

CA Output Management Web Services

Installation Guide

Version 2.0



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

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

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

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

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

The manufacturer of this Documentation is CA.

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

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA Chorus Software Manager (CA CSM)
- CA DRAS™
- CA View®
- CA Dispatch™
- CA Bundl®

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Overview 9

Audience	9
How the Installation Process Works.....	9
How the Installation Process Works with SMP/E Install	10
How the Installation Process Works in InstallAnywhere Based install	12

Chapter 2: Preparing for Installation 13

General Requirements	13
Supported Platforms	13
Java Web Application Servers	14
CA Common Services Requirements	14
Environment Variables	14
Additional Requirements	15
LMP Key Requirements	15
SMP/E Install Requirements.....	15
Security Requirements	16
Storage Requirements	16
DVD Space Requirements for Mainframes	17
InstallAnywhere based Install Requirements.....	17
Java Virtual Machine Requirements	17
Security Requirements on Other Platforms	17
Deployment Security.....	18
Storage Requirements	18
General USS Requirements	18
USS Security Requirements.....	19
Allocate and Mount a File System for Mainframe	20
Concurrent Releases	21

Chapter 3: Installing CA OM Web Services with SMP/E (USS) 23

Install Your Product Using CA CSM	23
How to Install Your Product Using CA CSM.....	23
Install Your Product Using Pax ESD or DVD	31
How to Install Your Product Using a Pax File	31
Allocate and Mount a File System.....	32
Acquire the Product Pax Files	35
Create a Product Directory from the Pax File	40

Copy Installation Files to z/OS Data Sets.....	41
Prepare the SMP/E Environment for Pax Installation	43
Run the Installation Jobs for a Pax Installation	45
Clean Up the USS Directory.....	46
Apply Preventive Maintenance.....	46

Chapter 4: Installing CA OM Web Services with InstallAnywhere **53**

Supported Platforms	53
Locate the Product Installer	54
Use a Web Browser	54
Use the DVD	54
InstallAnywhere Installation of CA OM Web Services on Windows.....	55
Installation Using the GUI Wizard	56
InstallAnywhere Installation of CA OM Web Services on Other Platforms.....	57
Installation Using the Console Mode	58
Installation Logging	59
Log Locations.....	59

Chapter 5: Uninstalling CA OM Web Services **61**

Uninstall	61
Launch the Uninstaller	61
Uninstall on Windows	62
Uninstall on Other Platforms	63

Chapter 6: Post-Installation and Configuration Tasks **65**

Configure CA OM Web Services	65
Running the Configuration Tool (Interactive Mode)	66
Configuration Tool First Steps.....	68
Configure CAICCI	69
Configure the License Server	70
Create or Manage Repository Definitions.....	71
Create Report List Data Dictionary Entries.....	77
Configuration Tracing.....	79
Save Configuration Changes	80
Manual Connect Pool Configuration	80
Prepare your Java Web Application Server	81
Install CCS Tomcat.....	82
Create Application Specific Instance of CCS Tomcat	83
IBM WebSphere Considerations	85
Deploy CA OM Web Services.....	85

Apache Tomcat	86
IBM WebSphere	87
Verify Installation	87
Connectivity Test.....	88
Retrieve a List of Reports	89
Retrieving Report Data.....	94
Chapter 7: Migrating Information	101
Migrate Information.....	102
Chapter 8: Applying Fixes to the Product	103
Apply Fixes on SMP/E Install	103
Apply Fixes on Other Platforms.....	104
Update Installation Using the GUI Wizard	105
Update Installation Using the Console Mode	105
Update Installation Using the Silent Mode	109
Appendix A: Installation Worksheet	111
CA CSM Installation-Mainframe	111
SMP/E JCL Installation-Mainframe.....	117
Appendix B: Creating Log Information	121
Log Levels	121
Update Configuration Files.....	122
Output Log Files	122
Index	123

Chapter 1: Overview

This guide introduces you to CA OM Web Services. It provides an overview of the wide scope of the product and its usability; it also supplies installation guidance specific to your environment.

This section contains the following topics:

[Audience](#) (see page 9)

[How the Installation Process Works](#) (see page 9)

Audience

This guide is for the Administrators who install, use, and maintain the product. This guide assumes that you are familiar with the underlying operating systems such as Linux, Solaris, HP-UX, or Microsoft Windows systems, terms, and concepts.

Readers of this book must have knowledge in the following areas, depending on the platform you are installing:

- JCL
- TSO/ISPF
- z/OS environment and installing software in this environment
- z/OS UNIX System Services
- Your organization IT environment, enterprise structure, and region structure

Consult with the following personnel, as required:

- Systems programmer for z/OS and VTAM definitions
- Storage administrator for DASD allocations

How the Installation Process Works

CA OM Web Services can be installed on multiple platforms based on the installation process methods selected.

This section describes how the installation process works in:

- SMP/E based install (Chorus Software Manager or JCL)
- InstallAnywhere based install

How the Installation Process Works with SMP/E Install

Note: The SMP/E based install only installs on the USS platform. For more information about installing on other platforms, see [How the Installation Process Works in InstallAnywhere Based install](#) (see page 12).

CA Technologies has standardized product installations across all mainframe products. Installation uses the following process:

- Acquisition—Transports the software to your z/OS system.
- Installation using SMP/E—Optionally creates a CSI environment and runs the RECEIVE, APPLY, and ACCEPT steps. The software is untailed.
- Deployment—Copies the target libraries to another system or LPAR.
- Configuration—Creates customized load modules, bringing the software to an executable state.

CA CSM provides a web-based interface to make the standardized installation process easier. Using CA CSM, someone with a limited knowledge of JCL and SMP/E can install a product.

Note: If you do not have CA CSM, you can download it from the Download Center at [the CA Support Online website](#). Follow the installation instructions in the CA Chorus Software Manager documentation bookshelf on the CA Chorus Software Manager product page. The standardized installation process can also be completed manually.

To install your product, do the following tasks:

1. Prepare for the installation by confirming that your site meets all installation requirements.
2. Use one of the following methods to acquire the product:
 - Download the software from CSO using CA CSM.
 - Download the software from CSO using Pax-Enhanced Electronic Software Delivery (ESD).
 - Order a DVD.
3. Perform an SMP/E installation using one of the following methods:
 - If you used CA CSM to acquire the product, start the SMP/E step from the SMP/E Environments tab in CA CSM.
 - If you used ESD to acquire the product, you can install the product in the following ways:
 - Install the product manually.
 - Use the Insert New Product option in CA CSM to complete the SMP/E installation.
 - If you used a DVD, install the product manually.

Note: If a CA Recommended Service (CA RS) package is published for your product, install it before continuing with the deployment.

4. Deploy the target libraries using one of the following methods:
 - If you are using CA CSM, deployment is required; it is a prerequisite for the configuration.
 - If you are using a manual process, deployment is an optional step.

Note: Deployment is considered part of starting your product.

5. Configure your product using CA CSM or manually.

Note: Configuration is considered part of starting your product.

How the Installation Process Works in InstallAnywhere Based install

For all supported platforms you can install using an InstallAnywhere based installer.

There are three InstallAnywhere installers:

- Windows
- Windows 64
- Multiplatform

This section outlines the basic steps needed for an InstallAnywhere install.

Follow these steps:

1. Locate the installer for your platform.

Note: For more information about locating the platform, see [Locating the Product Installer](#) (see page 54).

2. Run the installer.

Note:

- For more information running installer on other platforms, see [Installing CA OM Web Services with InstallAnywhere](#) (see page 53).

3. (Optional) Migrate old CA OM Web Services 1.0 repository definitions to the new CA OM Web Services 2.0 installation.

4. Configure your WAR or EAR file.

Note: For more information, see [Configure CA OM Web Services](#) (see page 65).

5. Setup your Java Web Application Server.

Note: For more information, see [Preparing your Java Web Application Server](#) (see page 81).

6. Deploy your CA OM Web Services war or ear file.

Note: For more information, see [Deploying CA OM Web Services](#) (see page 85).

7. Verify if CA OM Web Services is up.

Note: For more information, see [Connectivity Test](#) (see page 88).

8. Attempt accessing a report list and report data.

Note:

- For more information, see [Retrieve a List of Reports](#) (see page 89).
- For more information, see [Retrieve Report Data](#) (see page 94).
- Repository definitions and report list data dictionary entries must be setup during the configuration of your WAR or EAR file step to access data and report list.

Chapter 2: Preparing for Installation

This section describes what you need to know and do before you install the product.

This section contains the following topics:

[General Requirements](#) (see page 13)

[SMP/E Install Requirements](#) (see page 15)

[InstallAnywhere based Install Requirements](#) (see page 17)

[General USS Requirements](#) (see page 18)

[Concurrent Releases](#) (see page 21)

General Requirements

This section describes the requirements for the Installation of CA OM Web Services.

Supported Platforms

CA OM Web Services is a Java application that must be run on a Java virtual machine (JVM). Therefore, we expect that a Java-enabled operating environment with a supported version of the Java Runtime Environment is installed:

- Windows
- Linux
- z/Linux
- AIX
- HP-UX PA
- HP-UX IA
- Solaris
- USS

Java Web Application Servers

CA OM Web Services requires a Java Web Server. Therefore, we expect a Java Web Application Server installed and configured. Supported Java Web Application Servers include:

USS Platform

- Apache Tomcat supported release (Recommended from CA Common Services)
- IBM WebSphere supported release

Other Platforms

- Apache Tomcat (<http://tomcat.apache.org>)
- IBM WebSphere supported release

CA Common Services Requirements

The following CA Common Services are used with CA OM Web Services:

- CAIRIM
- CAICCI
- CA LMP
- Apache Tomcat (Only for Mainframe installation)

Note: If other CA Technologies products are installed at your site, some of these services are already installed.

Environment Variables

ivmhook

These parameters must not be included in the environment variables JAVA_TOOL_OPTIONS and _JAVA_OPTIONS:

- -agentlib:jvmhook
- -Xrunjvmhook

allowArraySyntax

Parameter required for Java 1.6, if you encounter ClassNotFoundException error.

- Add the following in the environment variable JAVA_OPT or the Java command to launch web application server:

```
-Dsun.lang.ClassLoader.allowArraySyntax=true
```

Additional Requirements

- CA DRAS™ (Distributed Repository Access System).

Note: CA DRAS™ is an optional component in the latest CA View® and CA Dispatch™ release. The stand-alone CA DRAS 11.5 installation will be required if using CA Bundl®.

One or more of the following Output Management repository products is required:

- CA View® (any supported release) with optional CA DRAS component installed
- CA Bundl® (any supported release) with CA DRAS 11.5
- CA Dispatch™ (any supported release) with optional CA DRAS component installed

LMP Key Requirements

The CA License Management Program (CA LMP) tracks licensed software in a standardized and automated way. CA LMP uses common real-time enforcement software to validate the user configuration. The CA LMP reports on activities that are related to the license, usage, and financials of CA Technologies products.

CA LMP includes the following features:

- Common Key Data Set can be shared among many CPUs.
- Check digits are used to detect errors in transcribing key information.
- The Execution Keys can be entered without affecting any CA Technologies software product already running.
- No special maintenance is required.

CA OM Web Services is licensed with an LMP key. You acquire the LMP key with one of the following methods:

- From your product media
- With ESD
- From <http://ca.com/support>

Note: The LMP key must be installed on the system where the CA DRAS task used for the License Check is executed.

SMP/E Install Requirements

This section describes the requirements for installation with SMP/E.

Security Requirements

To complete the tasks in this guide, you need the following security privileges:

USS Platform Requirements:

- Full authority (read/write/create/delete) for the SMP/E data sets.
- Authority to allocate the file system, create the initial directory, and mount the file system if creating a USS file system.
- Full authority (read/write/create/delete) for the USS directory.

Storage Requirements

Ensure that you have the following storage available:

USS (SMP/E):

- If you install the product with Pax ESD, 450 tracks for the downloaded files
- For the installation and setup:
 - Installation = 1650 tracks
 - SMP/E temporary libraries = 750 tracks

Target Libraries for Mainframes

The following table lists the amount of disk space that is required to install the target libraries:

Library Name	Blksize	Tracks	Dir Blks	Description
/cai/om_web_services		950		HFS/ZFS File SystemCommon
CAI.CDUZXML	32760	20	12	CA CSM Deployment and Configuration Services
CAI.CDUZJCL	32720	2012		JCL

Distribution Libraries for Mainframes

The following table lists the amount of disk space that is required to install the distribution libraries:

Library Name	Blksize	Tracks	Dir Blks	Description
CAI.ADUZHFS	32760	600	24	HFS Files

Library Name	Blksize	Tracks	Dir Blks	Description
CAI.ADUZSHEL	32760	20	12	Installation Shell Scripts
CAI.ADUZXML	32760	20	12	CA CSM Deployment and Configuration Services
CAI.ADUZJCL	32720	20	12	JCL

DVD Space Requirements for Mainframes

Ensure that you have sufficient free space in the USS file system that you are using for Pax ESD to hold the directory that the pax command and its contents create. You need approximately 3.5 times the pax file size in free space.

If you do not have sufficient free space, you will receive error message EDC5133I.

InstallAnywhere based Install Requirements

This section describes the installation requirements for other platforms.

Java Virtual Machine Requirements

The installer requires one of the following requirements be installed on your platform.

- Java JRE (Java Runtime Environment) 1.6.0 or above
- Java JDK (Java Development Kit) 1.6.0 or above

Security Requirements on Other Platforms

The security requirements on Windows, UNIX, or Linux are explained in the following sections:

Windows

If you install CA OM Web Services as an administrator you have to run the Configuration Tools, System Test Tools, and the Update Installer as an administrator.

If you install CA OM Web Services as a particular user, you run the Configuration Tools, System Test Tools, and the Update Installer as a user or administrator.

Unix/Linux/USS

If you install CA OM Web Services as root you run the Configuration Tools, run System Test Tools, and the Update Installer as root or using pseudo.

If you install CA OM Web Services as a non-super-user account you run the Configuration Tools, System Test Tools, and the Update Installer as a user, a member of a group who has access to the installed files, or root.

Note: For more information about security requirements on USS, see [General USS Requirements](#) (see page 18).

Deployment Security

To deploy your CA OM Web Services war or ear file, you must have the correct permissions to access the server machine, and deploy applications on the Java Web Application Server.

Note: For more information contact your system administrator, or access your Java Web Application Server documentation. For more information about security requirements on USS, see [USS Security Requirements](#) (see page 19).

Storage Requirements

Space Requirement for installation and configuration:

- Required Disk Space: 37 MB

Space Requirement for Java Web Application Server Deployment:

- Required Initial Disk Space: 20 MB

Note: Over time the log files can build up in the Tomcat server. For more information about log files, see [Creating Log Information](#) (see page 121).

General USS Requirements

The following software is required for both the SMP/E and InstallAnywhere installs on the USS platform:

- 5694-A01 any z/OS release that IBM supports
- z/OS UNIX System Services running in full function mode
- Java JDK (Java Development Kit) 1.6.0 or above

USS Security Requirements

To complete the tasks in this guide, you need the following security privileges:

USS Installation Requirements:

- Authority to allocate the file system, create the initial directory, and mount the file system if creating a USS file system.
- Full authority (read/write/create/delete) for the USS directory.

USS Configuration and Tomcat Deployment Requirements:

- Full authority (read/write/create/delete) for the USS directory where CA OM Web Services was installed.
- Authority to copy/delete the WAR file within the Apache Tomcat /webapps folder (for the deployment of the WAR).

Allocate and Mount a File System for Mainframe

CA OM Web Services require a zSeries File System (zFS) or Hierarchical File System (HFS) for its target libraries. An existing file system that meets the following requirements is used:

- Read/Write/Execute access for the owner and group owner.

Note: The USS commands are case-sensitive.

Follow these steps:

1. Allocate the zFS file system. Alternatively, go to step 2 for HFS.

```
//ALLOC EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//AMSDUMP DD SYSOUT=*
//SYSIN DD *
  DEFINE CLUSTER ( +
    NAME(yourZFS.dataset.name) +
    VOLUME(volume) +
    LINEAR +
    CYL(primary secondary) +
    SHAREOPTIONS(3,3) +
  )
/*
//FORMAT EXEC PGM=IOEAGFMT,REGION=0M,
// PARM=(' -aggregate yourZFS.dataset.name -compat')
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
//CEEDUMP DD SYSOUT=*
```

2. Allocate the HFS file system. Skip this step if zFS was allocated.

```
//ALLOC EXEC PGM=IEFB14
//FILESYST DD DSN=yourHFS.dataset.name,
// DISP=(NEW,CATLG,DELETE),
// UNIT=3390,VOL=SER=volume,
// DSNTYPE=HFS,
// SPACE=(CYL,(primary,secondary))
```

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

```
cd /u/apps/
mkdir cai
```

Note: This document refers to this structure as @pathprefix1@. The mount point is created.

4. Mount the file system. For example, from TSO, enter the following command:

```
MOUNT FILESYSTEM('yourZFS.dataset.name')  
MOUNTPOINT('@pathprefix1@')  
TYPE(HFS) MODE(RDWR)
```

The file system is mounted.

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

```
chmod -R 775 /@pathprefix1@/
```

Write access is not granted.

Note: For more information about the `chmod` command, see the *IBM z/OS UNIX System Services User Guide (SA22-7802)*.

Concurrent Releases

- CA OM Web Services 1.0 only supported installation on Microsoft Windows. You can install and use this release (on Windows) and continue to use an older release. However, the applications must use separate Java Web Application Servers.
- For all other platforms, there are no issues with concurrent release as CA OM Web Services 1.0 did not support platforms other than Microsoft Windows.

Chapter 3: Installing CA OM Web Services with SMP/E (USS)

This information lets you to get started with installing your product on the mainframe. These installation methods are only applicable for USS (UNIX System Services) regions on the mainframe.

The two mainframe installation methods, using SMP/E are:

- Install the Product using CA CSM
- Install the Product from the Pax-Enhanced ESD or DVD

This section contains the following topics:

[Install Your Product Using CA CSM](#) (see page 23)

[Install Your Product Using Pax ESD or DVD](#) (see page 31)

Install Your Product Using CA CSM

This information lets you to get started with installing your product using CA CSM.

How to Install Your Product Using CA CSM

As a system programmer, your responsibilities include acquiring, installing, maintaining, deploying, and configuring CA Technologies mainframe products on your system.

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

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

Before you use this scenario, you must have CA CSM installed at your site. If you do not have CA CSM installed, you can download it from the Download Center at <http://ca.com/support>. This web page also contains links to the complete documentation for CA CSM.

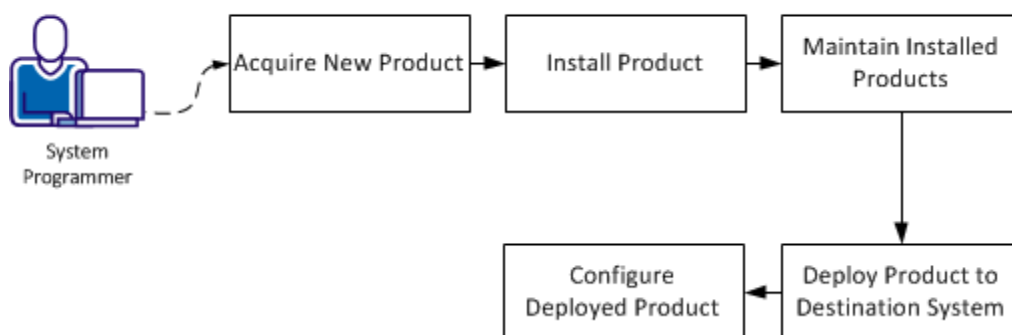
You access CA CSM from a web browser.

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

This scenario is a high-level overview of steps that you perform using CA CSM. For more detailed information, use the online help that is included in CA CSM.

You perform the following tasks to install products and manage them on your system:

How to Install Your Product Using CA CSM



1. Acquire a new product.
2. Install the product.
3. Maintain the installed products.
4. Deploy the product to the destination system.
5. Configure the deployed product.

Access CA CSM Using the Web-Based Interface

You access CA CSM using the web-based interface.

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

Follow these steps:

1. Start your web browser, and enter the access URL.

The login page appears.

Note: If the Notice and Consent Banner appears, read and confirm the provided information.

2. Enter your z/OS login user name and password.

The initial page appears. If you log in for the first time, you are prompted to define your account on [the CA Support Online website](#).

Note: For more information about the interface, click the online help link at the top right corner of the page.

3. Click New.

You are prompted for the credentials to use on [the CA Support Online website](#).

4. Specify the credentials, click OK, and then click Next.

You are prompted to review your user settings.

Note: These settings are available on the User Settings page.

5. Change the settings or keep the defaults, and then click Finish.

A dialog opens, which shows the progress of the configuration task. You can click Show Results to view the details of the actions in a finished task.

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

Acquire a New Product

Acquisition allows you to download products and product maintenance from the CA Support Online website at <http://ca.com/support> to a USS directory structure on your system. The products to which your site is entitled and the releases available are displayed in the Available Products section on the Products page.

You perform the following high-level tasks to acquire a product using CA CSM:

1. Set up a CA Support Online account at <http://ca.com/support>.

To use CA CSM to acquire or download a product, you must have a CA Support Online account. If you do not have an account, create one on <http://ca.com/support>.

2. Determine the CA CSM URL for your site.

To access CA CSM, you require its URL. You can get the URL from your site CA CSM administrator and log in using your z/OS credentials. When you log in for the first time, you are prompted to create a CA CSM account with your credentials that you use to access <http://ca.com/support>. This account enables you to download product packages.

3. Log in to CA CSM and go to the Products page to locate the product that you want to acquire.

After you log in to CA CSM, you can see the products to which your organization is entitled on the Products tab.

If you cannot find the product that you want to acquire, update the product list. CA CSM refreshes the product list through <http://ca.com/support> using the site IDs associated with your credentials.

4. Download the product installation packages.

After you find your product in the product list, you can download the product installation packages.

CA CSM downloads (acquires) the packages (including any maintenance packages) from the CA Support Online website.

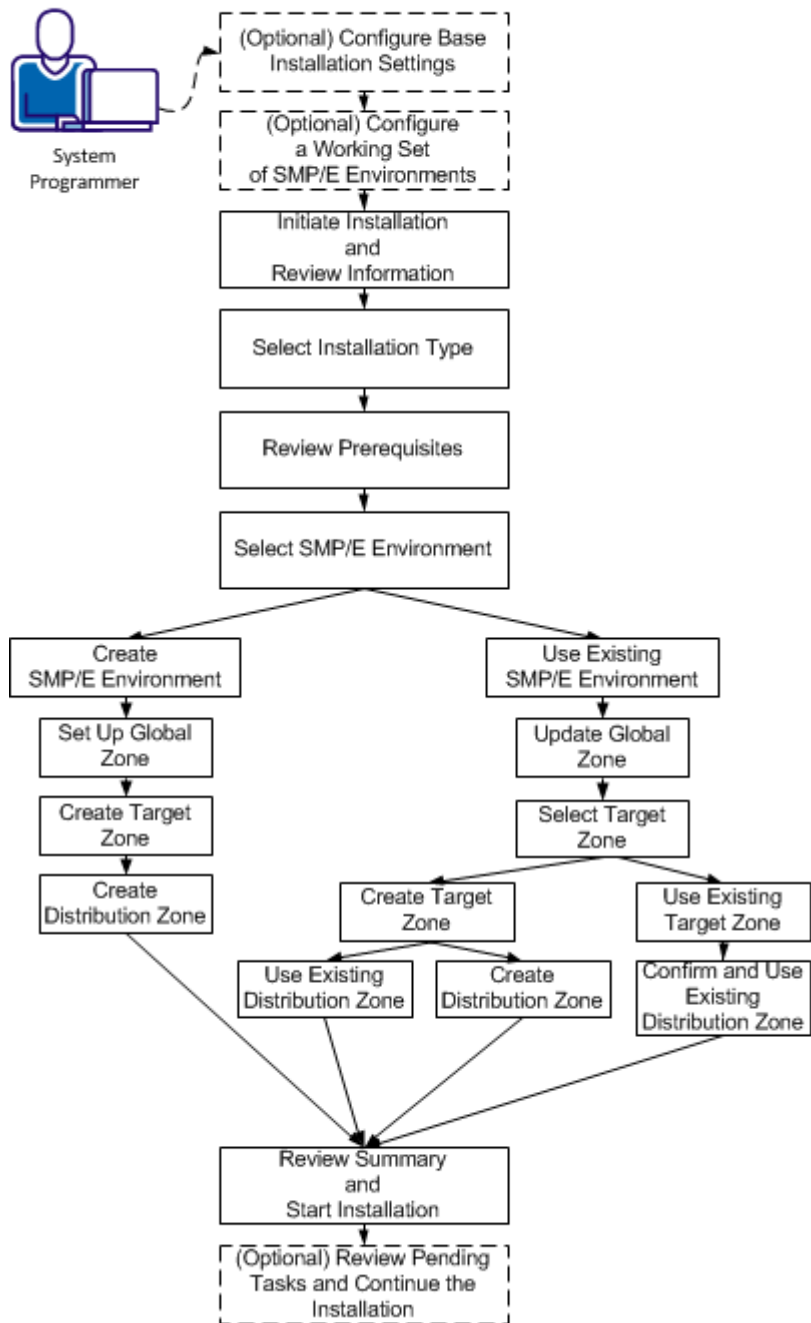
After the acquisition process completes, the product is ready for you to install or apply maintenance.

Install a Product

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

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

How to Install a Product



1. (Optional) On the Settings tab, click Software Installation under System Settings, and configure base installation settings.
2. (Optional) Click the SMP/E Environments tab, and configure a working set of SMP/E environments.
3. Click the Products tab and select a product that you want to install. Start the installation wizard and review product information.
4. Select an installation type.
5. Review installation prerequisites if any are presented.
6. Take *one* of the following steps to select an SMP/E environment:
 - Create an SMP/E environment:
 - a. Set up the global zone.
 - b. Create a target zone.
 - c. Create a distribution zone.
 - Use an existing SMP/E environment from your working set:
 - a. Update the global zone.
 - b. Set up the target zone: Create a target zone or use an existing target zone.
 - c. Set up the distribution zone: Create a distribution zone or use an existing distribution zone.
7. Review the installation summary and start the installation.
8. (Optional) Review pending tasks for the SMP/E environment where you are installing your product. Continue the installation, if applicable.

CA CSM installs the product.

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

Maintain the Installed Products

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

You can use CA CSM to maintain a CA Technologies product.

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

1. Verify that CA CSM recognizes the SMP/E environment where your product is installed. If not, migrate the SMP/E environment to CA CSM.

During the migration, CA CSM stores information about the SMP/E environment in the database.

2. From the Product tab, download the latest maintenance for the installed product releases.

If you cannot find the required release, perform the following steps to download the maintenance:

- a. Add the release manually.
 - b. Update the release.
3. Apply the maintenance.

CA CSM applies the maintenance to your product.

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

Deploy the Product to the Destination System

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

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

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

1. On the Deployments tab, set up methodologies.

Note: You can also set up methodologies when creating a deployment, or use existing methodologies, if you have set up any previously. If you do so, you can skip this step.

2. Start the New Deployment wizard to create a deployment. Complete each of the steps in the wizard. The wizard guides you through choosing deployment settings for your site. At any point, you can save your work and come back to it later.

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

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

Configure the Deployed Product

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

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

1. Select a configurable deployment on the Deployments tab to view details and products for that deployment.
2. Select a product in the deployment and start the Configuration wizard to create a configuration. Complete each of the steps in the wizard. The wizard has multiple levels of detailed instructions and guides you through choosing configuration settings for your site. At any point, you can save your work and come back to it later. Configurations where you have partially completed the steps in the wizard are listed on the Configurations tab. The steps in the wizard include the following:
 - a. Define a configuration name and select a system for the configuration.
 - b. Select configuration functions and options.
 - c. Define system preferences.
 - d. Create target settings.
 - e. Select and edit resources.
3. Build the configuration. The last step of the Configuration wizard lets you build the configuration. If needed, you can edit the configuration and can build the configuration again. Building the configuration closes the wizard and creates a configuration with all your settings.
4. (Optional) Validate the configuration. Validation verifies access to resources that are going to be used when you implement the configuration.

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

CA CSM configures the product.

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

Install Your Product Using Pax ESD or DVD

This information lets you to get started with installing your product using PAX ESD or DVD.

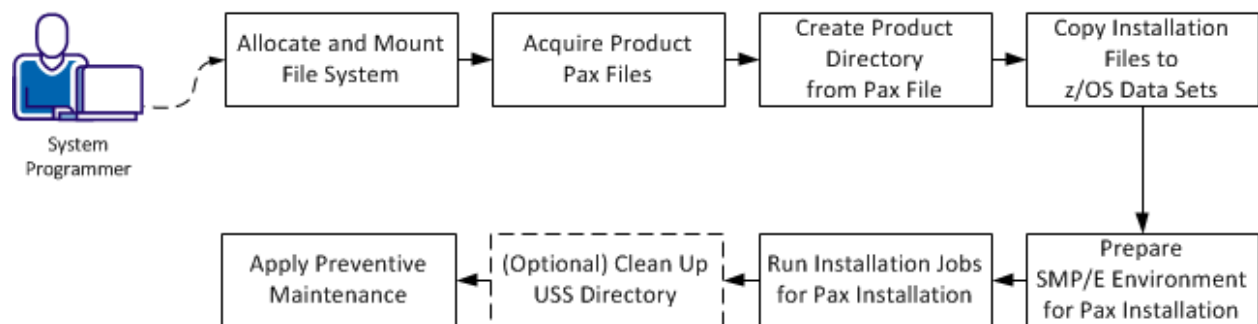
How to Install Your Product Using a Pax File

As a system programmer, your responsibilities include installing products on your mainframe system. With this option, you acquire a product pax file from <http://ca.com/support> or from a product DVD.

The DVD contains a folder that includes the pax file for the product. Product updates may have occurred after you acquired the product DVD. The files on the online site always have the most current product updates. To determine if you have the latest updates, go to <http://ca.com/support> and click Download Center.

You perform the following tasks to install a product with a pax file:

How to Install a Product Using a Pax File



1. Allocate and mount the file system.
2. Acquire the product pax files.
3. Create a product directory from the pax file.
4. Copy the installation files to z/OS data sets.

5. Prepare the SMP/E environment for a pax installation.
6. Run the installation job for a pax installation.
7. (Optional) Clean up the USS directory.
8. Apply preventive maintenance.

USS Environment Setup

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

- Receive product pax files from <http://ca.com/support>.
- Perform utility functions to unpack the pax file into MVS data sets that you can use to complete the product installation.

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

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

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

Important! Downloading pax files for the SMP/E installation as part of the Pax ESD process requires write authority to the UNIX System Services (USS) directories that are used for the Pax ESD process. In the file system that contains the Pax ESD directories, you also need free space approximately 3.5 times the pax file size to download the pax file and unpack its contents. For example, to download and unpack a 14 MB pax file, you need approximately 49 MB of free space in the file system hosting your Pax ESD directory.

Allocate and Mount a File System

The product installation process requires a USS directory to receive the pax file and to perform the unpack steps. We recommend that you allocate and mount a file system that is dedicated to the product acquisition and create the directory in this file system.

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

This procedure describes how to perform the following tasks:

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

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

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

Important! USS commands are case-sensitive.

Follow these steps:

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

- On a zFS, use the following sample:

```
//DEFINE EXEC PGM=IDCAMS
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//AMSDUMP DD SYSOUT=*
//SYSIN DD *
  DEFINE CLUSTER ( +
    NAME(your_zFS_data_set_name) +
    STORAGECLASS(class) +
    LINEAR +
    CYL(primary secondary) +
    SHAREOPTIONS(3,3) +
  )
/*
//FORMAT EXEC PGM=IOEAGFMT,REGION=0M,
// PARM=(' -aggregate your_zFS_data_set_name -compat')
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
//CEEDUMP DD SYSOUT=*
/*
```

- On an HFS, use the following sample:

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

The file system is allocated.

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

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

```
cd /u/maint/
mkdir CA
cd CA
mkdir CAPAX
```

Note: This document refers to this structure as *yourUSSpaxdirectory*.

The mount point is created.

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

- On a zFS, use the following sample:

```
MOUNT FILESYSTEM('your_zFS_data_set_name')
MOUNTPOINT('yourUSSpaxdirectory')
TYPE(ZFS) MODE(RDWR)
PARM(AGGRGROW)
```

- On an HFS, use the following sample:

```
MOUNT FILESYSTEM('your_HFS_data_set_name')
MOUNTPOINT('yourUSSpaxdirectory')
TYPE(HFS) MODE(RDWR)
```

The file system is mounted.

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

```
chmod -R 775 /yourUSSpaxdirectory/
```

Write access is granted.

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

Acquire the Product Pax Files

To begin the CA Technologies product installation procedure, copy the product pax file into the USS directory that you set up.

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

Use one of the following methods:

- Download the product pax file from <http://ca.com/support> to your PC, and then upload it to your USS file system.
If you download a zip file, you must unzip it before uploading to your USS file system.
- Download the pax files from <http://ca.com/support> directly to your USS file system.
- Download the pax file from the product DVD to your PC, and then upload the pax files to your USS file system.

This section includes the following information:

- A sample batch job to download a product pax file from the CA Support Online FTP server directly to a USS directory on your z/OS system
- Sample commands to upload a pax file from your PC to a USS directory on your z/OS system

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

Ensure that sufficient free space is available in the USS file system that you are using to hold the product pax file. If you do not have sufficient free space, error messages similar to the following appear:

```
EZA1490I Error writing to data set  
EZA2606W File I/O error 133
```

When the download finishes, the pax file size in your USS directory matches the value in the Size column for the corresponding pax file on the CA Technologies Products Download window.

Download Files to a PC Using Pax ESD

You can download product installation files from <http://ca.com/support> to your PC.

Follow these steps:

1. Log in to <http://ca.com/support>, and click Download Center.
The Download Center web page appears.
2. Under Download Center, select Products from the first drop-down list, and specify the product, release, and gen level (if applicable), and click Go.
The CA Product Download window appears.
3. Download an entire CA Technologies product software package or individual pax files to your PC. If you download a zip file, you must unzip it before continuing.

Note: For traditional installation downloads, see the *Traditional ESD User Guide*. For information about download methods, see the Download Methods and Locations article. Go to <http://ca.com/support>, log in, and click Download Center. Links to the guide and the article appear under the Download Help heading.

Download Using Batch JCL

You download a pax file from <http://ca.com/support> by running batch JCL on the mainframe. Use the sample JCL attached to the PDF file as CAtoMainframe.txt to perform the download.

Important! The PDF version of this guide includes sample JCL jobs that you can copy directly to the mainframe. To access these jobs, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click a file to view a sample JCL. We recommend that you use the latest version of Adobe Reader for viewing PDF files.

Note: We recommend that you follow the preferred download method as described on <http://ca.com/support>. This JCL procedure is our preferred download method for users who do not use CA CSM. We also include the procedure to download to the mainframe through a PC in the next section.

Follow these steps:

1. Replace *ACCOUNTNO* with a valid JOB statement.
The job points to your profile.
2. Replace *yourTCPIP.PROFILE.dataset* with the name of the TCP/IP profile data set for your system. Consult your local network administrators, if necessary.
The job points to your profile.
3. Replace *YourEmailAddress* with your email address.
The job points to your email address.

4. Replace *yourUSSpaxdirectory* with the name of the USS directory that you use for Pax ESD downloads.

The job points to your USS directory.

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

You have identified the product component to download.

6. Click Download for the applicable file.

Note: For multiple downloads, add files to a cart.

The Download Method window opens.

7. Click FTP Request.

The Review Download Requests window displays any files that you have requested to download.

Note: We send you an email when the file is ready to download or a link appears in this window when the file is available.

8. Select one of the following methods:

Preferred FTP

Uses CA Technologies worldwide content delivery network (CDN). If you cannot download using this method, review the security restrictions for servers that company employees can download from that are outside your corporate network.

Host Name: ftp://ftpdnloads.ca.com

Alternate FTP

Uses the original download servers that are based on Long Island, New York.

Host Name: ftp://scftpd.ca.com for product files and download cart files and ftp://ftp.ca.com for individual solution files.

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

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

9. Submit the job.

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

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

Example: CAtoMainframe.txt, JCL

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

```
//GETPAX JOB (ACCOUNTNO),'FTP GET PAX ESD PACKAGE',
//          MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to download a pax file directly from *
/* CA Support Online to a USS directory on your z/OS system.      *
/*                                                                *
/* When editing the JCL ensure that you do not have sequence numbers *
/* turned on.                                                    *
/*                                                                *
/* This job must be customized as follows:                       *
/* 1. Supply a valid JOB statement.                              *
/* 2. The SYSTCPD and SYSFTPD JCL DD statements in this JCL may be *
/* optional at your site. Remove the statements that are not    *
/* required. For the required statements, update the data set   *
/* names with the correct site-specific data set names.         *
/* 3. Replace "Host" based on the type of download method.      *
/* 4. Replace "YourEmailAddress" with your email address.       *
/* 5. Replace "yourUSSpaxdirectory" with the name of the USS    *
/* directory used on your system for Pax ESD downloads.        *
/* 6. Replace "FTP Location" with the complete path              *
/* and name of the pax file obtained from the FTP location     *
/* of the product download page.                                *
//*****
//GETPAX EXEC PGM=FTP,PARM=(EXIT',REGION=0M
//SYSTCPD DD DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSFTPD DD DSN=yourFTP.DATA.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//OUTPUT DD SYSOUT=*
//INPUT DD *
Host
anonymous YourEmailAddress
lcd yourUSSpaxdirectory
binary
get FTP_location
quit
```

Download Files to Mainframe through a PC

You download the product installation files to your PC and transfer them to your USS system.

Follow these steps:

1. Download the product file to your PC using one of the following methods:
 - Pax ESD. If you downloaded a zip file, first unzip the file to use the product pax files.
 - DVD. Copy the entire product software package (or individual pax files) to your PC.

The pax file resides on your PC.

Note: Do *not* change the format of the pax.Z.

2. Open a Windows command prompt.

The command prompt appears.

3. Customize and enter the following FTP commands:

```
FTP mainframe
userid
password
bin
lcd C:\PC\folder\for\thePAXfile
cd /yourUSSpaxdirectory/
put paxfile.pax.Z
quit
exit
```

mainframe

Specifies the z/OS system IP address or DNS name.

userid

Specifies your z/OS user ID.

password

Specifies your z/OS password.

C:\PC\folder\for\thePAXfile

Specifies the location of the pax file on your PC.

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

yourUSSpaxdirectory

Specifies the name of the USS directory that you use for Pax ESD downloads.

paxfile.pax.Z

Specifies the name of the pax file to upload.

The pax file is transferred to the mainframe.

Create a Product Directory from the Pax File

The pax command performs the following actions:

- Extracts the files and directories that are packaged within the pax file.
- Creates a USS directory in the same directory structure where the pax file resides.
- Automatically generates a product and level-specific directory name.

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

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

Use the sample JCL that is attached to the PDF file as [Unpackage.txt](#) (see page 41) to extract the product pax file into a product installation directory.

Important! The PDF version of this guide includes sample JCL jobs that you can copy directly to the mainframe. To access these jobs, click the paper clip icon at the left of the PDF reader. A window displaying attachments opens. Double-click a file to view a sample JCL. We recommend that you use the latest version of Adobe Reader for viewing PDF files.

Follow these steps:

1. Replace *ACCOUNTNO* with a valid JOB statement.
2. Replace *yourUSSpaxdirectory* with the name of the USS directory that you use for product downloads.

The job points to your specific directory.

3. Replace *paxfile.pax.Z* with the name of the pax file.

The job points to your specific pax file.

4. Submit the job.

The job creates the product directory.

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

Example: JCL File, Unpackage.txt, to Customize

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

```
//ESDUNPAX JOB (ACCOUNTNO), 'UNPAX PAX ESD PACKAGE',
// MSGCLASS=X, CLASS=A, NOTIFY=&SYSUID
//*****
/* This sample job can be used to invoke the pax command to create *
/* the product-specific installation directory. *
/* *
/* This job must be customized as follows: *
/* 1. Supply a valid JOB statement. *
/* 2. Replace "yourUSSpaxdirectory" with the name of the USS *
/* directory used on your system for Pax ESD downloads. *
/* 3. Replace "paxfile.pax.Z" with the name of the pax file. *
/* NOTE: If you continue the PARM= statement on a second line, *
/* start entering characters in column 16 and make sure *
/* the 'X' continuation character is in column 72. *
//*****
//UNPAXDIR EXEC PGM=BPXBATC,
// PARM='sh cd /yourUSSpaxdirectory/; pax -rvf paxfile.pax.Z'
/*UNPAXDIR EXEC PGM=BPXBATC,
/* PARM='sh cd /yourUSSpaxdirectory/; pax X
/* -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

Copy Installation Files to z/OS Data Sets

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

The file UNZIPJCL in the product directory contains a sample job to GIMUNZIP the installation package. You edit and submit the UNZIPJCL job to create z/OS data sets.

Follow these steps:

1. Locate and read the product readme file or installation notes, if applicable, which resides in the product-specific directory that the pax command created. This file contains the product-specific details that you require to complete the installation procedure.

You have identified the product-specific installation details.

2. Use ISPF EDIT or TSO ISHELL to edit the UNZIPJCL sample job. You can perform this step in one of the following ways:
 - Use ISPF EDIT. Specify the full path name of the UNZIPJCL file.
 - Use TSO ISHELL. Navigate to the UNZIPJCL file and use the E line command to edit the file.

The job is edited.

3. Change the SMPDIR DD PATH to the product-specific directory created by the pax command.

Your view is of the product-specific directory.

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

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

5. Change all occurrences of *yourHLQ* to the high-level qualifier (HLQ) for z/OS data sets that the installation process uses. We suggest that you use a unique HLQ for each expanded pax file to identify uniquely the package. Do *not* use the same value for *yourHLQ* as you use for the SMP/E RELFILES.

All occurrences of *yourHLQ* are set to your high-level qualifier for z/OS data sets.

6. Submit the UNZIPJCL job.

The UNZIPJCL job completes with a zero return code. Messages GIM69158I and GIM48101I in the output and IKJ56228I in the JES log are acceptable.

GIMUNZIP creates z/OS data sets with the high-level qualifier that you specified in the UNZIPJCL job. You use these data sets to perform the product installation. The pax file and product-specific directory are no longer needed.

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

Prepare the SMP/E Environment for Pax Installation

The members that are used in this procedure prepare the data sets, initialize the zones, and create the DDDEFs for CA OM Web Services.

Before you begin this procedure, confirm whether your product uses UNIX System Services (USS). If it does, establishing a hierarchical file system (HFS) may be required as part of the product installation or required as a feature of the product.

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

Follow these steps:

1. Customize the macro DUZSEDIT with your site-specific information and then copy the macro to your SYSPROC location. Replace the rightmost parameters for each ISREDIT CHANGE command. Each time you edit an installation member, type DUZSEDIT on the command line, and press Enter to replace the defaults with your specifications.

The macro is ready to customize the yourHLQ.SAMPJCL members.

Note: Set the DASD HLQ to the same value specified for yourHLQ for the unzip to DASD ESD JCL.

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

2. Open the SAMPJCL member DUZ1HOLD in an edit session and execute the DUZSEDIT macro from the command line.

DUZ1HOLD is customized.

3. Submit DUZ1HOLD.

This job produces the following results:

- A dataset is allocated, containing the error and fixcat HOLDDATA from CA Support Online.

4. Open the SAMPJCL member DUZ2ALL in an edit session and execute the DUZSEDIT macro from the command line.

DUZ2ALL is customized.

5. Submit DUZ2ALL.

This job produces the following results:

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

6. If your product requires HFS or if you want to install a feature of the product that requires HFS, complete the following substeps:

- a. Open the SAMPJCL member ccc1ALLU in an edit session and execute the DUZSEEDIT macro from the command line.

Note: All instances of ccc in this section indicate a three-character component code based on the FMID.

ccc2ALLU is customized.

- b. Submit ccc2ALLU.

This job allocates your HFS data sets.

- c. Open the SAMPJCL member ccc3MKD in an edit session and execute the DUZSEEDIT macro from the command line.

ccc3MKD is customized.

- d. Submit ccc3MKD.

This job creates all directories and mounts the file system.

7. Open the SAMPJCL member DUZ3CSI in an edit session and execute the DUZSEEDIT macro from the command line.

DUZ3CSI is customized.

8. Submit DUZ3CSI.

This job produces the following results:

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

9. If your product requires HFS or if you want to install a feature of the product that requires HFS, complete the following substeps:

- a. Open the SAMPJCL member ccc3CSIU in an edit session and execute the DUZSEEDIT macro from the command line.

ccc3CSIU is customized.

- b. Submit ccc3CSIU.

This job customizes the CSI by adding the DDDEFs associated with the directory.

Run the Installation Jobs for a Pax Installation

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

Note: The following steps include instructions to execute the [assign the value for hlq in your book]SEDIT macro each time you open a new SAMPJCL member. To edit all SAMPJCL members simultaneously, read and follow the instructions in the [assign the value for hlq in your book]AREAD member, and submit the [assign the value for hlq in your book]EDALL member.

Follow these steps:

1. Open the SAMPJCL member DUZ3RECD in an edit session, and execute the DUZSEDIT macro from the command line.
DUZ4RECD is customized.
2. Submit DUZ4RECD to receive SMP/E base functions.
Your product is received and now resides in the global zone.
3. Open the SAMPJCL member DUZ5APP in an edit session, and execute the DUZSEDIT macro from the command line.
DUZ5APP is customized.
4. Submit DUZ5APP to apply SMP/E base functions.
Your product is applied and now resides in the target libraries.
5. Open the SAMPJCL member DUZ6ACC in an edit session, and execute the DUZSEDIT macro from the command line.
DUZ6ACC is customized.
6. Submit DUZ6ACC to accept SMP/E base functions.
Your product is accepted and now resides in the distribution libraries.

Clean Up the USS Directory

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

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

- Pax file
- Product-specific directory that the pax command created and all of the files in it
- SMP/E RELFILES, SMPMCS, and HOLDDATA MVS data sets

These data sets have the HLQ that you assigned in the UNZIPJCL job.

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

Follow these steps:

1. Navigate to your Pax ESD USS directory.
Your view is of the applicable USS directory.
2. Delete the pax file by entering the following command:

```
rm paxfile
```

paxfile

Specifies the name of the CA Technologies pax file that you downloaded.

The pax file is deleted.

3. Delete the product-specific directory by entering the following command:

```
rm -r product-specific_directory
```

product-specific_directory

Specifies the product-specific directory that the pax command created.

The product-specific directory is deleted.

Note: You can also use TSO ISHELL to navigate to the pax file and product-specific directory, and delete them using the D line command.

Apply Preventive Maintenance

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

CA Support Online at <http://ca.com/support> has maintenance and HOLDDATA published since the installation data was created. After the maintenance process completes, the product is ready to deploy.

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

Note: To review the CA Technologies mainframe maintenance philosophy, see your *Best Practices Guide* or visit the [CA Next-Generation Mainframe Management page](#).

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

Follow these steps:

1. Check the Download Center at <http://ca.com/support> for PTFs that have been published since this release was created. If the base release was created recently, no PTFs will have been published yet. If PTFs exist, add published solutions for your product to your Download Cart, and click Checkout.

2. Specify that you want a complete package.

When processing completes, a link appears on the Review Download Requests page. You also receive an email notification.

3. Click the Alternate FTP link for your order to obtain FTP login information and the ZIP file location. Download the ZIP file into a USS directory on your z/OS system.

4. Run the CAUNZIP utility.

CAUNZIP unzips the package of published solutions and creates a SMPNTS file structure that the SMP/E RECEIVE FROMNTS command can process. For sample JCL to run the utility that is located in *yourHLQ.CAWOJCL(CAUNZIP)*, see the *CA Common Services for z/OS CAUNZIP Administration Guide*. After execution completes, the ZIPRPT data set contains the summary report. The summary report does the following:

- Summarizes the content of the product order ZIP file.
 - Details the content of each data set and the z/OS UNIX files produced.
 - Provides a sample job to receive the PTFs in your order.
5. Review the sample job that is provided in the CAUNZIP output ZIPRPT file. Cut and paste the JCL into a data set, specify your SMP/E CSI on the SMPCSI DD statement and submit the job to receive the PTFs in your order.

6. Verify that you have the values from the base installation in the DUZSEDIT macro that was customized in the installation steps.
7. Open the SAMPJCL member DUZ1HOLD in an edit session and execute the DUZSEDIT macro from the command line.
Note: Update DUZ1HOLD SAMPJCL to receive the HOLDDATA file.
DUZ1HOLD is customized.
8. Submit DUZ1HOLD.
The job downloads and receives the external HOLDDATA file.
9. Open the SAMPJCL member DUZ7RECH in an edit session and execute the DUZSEDIT macro from the command line.
DUZ7RECH is customized.
10. Submit DUZ7RECH.
The job receives the external HOLDDATA file.
11. Open the SAMPJCL member DUZ8APYP in an edit session and execute the DUZSEDIT macro from the command line.
DUZ8APYP is customized.
12. Submit DUZ8APYP.
The PTFs are applied.
13. (Optional) Open the SAMPJCL member DUZ9ACCP in an edit session and execute the DUZSEDIT macro from the command line.
DUZ9ACCP is customized.
14. (Optional) Submit DUZ9ACCP.
The PTFs are accepted.
Note: You do not have to submit the job at this time. You can accept the PTFs according to your site policy.

HOLDDATA

When you apply maintenance, you typically encounter SMP/E HOLDDATA. We use HOLDDATA to notify your SMP/E system of SYSMODs that have errors or special conditions. We support system and external HOLDDATA.

System HOLDDATA

System HOLDDATA indicates data that is an in-stream part of the SYSMOD, informing you of special conditions. The following reasons are used with SYSTEM HOLDDATA for CA OM Web Services:

ACTION

Indicates that you must perform special processing before or after you apply this SYSMOD.

AO

Affects automated operations. It changes either the message identifier or the displacement of a field inside the message.

DB2BIND

Indicates that DBRMs have changed and packages need to be rebound.

DDDEF

Indicates that data sets and DDDEFs are being added or modified.

DELETE

Deletes the SYSMOD load module. You cannot reverse this type of SYSMOD with the SMP/E RESTORE command.

DEP

Indicates a dependency for this SYSMOD that you must externally verify.

DOC

Indicates a documentation change with this SYSMOD.

DYNACT

Describes the steps to dynamically activate this fix without performing an IPL.

EC

Indicates that this SYSMOD requires a hardware engineering change. An EC hold SYSMOD usually does not affect the product unless the EC is present on the hardware device.

ENH

Introduces a small programming enhancement. The hold contains the instructions to implement the enhancement. If no action is needed to implement the enhancement, give a summary of the enhancement.

EXIT

Indicates that changes delivered by this SYSMOD require reassembly of user exits.

EXRF

Indicates that the SYSMOD must be installed in both the Active and Alternate Extended Recovery Facility Systems.

IPL

Indicates that an IPL is required for this SYSMOD to take effect. This is used only when there is no alternative for dynamic activation.

MSGSKEL

Indicates that the SYSMOD contains internationalized message versions that must be run through the message compiler for each language.

MULTSYS

Apply this SYSMOD to multiple systems for either pre-conditioning, coexistence, or exploitation.

RESTART

Indicates that after applying this SYSMOD, the site must perform a special restart as opposed to a routine restart.

SQLBIND

Indicates that a bind is required for a database system other than DB2.

SYSMOD

Indicates that some or all of the elements that this SYSMOD delivers are to be downloaded to a workstation.

Code a bypass operand on your APPLY command to install SYSMODs that have internal holds. Code the bypass operand only after you have performed the required action, or if you are performing the action after the APPLY, if that is appropriate.

External HOLDDATA

External HOLDDATA is not part of the PTF. The HOLDDATA resides in a separate file. The HOLDDATA is commonly used for SYSMODs that have been distributed and later are discovered to cause problems.

Download the external HOLDDATA from CA Support to a DASD file, and allocate the file to the SMPHOLD DD statement. To take care of the external HOLDDATA, receive it into your SMP/E environment. SMP/E receives the HOLDDATA from CA-supplied jobs.

If a SYSMOD has an unresolved hold error, SMP/E does not install it unless you add a bypass to your APPLY command. You can bypass an error hold in situations that are not applicable to you. Error holds that are not applicable to you can include a problem that happens only with a hardware device that you do not have or in a product feature that you do not use.

When CA Technologies publishes a SYSMOD that resolves the hold, the resolving SYSMOD supersedes the hold error. This action lets you apply the original SYSMOD in conjunction with the fixing SYSMOD.

A special HOLDDATA class that is called ERREL exists. We have determined that the problem fixed by the SYSMOD is more important than the one that it causes. We recommend that you apply these SYSMODs.

The only manual task is running a REPORT ERRSYSMODS. This report identifies the following:

- Any held SYSMODs already applied to your system
- Any resolving SYSMODs that are in RECEIVE status

SMP/E identifies the SYSMOD to apply to correct the situation.

Chapter 4: Installing CA OM Web Services with InstallAnywhere

This section contains information about:

- Installing the CA OM Web Services with InstallAnywhere.

This section contains the following topics:

[Supported Platforms](#) (see page 53)

[Locate the Product Installer](#) (see page 54)

[InstallAnywhere Installation of CA OM Web Services on Windows](#) (see page 55)

[InstallAnywhere Installation of CA OM Web Services on Other Platforms](#) (see page 57)

[Installation Logging](#) (see page 59)

Supported Platforms

CA OM Web Services is a Java application that must be run on a Java virtual machine (JVM). Therefore, we expect that a Java-enabled operating environment with a supported version of the Java Runtime Environment is installed.

Supported Platforms Include:

- Windows
- Linux
- z/Linux
- AIX
- HP-UX PA
- HU-UX IA
- Solaris
- USS (InstallAnywhere or SMP/E)

Note: For more information about USS installation with SMP/E, see [Installing CA OM Web Services with SMP/E \(USS\)](#) (see page 23).

Locate the Product Installer

CA OM Web Services is shipped on a DVD and can also be downloaded from the CA Support website.

Note: For more information about installing your product with SMP/E, see [Installing CA OM Web Services with SMP/E \(USS\)](#) (see page 23).

Installing your Product on the USS

[Installing CA OM Web Services with SMP/E \(USS\)](#) (see page 23)

Use a Web Browser

You can locate the correct CA OM Web Services installer through a web browser.

Follow these steps:

1. Download the ISO file
2. Mount/Extract the ISO file using an ISO reader of your choice.
3. Open install.htm in a web browser.
4. Choose an installer according to your operating environment.
5. Click to download the installer.

Use the DVD

From the DVD disk, follow these steps:

Follow these steps:

1. Open the folder InstData.
2. Locate a folder from the following list that is based on your operating environment:
 - Windows For Windows or Windows_x64
 - Multiplatform For all other platforms

Note: For more information about the SMP/E installation see [Installing CA OM Web Services with SMP/E \(USS\)](#) (see page 23).

InstallAnywhere Installation of CA OM Web Services on Windows

CA OM Web Services can be installed on the Windows platform.

Important! A valid JVM must be pre-installed on the system before running the installer. You can acquire a JVM from the vendors, such as IBM, Oracle, HP, or Apple.

Installation Using the GUI Wizard

On the Windows platform CA OM Web Services can be installed using a GUI.

Follow these steps:

1. Review the Introduction panel for information about the Installer and click Next.
2. Review the license agreement.
3. Scroll down, select the I accept...option and click Next.
4. Specify the folder where you want to install CA OM Web Services.

This folder contains the files that the installer generates.

5. Select a Java VM you want to use for the Configuration and System Test Tools.

The installer searches for existing Java virtual machines (VMs) from default folders on the system. You can click Search Another Location... to search other folders or click Choose Java Executable... to select a particular Java executable.

6. Select Deployment Method

You can select CA OM Web Services to be deployed as either a WAR or EAR file.

Note: For information about the correct format for your Java Web Application Server, see the Java Web Application Server documentation.

7. Review the settings that are displayed in the Pre-Installation Summary.
8. Click Install.
9. (Recommended) Select Whether to Launch Configuration Tool.

Note:

- After the installation is finished, the Configuration Tool pops up in a separate Window.
- The CA OM Web Services 2.0 Configuration Tool can be rerun.

10. Review the Installation Complete Summary.

Note: If your install had warnings or non fatal errors then you receive a summary message that starts with Warning or Non Fatal Failure. In this case, more information can be found in your install log, after finishing and closing the installer.

11. Click Done.

Note: If you chose to Launch Configuration Tool, it pops up in a separate Window when the installer closes. Instructions for the Configuration Tool are listed in a different section.

InstallAnywhere Installation of CA OM Web Services on Other Platforms

CA OM Web Services can be installed using console mode on these platforms:

- Linux
- z/Linux
- AIX
- HP-UX PA
- HU-UX IA
- Solaris
- USS

Important! A valid JVM must be preinstalled on the system before running the installer. You can acquire a JVM from the vendors, such as IBM, Oracle, HP, or Apple.

Installation Using the Console Mode

To install using the Console mode, follow these steps.

Follow these steps:

1. Review the Introduction.
2. Press Enter to continue.
3. Review the License Agreements.
4. Press Enter until you reach the end of the license agreement.

You are prompted with the message:

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N):

5. Enter Y to accept the license agreement.
6. Specify where you want to install CA OM Web Services.

Do one of the following:

- Press Enter to use the default folder.
- Enter a path to a specific folder.

This folder contains the files that are generated by the installer.

7. Select the Java Virtual Machine you want the installed CA OM Web Services to use.

Do one of the following:

- Enter 1 to have the installer search for existing Java VMs (virtual machine) from default folders on the computer.
- Specify the full path including the file name of your Java executable.

For example, `/usr/bin/java` or

`/sys/java64bt/v6r0m0/usr/lpp/java/J6.0_64/bin/java`

8. Select Deployment Method.

You can select CA OM Web Services to be deployed as either WAR or EAR file.

Note: For more information about the correct format for the Java Web Application Server, see your Java Web Application Server documentation.

9. Review the settings that are displayed in the Pre-Installation Summary.
10. Press Enter.
11. (Recommended) Select Whether to Launch Configuration Tool.

Note:

- The Configuration Tool opens in the same terminal, after you finish the installation.
- The CA OM Web Services 2.0 Configuration Tool can be rerun.

12. Review the Installation Complete Summary.

Note: If your install had warnings or non-fatal errors, you receive a summary message that starts with Warning or Non-Fatal Failure. In this case, more information can be found in your install log, after finishing and closing the installer and optionally the Configuration Tool.

13. Press Enter.

Note: If you chose to Launch Configuration Tool, it starts in the same terminal. Instructions for the Configuration Tool are listed in a different section.

14. Press Enter.

Installation Logging

This section provides you with instructions of how to review the logs that are produced by the installation of CA OM Web Services.

Note: When the installation summary starts with Warning, or Non-fatal Error the information about the error is logged in the installation logs.

Log Locations

There are three primary logs that are produced by CA OM Web Services installation.

- Primary Install Log
- Install Standard Out
- Install Standard Error

Log	File Name
Primary Install Log	CA_Output_Management_Web_Services_2.0_Install_<date_time>.log
Install Standard Out	ws_install_stdout.txt
Install Standard Error	ws_install_stderr.txt

Primary Install Log

The main install log is placed in:

```
$USER_INSTALL_DIR$\uninstaller\install_update_logs\
```

Note: If there is a failure early in the installation, or you cancel the installation then the log file is placed in your Home folder in USS/Unix/Linux or in the Desktop on Windows.

The filename for the primary install log is:

```
CA_Output_Management_Web_Services_2.0_Install_03_22_2013_12_21_57.log
```

Install Standard Out

The install standard out log is placed in:

```
$USER_TEMP$\ws_install_stdout.txt
```

Note: The temp folder can be found on the Windows by typing `echo %TEMP%` in the command prompt. The temp folder on USS/Unix/Linux systems is often `/tmp`.

Install Standard Error

The installation standard error is placed in:

```
$USER_TEMP$\ws_install_stderr.txt
```

Note: The temp folder can be found on Windows by typing `echo %TEMP%` in the command prompt. The temp folder on USS/Unix/Linux systems is `/tmp`.

Chapter 5: Uninstalling CA OM Web Services

This section contains instructions for uninstalling CA OM Web Services.

This section contains the following topics:

[Uninstall](#) (see page 61)

Uninstall

This section guides you through uninstalling the product on the different platforms for all InstallAnywhere installs.

Note: The SMP/E install does not have an uninstaller. Follow the standard SMP/E procedure to remove an SMP/E install.

Launch the Uninstaller

This section of the document helps you launch the uninstaller.

Follow these steps:

1. Find the uninstaller.
 - Windows: Find the uninstaller shortcut in the programs menu.
 - Other operating systems: Under the uninstaller folder in your install directory, find `uninstaller` or `uninstaller.jar` and run it. For example, type `./uninstaller` or `java -jar ./uninstaller.jar` under this folder.
2. Run the uninstaller.

Like the installer, CA OM Web Services uninstaller can be run in either GUI mode or Console mode. Follow the instructions that the wizard gives.

Uninstall on Windows

This section guides you through uninstalling the product on the Windows platform.

Note: If an administrator or a different user installed the product, try uninstalling by running the uninstaller as administrator.

Follow these steps:

1. Do one of the following:
 - Programs -> CA -> CA OM Web Services -> Uninstaller
 - All Programs -> CA -> CA OM Web Services -> Uninstaller
2. Do one of the following:
 - Click Uninstaller.
 - Right-click Uninstaller and Click Run as Administrator.

Note: If an administrator or a different user installed the product, try uninstalling by running the uninstaller as administrator.

A Success or Failure message is displayed.

Note: In case of some failure, certain files may not be deleted and may be listed.

3. Click Done.
4. (Optional) Manually delete your configuration backup folder.

Default:

<Install Location>\OM_WS_Config_Backup

Note: Since the Configuration Tool creates this folder, not the installer, the uninstaller does not delete it.

Uninstall on Other Platforms

This section guides you through uninstalling the product on Other Platforms for the InstallAnywhere install.

Note: The SMP/E install does not have an uninstaller. Follow standard SMP/E procedure to remove an SMP/E install.

Follow these steps:

1. Navigate to the uninstaller folder.

<Install Location>\uninstaller

2. Run the command `java -jar uninstaller.jar`.

The uninstaller should start.

Note: On the USS/Unix/Linux system, you must have the authority to delete the installed files, to run the uninstaller successfully. If you do not have the correct group or user access, be sure to use root or pseudo to run the uninstaller.

3. Press Enter to continue with the uninstall.

A Success or Failure message is displayed.

4. (Optional) Manually delete your configuration backup folder.

Default:

<Install Location>\OM_WS_Config_Backup

Note: Because the Configuration Tool creates the backup folder, not the installer, the uninstaller does not delete it.

Chapter 6: Post-Installation and Configuration Tasks

This section guides you through post-installation and configuration tasks for the CA OM Web Services.

Prerequisites:

- The TCP/IP address or the name and port number for the CAICCI Server to which you are connecting.
- CA Event Notification Facility (CAIENF) System ID.
- DRAS Server ID.
- DRAS Repository Names.

Checklist of post- installation:

- Test for successful installation of the CA OM Web Services.
- Configure CA International Common Communications Interface (CAICCI).
- Assign a DRAS LMP License Server.
- Create repository definitions for repositories you want to include in CA OM Web Services.
- Create Report List Data Dictionary (RLDD) entries.

This section contains the following topics:

[Configure CA OM Web Services](#) (see page 65)

[Prepare your Java Web Application Server](#) (see page 81)

[Deploy CA OM Web Services](#) (see page 85)

[Verify Installation](#) (see page 87)

Configure CA OM Web Services

This section describes what to know and do to configure CA OM Web Services.

Running the Configuration Tool (Interactive Mode)

You can change the initial configuration settings with the configuration tool available in CA OM Web Services.

After the product installation the configuration tool is located in the <product install>/utilities directory. This tool is used to modify settings in the following sections: CCI, License Server, and CA OM Web Services repositories. The configuration tool also lets you to generate the report list data dictionary.

You can execute "Configure_Web_Services" to use all functions or execute "Change_CCI_Settings", "Change_License_Server", "Change_Repository_Settings", or "Create_RLDD" to modify each individual section.

Note:

- You can run only one copy of the Configuration Tool at one time.
- The Windows users must run the configuration tool as an administrator, or a member of the administrator group if the install was run by the administrator.
 - Press SHIFT, right-click the configuration tool, and then select Run as administrator or Run as different user.
- The USS users can use ssh or telnet to connect to USS (if ssh or telnet connection is supported) or use OMWS to gain access to a USS console.
- The Configuration Tool is optionally run after the installer.

After the configuration tool is launched, it prompts you for the target CA OM Web Services package. Press Enter to use the default package or specify a CA OM Web Services package at a different location. The default package is the one installed from your initial installation.

Note: Since the package for updating is an EAR or a WAR file, you redeploy the archive after the update. The tracing information is available in the logs subfolder of the utilities folder.

More information:

[Configure CAICCI](#) (see page 69)

[Configure the License Server](#) (see page 70)

[Create or Manage Repository Definitions](#) (see page 71)

[Configuration Tracing](#) (see page 79)

Launch Configuration Tool HP/UX

Execute the desired command in the following format:

```
sh ./Configure_Web_Services
```

Launch Configuration Tool HP-UX IA64

Execute the desired command in the following format:

```
sh ./Configure_Web_Services
```

Launch Configuration Tool zLinux

Execute the desired command in the following format:

```
sh ./Configure_Web_Services
```

Launch Configuration Tool AIX

Execute the desired command in the following format:

```
sh ./Configure_Web_Services
```

Launch Configuration Tool Sun Solaris

Execute the desired command in the following format:

```
sh ./Configure_Web_Services
```

Launch Configuration Tool USS

Execute the desired command in the following format:

If you used SMP/E install:

```
Configure_Web_Services.sh
```

If you used InstallAnywhere install:

```
Configure_Web_Services
```

Launch Configuration Tool Windows

Execute the desired command by double clicking:

```
Configure_Web_Services.exe
```

Launch Configuration Tool Linux PC

Execute the desired command in the following format:

```
sh ./Configure_Web_Services
```

Configuration Tool First Steps

The CA OM Web Services Configuration Tool, in interactive mode, includes the following four sections:

- CCI Settings
- License
- Repository Inclusion and Setup
- Create Report List Data Dictionary.

Note: To configure and run all four sections, run "Configure_Web_Services".

Follow these steps:

1. Launch the Configure_Web_Services application to run all the sections of the interactive configuration tool.
2. Enter the location of the WAR, or EAR file.
3. Select backup folder location.

Note: If your selected backup folder location does not exist, you are prompted to create a configuration backup folder.

4. Load configuration settings from either the webapp or backup location.

Note: The loaded settings are the default settings that are listed in the configuration tool.

More information:

[Running the Configuration Tool \(Interactive Mode\)](#) (see page 66)

[Configuration Tracing](#) (see page 79)

Configure CAICCI

The CAICCI (CA International Common Communications Interface) is required for CA OM Web Services to connect to the host CA OM product (CA View®, CA Dispatch™, or CA Bundl®) repositories. Instances of CAICCI are installed as the servers and configured to communicate with other CAICCI servers running on the network. CA OM Web Services uses a CAICCI client that must be configured to allow communications with a single CAICCI server.

Because the CAICCI servers communicate with each other, CAICCI lets each server query for a list of running CA OM product repositories. Also, CAICCI allows all other CA OM Web Services communicate with other CA OM product repositories.

The CAICCI settings include CCI Server name, port, and System ID.

Follow these steps:

1. Launch either `Configure_Web_Services` or `Change_CCI_Settings`.
Follow the steps that are listed at *Running the Configuration Tool*.
2. Enter the Server Name or TCP/IP address for your CCI server.
3. Enter the Port number of your CCI server.
4. (Optional) Enter the System ID for accessing CCI.
5. (Optional) Test the CCI Connection.
A connection success or failure message is displayed.
6. Select Continue to Next Section to proceed to the DRAS LMP License Server Information section.

More information:

[Running the Configuration Tool \(Interactive Mode\)](#) (see page 66)

[Configuration Tool First Steps](#) (see page 68)

[Configuration Tracing](#) (see page 79)

Configure the License Server

CA OM Web Services uses CA Distributed Repository Access System (CA DRAS) server to act as its License Management Program (LMP) license check server.

Follow these steps:

1. Launch either `Configure_Web_Services` or `Change_License_Server`.
2. Follow the steps that are listed in [Configuration Tool First Steps](#) (see page 68).
3. (Optional) Complete the CCI Section.

Note: CCI Section is required only with the `Configure_Web_Services` launch.

4. Do one of the following processes:

- Select a DRAS server from the available license servers. This server acts as your license server.

Note: The list of available license servers is available only if you have previously entered valid CCI information. If you want to enter CCI information, launch either `Configure_Web_Services` or `Change_CCI_Settings`.

- Select Enter DRAS Domain. You can then type the domain of the DRAS server that you want to use for the license verification.

The domain format of a DRAS server is:

ENFSYSID:DRASSERV,

where,

ENFSYSID

It is the CA Event Notification Facility System ID.

DRASSERV

It is the DRAS server ID.

- Select No Change, to not change license server setting.

More information:

[Configure CAICCI](#) (see page 69)

[Running the Configuration Tool \(Interactive Mode\)](#) (see page 66)

[Configuration Tool First Steps](#) (see page 68)

[Configuration Tracing](#) (see page 79)

Create or Manage Repository Definitions

Repository definitions identify each repository that the CA OM Web Services accesses. You must specify an entry for each repository that the Web Service accesses in the repository definition file. The repository definition process can be accomplished using the configuration tool.

Important! If you want to migrate repositories from CA OM Web Services 1.0 installation, see [Migration Information](#) (see page 101) before continuing with this section.

Open Repository Settings

Using the CA OM Web Services Configuration Tool, you can list the current repositories that are defined to CA OM Web Services, remove, add, and update repositories.

Follow these steps:

1. Launch either `Configure_Web_Services` or `Change_Repository_Settings`.
2. Follow steps that are listed at [Configuration Tool First Steps](#) (see page 68).
3. (Optional) Complete CCI and the License Server sections, if running `Configure_Web_Services`.

When the Repository Settings Section opens you can see a list of several options, including a Continue to Next Section option. You can repeat the other options as required, and can then exit from this section by selecting Continue to Next Section.

4. (Optional) Run one or more of the following:
 1. Insert Repository
 2. List Current Repositories
 3. Remove a Repository
 4. Update a Repository.
5. Select Continue to Next Section.

The Create Report List Data Dictionary Entries section opens.

More information:

[Configure CAICC!](#) (see page 69)

[Running the Configuration Tool \(Interactive Mode\)](#) (see page 66)

[Configuration Tool First Steps](#) (see page 68)

[Insert a Repository](#) (see page 72)

[List Current Repositories](#) (see page 74)

[Remove a Repository](#) (see page 75)

[Update a Repository](#) (see page 76)

[Configuration Tracing](#) (see page 79)

Insert a Repository

To add a repository definition to the repository definition file, you have to use the Configuration Tool. The following repository information must be entered to add it into CA OM Web Services:

Name

Specifies the name to call the repository in CA OM Web Services. The name provided to the configuration tool is how the configuration tool refers to the repository in the future.

Repository Domain

Refers to the Domain. The three-part entities that identify each Host OM Product repository accessible on the network.

Repository Description

The repository description is a reminder of the intended function of this repository reference.

Repository Type

View – CA View®

Bundl -- CA Bundl®

Dispatch – CA Dispatch™

Repository Release

The release number of your host OM system (CA View®, CA Bundl®, or CA Dispatch™).

Follow these steps:

1. Follow the instructions listed in the section Open Repository Settings and navigate to the Repository Settings menu.
2. Select Insert a Repository.
3. Do one of the following to insert a repository:
 - Select a Repository to add from the list of available repositories.
Note: The list displays all the available repositories if you have already entered valid CCI information. If you need to enter CCI information, launch either `Configure_Web_Services` or `Change_CCI_Settings`.
 - Select Enter Domain Information.
 - Select Do Not Add a Repository.
Note: If you select this option you are navigated to the main Repository Settings menu.
4. Do one of the following to enter a repository name:
 - Type a Repository Name.

- Press Enter to use the default name.

Note:

- A default name is available only if you selected a repository from the available repositories list.
- You can add the same repository twice, if you refer to it with a different name.

5. Do one of the following to enter a repository domain:

- Type a Repository domain.

The domain format of a repository is:

```
ENFSYSID:DRASSERV:REPSNAME;
```

where,

ENFSYSID

Specifies the CA Event Notification Facility System ID.

DRASSERV

Specifies the DRAS server ID.

REPSNAME

Specifies the repository name as defined in DRAS by the ACCESS REPOSITORY statement.

- Press Enter to use the default domain.

Note:

- A default domain is available only if you selected a repository from the available repository list.

6. Do one of the following to enter a repository description:

- Enter a Repository description.
- Press Enter to use the default domain.

Notes:

- A default description is available only if you selected a repository from the available repository list.
- The repository description is a reminder of the intended function of this repository reference.

7. Select a Repository Type (CA View®, CA Bundl®, or CA Dispatch™).

8. Enter the Repository Release. Specify the release number in the format N.N (For example, CA View® r12.0 would be 12.0).

After entering this information, a success or failure message displays. For example COMMND999I: Repository Command completed successfully.

9. (Optional) Repeat from step 2 to add a new repository.

Note:

- You can add the same repository twice, if you refer to it with a different name.

10. Select Continue to Next Section.

After making changes to the Repository Definitions the Create Report List Data Dictionary appears.

More information:

[Create Report List Data Dictionary Entries](#) (see page 77)

[Open Repository Settings](#) (see page 71)

[Configuration Tracing](#) (see page 79)

List Current Repositories

You can list repositories that are already defined to CA OM Web Services. The configuration tool lists each repository's name and description.

Follow these steps:

1. Following the instructions that are listed in the Open Repository Settings you can navigate to the Repository Settings menu.
2. Select List Current Repositories.
A list of each repository that is defined to CA OM Web Services is listed.
3. Click Continue to Next.

After making changes to the Repository Definitions the Create Report List Data Dictionary appears.

More information:

[Create Report List Data Dictionary Entries](#) (see page 77)

[Open Repository Settings](#) (see page 71)

[Configuration Tracing](#) (see page 79)

Remove a Repository

You can remove repositories from the CA OM Web Services repository definition file.

Note: The actual repositories are unaffected.

Follow these steps:

1. Following the instructions listed in the section Open Repository Settings navigate to the Repository Settings menu.

2. Select Remove a Repository.

A numbered list of repositories is displayed. Each repository is listed in the following format: Name - Description.

3. Do one of the following:

- Enter the number of the repository you want to remove
- Enter the number for the Do Not Delete a Repository option

After entering this information a success or failure message is displayed. For example, COMMND999I: Repository Command completed successfully.

4. (Optional) Repeat steps 2 and 3 for each repository you want to delete.
5. Select Continue to Next Section.

After making changes to the Repository Definitions the Create Report List Data Dictionary appears.

Update a Repository

If required you can update an existing repository in CA OM Web Services.

Follow these steps:

1. Following the instructions that are listed in the section Open Repository Settings navigate to the Repository Settings menu.

2. Select Update a Repository.

A numbered list of repositories is displayed.

3. Do one of the following:

- Select a repository to update.
- Select Do Not Update a Repository.

Note: This option returns you to the main Repository Settings Menu.

4. Do one of the following for the repository domain:

- Enter a Repository Domain.

The domain format of a repository is:

ENFSYSID:DRASSERV:REPSNAME;

where

ENFSYSID

Specifies the CA Event Notification Facility System ID.

DRASSERV

Specifies the DRAS server ID.

REPSNAME

Specifies the repository name as defined in DRAS by the ACCESS REPOSITORY statement.

- Press Enter to retain the existing domain.

5. Do one of the following for the repository description:

- Enter a Repository Description.
- Press Enter to retain the existing description.

Note: The repository description is a reminder of the intended function of this repository reference.

6. Do one of the following to set the repository type:

- Select a Repository Type (CA View®, CA Bundl®, or CA Dispatch™).
- Press Enter to retain the existing type.

7. Do one of the following to set the repository release:

- Enter the Repository Release

Specify release numbers in the format N.N (for example, CA View® r12.0 would be 12.0).

- Press Enter to retain the current release number.

After entering this information, you can see a success or failure message, such as COMMND999I: Repository Command completed successfully.

8. (Optional) Repeat steps 2 through 8 for each repository you want to update.
9. Select Continue to Next Section.

After making changes to the Repository Definitions the Create Report List Data Dictionary menu appears.

More information:

[Open Repository Settings](#) (see page 71)

[Insert a Repository](#) (see page 72)

[Configuration Tracing](#) (see page 79)

Create Report List Data Dictionary Entries

The Report List Data Dictionary is an XML formatted file that includes an entry for each repository that is defined in the Repository Definition File. Each entry in the Report List Data Dictionary file defines internal information about the fields that are supported for the CA OM Web Services requests. The matching name entries in the Report List Data Dictionary and the Repository Definition File are required to process requests to the CA OM Web Services for each repository.

Before creating the Report List Data Dictionary for the Web Service, ensure at least one valid repository entry is defined to CA OM Web Services.

Create or re-create a Report List Data Dictionary when:

- Initially installing the CA OM Web Services
- Adding a repository definition to the repository definition file
- Installing a new release of a Host OM repository, which requires redefining the repository definitions of the repositories that CA OM Web Services accesses

When the Create Report List Data Dictionary section of the CA OM Web Services Configuration Tool is run, the repository definitions that exist in the Report List Data Dictionary (RLDD) are updated as they are encountered. Also the entries for new repositories are inserted.

Create Report List Data Dictionary Entries Procedure

You are prompted to generate the RLDD after editing the repository entries, from either `Configure_Web_Services`, or `Change_Repository_Settings`. You can also directly generate the RLDD by launching `Create_RLDD`.

Notes:

- To generate the Report List Data Dictionary requires a valid user name and password for each repository (CA View®, CA Bundl®, CA Dispatch™), you added to the CA OM Web Services.
- CCI Server and Port information are required to generate the Report List Data Dictionary. Run the CCI tool at least once before Generating the Report List Data Dictionary.

Follow these steps:

1. Launch either `Configure_Web_Services`, `Change_Repository_Settings`, or `Create_RLDD`.
2. Follow the steps that are listed in [Configuration Tool First Steps](#) (see page 68).
3. (Optional) Complete CCI, License Server, and/or Repository Management, if running `Configure_Web_Services` or `Change_Repository_Settings`.

The Create Report List Data Dictionary Entries section appears.

4. Do one of the following to trigger the generation:

- Select *Enter the same password* for each repository.

This option uses a single password for each repository.

Note: This option is useful if all your repositories use external security or you synchronize user names and passwords in some way other than external security.

- Select *Enter individual passwords* for each repository.

This option lets you specify a different password for each repository. A repository name is displayed and you are prompted to enter a user name and password. Repeat the step for each repository.

- Select *Do not generate report list data dictionary*.

This option allows you to continue to the next section without Generating the Report List Data Dictionary.

After entering all the Repository user names and passwords, a failure or success message is displayed.

If all updates, were successful the program automatically continues to the next section: Save Configuration Changes.

Otherwise, the Create Report List Data Dictionary Failure Options menu appears and you can then continue to Step 5.

5. Do one of the following to re-create the repository entries:

- Select Retry Create Report List Data Dictionary.

This option lets you go to the previous menu, the Create Report List Data Dictionary Entries Menu, so that you can reenter user names and passwords.

- Change Your Repository Entries.

This option lets you return to the Repository Settings menu. You can change or remove repository entries that cause the creation of the Report List Data Dictionary failure.

Note: This option is only available from Configure_Web_Services or Change_Repository_Settings.

- Click Continue to Next Section.

Important If the RLDD generation fails you cannot access CA OM Web Services or access certain repositories that are defined to it.

More information:

[Create Report List Data Dictionary Entries](#) (see page 77)

[Running the Configuration Tool \(Interactive Mode\)](#) (see page 66)

[Configuration Tool First Steps](#) (see page 68)

[Create or Manage Repository Definitions](#) (see page 71)

[Configuration Tracing](#) (see page 79)

Configuration Tracing

The Extra configuration tracing information is available for the configuration tool.

Note: This information includes DRAS discovery errors, CCI connection tests failure reasons, and additional Repository Definition and Report List Data Dictionary tracing.

View Configuration Tool Tracing

The extra tracing information is kept in the logs sub folder of the utilities folder.

Save Configuration Changes

You can save the changes after changing the configuration.

Follow these steps:

1. Do one of the following:
 - Select Save Configuration Changes (to the backup location and deployable). This saves your changes to the backup folder and webapp (WAR or the EAR file).
 - Discard Changes and Exit. This option ignores any changes that you made and exits without updating the backup folder or webapp (WAR or EAR file).

A success or failure message is displayed. If there is an error then that information is available in the log files.
2. Redeploy your WAR or EAR file to put the configuration changes on your server.

Manual Connect Pool Configuration

To address many Web Service connections, CA OM Web Services has a larger connection pool setup in the Web Services configuration file, OmWebService.cfg.

In the configuration file, a larger number must be set for omWebService.MaxConnections and a GROW action must be used for omWebService.MaxAction. You must manually modify this file, to make the required changes.

Follow these steps:

1. Locate the backup copy of OmWebService.cfg.

The default location is <product install location>/OM_WS_Config_Backup/OmWebService.cfg
2. Open the file with a text editor.
3. Edit omWebService.MaxConnections or omWebService.MaxAction properties.
4. Save Files.
5. Run Configure Tool in Non-Interactive Update mode.

```
java -jar <product install location>/utilites/lib/ConfigToolLauncher.jar "CA  
Output Management Web Services" "<product install  
location>\deployables\caomws20.war" "ConfigTool.properties" UPDATEWS "<product  
install location>\OM_WS_Config_Backup\" 2> updateError.log
```

Note: A success or failure message appears similar to running the configuration tool in interactive mode.

6. Redeploy your WAR or EAR file to put the configuration changes on your server.

Prepare your Java Web Application Server

CA OM Web Services is an application that runs in an HTTP/Application server and uses Axis2 for SOAP message handling. The installation and configuration of the HTTP/Application server is independent of CA OM Web Services. CA OM Web Services can be installed into existing implementations of supported servers.

For other InstallAnywhere based installs, Apache Tomcat (<http://tomcat.apache.org>) or IBM WebSphere can be used. For the SMP/E based install on the (USS) platform, Apache Tomcat from CA Common Services is used.

This topic covers setting up CA Common Services Apache Tomcat (CCS Tomcat) on the mainframe and IBM WebSphere considerations (if deploying a WAR file). For other platforms, refer to the documentation of your preferred web server.

If you are using CA OM Web Services on a distributed platform, you can proceed to Deploy CA OM Web Services.

Install CCS Tomcat

If an existing CCS Tomcat installation or instance is used, you can proceed to Create Application Specific Instance of CCS Tomcat (create an instance specifically for CA OM Web Services) or Deploy CA OM Web Services (use a shared instance).

To build a Tomcat instance to support CA OM Web Services on the mainframe, the supported version of Apache Tomcat can be installed from CA Common Services for z/OS. For more information about this process, see the *CA Common Services for z/OS Installation Guide*.

When installing the CCS Tomcat, the following (Tomcat-specific) information is required:

SPMJHOME Directory

Specifies the IBM Java Runtime Path. This is the location (parent folder) of a pre-existing IBM Java installation. The SMP/E APPLY processing requires the use of applications under this Path (in the /bin folder).

Example: /sys/java31bt/v6r0m1/usr/lpp/java/J6.0.1

TPV-TOMCAT Directory

Specifies the top-level USS folder for the Tomcat installation. Sub-folder /CCS/tpv is created under this folder. The tpv folder is used as the mount point for the allocated zFS file system. The Tomcat files and folder are under the tpv folder.

Example: /cai/CASoftware

The actual mount point: /cai/CASoftware/CCS/tpv

Target z/OS data set HLQ for the USS file system

Specifies the data set high-level qualifier for the zFS file to be allocated. This defaults to the Data Set Name Prefix previously specified for the SMP/E Target data sets.

Important: This zFS file system must be mounted. The MSM Installation mounts this when created. However, this is a one-time mount that does not persist following an IPL. If this Tomcat is to be used for production, this zFS dataset must be added to the system's auto-mount table.

Create Application Specific Instance of CCS Tomcat

With CCS Tomcat installed, an application-specific instance of it can be created for CA OM Web Services. If an existing CCS Tomcat instance is used, you can proceed and Deploy CA OM Web Services.

To create an application-specific instance, the installed CCS Tomcat folders and files without the Tomcat programs are copied. This copy is configured to run as a started task and CA OM Web Services is deployed here.

Follow these steps:

1. Identify the CCS Tomcat installation that is used as the basis for this new instance. The name of the folder is '/cai/CASoftware/CCS/tpv/tomcat'. The folder ending at tpv is, later referred to as INSTALL_HOME.

Note: The tpv folder contains a 'tomcat' symbolic link to a folder named either 'apache-tomcat-6.0.29' or 'apache-tomcat-7.0.34'.

2. Identify the JAVA_HOME folder. The name of the folder is '/sys/java31bt/v6r0m1/usr/lpp/java/J6.0.1'.

Note: It is recommended to use the same 'SPMJHOME Directory' value that is used when CCS Tomcat was installed.

3. In the CAI.CDUZJCL, edit and submit job TOMC@IN1. This job allocates a new zFS dataset and mounts it. This zFS dataset must be added to the auto-mount table. Alternatively, you can use an existing file system – bypass all steps (delete or comment) except the last step, CR8TDIR, which creates the 'tomcat' folder for the instance. Refer to instructions in the JCL. Make note of the PRODDIR value as it is needed in subsequent steps and it is referred to as PRODUCT_HOME.

Review the results of the job. A new USS folder is created, PRODDIR/tomcat where PRODDIR is a folder of your choice.

Important: This zFS file system must be mounted. This job mounts this when created. However, this is a one-time mount that does not persist following an IPL. If this Tomcat is used for production, this zFS dataset must be added to the systems' auto-mount table.

4. In the CAI.CDUZJCL, edit and submit job TOMC@02. This job copies the CCS Tomcat installation to the PRODDIR/tomcat folder created in the previous step.

Review the results of the job. Under the USS folder that is created in the previous step, there are several new sub-folders and files. This is a copy of the CCS Tomcat installation. The /lib folder is removed and /bin is with only one file.

5. In the CAI.CDUZJCL, edit member TOMCPROC. This is the started task JCL for Tomcat. Do the following:

1. Rename the member as per your site standards for a started task name. This can be done when the PROC is copied to a system data set such as SYS1.PROCLIB.
2. Set the STDENV DD DSN value to reference the configured copy of TOMCPARM.

Note: The started task needs security permissions for read/execute access to the installed CCS Tomcat (INSTALL_HOME) and read/write/execute access to the product-specific instance (PRODUCT_HOME).

6. In the CAI.CDUZJCL, edit member TOMCPARM. This is the parameter file that contains the environment variables for the Tomcat for the task that is started. Do the following:
 1. Rename this member as per your site standards. This can be done when this member is copied to a system data set such as SYS1.PARMLIB.
 2. Set INSTALL_HOME to the parent of the CCS Tomcat installation. This is the value from step 1 less the "tomcat" sub-folder. This folder should have a sub-folder named tomcat a symbolic link to a release-specific tomcat folder. If there is a release specific tomcat folder and not a tomcat symbolic link, you will need to modify CATALINA_HOME to use the release-specific folder.
 3. Set PRODUCT_HOME to the parent of the product-specific Tomcat instance. This is the PRODDIR value from step 4.
 4. Set JAVA_HOME to the JAVA_HOME folder. This is the value from step 2.
7. Update the product specific Tomcat's server.xml file.
 1. Edit (ASCII) file server.xml in folder \${INSTALL_HOME}/tomcat/conf.
 2. If there are other instances of Tomcat running on the same mainframe system, the ports that are used must be changed. At a minimum, shut down the connector ports.

Note: For more information, see the Apache Tomcat web site (<http://tomcat.apache.org>).
8. (Optional) Update the product-specific Tomcat's tomcat-users.xml file.
 1. Edit (ASCII) file tomcat-users.xml in folder \${INSTALL_HOME}/tomcat/conf.

Note: By default, Tomcat users are not defined. It is recommended to define at least one password-protected user with roles="manager,manager-gui,admin".
 2. Once the product-specific instance of Tomcat is configured, start the task verify Tomcat is working by accessing the Tomcat Web Application Manager page using the URL . You are prompted for Tomcat user and password.

Note: The verification is possible only if a Tomcat user was defined.

IBM WebSphere Considerations

Ensure that all the fixes for the WebSphere server are applied before deploying the CA OM Web Services on WebSphere.

To run CA OM Web Services on WebSphere with a WAR file, set the Class loader order to Classes loaded with the local class loader first to load libraries within the CA OM Web Viewer package and last for the parent. However, if you selected to produce an EAR file during the installation, then this setting is automatically included in the EAR file, so that you can deploy this EAR file on WebSphere using the default settings.

Deploy CA OM Web Services

Once CA OM Web Services is installed and configured the caomws20 WAR or EAR file in the /deployable folder, must be deployed to a Java Web Application Server such as Apache Tomcat or IBM WebSphere.

Apache Tomcat

To deploy a WAR file to Apache Tomcat there are two methods.

Method 1: Deploy using the Tomcat Manager

Follow these steps:

1. Log in to the Tomcat Web Application Manager <http://yourserver:8080/manager/html> using a web browser.
Note: To define your credentials to the manager application, edit `tomcat-users.xml`. For more information, see Tomcat documentation.
 2. In the Tomcat Web Application Manager under Deploy, select or upload the configured WAR file.
 3. For the Deploy directory or WAR file on the server, fill in the form using the following information:
 - Context Path (required): `/caomws20`
 - XML Configuration file URL:
 - WAR or Directory URL: `install_folder/deployable/caomws20.war`
1. Click Deploy.
 2. For the WAR file to deploy, the WAR file must be present on the system where the web browser is run. Browse to the folder containing the configured WAR file, select it, and then click Deploy to upload.

Method 2: Deploy statically to Tomcat

Follow these steps:

1. If Tomcats' `server.xml` `autoDeploy` setting is true, then copy the configure WAR file from the `/deployable` folder into the `$CATALINA_BASE/webapps`. It is automatically deployed.
2. If Tomcats' `autoDeploy` attribute is false, then extract manually the WAR file into a folder named `caomws20` under `$CATALINA_BASE/webapps`. The manual extraction can be done with the following commands:

```
cd $CATALINA_BASE/webapps
mkdir caomws20
cd caomws20
jar xf install_folder/deployable/caomws20.war
```

Note: For more information, see the Apache Tomcat web site <http://tomcat.apache.org>.

IBM WebSphere

To deploy the CA OM Web Services, on IBM WebSphere do the following.

Follow these steps:

1. Log in to the WebSphere Administration Console.
2. If deployment is for the first time, then under Applications, select New Application, and then New Enterprise Application. Follow the wizard to create the application, uploading the configure EAR file from the /deployable folder when prompted.
3. If the application is already deployed and a new EAR must be uploaded for updating either the fixes or configuration changes, then locate the existing application under Application Types -> WebSphere enterprise applications.

Note: For more information, see the IBM WebSphere product documentation and website.

Important! If attempting to deploy a WAR file on WebSphere, set class loader order to Classes loaded with local class loader first (parent last), at both application level and module level.

Verify Installation

Verifying your installation consists of three parts:

- Connect to the "Ping" Web Service
- Retrieve a List of Reports
- Retrieve Report Data

Connectivity Test

The CA OM Connectivity Test Utility verifies installation of the CA OM Web Services on your system. This command "pings" the Web Services Server to ensure that it is up and running.

Note: This utility does not access any of your Host OM Products (CA View®, CA Dispatch™, and CA Bundl®) repositories. This command requires that the CA OM Web Services is deployed to a server, and that the server is started.

Follow these steps:

1. Open a Command Prompt in Windows or Terminal in Unix/Linux/USS.
2. Navigate to the Utilities folder.

Windows default:

C:\Program Files\CA\CA_OM_Web_Services\utilities

USS (Installed by InstallAnywhere)/Unix/Linux default:

/usr/local/CA_OM_Web_Services/utilities

USS (Installed by SMP/E):

/cai/om_web_services/utilities

Other:

<CA OM Web Services Install Location>/utilities

3. Invoke the Ping Server command.

Note: For more information about how to invoke a program on your platform, see [Running the Configuration Tool \(Interactive Mode\)](#) (see page 66). For Windows, you launch the tool from a command prompt.

4. Usage and parameters are:

Usage:

Ping_Server <server> <port-number> [protocol]

Where,

Server

Signifies the server where the web service runs.

port-number

Signifies the port number where the web service runs.

Protocol

(Optional) Either "http" non-ssl or "https" for ssl

Retrieve a List of Reports

The report list command, `Report_List_Test`, is a test utility, which retrieves a list of reports accessible in a repository that is defined in CA OM Web Services. You can use the Configuration Tool to define Repositories. The report list command specifies the report name or document type, or both. The command retrieves reports matching these criteria and displays a limited subset of the report information/attributes.

The `Report_List_Test` command generates a list of reports for a specified repository that is defined in CA OM Web Services. The CA OM Web Services must be started to run this command. The `Report_List_Test` command runs through a Web Service request. It is not required to run on the same computer as the server where the CA OM Web Services is installed.

The information that is returned by the command includes the report name, a report description, an archive date, an archive time and optionally a report handle that identifies the report.

Note: The Repository definitions and report list data dictionary entries must be set up during configuring your WAR or EAR file step to access the data and report list.

This section includes:

- Instructions for setting up the test tool
- Instruction for running the tool

Setup Report List Test Tool

This tool requires you define your CA OM Web Services servers URL and port number before running the tool, if you are not running on localhost port 8080. By default, the tool points to a URL of localhost and port 8080.

The server name should be the address of the server where you deployed CA OM Web Services. The port is the http or https port of the server where you deployed CA OM Web Services.

Note:

- The setup is required to be done only once. However, if you change the server URL/machine name or/and port on the server where you installed CA OM Web Services, you have to run the setup again.
- By default, the tool points to a URL of localhost and port 8080.

Instructions for Setting-Up Test Tool (SMP/E based install on USS)

The following is how to define your server and port, if you installed with the SMP/E install on USS.

Follow these steps:

1. Navigate to the Utilities folder.

USS (Installed by SMP/E) default:

`/cai/om_web_services/utilities`

2. Edit `Report_List_Test.sh`. You can use `oedit` or `vi`, depending on your terminal.

3. Change the server property.

Replace: `-Dservername=localhost`

With: `-Dservername=server.company.com`

Note: The server name is the address of the server where you deployed the CA OM Web Services.

4. Change the port property.

Replace: `-Dport =8080`

With: `-Dport=8081`

Note: The port is the http or https port of the server where you deployed CA OM Web Services.

5. Save your file changes. You can now run the Report List Test Tool.

Instructions for Setting-Up Test Tool (InstallAnywhere based install on any platform)

The following is how to define your server and port, if you installed with an InstallAnywhere based installation on any supported platform.

Follow these steps:

1. Navigate to the Utilities folder.

Windows default:

C:\Program Files\CA\CA_OM_Web_Services\utilities

USS (Installed by InstallAnywhere)/Unix/Linux default:

/usr/local/CA_OM_Web_Services/utilities

Other:

<CA OM Web Services Install Location>/utilities

2. Edit Report_List_Test.lax. You can use programs such as notepad, oedit, or vi, depending on your terminal and platform.
3. Find the lax.nl.java.option.additional property and edit the server section of the property lax.nl.java.option.additional.

Replace: -Dservername=localhost

With: -Dservername=server.company.com

Note: The server name is the address of the server where you deployed CA OM Web Services.

4. Edit the port section of the property lax.nl.java.option.additional.

Replace: -Dport =8080

With: -Dport=8081

Note: The port is the http or https port of the server where you deployed CA OM Web Services.

5. Save your file changes. You can now run the tool.

Running the Report List Test Tool

The report list tool gives you a list of reports in a particular repository.

Follow these steps:

1. Open a Command Prompt in Windows or Terminal in Unix/Linux/US.
2. Navigate to the Utilities folder.

Windows Default:

```
C:\Program Files\CA\CA_OM_Web_Services\utilities
```

USS/Unix/Linux Default:

```
/usr/local/CA_OM_Web_Services/utilities
```

USS (Installed by SMP/E):

```
/cai/om_web_services/utilities
```

Other:

```
<CA OM Web Services Install Location>/utilities
```

3. Invoke the Report_List_Test command.

Note: For more information about how to invoke a program on your platform, see [Running the Configuration Tool \(Interactive Mode\)](#) (see page 66). For the Windows, you launch the tool from a command prompt.

4. Usage and parameters are:

Usage:

```
Report_List_Test -f {function} -u {userid} -p {password} -r  
{repositorydefinitionname} -n {reportnamemask} -d {doctypemask} -h -l -b -c  
{recipient} -m {mailcode} -o {timeoutvalue}
```

Note: To redirect the output to a file add the following to the end of the command:

Text:

```
> filename.txt
```

Parameters:

The following are the parameters for generating report lists.

Note: All the parameters that include spaces or special characters such as % or \$ are enclosed in quotes.

-f

Indicates the function to be performed by the command:

list

Retrieves a list of field attributes for each report.

help

Displays command usage help.

-u

Specifies the user ID for the request and is required.

-p

Specifies the password for the request.

-r

Specifies a repository definition entry name that identifies the repository with the reports to be listed.

Required for the reportlist.bat command.

-n

Specifies a report name or report name mask (one or more characters followed by an asterisk). The report name is the name of a report in the specified repository and is case sensitive. Specifying "a*" matches all reports with report names starting with a. Specifying "A" matches all reports with report names starting with an upper case A.

This parameter is not required; if omitted, all report names are selected.

-d

(Optional) Specifies a report type or a report type mask. Report type is the type of the report in the specified repository. Report types include "TEXT" for text reports and "AFP" for AFP reports. Binary reports are generally listed as period followed by extension in capitals: .XLS or .DOC. Wildcard * may also be used. For example, ".DOC*" will return both ".DOC" and ".DOCX" files.

This parameter is not required; if omitted, all reports types are selected.

-h

Displays the report's handle with each report.

-l

Produces a log file for audit purposes and must be specified with a filename for logging purposes.

-c

Specifies the recipient ID for requests accessing CA Dispatch™ repositories.

Required if accessing CA Dispatch™.

-m

Specifies the mailcode for requests accessing CA Bundl® repositories.

Required if accessing CA Bundl®.

-b

Saves the specified file, if it exists, before overwriting for the new request.

-o

Specifies the number of milliseconds for the code to wait for a response from the web server.

Default: 10 seconds

Retrieving Report Data

The report command, `Report_Fetch_Test`, is a test utility, which retrieves a report from a repository. You specify the report and repository as a parameter to the command.

A report handle identifies the report to download, and must be included as a parameter to the report command.

The report command retrieves a report from a specified repository that is defined in CA OM Web Services. CA OM Web Services must be started to run this command. The `Report_Fetch_Test` command runs through a Web Service request and it is not required to run on the same server where the CA OM Web Services is installed.

Important! Test files that are downloaded to USS are in the ASCII format, and require an ASCII reader, such as z/OS UNIX Directory List Utility (va option).

Note: When the report command retrieves a text report, the data is returned in XML format. The syntax rules for XML are followed; the symbols `<`, `>` are represented as `<` and `>` in the file. Viewing the file in a browser converts the tags to the `<` and `>` symbols. If you view the file in a text editor, you can see `<` and `>` tags. See the XML standard for other symbols. The Repository definitions and report list data dictionary entries must be set up during configuring your WAR or EAR file step to access the data and report list.

This section includes:

- Instructions for setting up the test tool
- Instructions for running the tool

Setup Report Fetch Test Tool

This tool requires you to define your CA OM Web Services server's URL and port number before running the tool, if you are not running on localhost port 8080. By default, the tool points to a URL of localhost and port 8080.

The server name is the address of the server where you deployed CA OM Web Services. The port is the http or https port of the server where you deployed CA OM Web Services.

Note:

- The setup is done only once. However, if you change the server URL/machine name or/and port on the server where you installed CA OM Web Services, you have to setup again.
- By default, the tool points to a URL of localhost and port 8080.

Instructions for Setting-Up Test Tool (SMP/E based install on USS)

The following is how to define your server and port, if you installed with the SMP/E install on USS.

Follow these steps:

1. Navigate to the Utilities folder.

USS (Installed by SMP/E) default:

`/cai/om_web_services/utilities`

2. Edit `Report_List_Test.sh`. You can use `oedit` or `vi`, depending on your terminal.
3. Change the server property.

Replace: `-Dservername=localhost`

With: `-Dservername=<servername>` (For example: `server.company.com`)

Note: The server name is the address of the server where you deployed CA OM Web Services.

4. Change the port property.

Replace: `-Dport =8080`

With: `-Dport=<port-number>`

Note: The port number is the http or https port of the server where you deployed CA OM Web Services.

5. Save your file changes. You can now be able to run the Report List Test Tool.

Instructions for Setting-Up Test Tool (InstallAnywhere based install on any platform)

The following is how to define your server and port, if you installed with an InstallAnywhere based installation on any supported platform.

Follow these steps:

1. Navigate to the Utilities folder.

Windows Default:

C:\Program Files\CA\CA_OM_Web_Services\utilities

Unix/Linux Default:

/usr/local/CA_OM_Web_Services/utilities

Other:

<CA OM Web Services Install Location>/utilities

2. Edit Report_List_Test.lax. You can use programs such as notepad or vi, depending on your terminal and platform.

3. Find the lax.nl.java.option.additional property.

4. Edit the server section of the property lax.nl.java.option.additional.

Replace: -Dservername=localhost

With: -Dservername=server.company.com

Note: The server name is the address of the server where you deployed CA OM Web Services.

5. Edit the port section of the property lax.nl.java.option.additional.

Replace: -Dport =8080

With: -Dport=8081

Note: The port is the http or https port of the server where you deployed CA OM Web Services.

6. Save your file changes. You can now be able to run the tool.

Running the Report Fetch Test Tool

The report fetch tool lets you download a report from a particular repository.

Important! Files that are downloaded to USS are in the ASCII format, and require an ASCII reader, such as z/OS UNIX Directory List Utility (va option).

Follow these steps:

1. Open a Command Prompt in Windows or Terminal in Unix/Linux/USS.
2. Navigate to the Utilities folder.

Windows Default:

C:\Program Files\CA\CA_OM_Web_Services\utilities

Unix/Linux Default:

/usr/local/CA_OM_Web_Services/utilities

USS (Installed by SMP/E) default:

/cai/om_web_services/utilities

Other:

<CA OM Web Services Install Location>/utilities

3. Invoke the Report_Fetch_Test command.

Note: For more information about how to invoke a program on your platform, see [Running the Configuration Tool \(Interactive Mode\)](#) (see page 66). For Windows, you launch the tool from a command prompt.

4. Usage and Parameters are:

Usage:

```
Report_Fetch_Test -f {function} -u {userid} -p {password} -r
{repositorydefinitionname} -t {reporttypemask} -L {lowerpagenum} -H
{upperpagenum} -h {reporhandle} -F {filename} -l {logfile} -b -o
{timeoutvalue}
```

Parameters:

The following are the command parameters for retrieving reports.

Note: All parameters that include spaces or special characters such as % or \$ are enclosed in quotes.

-f

Indicates the function the command performs:

get

Gets the report.

help

Displays command usage help.

-u

(Required for get function) Specifies the user ID for the request.

-p

Specifies the password for the request.

-r

(Required for get function) Specifies a repository definition entry name that identifies the repository where the report is located.

-t

Specifies a report type or a report type mask. Report type is the type of the report in the specified repository.

Report types are:

TEXT

For text reports

AFP

For AFP reports

AFPtoPDF

For report you want to transform to PDF

Note: The AFPtoPDF option is only valid if the underlying Output Management product supports the AFP to PDF transformation.

OTHER

For other report types (will be treated as binary).

This parameter is required.

-h

(Required for get function) Specifies the report handle of the report to retrieve. Enclose the report handle in double quotes.

-L

Specifies the lower page range for retrieval of a text report.

If both pageto and pagefrom are omitted, the first five pages of the report are retrieved. If pageto is specified but pagefrom is not, pagefrom is calculated as five pages lower than the pageto value. If pageto is less than five, pagefrom is the first page of the report. If you specify a pagefrom value that is greater than the number of pages in the report, the command returns no data.

If the report type is not text, this parameter is ignored.

-H

Specifies the upper page range for retrieval of text reports.

If both pageto and pagefrom are omitted, the first five pages of the report are retrieved. If pagefrom is specified but pageto is not, pageto is calculated as five pages higher than the pagefrom value. If the pageto value is greater than the number of pages in the report, the request stops retrieval at the last page of the report.

If the report type is not text, this parameter is ignored.

-F

(Required for get function) Specifies the name and path of the report after download.

-l

Produces a log file for audit purposes and must be specified with a filename for logging purposes.

-b

Backs up the specified file (-F), if the file exists, before overwriting the file for the new request.

-o

Specifies the number of milliseconds for the code to wait for a response from the web server.

Default: 10 seconds

Chapter 7: Migrating Information

This section contains the following topics:

[Migrate Information](#) (see page 102)

Migrate Information

This section describes how to migrate the CA OM Web Services 1.0 repository definitions to the CA OM Web Services 2.0 installation.

Important! It is suggested that you run this step before creating any repository definitions in CA OM Web Services, to avoid overwriting of those definitions.

This process requires your old repository definition file. This file name is rdf.xml.

Note: This file can be renamed or placed in a different location that is based on the following property in the OmWebService.cfg file.

Property:

```
omWebService.RepositoryDefinitionFile=/config/rdf.xml
```

Normal File Location:

```
Unicenter Output Management Web  
Services\jakarta-tomcat-4.1.24\webapps\caomws\config
```

Note: For more information, see the *CA OM Web Services 1.0 documentation*.

Follow these steps:

1. Obtain the old rdf.xml file.
2. Run the Change_CCI_Settings to set up the CCI settings.
Note: For more information, see [Configure CAICCI](#) (see page 69).
3. Run Change_License_Server to set up your license server.
Note: For more information, see [Configure the License Server](#) (see page 70).
4. Copy the contents of your rdf.xml file into your backup folders rdf.xml file.

Default Location:

```
<CA_OM_Web_Services_Install_Directory>\OM_WS_Config_Backup\rdf.xml
```

5. Run Create_RLDD.

This creates the Report List Data Dictionary that is based on your Repository Definitions.

Important! Be sure to select Load configuration settings backup location.

Note: For more information about loading configuration setting from backup location, see [Configuration Tool First Steps](#) (see page 68).

6. Deploy your WAR/EAR file and continue with other Post-Installation and Configuration Tasks.

Chapter 8: Applying Fixes to the Product

CA provides an Update Installer to ship the updates and help you upgrade an existing CA OM Web Services in Version 2.0 or later.

This section contains the following topics:

[Apply Fixes on SMP/E Install](#) (see page 103)

[Apply Fixes on Other Platforms](#) (see page 104)

Apply Fixes on SMP/E Install

CA OM Web Services fixes are delivered as SMP/E Maintenance. Fixes can be installed using CA Chorus Software Manager or using SMP JCL.

Note: For more information about applying Fixes, see [Apply Preventive Maintenance](#) (see page 46).

Once all fixes are applied, the CA OM Web Services WAR file must be again configured, and deployed to Apache Tomcat.

If CA OM Web Services is already configured (folder <product install location>/OM_WS_Config_Backup exists), the Update_Refresh.sh utility can be used.

Follow these steps:

1. Navigate to the <product install location>/utilities folder. It contains shell script Update_Refresh.sh.
2. Execute the Update_Refresh.sh shell script.

Note: To perform the step you may need SUPERUSER authority. If you don't have the authority, an updated WAR file may be created in a different folder (path will be listed in the output messages).

3. The WAR file, previously updated by the applied fixes, is refreshed with the saved configuration settings.

Once the WAR file is updated, perform the Apache Tomcat deployment. For more information about the deployment, see [Apache Tomcat](#) (see page 86).

Apply Fixes on Other Platforms

CA OM Web Services fixes are delivered with the same tool as the full installation.

Note: For more information about starting the update installer on your specific platform, see [Installing CA OM Web Services with InstallAnywhere](#) (see page 53).

Depending on the running environment, the installer automatically runs in graphical (GUI) or console mode. Alternatively, you can also select silent mode for the non-interactive installation.

Update Installation Using the GUI Wizard

CA OM Web Services can be installed using the GUI (Graphic User Interface) mode.

Follow these steps:

1. Select a locale from the Choose Locale drop-down menu, and click OK.
2. Review the Introduction panel for information about the Installer and click Next.
3. Specify the folder where you installed CA OM Web Services.
4. According to the deployment method of your previous version of CA OM Web Services, do one of the following:
 - If you produced CA OM Web Services WAR files in your previous installation:
 - Select "Update Web Services WAR file"
 - Specify the path of your WAR file
 - If you have a CA OM Web Services EAR file:
 - Select "Update a Web Services EAR file"
 - Specify the path of your EAR file
5. The update installer backs up your original CA OM Web Services as a pair of WAR file. These files are placed into a folder that is specified in this panel.

Note: The backup step is recommended. However, if you do not need a backup by the update installer, select "No backup." Ensure you have write permission to the backup folder. The update installer will also check whether this folder exists. If this folder does not exist, it will be created after installation starts.
6. Review the settings that are displayed in the Pre-Installation Summary and click Install to start the Installation.
7. Review the Install Complete Information.

Note: If your install had warnings or non-fatal errors, you receive a summary message that starts with Warning or Non-Fatal Failure. In this case, more information can be found in your install log, after finishing and closing the installer.
8. Click Done.

Update Installation Using the Console Mode

The steps in this section explain how to install CA OM Web Services using the Console mode.

Step 1. Introduction and License Agreements

Follow these steps:

1. Choose a locale and press Enter to continue.
2. Review the following Introduction.

=====

Introduction

InstallAnywhere will guide you through the installation of CA Output Management Web Services 2.0. It is strongly recommended that you quit all programs before continuing with this installation. Respond to each prompt to proceed to the next step in the installation. If you want to change something on a previous step, type 'back'. You may cancel this installation at any time by typing 'quit'.

3. Press Enter to continue.

Step 2. Supply the Installation Information

Specify where the CA OM Web Services is installed. Then confirm the location with "Y".

=====

Choose Previous Install Folder

Please choose the destination of your previous install folder for your CA OM Web Services r2.

Where Was Your Previous Install?

Default Install Folder: /usr/local/CA_OM_Web_Services
ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
INSTALL FOLDER IS: /usr/local/CAOMWS
IS THIS CORRECT? (Y/N):

Step 3. Select an Update Target

According to the deployment method of your previous version of CA OM Web Services, select one option from the list:

```

=====
Select an Update Target
-----
Enter requested information
  1- Update a Web Services WAR file
  2- Update Web Services EAR file

ENTER THE NUMBER OF THE DESIRED CHOICE:
=====
=====
=====
Update Web Services WAR file
-----
Enter the full path of the Web Services WAR file
(DEFAULT: /usr/local/CAOMWS/deployable/caomws20.war):

```

Step 4. Backup the Original CA OM Web Services

The update installer backs up your original CA OM Web Services as a pair of WAR files into a folder specified in this step.

Note: The backup step is recommended. If you do not need a backup by the update installer, select "No backup."

```

=====
Backup the Original CA OM Web Services
-----
Enter requested information
  ->1- Backup the original CA OM Web Services (Recommended)
      2- No backup

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE
DEFAULT:

```

Step 5. Complete the Installation

Follow these steps:

1. Review the options displayed in the Pre-Installation Summary.

```
=====
Pre-Installation Summary
-----
```

Please Review the Following Before Continuing:

Product Name:

CA Output Management Web Services 2.0

Target to Apply the Updates

/usr/local/CAOMWS/deployable/caomws20.war

Backup Folder

Not available

PRESS <ENTER> TO CONTINUE:

2. Press Enter to continue.

```
=====
Ready To Install
-----
```

InstallAnywhere is now ready to install CA Output Management Web Services 2.0 onto your system.

PRESS <ENTER> TO INSTALL:

3. Review the Install Complete information.
4. Press Enter to Install.

```
=====
Installation Complete
-----
```

Congratulations! CA Output Management Web Services 2.0 has been successfully installed to:

/usr/local/CAOMWS/deployable/caomws20.war

Backup Folder:

/usr/local/CAOMWS/backup

PRESS <ENTER> TO EXIT THE INSTALLER:

5. Press Enter to exit installer.

Update Installation Using the Silent Mode

In the silent mode, install options can be specified as command-line switches or in a text file that is passed as a parameter to the command. The install options on the command-line is prefixed by -D and separated by space. In the text file, each option occupies new line. If backslash is present in path, it must be escaped (\\).

Note: The file must be saved in UTF-8 encoding without a BOM mark on the beginning.

The following are the install options:

USER_INSTALL_DIR=<path>

Specifies the directory where the product is installed. If the directory contains spaces, enclose it in double-quotes.

USER_INPUT_BACKUP_YES=<1/0>

Specifies if the WAR/EAR file is backed up before update (Yes/No).

USER_INPUT_BACKUP_FOLDER=<path>

Specifies the path to the backup folder. A folder is created if it does not exist.

USER_INPUT_WAR=<1/0>

Web Services WAR file is updated (Yes/No).

USER_INPUT_WAR_1_PATH=<path>

Full path to existing EAR file for update.

USER_INPUT_EAR=<1/0>

Web Services EAR file is updated (Yes/No).

USER_INPUT_EAR_PATH=<path>

Full path to existing WAR file for update.

Use one of the following commands to silently install the CA OM Web Services:

- With options specified in a text file:
java -jar CAOMWS2U.jar -i silent -f <text file>
- With options specified on the command line:
java -jar CAOMWS2U.jar -i silent [-D<option>]
- WAR update example:
java -jar CAOMWS2U.jar -i silent -DUSER_INPUT_WAR=1
-DUSER_INPUT_WAR_1_PATH=<war file>

Appendix A: Installation Worksheet

This appendix contains worksheets for information required to install and configure the product.

This section contains the following topics:

[CA CSM Installation-Mainframe](#) (see page 111)

[SMP/E JCL Installation-Mainframe](#) (see page 117)

CA CSM Installation-Mainframe

The following information is required during the installation of the product using CA Chorus Software Manager.

SMP/E Environment Name and CSI VSAM Parameters:

SMP/E Environment Name

Defines the SMP/E environment name.

Example: Web Services production system

Data Sets Prefix

Defines the prefix for the name of the CSI VSAM data set.

Example: CAI.OMWS

Note: .CSI is appended to the prefix value.

Catalog

Defines the name of the SMP/E CSI catalog.

SMP/E Data Sets Allocation Parameters:

High-Level Qualifier

Specifies the high-level qualifier (HLQ) for all SMP/E data sets that are allocated during installation. Product packaging defines the low-level qualifiers (LLQ). The low-level qualifiers cannot be changed.

Example: CAI.OMWS

DSN Type

Specifies the DSN type for allocating SMP/E data sets.

Default: LIBRARY

SMS Parameters (mutually exclusive with Data set Parameters)

Specifies if the SMP/E environment is using SMS parameters.

Storage Class

Defines the SMS storage class for SMP/E data sets.

Management Class

Defines the management class for SMP/E data sets.

Data Class

Defines the data class for SMP/E data sets.

Data set Parameters (mutually exclusive with SMS Parameters)

Specifies if the SMP/E environment is using data set parameters.

VOLSER

Defines the volume serial number to place the data sets. The volume must have enough space for allocating the data sets.

Note: This field is mandatory if you set Catalog to No.

UNIT

Defines the type of the DASD on which to place data sets.

Catalog

Specifies if the SMP/E data set requires to be cataloged.

Target Zone Name and CSI VSAM Parameters:

Target Zone Name

Defines the name for the target zone.

Default: CAIT0

Data Sets Prefix

Defines the prefix for the name of the target zone data set.

Note: This field is only enabled when you have the Create New CSI Data Set check box selected.

Default: Value from the prior panel.

Catalog

Defines the name of the SMP/E target zone catalog.

Note: This field is only enabled when you have the Create New CSI Data Set check box selected.

Default: Value from the prior panel.

Target Libraries Allocation Parameters:

High-Level Qualifier Default

Specifies the high-level qualifier (HLQ) for all target zone data sets that are allocated during installation. Product packaging defines the low-level qualifiers (LLQ) and they cannot be changed.

Example: CAI.OMWS

DSN Type

Specifies the DSN type for allocating target zone data sets.

Default: LIBRARY

SMS Parameters (mutually exclusive with Data set Parameters)

Specifies if this target zone uses SMS parameters.

Storage Class

Defines the SMS storage class for target zone data sets.

Management Class

Defines the management class for target zone data sets.

Data Class

Defines the data class for target zone data sets.

Data set Parameters (mutually exclusive with SMS Parameters)

Specifies if this target zone uses data set parameters.

VOLSER

Defines the volume serial number to place the data sets. The volume must have enough space for allocating the data sets.

UNIT

Defines the type of the DASD to place the data sets.

Catalog

Specifies if you want SMP/E data set to be cataloged.

Target Zone Parameters:

Operating System: SMPJHOME

Specifies the IBM Java Runtime Path. This is the location (parent folder) of a pre-existing IBM Java installation. The SMP/E APPLY processing requires the use of applications under this Path (in the /bin folder).

Default: /your/smpjhome/directory/

Example: /sys/java31bt/v6r0m1/usr/lpp/java/J6.0.1/

USS Directory: OUTPUT MANAGEMENT WEB SERVICES

Defines the top-level USS folder for the target zone elements. This folder must exist, or can be created on, a mounted USS file system. Web Services is installed into this folder.

Default: /cai/om_web_services

Note: This refers to a CSM install, not an InstallAnywhere install. For more information about installing with CSM, see [How to Install Your Product Using CA CSM](#) (see page 23).

Distribution Zone Name and CSI VSAM Parameters:

Distribution Zone Name

Defines the name for the distribution zone.

Default: CAID0

Data Sets Prefix

Defines the prefix for the name of the distribution zone data set.

Note: This field is enabled only when the Create New CSI Data Set is selected.

Default: Value from the prior panel.

Catalog

Defines the name of the SMP/E distribution zone catalog.

Note: This field is enabled only when the Create New CSI Data Set is selected.

Default: Value from the prior panel.

Distribution Libraries Allocation Parameters

High-Level Qualifier

Specifies the high-level qualifier (HLQ) for all distribution zone data sets that are allocated during installation. Product packaging defines the low-level qualifiers (LLQ) that cannot be changed.

DSN Type

Specifies the DSN type for allocating target zone data sets.

Note: This field is enabled only when the Create New CSI Data Set is selected.

Default: LIBRARY

SMS Parameters (mutually exclusive with Data set Parameters)

Specifies if this target zone uses SMS parameters.

Storage Class

Defines the SMS storage class for target zone data sets.

Management Class

Defines the management class for target zone data sets.

Data Class

Defines the data class for target zone data sets.

Data set Parameters (mutually exclusive with SMS Parameters)

Specifies if this target zone uses data set parameters.

VOLSER

Defines the volume serial number on which to place data sets. The volume must have enough space for allocating the data sets.

UNIT

Defines the type of the DASD to place the data sets.

Catalog

Specifies if you want SMP/E data set to be cataloged.

SMP/E JCL Installation-Mainframe

The following information is required during the installation of the product using SMP/E JCL. This is used when customizing the DUZSEEDIT member in the SAMPJCL dataset.

JOBCARD1

Defines the job card information

Default: //JOBNAME JOB (ACCT INFO),'JOB DESC',CLASS=X,

JOBCARD2

Defines the job card information

Default: //MSGCLASS=X,NOTIFY=,LINES=9999,TIME=1440

JOBCARD3

Defines the job card information

Default: //*

JOBCARD4

Defines the job card information

Default: //*

VOLINFO

Edit the SMS VOLINFO statement. If you do not use SMS, comment out the SMS VOLINFO statement and uncomment the statement using VOL=SER, then edit that statement. This information is used when creating the product and SMP/E datasets.

Default: MGMTCLAS=XXXXXXXX,STORCLAS=XXXXXXXX,DATACLAS=XXXXXXXX

Alternate: VOL=SER=XXXXXX,UNIT=YYYYYY

CSIVOLINF

Edit the SMS CSIVOLINF statement. If you do not use SMS, comment out the SMS CSIVOLINF statement and uncomment the statement using VOL=SER, then edit that statement. This information is used when creating the CSI VSAM dataset.

Default: MGMTCLAS(XXXXXXXX) STORCLAS(XXXXXXXX) DATACLAS(XXXXXXXX)

Alternate: VOLUME(XXXXXX)

GLOBALHLQ

Defines the SMP/E High level qualifier for your GLOBAL ZONE.

Default: CAI

CAIT0HLQ

Defines the SMP/E High level qualifier for your CAIT0 TARGET ZONE.

Default: CAI

PRODHLQ

Defines the Product dataset high level qualifier.

Default: CAI

DASDHLQ

Required if installing from DASD. Defines the high level qualifier that was specified for yourHLQ when the UNZIPJCL job was run.

Default: CAI

SAMPHLQ

Defines the high level qualifier that is used for the SAMPJCL dataset.

Default: CAI

TAPEUNIT

Defines the appropriate tape generic device-type or symbolic group name.

Default: CART

DISKUNIT

Defines the disk unit name.

Default: SYSALLDA

SMPETEMP

Defines the SMP/E Temp File prefix.

Default: CAI

TCPIPDSN

Defines the data set used to obtain parameters that are defined by TCPIP.DATA.

Default: TCPIP_HLQ

EMAILADR

Defines the email address. This value is used for anonymous FTP in order to download the CA HOLDDATA.

Default: EMAIL_ADDRESS

ZNCAIT0

Defines the Target Zone name within CSI or default to CAIT0

Default: CAIT0

ZNCAID0

Defines the Distribution Zone name within CSI or default to CAID0

Default: CAID0

SMPJHOME

Specifies the IBM Java Runtime Path. This is the location (parent folder) of a pre-existing IBM Java installation. The SMP/E APPLY processing requires the use of applications under this Path (in the /bin folder).

Default: /your/smpjhome/directory/

Example: /sys/java31bt/v6r0m1/usr/lpp/java/J6.0.1/

@pathprefix1@

Defines the top-level USS folder for the target zone elements. This folder must exist, or can be created on, a mounted USS file system. Web Services is installed into this folder.

Default: /cai/om_web_services

Note: This section refers to SMP/E JCL install, not InstallAnywhere install.

Appendix B: Creating Log Information

CA OM Web Services Version 2.0 leveraged Apache Log4j library to implement the logging function in the product. It provides web applications and components with the ability to log hierarchically across various log levels without the need to rely on a particular logging implementation. The logging frameworks used by the product and its components run independently of each other and provide output to separate log files.

This section contains the following topics:

[Log Levels](#) (see page 121)

[Update Configuration Files](#) (see page 122)

[Output Log Files](#) (see page 122)

Log Levels

For support and debug purposes, the log4j facility is enabled with CA OM Web Services Version 2.0 and middle-tier components with a default trace priority level set to ERROR.

The priorities from lowest to highest are as follows:

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

Due to performance considerations and file disk space, the INFO and DEBUG levels are *not* recommended for use with CA OM Web Services Version 2.0 in production.

The lower levels are used only for requests from CA Support to gather more debug log records for problem detection.

Update Configuration Files

Under the web application deployment directory, there is a sub-directory for logging configuration files. One sub-directory, /config, holds the trace configuration files, OmCCITrace.cfg, OmJDrasTrace.cfg, and OmTrace.cfg.

```
..\webapps\caomws20\config
```

You can update the log levels and get more trace messages besides error messages into the log files by upgrading the level for the parent class category or individual class category to WARN, INFO, or DEBUG level.

For example, in OmCCITrace.cfg, OmJDrasTrace.cfg, OmTrace, change the level as follows:

From

```
log4j.category.com.ca.erm.cciclient.cci.=ERROR, A1  
log4j.category.com.ca.omgmt.drasci=ERROR, A2  
log4j.category.com.ca.omgmt.webservice=ERROR, A3
```

To

```
log4j.category.com.ca.erm.cciclient.cci.=INFO, A1  
log4j.category.com.ca.omgmt.drasci=DEBUG, A2  
log4j.category.com.ca.omgmt.webservice=WARN, A3
```

Note: You do *not* have to restart CA OM Web Services Version 2.0 after the configuration update. You can use the new trace settings within a short time.

Output Log Files

Under the web application deployment directory, there is a sub-directory for holding the output log files ccitrace.log, jdrastrace.log, and webservicetrace.log for each component.

```
..\webapps\caomws20\logs
```

The log records output to these log files can be used for problem tracking, which is based on requests from CA Support.

Index

A

- Access CA CSM Using the Web-Based Interface • 25
- Acquire a New Product • 25
- Acquire the Product Pax Files • 35
- Additional Requirements • 15
- Allocate and Mount a File System • 32
- Allocate and Mount a File System for Mainframe • 20
- Apache Tomcat • 86
- Apply Fixes on Other Platforms • 104
- Apply Fixes on SMP/E Install • 103
- Apply Preventive Maintenance • 46
- Applying Fixes to the Product • 103
- Audience • 9

C

- CA Common Services Requirements • 14
- CA CSM Installation-Mainframe • 111
- CA Technologies Product References • 3
- Clean Up the USS Directory • 46
- Concurrent Releases • 21
- Configuration Tool First Steps • 68
- Configuration Tracing • 79
- Configure CA OM Web Services • 65
- Configure CAICCI • 69
- Configure the Deployed Product • 30
- Configure the License Server • 70
- Connectivity Test • 88
- Contact CA Technologies • 3
- Copy Installation Files to z/OS Data Sets • 41
- Create a Product Directory from the Pax File • 40
- Create Application Specific Instance of CCS Tomcat • 83
- Create or Manage Repository Definitions • 71
- Create Report List Data Dictionary Entries • 77
- Create Report List Data Dictionary Entries Procedure • 78
- Creating Log Information • 121

D

- Deploy CA OM Web Services • 85
- Deploy the Product to the Destination System • 29
- Deployment Security • 18
- Distribution Libraries for Mainframes • 16

- Download Files to a PC Using Pax ESD • 36
- Download Files to Mainframe through a PC • 39
- Download Using Batch JCL • 36
- DVD Space Requirements for Mainframes • 17

E

- Environment Variables • 14
- Example
 - CAtoMainframe.txt, JCL • 38
 - JCL File, Unpackage.txt, to Customize • 41
- External HOLDDATA • 50

G

- General Requirements • 13
- General USS Requirements • 18

H

- HOLDDATA • 48
- How the Installation Process Works • 9
- How the Installation Process Works in InstallAnywhere Based install • 12
- How the Installation Process Works with SMP/E Install • 10
- How to Install Your Product Using a Pax File • 31
- How to Install Your Product Using CA CSM • 23

I

- IBM WebSphere • 87
- IBM WebSphere Considerations • 85
- Insert a Repository • 72
- Install a Product • 26
- Install CCS Tomcat • 82
- Install Standard Error • 60
- Install Standard Out • 60
- Install Your Product Using CA CSM • 23
- Install Your Product Using Pax ESD or DVD • 31
- InstallAnywhere based Install Requirements • 17
- InstallAnywhere Installation of CA OM Web Services on Other Platforms • 57
- InstallAnywhere Installation of CA OM Web Services on Windows • 55
- Installation Logging • 59
- Installation Using the Console Mode • 58
- Installation Using the GUI Wizard • 56

Installation Worksheet • 111
Installing CA OM Web Services with InstallAnywhere
• 53
Installing CA OM Web Services with SMP/E (USS) •
23
Instructions for Setting-Up Test Tool
(InstallAnywhere based install on any platform) •
91, 96
Instructions for Setting-Up Test Tool (SMP/E based
install on USS) • 90, 95

J

Java Virtual Machine Requirements • 17
Java Web Application Servers • 14

L

Launch Configuration Tool AIX • 67
Launch Configuration Tool HP/UX • 66
Launch Configuration Tool HP-UX IA64 • 67
Launch Configuration Tool Linux PC • 67
Launch Configuration Tool Sun Solaris • 67
Launch Configuration Tool USS • 67
Launch Configuration Tool Windows • 67
Launch Configuration Tool zLinux • 67
Launch the Uninstaller • 61
List Current Repositories • 74
LMP Key Requirements • 15
Locate the Product Installer • 54
Log Levels • 121
Log Locations • 59

M

Maintain the Installed Products • 28
Manual Connect Pool Configuration • 80
Migrate Information • 102
Migrating Information • 101

O

Open Repository Settings • 71
Output Log Files • 122
Overview • 9

P

Post-Installation and Configuration Tasks • 65
Prepare the SMP/E Environment for Pax Installation
• 43
Prepare your Java Web Application Server • 81

Preparing for Installation • 13
Primary Install Log • 60

R

Remove a Repository • 75
Retrieve a List of Reports • 89
Retrieving Report Data • 94
Run the Installation Jobs for a Pax Installation • 45
Running the Configuration Tool (Interactive Mode) •
66
Running the Report Fetch Test Tool • 97
Running the Report List Test Tool • 92

S

Save Configuration Changes • 80
Security Requirements • 16
Security Requirements on Other Platforms • 17
Setup Report Fetch Test Tool • 95
Setup Report List Test Tool • 89
SMP/E Install Requirements • 15
SMP/E JCL Installation-Mainframe • 117
Step 1. Introduction and License Agreements • 106
Step 2. Supply the Installation Information • 106
Step 3. Select an Update Target • 107
Step 4. Backup the Original CA OM Web Services •
107
Step 5. Complete the Installation • 108
Storage Requirements • 16, 18
Supported Platforms • 13, 53
System HOLDDATA • 49

T

Target Libraries for Mainframes • 16

U

Uninstall • 61
Uninstall on Other Platforms • 63
Uninstall on Windows • 62
Uninstalling CA OM Web Services • 61
Unix/Linux/USS • 18
Update a Repository • 76
Update Configuration Files • 122
Update Installation Using the Console Mode • 105
Update Installation Using the GUI Wizard • 105
Update Installation Using the Silent Mode • 109
Use a Web Browser • 54
Use the DVD • 54
USS Environment Setup • 32

USS Security Requirements • 19

V

Verify Installation • 87

View Configuration Tool Tracing • 79

W

Windows • 17