwise as clear text.

KEY="encryptionkey"

The encryptionkey, together with a fixed key, encrypts the password value.

USER="userid"

The user ID to be used when connecting to the datasource.

CAEEM Structure

The attributes for the CAEEM structure are as follows:

HOST="xxxxx"

The host name or IP address of the machine on which the CA EEM server is located.

Range: 1 to 64 characters

Default: "localhost"

LOG Structure

Note: This LOG structure is for the MANAGEMENTCENTERSERVER structure only.

The attributes for the LOG structure are as follows:

DATEFORMAT="US|EUROPEAN"

The required date format.

Default: "US"

PATH="xxxx"

The name of the log output file path.

Default: "/tmp/CA_XCOM/"

LEVEL="INFO|ERROR|WARN"

The required log message level.

INFO

Informational warnings and error messages

ERROR

Error messages

WARN

Warning and error messages

Default: INFO

TRACE Structure

CA Technologies recommends using the trace file primarily for debugging. It is a text file and its location is specified in the Global Parameter XML structure in the TRACE structure.

Note: The trace records are free format.

The attributes for the TRACE structure are as follows:

PATH="xxxx"

The name of the trace output file path.

Default: "/tmp/CA_XCOM/"

LEVEL="level"

The required trace level.

Range: 0 through 10, where 0 does not write any trace. As the trace level number increases, more detailed information is written to the trace file.

Default: 0

USERNAME Structure

The attribute for the USERNAME structure is as follows:

CASEINSENSITIVE="YES|NO"

Specifies whether the entered user name at login time is case-sensitive.

If the parameter is omitted or set to YES, then the entered user name is treated as case-insensitive and matches with a user name in the Users database, ignoring the case. The user name with the lowest user_row ID in the Users database is used as the login user.

If the parameter is set to NO, then the entered user name is treated as it is, with no upper/lower case conversion.

Default: "YES"

INTERFACESERVER Structure

The INTERFACESERVER structure contains the JDBC, KEYSTORE, and LOG structures.

The attribute for the INTERFACESERVER structure is as follows:

QUERYCOUNT="n"

The number of HISTORYITEMS to be returned by a QUERYHISTORY inquiry.

JDBC Structure

Note: This JDBC structure is for the INTERFACESERVER structure only.

The attributes for this JDBC structure are as follows:

DATASOURCE="datasource"

The JDBC datasource to be used.

PASSWORD="password"

The password to be used when connecting to the datasource. If KEY is specified, the password is represented in encrypted form; otherwise, it is represented as clear text.

KEY="encryptionkey"

The encryptionkey, together with a fixed key, encrypts the password value.

USER="userid"

The user ID to be used when connecting to the datasource.

KEYSTORE Structure

The attributes for the KEYSTORE are as follows:

PATH="path"

Specifies the location of the JCA keystore.

PASSWORD="password"

Specifies the hex digits of the encrypted password for the keystore.

KEY="encryptionkey"

Specifies the hex digits of a key value used by the password encryption algorithm.

LOG Structure

Note: This LOG structure is for the INTERFACESERVER structure only.

The attributes for this LOG structure are as follows:

DATEFORMAT="US|EUROPEAN"

The required date format.

Default: "US"

PATH="xxxx"

The name of the log output file.

Default: None

LEVEL="INFO|ERROR|WARN"

The required log message level.

INFO

Informational warnings and error messages

ERROR

Error messages

WARN

Warning and error messages

Default: INFO

Glossary

DB2 UDB (Universal Data Base)

DB2 UDB (Universal Data Base)—*DB2 UDB* is an enhanced version of the DB2 Relational Database Management System. It is used to define and manage the XCOM Management Center relational data bases that are used for XCOM Management Center processing.

Embedded Entitlements Manager (EEM)

A CA Technologies product providing user authentication and authorization services.

Metatransfer Protocol

XCOM TCP/IP metatransfer protocol is an XCOM-proprietary protocol that is implemented by CA XCOM Data Transport servers to provide control functions. These control functions enable CA XCOM Data Transport servers to be instructed to schedule transfers or to change the status of a previously scheduled transfer. They also enable history data to be retrieved for previously scheduled, active, and completed transfers. The metatransfer interface is supported on the MVS, Windows, and UNIX platforms.

SOAP (Simple Object Access Protocol)

SOAP (*Simple Object Access Protocol*) is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on XML as its message format and usually relies on other Application Layer protocols such as HTTP for message negotiation and transmission.

Index

T

transfer protocols • 14

W

WEBSERVICES structure • 237
website, CA XCOM Data Transport • 61
Wizard • 122

X

XCOM Global Parameters structure • 234
XCOM header version • 231
XML formats • 191
XNODESPEC • 210
XTRACE • 232