Oracle® Enterprise Content Management Application Adapters (Managed Attachments Solution)

Installation and Configuration Guide

Release 10*g*R3

August 2010

Oracle ECM Application Adapters (Managed Attachments Solution) Installation and Configuration Guide, Release 10*g*R3

Primary Author: Sarah Howland

Contributor: Kevin de Smidt, Jason Schindhelm, Kevin Cocilo, Rama Vijjapurapu, Ansuman Roy, Sreekanth Chintala, Anand Vaidyanathan, Gonzalo Serrano, Nathan Angstadt.

Contents

3 Managed Attachments Functionality

A Managed Attachments Solution Tables

Preface

This guide describes how to install, configure, and use the ECM Application Adapter for Universal Content Management.

Audience

This document is intended for administrators configuring integrations between Content Server and E-Business Suite and PeopleSoft systems via Application Extension Framework (AXF).

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Overview

The Oracle Enterprise Content Management Application Adapters (Managed Attachments Solution) allows E-Business Suite and PeopleSoft users to attach, scan, and retrieve attachments stored in an Oracle UCM Content Server repository. An Oracle UCM repository enables users throughout an enterprise to view, collaborate on, and retire content, ensuring that content is secure, accurate, and up-to-date.

With this adapter, Oracle UCM documents are listed as managed attachments to business application entities in a customizable screen launched from a menu, link, or button, depending on business application configuration. For example, a business application user displays an Employee record, invokes the Managed Attachment functionality by selecting a specified command from a menu or clicking a button, and attaches a passport image and supporting identity documents.

This chapter covers the following topics:

- "About This Guide" on page 1-1
- "Business Application User View" on page 1-2
- "About the Managed Attachments Solution" on page 1-2
- "User Authentication" on page 1-3
- "Document Security" on page 1-3

1.1 About This Guide

This guide describes how to install, configure, and use the Oracle Enterprise Content Management Application Adapters (Managed Attachments Solution).

- Chapter 1, "Overview", provides user and administrator overview information about the adapter.
- Chapter 2, "Installation and Configuration", describes how to install and configure each portion of the adapter, including AXF, E-Business Suite and PeopleSoft plug-ins, and Oracle UCM components. It also covers configuring optional Oracle Distributed Document Capture and AutoVue portions, security and users, and customization.
- Chapter 3, "Managed Attachments Functionality", provides information on options available to business application users in the Managed Attachments screen.
- Appendix A, "Managed Attachments Solution Tables", provides reference information for the tables used in the adapter and examples of their use.

1.2 Business Application User View

Business application users can perform these tasks in the Managed Attachments Screen:

- Check in new documents to Content Server and attach them to the selected business application entity
- Scan and import documents via Oracle Distributed Document Capture, attaching them to the selected business application entity
- Open documents in their native application, Web-viewable format, or AutoVue viewer (if configured)
- Detach documents from the selected business application entity
- Search Content Server and attach documents to the selected business application entity from the Oracle UCM repository
- Check out documents, locking them to changes by other users
- Modify a document’s metadata values
- If configured, view a previous attached revision and update the attachment revision
- View an attached document’s information

For details about how users work with Oracle UCM documents in a business application, see "Managed Attachments Functionality" on page 3-1.

1.3 About the Managed Attachments Solution

Application Extension Framework (AXF) is a command-driven, web services integration, typically between a business application such as E-Business Suite or PeopleSoft, and a repository such as Universal Content Management. An **AXF solution** is a micro-application whose components are created using the AXF infrastructure.

The Managed Attachments solution for Enterprise Content Management uses an AXF solution namespace called **UCM_Managed_Attachments** to orchestrate user requests from the business application to display the Managed Attachments user interface for the Oracle UCM Content Server repository.

- When the business application user activates the Managed Attachments command from a business application entity, the adapter makes an AXF request. The solution supports a single AXF command namespace called **UCM_Managed_Attachments**, which invokes the AF_GRANT_ACCESS command.
- The **AF_GRANT_ACCESS** command implements the **AF_GRANT_ACCESS** service. This Oracle UCM service temporarily grants a user who has logged into the business application access to all Oracle UCM documents associated with the selected business application entity and to which the user has security group access. This service also returns an AXF response containing a Managed Attachments URL to invoke the Oracle UCM **attachments framework search**. This framework search lists all documents associated with the business application entity.
- With the returned URL, the adapter opens the Managed Attachments browser window for the business application user, also displaying key values (AFLabel) for the business application entity with which the attachment list is associated.

How Oracle UCM Access is Granted to the Business Application User

The adapter uses a temporary authorization mechanism for managed attachments access. Communicating through a trusted RIDC mechanism, AXF invokes the AF_GRANT_ACCESS service with the application entity and user information needing authorization. The AF_GRANT_ACCESS service grants access to the user for the specified period of time, then ends the user session.

1.4 User Authentication

Business application users must have a Content Server account in order to display the Managed Attachments screen within the supported business application entity. In addition, the authentication model configured for Content Server and the business application determines how users are authenticated the first time they activate managed attachments from a business application record:

- **Content Server configured for single sign-on (SSO):** If the business application is not configured for SSO, the Oracle UCM SSO login prompt is displayed. (If the business application is configured for SSO, the user has already been authenticated so no login prompt is displayed.)
- **Content Server *not* configured for SSO:** The Content Server login prompt is displayed, regardless of the selected business application authentication model.

Note: No user authentication is needed for AXF, as long as security checks are properly configured, as described in "Managing Authentication and Security" on page 2-29.

1.5 Document Security

When checking documents into Content Server via the Managed Attachments user interface, users decide how they want them accessed, by choosing one of two modes:

- **private** (not shared): These documents can be accessed only through their associated business application entity screens via the Managed Attachments user interface. Users (including the user who checks in a document) cannot search for or access a private document via any other standard Oracle UCM user interface. This is the default security mode when checking in a new document via the Managed Attachments user interface.
- **shared**: These documents are more easily accessed than private documents, because their security is managed by Oracle UCM. In addition to access through their associated business application entity screens via the Managed Attachments user interface, any Oracle UCM user with a document's assigned security group access can search for and access the document via any standard Oracle UCM user interface.

Note: Only shared documents can be viewed in AutoVue (if configured). Private documents cannot be viewed. For details, see "Configuring Oracle AutoVue Document Viewing" on page 2-33.

Note: Private (not shared) documents are automatically assigned to a special security group called *AFDocuments*, and users who have access to the business application entity are granted temporary access to the documents when they invoke the Managed Attachments user interface. In certain exceptional cases, special users may be granted direct access to the AFDocuments security group by permanent assignment of the AFRead, AFWrite, AFDelete or AFAdmin roles for the AFDocuments security group, in which case the user could access a private document via any standard Oracle UCM user interface.

---

2 Installation and Configuration

This chapter describes how to install and configure the Oracle Enterprise Content Management Application Adapters (Managed Attachments Solution). It covers the following topics:

2.1 Adapter Installation Requirements

The Oracle Enterprise Content Management Application Adapters (Managed Attachments Solution) consists of optional solutions installed over a base configuration of AXF and Oracle UCM files standard to adapters that use AXF functionality.

The adapter requires the following:

- "Application Server / Database (Windows or Linux)" on page 2-2
- "E-Business Suite Release 11.5.10+, 12.0.4+ or 12.1.1+" on page 2-2
- "PeopleSoft Enterprise" on page 2-2
- "Oracle UCM 10gR3 v10.1.3.5.1+ and related files" on page 2-3
- "Oracle Distributed Document Capture v10.1.3.5+ and related components" on page 2-4
- "Oracle VueLink 19.3 for Oracle UCM" on page 2-4

2.1.1 Application Server / Database (Windows or Linux)

AXF requires Application Server 10gR3 Standard Edition or Application Server 10gR3 Enterprise Edition release 10.1.3.x, backed by an Oracle database. Be sure to check the certification matrix (link below) for information about Application Server versions and corresponding supported database releases. These administrative tasks may require assistance from your DBA or IT team.

http://www.oracle.com/technology/software/products/ias/files/oracle_soa_certification_r3_10.1.3_matrix.xls

---

Notes:

- Oracle Database 10g XE is not recommended for AXF production environments.
- Oracle Database 10g must be properly installed, configured, and patched to the correct version for use by your Application Server.
- Note the Application Server address, administration usernames and passwords, and instance name.

2.1.2 E-Business Suite Release 11.5.10+, 12.0.4+ or 12.1.1+

A fully functioning Oracle E-Business Suite system.

Important: Install AXF on a separate application server from the E-Business Suite Application Server.

- E-Business Suite Forms Builder is required for .PLL compilation.
  - For Oracle 11i, Forms 6.0 Version 6.0.8.25.2+
  - For Oracle 12, Forms Builder Version 10.1.2.0.2+
- If using Single Sign-On, an Oracle Identity Management (OIM) / OID Server is required.

Note: The ECM Adapter for Oracle UCM supports E-Business Suite Forms only. OAF web pages are not currently supported.

In this release, the adapter is localized for English only.

2.1.3 PeopleSoft Enterprise

Important: Install AXF on a separate application server from the PeopleSoft Application Server.

A fully functioning Oracle PeopleSoft system.

- PeopleTools 8.48.x or 8.49.x
- To avoid duplicate logins, Oracle Single Sign-On or Oracle Access Manager is required.

Note: If using Single Sign-On, an Oracle Identity Management (OIM) / OID Server is required.

2.1.4 Oracle UCM 10gR3 v10.1.3.5.1+ and related files

Supported browsers for this adapter include Internet Explorer versions 6.x and 7.x. Mozilla Firefox version 3.0.x is also supported by the Managed Attachments Solution.

- E-Business Suite browser support is currently limited to Mozilla Firefox version 3.0.x and only with E-Business Suite version 12.0.6 or above (refer to My Oracle Support at http://myoraclesupport.oracle.com for additional information on E-Business Suite browser support).
- Note that the Mozilla Firefox browser is not supported for scan functionality via Oracle Distributed Document Capture, which currently requires Internet Explorer.

Notes: This adapter supports Metadata Only Search or Database - Full Text Search. (It does not support Oracle Text - Full Text Search.)

If using an IIS ISAPI filter for Oracle UCM, the filter must be release 5.1.1.101 or higher. If using an Apache filter, the filter must be release 5.1.1.96 or higher.

Follow these steps to install Content Management System Server, version 10.1.3.5.1.

1. Install 10.1.3 Content Server base using ContentServer_Windows_10gR3_YYYYMMDD.zip.
2. Apply 10.1.3.5.1 patches on top of the base installation.
   - Install the CS10gR35UpdateBundle-YYYYMMDD.zip component (Build 15 or higher). For detailed installation instructions, refer to readme.html packaged within the zip file.
   - From the CS10gR35UpdateBundle-YYYYMMDD.zip file, install the following extra component, an extra component not part of typical component installation:

     component\CS10gR35UpdateBundle\extras\BrowserURLPath.zip
   - Install the CS10gR34NativeUpdate-YYYYMMDD.zip component (Build 6 or higher). For detailed installation instructions, refer to the readme.html packaged within the zip file.
3. Ensure that the following versions of components are installed.
   - BrowserUrlPath 2009_07_16 (build 14) br-10g-10.1.3.5-release or higher
   - NativeOsUtils 090415 (build $Rev: 73693 $) or higher
   - CS10gR35UpdateBundle 2009_07_27 (build 15) or higher
   - ContentFolios 1.0.0.100 ($Rev: 74704 $) br-10g-10.1.3.5-release or higher

2.1.5 Oracle Distributed Document Capture v10.1.3.5+ and related components

---

Note: The requirements listed in this section apply only if using Oracle Distributed Document Capture for optional scanning functionality.

- User: Internet Explorer 6 or above is required.
- Administration: Oracle Distributed Document Capture Release 10.1.3.5 is required. After this installation, apply cumulative patch 9459254 or higher (available on My Oracle Support).

2.1.6 Oracle VueLink 19.3 for Oracle UCM

Note: The requirements listed in this section apply only if providing optional document viewing with the adapter via Oracle AutoVue.

For complete installation requirements for integrating AutoVue viewing with Oracle UCM, see the system requirements section in the *Oracle VueLink 19.3 for Oracle UCM System Administrator Manual* (or higher). Requirements include:

- AutoVue Web Version 19.3 (and any service packs for 19.3) or AutoVue 20 (and any service packs for 20).
- Oracle VueLink 19.3 for Oracle UCM, the AutoVue VueLink integration for Oracle UCM.

2.2 About the Adapter Files

The Oracle Enterprise Content Management Application Adapters (Managed Attachments Solution) provide a single adapter that covers E-Business Suite and PeopleSoft use for Managed Attachments.

Figure 2–1 illustrates the Managed Attachments architecture when installed for E-Business Suite use, and Figure 2–2 illustrates PeopleSoft installation.

Figure 2–1 Managed Attachments Architecture for E-Business Suite Adapter for ECM

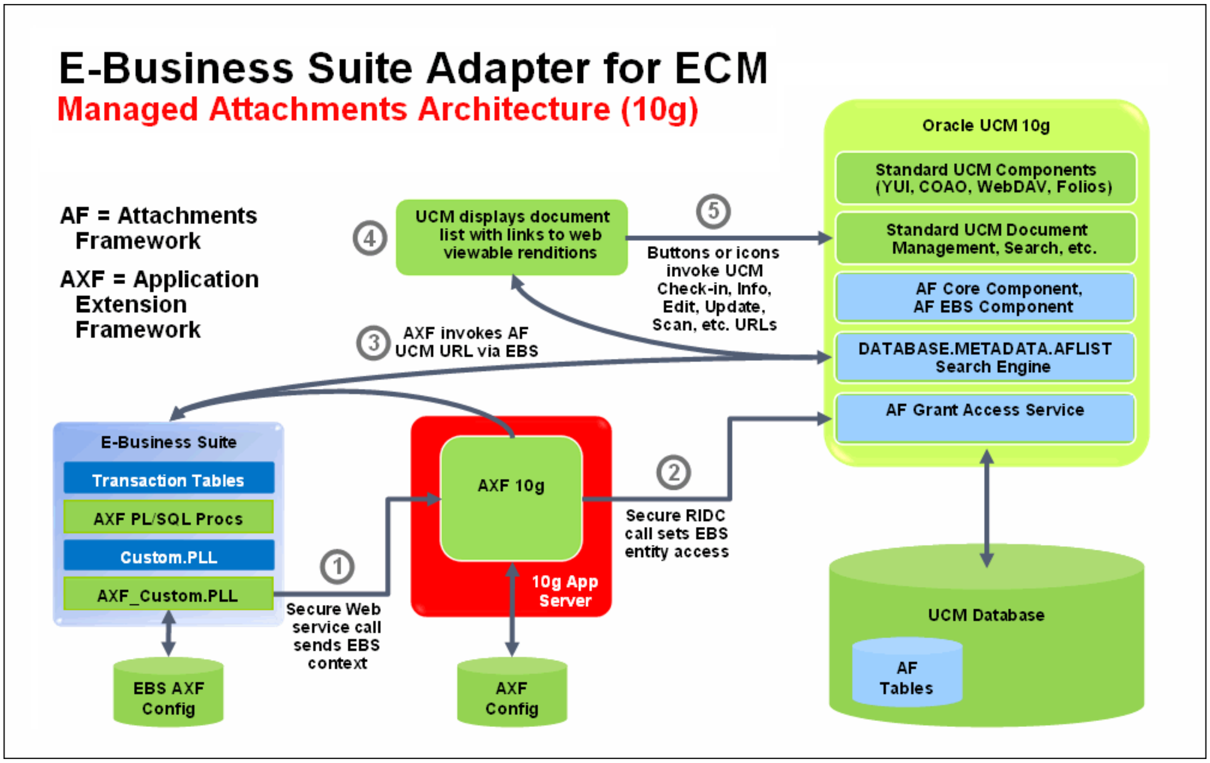
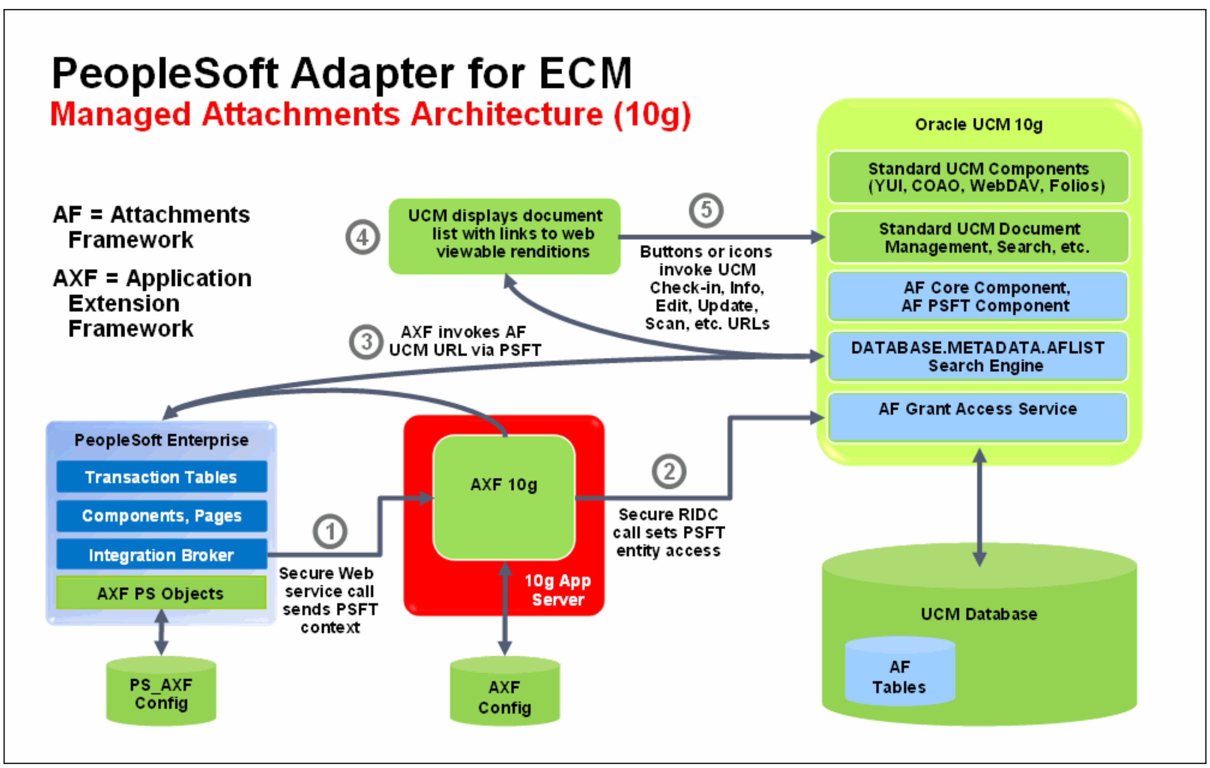


Figure 2–2 Managed Attachments Architecture for PeopleSoft Adapter for ECM



The adapter includes the following parts:

Application Extension Framework (AXF)

This portion consists of an AXF Java EE ear file and configuration scripts that create AXF solution tables. See "Installing and Configuring AXF" on page 2-6.

Business Application Plug-In

This portion consists of a business application plug-in (E-Business Suite and/or PeopleSoft).

- Configuring the E-Business Suite plug-in consists of running PL/SQL scripts against the E-Business Suite database that populate tables and configure functionality. You also upload files to the E-Business Suite system that integrate custom actions with pre-existing E-Business Suite Forms. See "Installing and Configuring the E-Business Suite Plug-In" on page 2-11.
- Configuring the PeopleSoft plug-in consists of importing the PeopleSoft project, configuring the Integration Broker to communicate with AXF, setting user roles, and enabling AXF functionality on PeopleSoft pages. See "Installing and Configuring the PeopleSoft Plug-In" on page 2-17.

Oracle UCM Components

This portion includes Oracle UCM components bundled in zip files that you install and enable via Component Manager. They include the AppAdapter framework core files and business application-specific files.

See "Installing and Configuring the Oracle UCM Components" on page 2-23.

2.3 Installing and Configuring AXF

This section describes how to install core AXF and adapter components using standard AXF distribution files. It covers the following topics:

2.3.1 Unzipping the Adapter Patch File

Follow these steps to obtain and unzip the adapter patch file. This file contains AXF and business application plug-in files. For information about Oracle UCM components, see "Installing and Configuring the Oracle UCM Components" on page 2-23.

1. Locate the latest AXF Patch (1.3.4 or higher) on My Oracle Support (support.oracle.com) under the **Oracle Imaging and Process Management** product.
2. Create a temporary folder called `AXF_INSTALL_DIR`. Copy the installation package to your Application Server middle tier and then unzip the package into this folder.

This location is referred to as *AXF_INSTALL_DIR* throughout this guide.

3. Unzip the AXF Patch (1.3.4 or higher) file into the AXF_INSTALL_DIR directory.

2.3.2 Creating an AXF Configuration Database User

AXF (including the adapter) utilizes an AXF database that is used as a configuration data store. This database requires a user configured with the appropriate access permissions.

The AXF infrastructure and installed solutions require a database user with the appropriate privileges for installation. The system will not function without a database for the configuration store. It is highly recommended that you create a new user to store this data rather than using a system or default account. This prevents AXF tables mixing with tables that belong to other applications. Consult with your DBA to ensure that a secure user configuration is used both before and after installation and that the configuration meets your organization's database security requirements.

1. Create a user named `AXF` in the AXF configuration database.
2. Assign the new user the following privileges in order to properly install AXF. The AXF user's access privileges can be reduced after completing the installation.
   - Tablespace privileges for default or target tablespace
   - Non-zero quota in default tablespace
   - Connect role
   - Create index
   - Create table
   - Create sequence
   - Create session
   - Create synonym
   - Insert table
   - Select table
   - Select sequence
   - Update table

2.3.3 Installing AXF

An AXF install script is provided for both Windows and Unix-based platforms and is located in the /install directory of the AXF installation package. The install script automatically performs configuration and deployment of the AXF .ear file and creates the required tables for AXF solutions.

> **Note:** The Automated AXF Installation Script does not configure E-Business Suite or PeopleSoft plug-ins. These components are configured in later sections.

The Installer performs the following tasks:

- Creates Application Server database tables to support AXF
- Creates a data source for connecting to Application Server

- Creates a data source for connecting to E-Business Suite. (This task does not apply to PeopleSoft.)
- Configures properties of the AXF EAR based on `installer.properties`
- Deploys the configured `.ear` to the specified Application Server

2.3.3.1 Configuring the Automated AXF Installation Script

Follow the steps in this section to modify parameters in the installation script to match your environment.

1. From the */dbscripts* directory, open the AXF_ATTACHMENTS_CONFIG.sql script.

   Note: Install AXF on a separate application server from the E-Business Suite or PeopleSoft Application Server.

   ---

2. Change the machine name and port for the *UCM_CONNECTION_STR* parameter to match your Oracle UCM installation. The port number should correspond to that of the Content Server's web server port. Change the */idc/* portion of the URL to match your Oracle UCM installation’s web root (i.e. */ucm_web_root/*).
3. Change the `[ContentServerProfile]` parameter to either *EBSProfile* or *PSFTProfile* to match your business application.
4. Change the `[ResultTemplate]` parameter to either *EBS_LIST* or *PSFT_LIST* to match your business application.
5. Change the machine name and port for the *RIDC_CONNECTION_STR* parameter to match your Oracle UCM installation. The port number should correspond to that of the Content Server’s Intradoc server port that receives RIDC calls. (To find the value for the Oracle UCM server port, locate the IntradocServerPort config value in config.cfg.)

   In the next section, the AXF installation script automatically runs the AXF_ATTACHMENTS_CONFIG.sql script.

2.3.3.2 Running the Automated AXF Installation Script

Note: A Java Virtual Machine (JVM) release 1.5 or higher is required to run this script successfully.

To run the AXF installation script:

1. Start your AXF configuration database and ensure that an AXF user has been created with the required privileges, as previously described in "Creating an AXF Configuration Database User" on page 2-7.
2. Modify the values in *AXF_INSTALL_DIR*`/install/installer.properties` to match your environment configuration. Folder paths in the `installer.properties` must be entered with Unix folder delimiters (`/`) even when running on Windows.

   Modify the following values:

Property	Description
oracle.home	Application Server Oracle Home (ORACLE_HOME)
j2ee.home	Application Server J2EE (OC4J) Home (J2EE_HOME)
java.home	Java JDK/JRE Home (JAVA_HOME) - NOTE: JAVA_HOME variable must be set in the environment for ANT to work properly
oc4j.admin.user	OC4J Administrative User
oc4j.admin.password	OC4J Administrative User password
oc4j.deploy.uri	OPMN URI for .ear deployment - verify that your container name (oc4j_soa, home, etc.) is correct
db.axf.user	AXF configuration database user, as described in "Creating an AXF Configuration Database User" on page 2-7
db.axf.password	AXF configuration database user password
db.axf.connection	JDBC connection string for SOA database
db.ebs.user	The AXF E-Business Suite configuration schema user, as described in "Creating an AXF E-Business Suite Configuration Schema User" on page 2-12. **Important:** This setting applies to E-Business Suite only. If using PeopleSoft, edit the *AXF_INSTALL_DIR*/install/install.xml file and comment out the line shown below: <!-- comment the line below if not using E-Business Suite --> <antcall target="ebs-createDS" />
db.ebs.password	Password for E-Business Suite configuration schema user. (This setting applies to E-Business Suite only. See db.ebs.user description.)
db.ebs.connection	JDBC connection string for the E-Business Suite database. (This setting applies to E-Business Suite only. See db.ebs.user description.)

WARNING: Passwords used in installation are stored in cleartext in the *installer.properties* file and are echoed to *install.out* when the installer is run. Ensure that these files are handled properly and that files are removed or secured immediately following installation.

3. From the *AXF_INSTALL_DIR/dbscripts* directory, modify the **CreateAxfData.sql** script to match your environment. Modify the machine name and port in *ERROR_URL* and *webSecurityCheckUrl* to match your Application Server installation.

4. (Linux/Unix Only) If your Application Server is installed in a Linux or Unix environment, the files *AXF_INSTALL_DIR*/install/install.sh and *AXF_INSTALL_DIR*/install/ant/bin/ant must be granted execute permissions. While the procedure varies from environment to environment, this can generally be accomplished by issuing the following command:

```
chmod u+x install.sh ./ant/bin/ant
```

5. From the *AXF_INSTALL_DIR*/install/ directory, run install.sh (Linux/Unix) or install.bat (Windows).

> **Note:** If the following error is displayed during installation, it is a non-fatal error and can be ignored:
>
> *Unable to locate tools.jar \ Expected to find it in /usr/java/jre1.5.0_06/lib/tools.jar*

6. When the installation completes, use the `install.out` file to verify that the application deployment was successful.
7. Destroy or obfuscate the `install.out` file according to the security policies of your organization.
8. Protect the `installer.properties` file according to the security policies of your organization.

2.3.3.3 Verifying the Installation

A simple solution called *HelloWorld* is included with AXF to verify that the AXF infrastructure is properly installed. HelloWorld is a solution which simply returns a `Hello` string. To enable the HelloWorld solution:

1. Connect to the AXF database (not the E-Business Suite database) as the AXF database user and run the insertHelloCommand.sql script from the following directory.

   `AXF_INSTALL_DIR/drivers/HelloWorld/dbscripts`

2. Access the driver page of the AXF Web application using the following URL:

   http://*host*:*port*/axf-web/faces/Driver.jspx

3. Enter the following values:
   - Solution Namespace: `HelloWorld`
   - Command Namespace: `Hi`
   - User Name: `jcooper`
4. Click **Execute Command**.

   An AXF response should display with a populated Conversation ID. If the response is returned, the AXF infrastructure is functioning correctly and commands can be added and executed.

2.3.4 Configuring AXF For a Clustered Environment

When configuring the adapter in a clustered environment, the Managed Attachments solution will not be clustered. Instead, it will point to the server that is configured in the AXF configuration.

2.3.5 Configuring AXF Logging

Use the AXF logs to isolate issues in solution configuration. By default, AXF logging automatically occurs as part of Application Server logging. Follow these steps to configure separate AXF logging.

1. Add a log handler to the Application Server configuration.

```
$J2EE_HOME/config/j2ee-logging.xml
<log_handler name='axf-handler'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='path'  value='%ORACLE_HOME%/j2ee/%OPMN_PROC_TYPE%/log/axf'/>
<property name='maxFileSize' value='3485760'/>
<property name='maxLogSize' value='3485760'/>
<property name='encoding' value='UTF-8'/>
<property name='supplementalAttributes'  value='J2EE_APP.name,J2EE_
MODULE.name,WEBSERVICE.name,WEBSERVICE_PORT.name'/>
</log_handler>
```

2. Add a logger and set the level from the Log Levels (ODL Message Types) listed in Table 2–1. You can set the logging level in the XML file or via Enterprise Manager.

```
$J2EE_HOME/config/j2ee-logging.xml
<logger name='oracle.imaging' level='NOTIFICATION:1' useParentHandlers='false'>
<handler name='axf-handler'/>
</logger>
<logger name='oracle.imaging.axf' level='NOTIFICATION:1'
useParentHandlers='false'>
<handler name='axf-handler'/>
</logger>
```

Table 2–1 Available Log Levels

Log Type	Description	Log Level (ODL Message Type)
NULL	The logger inherits the log level set for its parent.	n/a
SEVERE	Log system errors requiring attention from the system administrator.	ERROR:1
WARNING	Log actions or conditions discovered that should be reviewed and may require action before an error occurs.	WARNING:1
INFO	Log normal actions or events. This could be a user operation, such as login completed, or an automatic operation, such as a log file rotation.	NOTIFICATION:1
CONFIG	Log configuration-related messages or problems.	NOTIFICATION:16
FINE	Log trace or debug messages used for debugging or performance monitoring. Typically contains detailed event data.	TRACE:1
FINER	Log fairly detailed trace or debug messages.	TRACE:16
FINEST	Log highly detailed trace or debug messages.	TRACE:32

3. Restart oc4j if it is running. The logger will be displayed in Enterprise Manager. You can change the logging level at runtime.

2.3.6 Setting User Locales

To prevent issues with different locales when invoking AXF, business application users should set the same values for their user locale preference and their browser locale. The same value should also be set for the Oracle UCM locale.

2.4 Installing and Configuring the E-Business Suite Plug-In

Follow the steps in this section if integrating E-Business Suite with the adapter. For PeopleSoft integration, see "Installing and Configuring the PeopleSoft Plug-In" on page 2-17.

This section covers the following topics:

- "Creating an AXF E-Business Suite Configuration Schema User" on page 2-12
- "Configuring the E-Business Suite Database" on page 2-12
- "Compiling E-Business Suite Forms" on page 2-14
- "Enabling or Disabling the Paperclip Attachments Option" on page 2-16
- "Configuring E-Business Suite Logging" on page 2-17

2.4.1 Creating an AXF E-Business Suite Configuration Schema User

AXF utilizes an E-Business Suite database used to store PL/SQL procedures and E-Business Suite configuration information for the integration. This database requires a user that is configured with the appropriate access permissions.

Create a user named `AXF` for use by AXF within the E-Business Suite database. A system account username and password is required to create the user. For assistance creating the user, contact your DBA. The AXF E-Business Suite configuration schema user must have the following access privileges:

- Create table
- Create sequence
- Create public synonym
- Create session
- Create procedure
- Unlimited tablespace

2.4.2 Configuring the E-Business Suite Database

Installation of the E-Business Suite portion of AXF requires an active connection to the E-Business Suite database, general database experience, and knowledge of E-Business Suite Forms Builder. Consult your local DBA for assistance with these tasks. The instructions below assume the use of SQL*PLUS, but you can use any tool capable of querying the Oracle Database.

To configure the E-Business Suite database:

1. Locate the scripts in the following folders. Separate folders are provided for E-Business Suite releases 11 and 12.
   - `AXF_INSTALL_DIR/ebs/R12/`
   - `AXF_INSTALL_DIR/ebs/R11/`
2. Using SQL*PLUS, log in to the E-Business Suite database as the AXF E-Business Suite configuration schema user (AXF).

   This user was previously created, as described in "Creating an AXF E-Business Suite Configuration Schema User" on page 2-12.
3. As the AXF user, execute the **AXF_CREATE_TABLES_SYNONYM** script from the applicable E-Business Suite location. This script creates the tables and synonyms used by AXF.

   To execute the script, enter:

   ```
   @AXF_CREATE_TABLES_SYNONYM.sql
   ```

Verify that the following tables were created: AXF_COMMAND_PARAMETERS, AXF_COMMANDS, AXF_CONFIGS, AND AXF_FND_MAP.

4. As the AXF user, execute the **AXF_EBS_PROPERTIES_DATA**.sql script from the applicable E-Business Suite location.

   To execute the script, enter:

   `@AXF_EBS_PROPERTIES_DATA.sql`

5. Log in as the APPS user.

6. As the APPS user, execute the **AXF_APPS_INIT** script from the applicable E-Business Suite location.

   To execute the script, enter:

   `@AXF_APPS_INIT.sql`

7. As the APPS user, execute the **AXF_ADD_EBS_ATTACHMENT_PROC_R12** or **AXF_ADD_EBS_ATTACHMENT_PROC_R11** script from the applicable E-Business Suite location. This script creates a stored procedure for inserting attachments to the transaction record.

   Execute the script by entering the command appropriate for your version:

   `@AXF_ADD_EBS_ATTACHMENT_PROC_R12.sql`

   `@AXF_ADD_EBS_ATTACHMENT_PROC_R11.sql`

   > **Note:** This compilation may result in warnings, which can be ignored.

8. As the APPS user, execute the **AXF_MANAGED_ATTACH_AVAIL**, **AXF_MANAGED_ATTACH_VALUES**, and **AXF_MANAGED_ATTACHMENT_DATA** scripts from the applicable E-Business Suite location.

   Execute the scripts by entering:

   `@AXF_MANAGED_ATTACH_AVAIL.sql`

   `@AXF_MANAGED_ATTACH_VALUES.sql`

   `@AXF_MANAGED_ATTACHMENT_DATA.sql`

9. As the APPS user, execute the **AXF_SOAP_CALL_PROC** script from the applicable E-Business Suite location. This script creates a stored procedure to make SOAP calls from PL/SQL.

   Execute the script by entering:

   `@AXF_SOAP_CALL_PROC.sql`

10. From the /ebs/r11 or /ebs/r12 directory, modify the AXF_EBS_ATTACHMENTS_CONFIG.sql script. Modify the machine name and port in the *`SolutionEndPoint`* parameter to match your AXF machine and port. Also, modify the `EBS_instanceA` value to one that uniquely identifies the E-Business Suite instance you are configuring.

11. Log in as the AXF user.

12. As the AXF user, run the **AXF_EBS_ATTACHMENTS_CONFIG** script for your E-Business Suite version, from the applicable E-Business Suite location.

    To execute the script, enter:

```
@AXF_EBS_ATTACHMENTS_CONFIG.sql
```

2.4.3 Compiling E-Business Suite Forms

AXF installation requires a number of files to be uploaded to the E-Business Suite system. This enables a seamless integration of custom actions with pre-existing E-Business Suite Forms.

Note: For information on using Oracle Forms Builder, see the following E-Business Suite documentation:

`http://www.oracle.com/technology/documentation/applications.html`

Follow these steps to copy the AXF_CUSTOM.pld file, convert it to an AXF_CUSTOM.pll file, make modifications, and then compile it to an AXF_CUSTOM.plx file.

1. For the applicable version listed below, copy the **AXF_CUSTOM.pld** file to the E-Business Server (to **FORMS_PATH** for E-Business Suite 12, or **FORMS60_PATH** for E-Business Suite 11).

   E-Business Suite 12: AXF_INSTALL_DIR/ebs/R12/AXF_CUSTOM.pld

   E-Business Suite 11: AXF_INSTALL_DIR/ebs/R11/AXF_CUSTOM.pld

   ---

   Note: If you are using a Linux/UNIX system and copied the .PLDs from a Windows machine, issue the `dos2unix` command before converting it below.

   ---

2. Open Oracle Forms Builder and connect to the E-Business Suite database as the APPS user. Forms Builder is typically located in the `/bin/` subdirectory of your database's Oracle Home.

   Note: Be sure to connect to the E-Business Suite database. If you fail to connect, verify the tnslistener.ora file.

   ---

3. In Forms Builder, open and convert `AXF_CUSTOM.pld` to AXF_CUSTOM.pll, by selecting **File**, then **Administration**, then **Convert**. Select **PL/SQL libraries** and **Text to binary** while converting the file.

   Note: If the following error is displayed during conversion of AXF_CUSTOM.PLD to AXF_CUSTOM.PLL, repeat this step until the file successfully converts.

   PDE-PL1038 - Can not open file as a PL/SQL Library

   Note: If the following error is displayed during conversion, click **OK** repeatedly until the file successfully converts.

   PDE-PLI018 - Could not find library AXF_CUSTOM

   ---

4. From the File menu, open `AXF_CUSTOM.pll`. Select **Program**, then **Compile pl/sql**, then **All** (E-Business Suite 12) or **Program**, then **Compile**, then **All** (E-Business Suite 11).
5. Compile `AXF_CUSTOM` into a module (`.plx`) by selecting **Program**, then **Compile Module** (E-Business Suite 12) or **File**, then **Administration**, then **Compile File** (E-Business Suite 11).

> **Notes:**
>
> - AXF_CUSTOM must be compiled using the APPS schema user ID.
> - If you encounter the following identifier or other errors referencing objects in APPCORE.pll while compiling, this indicates that the `APPCORE.pll` file must be attached to your form:
>
>   ```
>   'APP_SPECIAL.ENABLE' must be declared
>   ```

6. Select **File**, then **Connect**, and ensure that you are connected to the database as the APPS user.
7. Back up the `CUSTOM.pll` file.

> **WARNING:** **Modifications to CUSTOM.pll are modifications to the E-Business Suite infrastructure. Ensure that this file is appropriately backed up before making changes.**

8. Open `CUSTOM.pll` by selecting **File**, then **Open**, and selecting **PL/SQL Libraries** (`*.pll`) in the Files of Type field. After opening the file and expanding Program Units, right-click the custom package body of CUSTOM.pll and select **pl/sql editor**.
9. In the body text of `CUSTOM.pll`, modify the following text formatted in bold italics. If the file contains other customizations, place the following modification at the end of the existing code inside each function/procedure.

```
function zoom_available return boolean is
begin

-- Required for ALL integrations
return true;
end zoom_available;
```

> **IMPORTANT:** Be sure to modify the body text of the pll, NOT its header. Scroll down until you reach the following comment header:
>
> ```
> - -Real code starts here
> ```

10. In the body text of `CUSTOM.pll`, modify the following text formatted in bold italics. If the file contains other customizations, place the following modification after the existing code inside each function/procedure.

```
procedure event(event_name varchar2) is
begin
```

```
-- Required for AXF integrations
AXF_CUSTOM.event(event_name);
null;

end event;
```

Note: Do not remove the `null;` line.

11. With `CUSTOM.pll` open, determine if AXF_CUSTOM is listed as an attached library.
    - If it is listed, highlight AXF_CUSTOM and click the minus (-) symbol to detach it. Then reattach AXF_CUSTOM by highlighting Attached Libraries under CUSTOM and clicking the plus (+) symbol; browse to AXF_CUSTOM.pll and select it.
    - If it is not listed, attach AXF_CUSTOM by highlighting Attached Libraries under CUSTOM and clicking the plus (+) symbol; browse to AXF_CUSTOM.pll and select it.

    When prompted to remove the path, click **Yes**.
12. With `CUSTOM.pll` open, verify that APPCORE and APPCORE2 are listed as attached libraries to AXF_CUSTOM.pll. If not listed, attach them. If listed, detach and attach them.
13. With `CUSTOM.pll` open, select **Program**, then **Compile pl/sql,** then **All** (E-Business Suite 12) or **Program**, then **Compile**, then **All** (E-Business Suite 11).
14. Compile CUSTOM into a module (.plx) by selecting **Program**, then **Compile Module** (E-Business Suite 12) or **File**, then **Administration**, then **Compile File** (E-Business Suite 11).
15. Save all before exiting Forms Builder. Verify that the Zoom menu command is displayed in the appropriate E-Business Suite forms.

2.4.4 Enabling or Disabling the Paperclip Attachments Option

By default, the E-Business Suite paperclip attachment option is disabled as part of Managed Attachments configuration. To use this native E-Business Suite attachments feature in coexistence with the ECM Managed Attachments solution, you must re-enable the paperclip icon as described below.

Note: This section applies to E-Business Suite use only.

1. Add the following row to the AXF_PROPERTIES table:

Table 2–2 AXF_PROPERTIES Values For PaperClip Use

PROPNAME	PROPVALUE
AXF_PAPERCLIP	Set to TRUE to enable the paperclip option, or FALSE (default) to disable it.

For more information, see "AXF_PROPERTIES Table (E-Business Suite)" on page A-12.

2.4.5 Configuring E-Business Suite Logging

You enable logging for specific forms in the AXF_CONFIGS table, as described in "AXF_CONFIGS Table (E-Business Suite)" on page A-8.

To enable logging for a particular Form function, set the LOGENABLED field to either `1`, `YES` or `TRUE` and the file will be created in the UTL_FILE_DIR folder. Consult with your DBA to verify that the UTL_FILE_DIR folder is available and accessible. Log files are named *Username_MASTER_LOG.txt*, and continue to grow as items are appended.

2.5 Installing and Configuring the PeopleSoft Plug-In

Follow the steps in this section if integrating PeopleSoft with the adapter. For E-Business Suite integration, see "Installing and Configuring the E-Business Suite Plug-In" on page 2-11.

> **Note:** PeopleSoft integration does not require an additional database user, as all necessary tables are created when importing a project. For information on importing a project, see "Importing the PeopleSoft Project" on page 2-17.

Follow these main steps to configure PeopleSoft components for the attachments solution:

- "Importing the PeopleSoft Project" on page 2-17
- "Configuring Integration Broker to Communicate with AXF" on page 2-18
- "Adding the AXF_ROLE to PeopleSoft" on page 2-20
- "Assigning Users the AXF_ROLE" on page 2-20
- "Determining Primary Keys for PeopleSoft Screens" on page 2-21
- "Enabling AXF Components on PeopleSoft Pages" on page 2-22
- "Configuring PeopleSoft Logging" on page 2-23

2.5.1 Importing the PeopleSoft Project

Follow these steps to import the PeopleSoft project:

1. As a user with administrative privileges, create a tablespace called `AXF` in the database containing the PeopleSoft schemas.

   > **Note:** SQL Server automatically creates the tablespace upon importing the project. If your PeopleSoft installation uses a SQL Server, this step is not required.

2. Start the PeopleSoft Application Designer in two-tier mode and log in as the user with administrative privileges.
3. From the menu, select **Tools**, then **Copy Project**, then **From File**. The Copy From File screen is displayed.
4. Locate the `AXF_INSTALL_DIR/psft` directory, found in the AXF file you previously unzipped in "Unzipping the Adapter Patch File" on page 2-6.

5. Select the **psft** directory, then select the **AXF_PS_INTEGRATION** directory and click **Open**.

   The second AXF_PS_INTEGRATION directory contains the project XML files, but you must select its parent directory (of the same name) to access them from the PeopleSoft Application Designer. The AXF_PS_INTEGRATION project is displayed in the lower pane of the screen.

6. Click **Select**, select all definition types, and click **Copy**. The project files begin copying.
7. After all files have copied, select **Build**, then **Project** from the menu. The Build screen is displayed.
8. Select the **Create Tables** and **Execute SQL Now** options, and click **Build**. You can monitor the build status as the files are imported into PeopleSoft.
9. Once done, check the PSBUILD.LOG file to verify that the project imported successfully.
10. If the log file shows *tablespace 'AXF' does not exist* errors, the tablespace was not created properly. Manually create a tablespace called `AXF` in the same database you logged into when starting the PeopleSoft Application Designer, then return to step 5 to rebuild the project.
11. Click **Save All**.

2.5.2 Configuring Integration Broker to Communicate with AXF

Importing the AXF_PS_INTEGRATION project into PeopleSoft also imports the Integration Broker connection information. These components contain information needed to connect from PeopleSoft to the AXF Server. This section describes how to access this information in the PeopleSoft web client and edit it to point to the AXF Server.

Complete the steps in the sections listed below to configure communication between the Integration Broker and AXF:

- "Configuring Communication With a 10g AXF Server" on page 2-18
- "Encrypting the Gateway Password" on page 2-19
- "Setting Up the Service Operation Routings" on page 2-19
- "Validating Domain Status" on page 2-20

> **Note:** A PeopleSoft local integration gateway must be set up for PeopleSoft external communications. See the PeopleSoft Enterprise documentation for information about setting up gateways. You can then proceed with configuring the PeopleSoft service operation to communicate with a 10g AXF server.

2.5.2.1 Configuring Communication With a 10g AXF Server

1. In PeopleSoft Server, open **PeopleTools**, then **Integration Broker**, then **Integration Setup**. The Integration setup menu expands to show the available options.
2. Click **Nodes**.
3. On the Find an Existing Value tab, select **Node Name**, enter `AXF` in the Node Name field, and click **Search**.

4. From the search results, click the **AXF_SOLUTION_MEDIATOR_10G** link.
5. Click the Connectors tab.
6. Set the Host property name to the AXF Server name or IP address.
7. Set the URL property name to the following URL:

   `http://`*`AXF_Server name or IP address`*`:`*`port_number`*`/imaging-bai-axf/AxfSolutionMediator`

8. Click **Save**.
9. Click **Ping Node** to verify that the node is configured properly.
   - If configured properly, the word *Success* is displayed in the message text area of the Ping NodeResults page. Proceed to "Setting Up the Service Operation Routings" on page 2-19 and "Validating Domain Status" on page 2-20.
   - If *Success* is not displayed, see "Encrypting the Gateway Password" on page 2-19. Return to the Node Configuration page to reenter values until you can ping the node successfully.

2.5.2.2 Encrypting the Gateway Password

If *Success* is not displayed after pinging the node, you may need to encrypt the secureFileKeystorePasswd value under Gateway Properties, as described in the following steps.

1. In PeopleSoft Server, open **PeopleTools**, then **Integration Broker**, then **Configuration**, then **Gateways**.
2. Search for and open the LOCAL gateway, then click the **Gateway Setup Properties** link.
3. Sign on to access the integrationGateway.properties file.
4. Click the **Advanced Properties Page** link.
5. Use the Password Encryption Utility on the Gateway Properties page to encrypt the secureFileKeystorePasswd value.
6. In the Gateway Properties screen, paste the encrypted password after **secureFileKeystorePasswd=** and click **OK**.

2.5.2.3 Setting Up the Service Operation Routings

1. From the Integration Setup Menu, select **Service Operations**.
2. On the Find Service Operation tab, enter `AXF` in the Service Operation field and click **Search**. A single results listing is returned.
3. Click the **AXF_EXECUTE** link.
4. Click the Routings tab.
5. Verify that the AXF_SM_ROUTING_10G routing definition's status is Active. If it is not, choose the Selected field, click the **Activate Selected Routings** button, and ensure that all other routing definition are set to Inactive.

   Important: Ensure that the 10g routing definition is active and the 11g one is deactivated.

6. Click the Save button.

2.5.2.4 Validating Domain Status

Once you have configured the Integration Broker to communicate with AXF, follow these steps to verify its status.

1. Navigate to the Service Operation Monitor page by selecting **PeopleTools,** then **Integration Broker,** and then **Service Operations Monitor**. The Service Operations Monitor page is displayed.
2. Click **Domain Status** under the **Administration** section. The Domain Status page is displayed.
3. Verify that the domain status is listed as **Active** next to the PeopleSoft Server. If not, select **Active** from the Domain Status menu and click **Update**.

2.5.3 Adding the AXF_ROLE to PeopleSoft

To ensure that appropriate PeopleSoft users have access to AXF functionality, follow these steps to add the AXF_ROLE and permissions to PeopleSoft.

1. In PeopleSoft Server, open **PeopleTools**, then **Security**, then **Permissions & Roles**. The Permissions & Roles menu expands to show available options.
2. Click **Roles**. The Roles page is displayed.
3. Click the **Add New Value** tab.
4. Enter `AXF_ROLE` in the Role Name field and click **Add**. The Role Name field is cleared and the AXF_ROLE is added. You may need to enter a description and click **Save**.
5. Click **Roles**. Click the **Find an Existing Value** tab and find AXF_ROLE from the listing of available roles. Click AXF_ROLE, and its details are displayed.
6. Click the **Permission Lists** tab, enter `AXF_PERMS` in the Permission List field, and click **Save**.

2.5.4 Assigning Users the AXF_ROLE

After creating the AXF_ROLE in PeopleSoft, follow these steps to assign the role to all users that require access to AXF functionality.

> **Note:** For AXF calls to be processed correctly from PeopleSoft, all users needing access to AXF functionality must be assigned the AXF_ROLE in PeopleSoft.

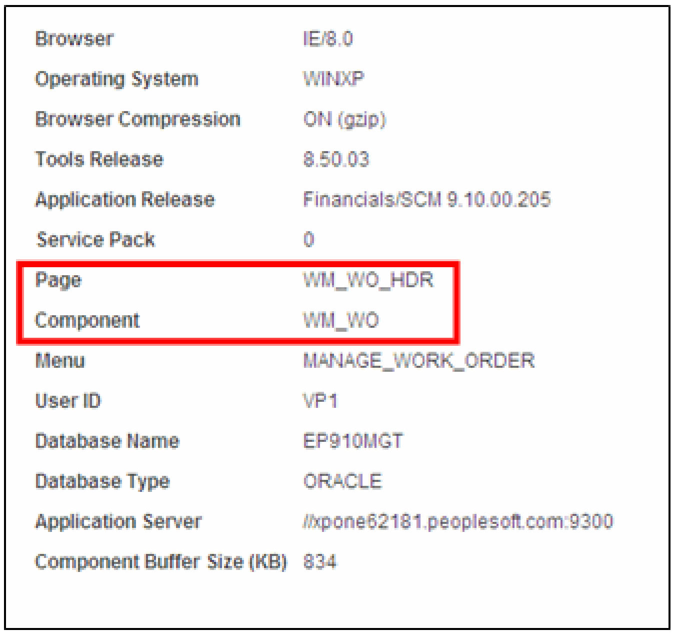
1. In PeopleSoft Server, open **PeopleTools**, then **Security**, then **User Profiles**. The User Profiles menu expands to show available options.
2. Click **User Profiles**. The User Profiles page is displayed.
3. Select the criteria by which to search, enter it in the search field, and click **Search**. A listing of users is displayed.
4. Click the user to which to assign the role. A detailed page of user information is displayed.
5. Click the **Roles** tab. A listing of roles assigned to the user is displayed.
6. Enter `AXF_ROLE` in a blank field (clicking the + icon to create a blank row if needed), or click the magnifying glass icon to search for the role.

7. Click **Save**. The user can now access AXF functionality on PeopleSoft pages.

2.5.5 Determining Primary Keys for PeopleSoft Screens

Follow these steps to determine the primary keys for a specific PeopleSoft screen:

1. In the PeopleSoft application, navigate to the page to enable.
2. Press **Ctrl+J**. In the info page, note the Page and Component entries for the selected screen.



3. In the Application Designer, select **File/Open** and choose **Page** from the Definition field.
4. In the Name field, enter the page name you noted in step 2 and click **Open**.
5. Select the Order tab at the top.
6. From the set of fields listed, identify the field that is the most likely unique id (for example, VOUCHER_ID for Invoice Entry) and note the record name.
7. From the Insert menu, select the **Definitions into Project** command, and select **Records** from the Definition Type field.
8. In the Name field, enter the record name you noted in step 6 and click **Insert**.
9. Select the record in the list and click **Insert** again. The record is inserted into the Project Tree on the left.
10. Expand the Records tree on the left, then expand the record you added. The primary keys are listed at the top, with a gold key icon to the left of the key name. Note the primary keys. See "PeopleSoft Tables" on page A-13.

2.5.5.1 Sample Primary Keys

Table 2–3 Sample Primary Keys

Screen	Page Name	Record Name	Primary Key
Maintenance Management / Work Order Management / Work Order	WM_WO_HDR	WM_WO_HDR	BUSINESS_UNIT
Maintenance Management / Work Order Management / Work Order	WM_WO_HDR	WM_WO_HDR	WO_ID
Asset Management / Asset Transactions / Owned Assets	ASSET_GENERAL_01	ASSET	BUSINESS_UNIT
Asset Management / Asset Transactions / Owned Assets	ASSET_GENERAL_01	ASSET	ASSET_ID
Quick Invoice Entry	VCHR_QV_SBP_HDR	VCHR_HDR_QV	BUSINESS_UNIT
Quick Invoice Entry	VCHR_QV_SBP_HDR	VCHR_HDR_QV	VOUCHER_ID

2.5.6 Enabling AXF Components on PeopleSoft Pages

You configure AXF components on PeopleSoft pages using the PeopleSoft Application Designer and the AXF tables in PeopleSoft. For PeopleSoft table descriptions and examples, see "PeopleSoft Tables" on page A-13.

Follow these steps to enable an AXF component on a PeopleSoft page.

1. Open the AXF_PS_Integration Project in PeopleSoft Application Designer.
2. Open a PeopleSoft page to enable. For example, open VCHR_HDR_QV2.
3. Select a button or link and drag it onto the PeopleSoft page in an appropriate location.

   PeopleSoft user interface items refer to AXF buttons, links, and menus you place on a PeopleSoft page. Five of each are provided (for example, AXF_BUTTON_1 through _5). For more information and configuration examples, see "PS_AXF_COMMANDS Table (PeopleSoft)" on page A-14.
4. Save the page.
5. Configure the following PeopleSoft AXF tables to associate a command with the newly added button or link. See the following sections for table descriptions and examples:

   - "PS_AXF_CONFIG Table (PeopleSoft)" on page A-13
   - "PS_AXF_COMMANDS Table (PeopleSoft)" on page A-14
   - "PS_AXF_CMD_PARAMS Table (PeopleSoft)" on page A-15

     Use the PS_AXF_CMD_PARAMS Table (PeopleSoft) to configure a label for the list of attachments. You can use a combination of constant and data values to display key information, as described on page A-16.

Important Points About User Interface Items

- You must specify a PeopleSoft role (in the PS_AXF_COMMANDS Table (PeopleSoft)) to grant users permission to use a specified user interface item. If a user lacks the permissions, the item is not displayed.
- A user interface item becomes active when it is positioned on a page. If AXF_BUTTON_1 is placed on multiple pages in the same PeopleSoft component, it shares the same configuration across the pages. To configure different actions for

each page, use a different user interface item (for example, AXF_BUTTON_2). Note that you can re-use user interface items on different PeopleSoft components without conflicts.

2.5.7 Configuring PeopleSoft Logging

The AXF PeopleSoft adapter uses standard apache log4j logging. Logging can be activated and managed through the log4j.properties file. This file is located in the `PeopleSoft Installation Directory/class` directory. Set the following options:

```
# A1 is set to be a ConsoleAppender which outputs to System.out.
log4j.appender.A1=org.apache.log4j.DailyRollingFileAppender
log4j.appender.A1.File=./LOGS/PS_AXF.log

# A1 uses PatternLayout.
log4j.appender.A1.layout=org.apache.log4j.PatternLayout
log4j.appender.A1.DatePattern=.yyyy-MM-dd
log4j.appender.A1.layout.ConversionPattern=%d{DATE} [%t] %-5p %c %x - %m%n

log4j.category.com.oracle.axf=DEBUG, A1
```

At a minimum, define an appender with a valid file location, and the level of messages to report (see above). Valid levels include the following in order of decreasing detail, where DEBUG displays all messages and detail:

- DEBUG
- INFO
- WARN
- ERROR
- FATAL

Note: For detailed information about log4j, see the log4j documentation.

2.6 Installing and Configuring the Oracle UCM Components

Follow the sections listed below to install and configure Managed Attachments solution Oracle UCM components and test the completed solution.

- "Installing and Enabling Oracle UCM Components" on page 2-23
- "Verifying Required Oracle UCM Components and Configuration" on page 2-25
- "Configuring the Preferences.hda File" on page 2-26
- "Testing the Managed Attachments Solution" on page 2-29

2.6.1 Installing and Enabling Oracle UCM Components

Follow these steps to install the Oracle UCM components using Component Manager.

1. Create a temporary folder called *UCM_ADAPTER_INSTALL_DIR*.
2. Locate the following Managed Attachments patch from My Oracle Support (support.oracle.com) and unzip it into the folder you created in step 1:

   EBS/PSFT Adapter Managed Attachments 10.1.3.5.2 Patch (Build 1) or higher

Its contents (listed below) are placed in a subfolder called *ucm*.

– AppAdapterCore.zip (required)

– AppAdapterEBS.zip (only required for E-Business Suite integration)

– AppAdapterPSFT.zip (only required for PeopleSoft integration)

Important: Do not unzip these files, as they are read in as zip files in later steps.

---

3. If upgrading from an earlier installation of the E-Business Suite adapter, follow these additional upgrade steps. (If not upgrading, proceed to the next step.)

   a. Log in to the Oracle UCM schema of the database as the user that Oracle UCM server uses for its operations.

   b. From the UCM_ADAPTER_INSTALL_DIR/ucm/upgrade directory, run the script appropriate for your database type:

      `ebs_adapter_upgrade_oracle.sql` (for Oracle DB)

      `ebs_adapter_upgrade_sqlsvr.sql` (for SQL Server)

   c. Ensure that the AFObjects table structure was updated.

      The scripts add two new columns (dAFID and dID) to the AFObjects table, populate dAFID values, and make dAFID the primary key.

   d. See "Backing Up Customizations Before Upgrading" on page 2-25 to back up previous customizations as needed.

4. Log in to Content Server as an administrator.

5. Select **Admin Server** from the Administration menu.

   The Content Admin Server page is displayed.

6. Click the name of the Content Server instance where the component will be installed.

   The Content Admin Server <*instance_name*> page is displayed.

7. Click **Component Manager**.

   The Component Manager page is displayed.

8. Click **Browse**, navigate to the AppAdapterCore.zip file, and select it.

9. Click **Open**.

   The path is displayed in the Install New Component field.

10. Click **Install**.

    Component Manager lists the zip file contents to be installed.

11. Click **Continue**.

    Component Manager displays a message that the AppAdapterCore component was uploaded and installed successfully. The message asks if you want to enable the component immediately or return to the Component Manager.

12. Return to the Component Manager.

13. Click **Browse**, navigate to the appropriate business application zip file (*AppAdapterEBS.zip* for E-Business Suite or *AppAdapterPSFT.zip* for PeopleSoft), and select it.
14. Click **Open**.

    The path is displayed in the Install New Component field.
15. Click **Install**.

    Component Manager lists the zip file contents to be installed.
16. Click **Continue**.

    Component Manager displays a message that the business application component you selected was uploaded and installed successfully. The message asks if you want to enable the component immediately or return to the Component Manager.
17. Return to the Component Manager.

    To install both business applications, return to step 13, and continue the steps, selecting the other business application this time.
18. Enable all of the components you installed and restart Content Server.
19. Check the Content Server and database logs to ensure that no application adapter install errors occurred.

2.6.1.1 Backing Up Customizations Before Upgrading

If upgrading from a previous version of the E-Business Suite adapter (Managed Attachments solution), you may need to perform these additional upgrade steps before installing Oracle UCM components. See step 3 in "Installing and Enabling Oracle UCM Components" on page 2-23.

1. Back up Content Server rule and profile customizations.

   Installing the new adapter overwrites existing rules and profiles. If your previous installation includes customizations to Content Server rules and profiles, back up these rules and profiles using a CMU bundle before installing Oracle UCM components. After installation, you will need to create new rules and profiles, and manually apply any customizations.
2. Back up the config.cfg file.

   This adapter release stores environment variables using a preferences.hda file instead of config.cfg. After installation, you will need to manually copy configuration preferences from config.cfg to preferences.hda.
3. Back up any other template or resource include customizations and modifications.

   Some resource includes and templates have changed in this release. You will need to manually set these customizations after installation.

2.6.2 Verifying Required Oracle UCM Components and Configuration

Follow these steps to verify that required Oracle UCM components are enabled on the Content Server.

1. Log in to Content Server as an administrator.
2. Click the **Configuration for [Instance]** link in the content server Administration tray.
3. In the Features And Components section, click **Enabled Component Details**.

4. From the details shown, verify that the following components are enabled. If a component is not listed, install and enable it according to its installation documentation.

   The following components must be at or above the version level included with Oracle UCM 10gR3 v10.1.3.5:

   - YahooUserInterfaceLibrary
   - CheckoutAndOpenInNative
   - CoreWebdav

   The following components must be at or above these version levels:

   - BrowserUrlPath 2009_07_16 (build 14) br-10g-10.1.3.5-release or higher
   - NativeOsUtils 090415 (build $Rev: 73693 $) or higher
   - CS10gR35UpdateBundle 2009_07_27 (build 15) or higher
   - ContentFolios 1.0.0.100 ($Rev: 74704 $) br-10g-10.1.3.5-release or higher

5. In the User Admin applet, ensure that the roles below have the correct access level to the corresponding security groups.

   In Content Server, select the Administration option from the main menu, choose **Admin Applets**, then **User Admin**. Select **Security**, then **Permissions by Role**.

   - AFAdmin: AFDocuments (RWDA) and no permissions on any other groups
   - AFDelete: AFDocuments (RWD) and no permissions on any other groups
   - AFWrite: AFDocuments (RW) and no permissions on any other groups
   - AFRead: AFDocuments (R) and no permissions on any other groups

2.6.3 Configuring the Preferences.hda File

Installing and enabling the AppAdapter component creates a default configuration file called **preferences.hda**.

Follow these steps to modify the preferences.hda file.

1. Open the preferences.hda file in the following directory:

   UCM_Instance`/data/appadapter`

   This file provides Oracle UCM adapter configuration options in the ResultSet sections described in Table 2–5.

Table 2–4 ResultSet Sections in Preferences.hda File

Section	Description
AFEnvironmentConfiguration	Use to configure Oracle UCM environment variables for the adapter. For example, enable and configure scanning or AutoVue document viewing, and hide or display buttons for specified business entities. For more information, see Table 2–5 and "Customizing the Adapter" on page 2-41.
AFRelationshipAttributes	Use to configure custom relationships between attached documents and business entities. For example, enable attached document printing for certain business entities but not for other entities. For more information, see "Configuring Relationship Attributes" on page 2-47.
AFRevisionSpecificEntities	Use to enable users to access the document version that was attached, even if the document was later updated. For more information, see "Configuring Revision-Specific Mode" on page 2-48.

2. Scroll to the AFEnvironmentConfiguration ResultSet section, and edit the entries listed in Table 2–5 as needed. For more information about customizing the attachments solution using these variables, see "Customizing the Adapter" on page 2-41.

> **Note:** You can specify preferences on a global, application, and application+business entity level. For more information and examples, see "Customizing at Global, Application, and Business Entity Levels" on page 2-42.

Table 2–5 Preferences.hda Environment Variables

Field	Default Value	Description
AppAdapterGrantPrivilege	W	Specifies the access level to be granted to all users if the AF_GRANT_ACCESS service's *dPrivilege* parameter is not specified. Valid values include: R (read), W (write), D (delete) and A (admin). For more information, see "AFGrants Table" on page A-17.
AppAdapterGrantHours	0.5	Specifies the time in hours for which the user session remains available. This value is used only if the AF_GRANT_ACCESS service's *numHours* parameter is not specified. Valid values are numbers with optional decimal. For more information, see "AFGrants Table" on page A-17.
AppAdapterMaxGrantHours	24	Specifies the maximum time in hours for which the user will be granted access to the Managed Attachments screen. Valid values are numbers with decimal. For example, suppose AppAdapterGrantHours is set to 1 hour and AppAdapterMaxGrantHours is set to 24 hours. If the user accesses the Managed Attachments screen from the business application at 12:00 (noon), dExpirationDate in the AFGrants Table is set to 13:00 and dMaxExpiration is set to 12:00 (noon) the next day. If at 12:30, the user performs an action (such as checking in a document), dExpirationDate changes to 13:30, and so on. This means that the user can have access to the Managed Attachments screen up to 24 hours if at any given time the gap between two requests is less than one hour. Regardless, once 24 hours is reached, access is denied. This prevents a user from keeping access open for very long periods of time without user action, and prevents access from expiring if a user is actively using the system.
AppAdapterKeyDelimiter	|	This is the internal delimiter, used to concatenate primary keys and values passed as parameters. See "AFGrants Table" on page A-17. The default delimiter is a | (pipe) character.
ODDCURLPath		Enables document attachment scanning and importing via Oracle Distributed Document Capture. For configuration instructions, see "Configuring Oracle Distributed Document Capture" on page 2-35. This entry specifies the web address to Oracle Distributed Document Capture. **Format:** `ODDCURLPath=http://`*`ODDC_host/ODDC_webcapture_address`* **Example:** `ODDCURLPath=http://xyz/webcapture.asp`
ODDCScanAction	1	Use to configure document attachment scanning and importing via Oracle Distributed Document Capture, as described in"Configuring Oracle Distributed Document Capture" on page 2-35. In this entry, specify the scan action to be performed, where: ▪ 1 = Scan ▪ 2 = Import

AutoVueURLPath		Enables AutoVue viewing of attached documents via Oracle AutoVue Web Version. For configuration instructions, see "Configuring Oracle AutoVue Document Viewing" on page 2-33. This entry specifies the AutoVue servlet to be run.
		Format:
		`AutoVueURLPath=http://`*`ucm_hostname:port/web_root`*`/jsp/autovue/csiApplet.jsp`
		Example:
		`AutoVueURLPath=http://ucm1.mycompany.com/idc/jsp/autovue/csiApplet.jsp`

AppAdapterAutoVueIconVisible	false	Specifies if the **AutoVue** icon is displayed in the Actions column of the Managed Attachments screen. For more information, see "Configuring Oracle AutoVue Document Viewing" on page 2-33.

Table 2–5 (Cont.) Preferences.hda Environment Variables

Field	Default Value	Description
AppAdapterDetachBtnVisible	true	Specifies if the **Detach** button is displayed in the Managed Attachments screen.
AppAdapterRefreshBtnVisible	true	Specifies if the **Refresh** button is displayed in the Managed Attachments screen.
AppAdapterCheckinNewBtnVisible	true	Specifies if the **New** button is displayed in the Managed Attachments screen.
AppAdapterRepoAttachBtnVisible	true	Specifies if the **From Repository** button is displayed in the Managed Attachments screen.
AppAdapterFrameLessWindowRequired	true	Specify if standard browser menu options are hidden in browser windows that open from the attachments display (true) or displayed (false).
AppAdapterConfigureBtnVisible	true	Specifies if the **Configure** button is displayed in the Managed Attachments screen.
AppAdapterScanBtnVisible	false	Specifies if the **Scan** button is displayed in the Managed Attachments screen.

3. Restart Content Server.

2.6.4 Testing the Managed Attachments Solution

Test the configuration for your selected business application by following the steps listed in "Displaying Managed Attachments in E-Business Suite" on page 3-2 or "Displaying Managed Attachments in PeopleSoft" on page 3-2.

2.6.4.1 Additional Verification

To confirm that you have met Oracle UCM 10.1.3.5 prerequisites, perform the following steps:

1. Enter the following URL:

   `http://`*`UCM hostname or IP address:WebServerPort/ucm web root`*`/idcplg?idcfilter=filterversion`

   If using an Apache filter for Oracle UCM, a value of *Oracle 10gR3 Apache UCM Filter 5.1.1.96* (or higher) should be returned.

2. Enter the following URL:

   `http://`*`UCM hostname or IP address:WebServerPort/ucm web root`*`/idcplg/_p/min?IdcService=GET_DOC_PAGE&Action=GetTemplatePage&Page=HOME_PAGE&Auth=Internet`

   A search page without the top level Content Server menus should be returned. Clicking **Search** should display search results, and the `/_p/min` should be preserved in the search results URL.

2.7 Managing Authentication and Security

This section provides instructions on managing authentication and security for the adapter. It covers the following topics:

- "Securing AXF via Oracle Internet Directory and Single Sign-On" on page 2-30
- "Configuring SSL for AXF (E-Business Suite)" on page 2-31
- "Securing Communications" on page 2-32

- "Managing Business Application and Oracle UCM Users" on page 2-33

2.7.1 Securing AXF via Oracle Internet Directory and Single Sign-On

If you are using Oracle Internet Directory (OID) and Single Sign-On (SSO), follow the steps below to secure AXF.

These services must be installed and configured if they are not currently part of your environment. For more information, see the section describing Oracle Identity Management in the *OC4J Security Guide*.

To secure AXF using OID and OSSO:

1. Verify that Oracle Identity Manager is installed and that the appropriate groups and users that require access to AXF are set up on OID. It may be convenient to define a group (for example, `APUsers`) and add the OID users and groups that require access to AXF to this new group.
2. Verify that the Application Server on which the AXF framework runs is a registered OSSO partner with OID.
3. Modify `mod_osso.conf`, found at *ORACLE_SOA_HOME*`/Apache/Apache/conf`, by inserting the following within the `<IfModule mod_osso.c>` element:

```
<Location /axf-web>
   require valid-user
   AuthType Basic
</Location>
```

4. Modify `orion-application.xml`, found inside the `/META-INF` subdirectory of the `ImagingBaiAxf` EAR file, to map the appropriate OID users and groups to the `users` logical group. For example, if there is an `APUsers` group that needs access to the AXF, insert the following node within the `<orion-application>` element:

```
<!-- Map OID groups and users to the Users logical group -->
<security-role-mapping name="users">
   <group name="APUsers" />
</security-role-mapping>
```

> **Note:** This file must be modified before deploying the AXF EAR.

5. Restart the Application Server and verify that the AXF functionality works correctly within the OSSO configuration.
6. Modify `web.xml` (portion displayed below) in the following ways. This file is located at:

   Oracle Application Server`\`*J2EEHome*`\`*Instance*`\applications\ImagingBaiAxf\imaging-bai-axf-web\WEB-INF\web.xml`

   - Modify `realm-name`.
   - Ensure that `role-name` matches `security-role-mapping name` specified in `orion-application.xml` (see step 4).
   - Based on the customer's environment, change `auth-method` and `form-login-page`, if needed.

```
<login-config>
```

```
        <auth-method>FORM</auth-method>
        <realm-name>jazn.com</realm-name>
        <form-login-config>
        <form-login-page>/login.jspx</form-login-page>
        <form-error-page>/loginError.jspx</form-error-page>
    </form-login-config>
</login-config>

<security-role>
    <description>Any Public User</description>
    <role-name>users</role-name>
</security-role>
```

2.7.2 Configuring SSL for AXF (E-Business Suite)

Perform the following procedures to specify E-Business Suite system settings for SSL configuration for AXF:

> **Note:** This section applies only to E-Business Suite.

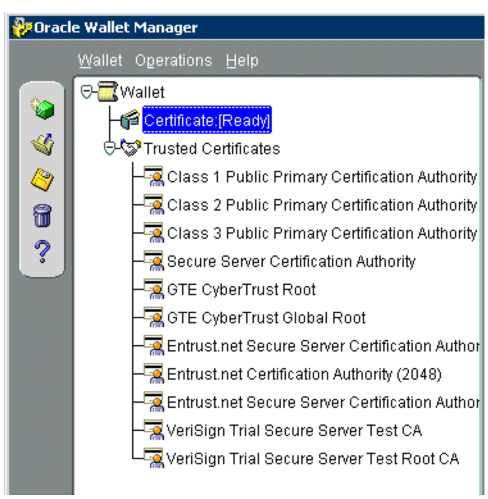
- Configuring the Oracle Wallet
- Configuring the Integration for SSL

Configuring the Oracle Wallet

1. Run Oracle Wallet Manager. In Linux, the owm executable can be found at the following location:

   `//ORACLE_HOME/bin/ as owm`

2. Create a new wallet. Using the wizard, enter the required information to create a new certificate. Export to a file.
3. Submit the certificate request to CA (Certificate Authority, such as Verisign) to purchase a new certificate.
4. Save the SSL certificates with a .cer extension. Most likely, the CA provided an SSL certificate, an Intermediate certificate, and a Trusted Root certificate via e-mail.
5. Import the Root and Intermediate certificates into the Oracle wallet by right-clicking Trusted Certificates (as shown below) and importing.



6. Import the SSL certificate into the wallet manager.

   If the process is successfully completed, a Ready status is displayed.

   > **Tip:** To import the SSL certificate, you may need to right- click the Certificate Requested tree item.

7. Save the wallet in one of the folders defined in the FORMS_PATH. (It is saved with the name *ewallet.p12*).

Configuring the Integration for SSL

1. On the E-Business Suite database, run the SQL statements listed below.

```
update AXF_PROPERTIES set propvalue='file:<walletpath>\' where propname = '
AXFWalletPath';
update AXF_PROPERTIES set propvalue='walletpassword' where propname = '
AXFWalletPwd ';
update AXF_PROPERTIES set propvalue='ON/OFF' where propname = 'SecureMode';
commit;
```

2. In the E-Business Suite AXF_CONFIGS table, update the SOLUTIONENDPOINT value to reflect the SecureMode setting.

   - If SecureMode is on, this value should start as `https://`

     When SecureMode is on, the integration will attempt to connect to the AXF application using SSL (https).

   - If SecureMode is off, this value should start as `http://`

2.7.3 Securing Communications

This adapter orchestrates calls from E-Business Suite and PeopleSoft to AXF and from AXF to Oracle UCM. Follow the steps in this section to secure their communications.

- "Between the Business Application and AXF" on page 2-32
- "Between AXF and Oracle UCM" on page 2-33

2.7.3.1 Between the Business Application and AXF

Follow these steps to configure the security mode IpSecurityCheck, which specifies that AXF accepts requests only from E-Business Suite or PeopleSoft servers set to be trusted.

1. In the AXF_TRUSTED_IP table, define IP addresses to be trusted. See "AXF_TRUSTED_IP Table" on page A-3.

2. Specify *`IpSecurityCheck`* for the securityClass parameter in the AXF_SYSTEM_PARAMETERS Table, as in:

   oracle.imaging.bai.axf.security.IpSecurityCheck

   > **Note:** You can also bypass any additional security check using the NullSecurityCheck option.
   >
   > To configure this security mode, specify *`NullSecurityCheck`* for the securityClass parameter in the AXF_SYSTEM_PARAMETERS Table, as in:
   >
   > oracle.imaging.bai.axf.security.NullSecurityCheck

2.7.3.2 Between AXF and Oracle UCM

Follow these steps to enable trusted communication between the host on which AXF is running and the Oracle UCM server. On the Oracle UCM server, you have two options for this configuration step: either via the System Properties application or by editing the config.cfg file.

Using the Content Server System Properties Application

1. Open the System Properties utility for the Oracle UCM instance.
2. Select the Server tab.
3. Identify the AXF host by either entering a name in the **Hostname Filter** field or an address in the **IP Address Filter** field.
4. Click OK and restart Content Server.

By Editing the Content Server Config.cfg File

1. Open the config.cfg file.
2. Locate the SocketHostAddressSecurityFilter entry, and edit it to include the IP address of the machine on which AXF is running.
3. Restart Content Server.

2.7.4 Managing Business Application and Oracle UCM Users

Keep the following guidelines in mind when managing E-Business Suite or PeopleSoft users for Managed Attachments access (for example, when managing users in a central repository via SSO):

- In order for business application users to access Managed Attachments functionality, their E-Business Suite or PeopleSoft username MUST match their Oracle UCM username.
- When creating Oracle UCM users (global or local), add them with default roles. Do NOT select the AFRead, AFWrite, AFDelete, or AFAdmin roles.

  The adapter dynamically assigns roles to the user: Roles are granted to the user based on dPrivilege's value when the AF_GRANT_ACCESS service is invoked (see "AFGrants Table" on page A-17); or, if not specified, based on the configuration variable AppAdapterGrantPrivilege's value (see "Configuring the Preferences.hda File" on page 2-26). Depending on the privilege (R, W, D, or A), a predefined role is dynamically assigned to the user.

> **Caution:** Do not delete the AFRead, AFWrite, AFDelete, AFAdmin roles from the system.

2.8 Configuring Oracle AutoVue Document Viewing

The default document viewing option for the Managed Attachments screen is the standard web rendition provided by Oracle UCM. For enhanced viewing options, the adapter also supports Oracle AutoVue via VueLink for Oracle UCM, where non-private attachments of virtually any document type are available for viewing, printing, collaboration, annotation, and mark up, delivered securely using Web technologies. For AutoVue requirements, see "Oracle VueLink 19.3 for Oracle UCM" on page 2-4.

Important Points About the AutoVue/Adapter Integration

- All non-private attachments can be viewed through AutoVue. For details on shared versus private documents, see "Document Security" on page 1-3.
- The VueLink integration serves as a bridge that securely streams documents from the Content Server repository to AutoVue for viewing, digital markup and collaboration. Digital markups are saved in the Content Server repository and associated with the attached document.
- By default, AutoVue is turned off in the Managed Attachments solution. You activate it in the preferences.hda file, by displaying the AutoVue icon and identifying the URL to the AutoVue servlet to launch when the user clicks the **View in AutoVue** icon.
- As with other preferences settings, you can enable the AutoVue integration at the global, application, and/or business entity level.
- AutoVue trusts the user authentication against Oracle UCM. Once authenticated to Oracle UCM, no further authentication to AutoVue is required for users to view attached documents via AutoVue.
- Viewing or annotating a document in AutoVue does not check it out or prevent it from being edited by others. Annotations are contained in a separate layer from their corresponding document.

Follow these steps to enable and configure AutoVue document viewing globally, or for a specific application or business entity.

1. Configure the Oracle UCM/AutoVue integration.

   Follow the procedures outlined in the *Oracle VueLink 19.3 for Oracle UCM System Administrator Manual*.

2. In the preferences.hda file, modify the global AutoVue setting, if needed. For general information, see "Configuring the Preferences.hda File" on page 2-26.

3. Optionally specify application or business entity settings by adding new rows in the AFEnvironmentConfiguration resultset for the AppAdapterAutoVueIconVisible and AutoVueURLPath variables, where:

   - dAFApplication: Application in which to display or hide button
   - dAFBusinessObjectType: Business entity within application in which to display or hide button

   Example 2–1 contains several AutoVue settings. The first entry hides the **View in AutoVue** icon globally. The next two entries enable and display the icon for the PSFT_Instance_A application. The last two entries enable and display the icon for the PSFT_Instance_B application, but *only* within its PIM business entity.

Example 2–1 AutoVue Entries in Preferences.hda File

```
AppAdapterAutoVueIconVisible
false

AutoVueURLPath
http://ucm1.mycompany.com/idc/jsp/autovue/csiApplet.jsp
PSFT_Instance_A

AppAdapterAutoVueIconVisible
true
PSFT_Instance_A
```

```
AutoVueURLPath
http://ucm1.mycompany.com/idc/jsp/autovue/csiApplet.jsp
PSFT_Instance_B
PIM

AppAdapterAutoVueIconVisible
true
PSFT_Instance_B
PIM
```

4. Restart the Content Server.

2.9 Configuring Oracle Distributed Document Capture

This section covers the following topics:

Note: For installation requirements specific to Oracle Distributed Document Capture use with this adapter, see "Oracle Distributed Document Capture v10.1.3.5+ and related components" on page 2-4.

2.9.1 About Document Scanning Using Oracle Distributed Document Capture

The Oracle Distributed Document Capture application allows an application such as the adapter to direct it to scan a document and pass in document index values. This allows users to scan documents or import scanned image files from the Managed Attachments screen and attach them to the selected business application record.

When configured for the adapter, document scanning works as follows:

- A **Scan** button is added to the Managed Attachments screen (see "Managed Attachments Screen" on page 3-10). The user clicks the button, and selects options such as a **document classification**, which is assigned to an Oracle Distributed Document Capture scan profile. For example, the user might select a classification of *Identity Documents* to scan a photocopy of a driver's license or passport. (An Oracle Distributed Document Capture scan profile specifies scanning, importing, and indexing settings.) The user also specifies whether the document should be shared, and if so the user specifies a security group (from those to which the user has access) for the shared document.
- When the user clicks the **Scan Document** button, Oracle Distributed Document Capture's remote client launches in a new window, automatically authenticates and logs in the user, and passes in parameters such as the scan profile to be used and business application entity values for later attachment.
- Within the Oracle Distributed Document Capture client, the user reviews the document, makes changes as needed, completes any index fields configured in the scan profile, then sends the batch. Sending the batch commits the new document to Oracle UCM using a commit profile specified for the scan profile. (A Capture

Oracle UCM commit profile specifies connection information and field mappings between Capture and Content Server metadata fields.)

- Upon successful sending, the user returns to the Managed Attachments screen and refreshes the display to view the newly scanned document or imported scanned image file.

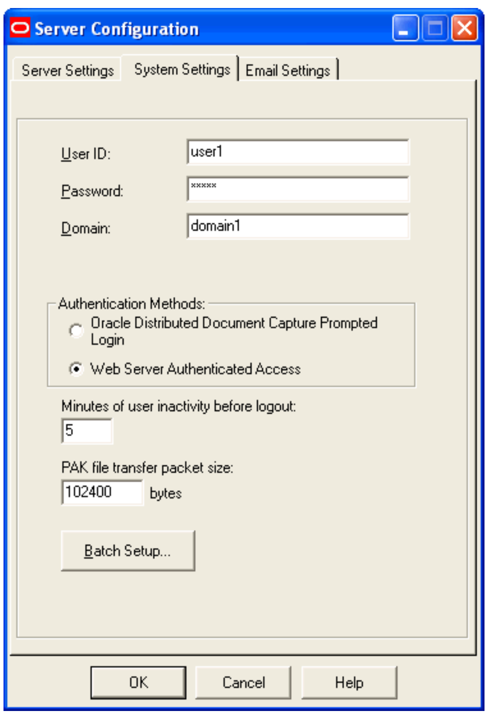
2.9.2 Configuring Oracle Distributed Document Capture For the Adapter

Follow these steps to configure attachment scanning on the Oracle Distributed Document Capture side.

1. Ensure that Oracle Distributed Document Capture is set for automatic login (optional).

   On the System Settings tab of the Distributed Document Capture Server Configuration application shown in Figure 2–3, select **Web Server Authenticated Access** from the Authentication Methods options. This allows the client to launch automatically without users needing to log in. For details, see the section on authentication in the *Installation Guide for Oracle Distributed Document Capture*.

Figure 2–3 Distributed Document Capture Server Configuration, System Settings Tab

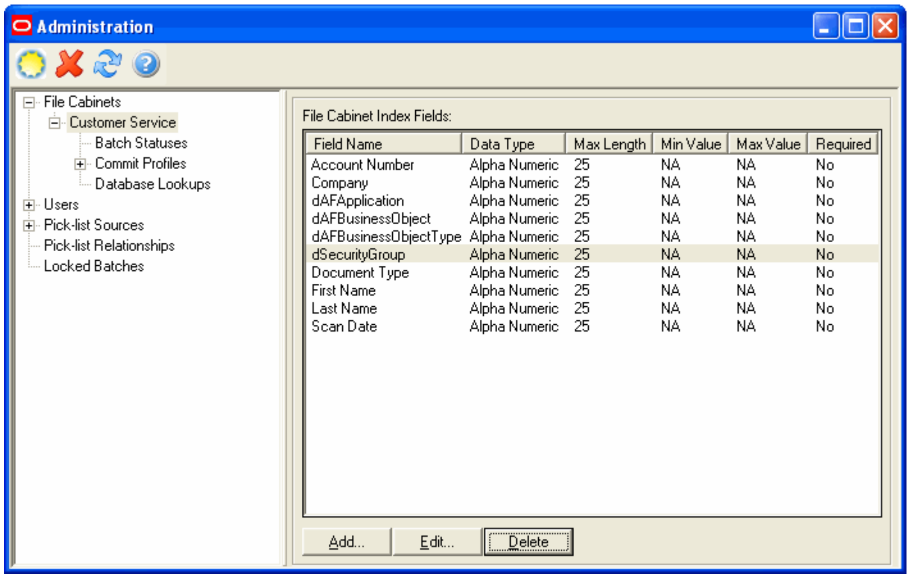


2. In Capture Administration, add index fields to a selected file cabinet for capturing values for new documents, as shown in Figure 2–4. For details, see the section on Capture Administration in the *Administrator's Guide for Oracle Distributed Document Capture*.

   - Create index fields for values you want saved with attached documents on the Content Server. For example, you might configure a Doc Type pick-list index field for users to select from standard document types.
   - Create the following alphanumeric index fields to contain the business application entity values:

– dAFApplication
– dAFBusinessObjectType
– dAFBusinessObject
– dSecurityGroup

Figure 2–4 Capture Administration, Index Fields



3. In Oracle Distributed Document Capture's Profile Administration, create a scan profile, as shown in Figure 2–5. You will later associate this scan profile with one or more document classifications, so that when a user selects a classification, the associated scan profile's settings are used. For details, see the section on scan profiles in the *Administrator's Guide for Oracle Distributed Document Capture*.

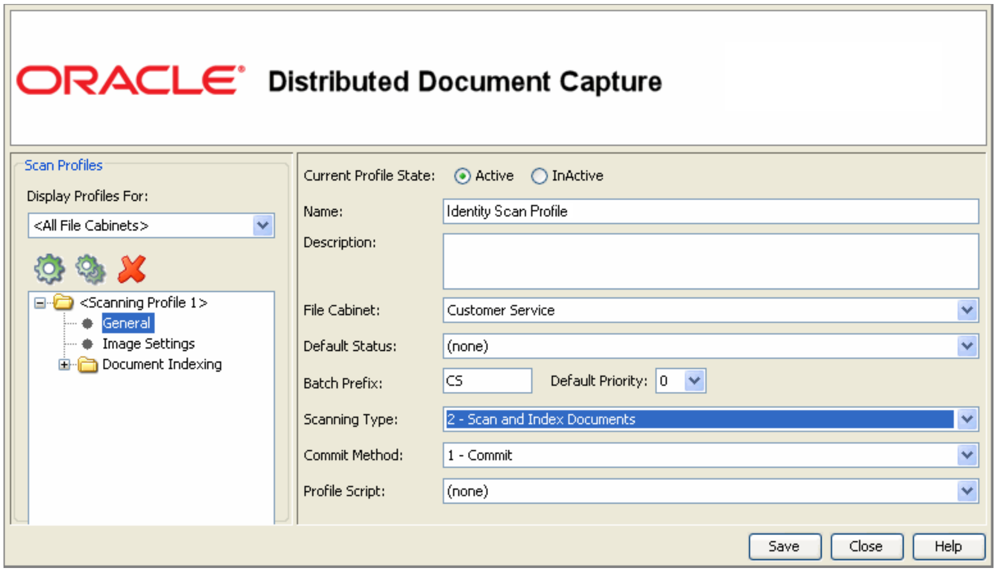
   - On the General pane, select **2 - Scan and Index Documents** in the Scanning Type field. This scanning type includes indexing, and scans or imports pages into a single document in a batch. Specify a file cabinet and batch prefix.

   - On the Document Indexing pane, move all fields you want displayed to users to the Selected Fields box.

   > **Note:** Typically, you would not select the business application entity fields (dAFBusinessObject, for example) for display to users. If you choose to display them, lock them on the Field Properties pane to prevent users from changing their values.

   - On the Field Properties, Auto Populate, and Database Lookup panes, configure any pick-lists, database lookups, or autopopulating needed for indexing. Save the scan profile.

Figure 2–5 Scan Profiles, Oracle Distributed Document Capture Profile Administration



4. Create an ini (standard Java properties) file to add custom Content Server fields. This allows business application entity values to pass from Capture to Content Server.

   - Name the file *ucm_config.ini* and save it in the *Oracle\Document Capture\OracleUCM* folder.
   - Enter the following lines:

   ```
   # Custom Content Server fields
   CUSTOMFIELD_1_Name=dAFApplication
   CUSTOMFIELD_2_Name=dAFBusinessObjectType
   CUSTOMFIELD_3_Name=dAFBusinessObject
   ```

5. In Capture Administration, create an Oracle UCM commit profile to commit the scanned or imported documents to Oracle UCM when users send a completed batch.

   This commit profile specifies how to connect to the Content Server and how the business application and Capture values are passed to the Content Server. For information about creating Oracle UCM commit profiles, see the section on committing profiles in the *Administrator's Guide for Oracle Distributed Document Capture*.

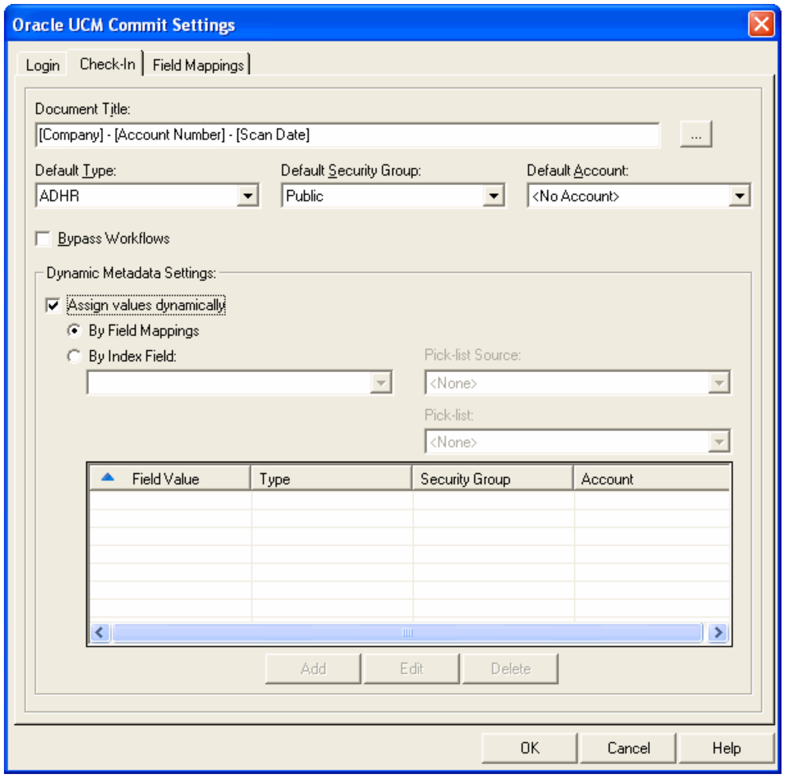
   - Select **Oracle UCM Commit Driver** in the Commit Driver field. Click the **Configure** button adjacent to the Commit Driver field.
   - On the Login tab, specify settings for logging in to the Content Server instance. (The other tabs become active after you log in.) Use the following form for the Content Server URL:

     ```
     http://UCM hostname or IP address:WebServerPort/ucm web root/idcplg
     ```

     The Content Server user specified must have been assigned the AFWrite role for the AFDocuments security group. It is recommended that a special Capture user specific to the Managed Attachments Solution be created for this purpose to ensure regular users not gain write access to the AFDocuments security group, which is reserved for the Managed Attachments solution.

- On the Check-In tab, choose **Assign values dynamically** and **By Field Mappings** fields, as shown in Figure 2–6. Also specify how you want documents named in the **Document Title** field.

Figure 2–6 Capture Administration, Check-In for Oracle UCM Commit Settings



- On the Field Mappings tab, map Capture fields whose values you want written to Content Server fields. See Figure 2–7.

  Be sure to map the following business application entity fields you created in step 2, as they are required to attach the new Oracle UCM document to the business application entity:

  – dAFApplication

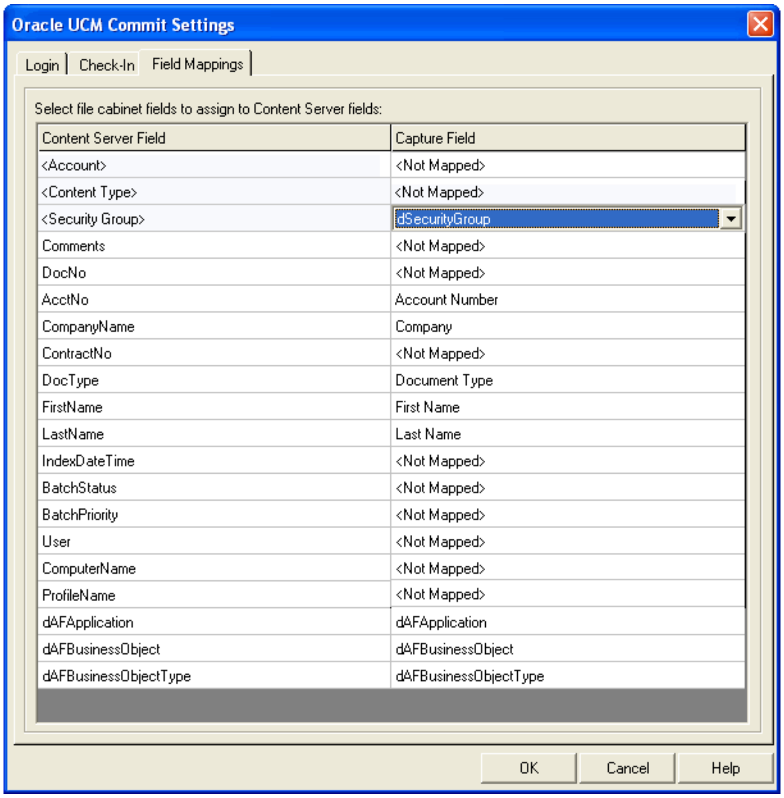
  – dAFBusinessObjectType

  – dAFBusinessObject

  – dSecurityGroup

- Activate the business application-Oracle UCM commit profile.

Figure 2–7 Capture Administration, Field Mappings for Oracle UCM Commit Settings



2.9.3 Configuring Oracle UCM for Distributed Document Capture Via the Adapter

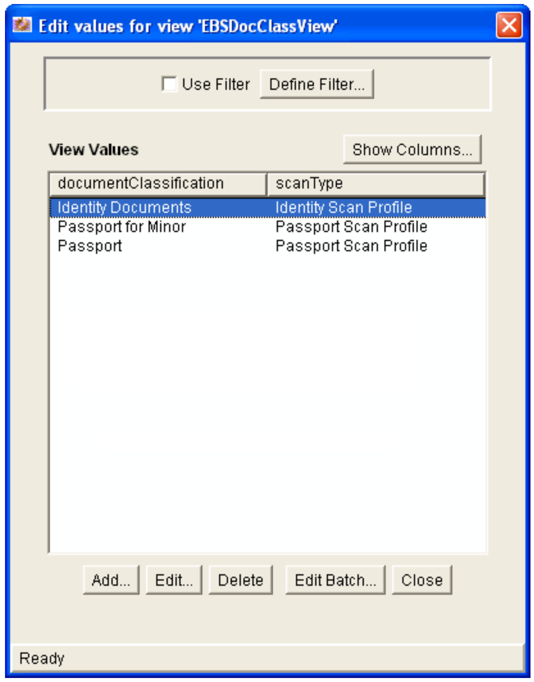
Follow these steps to configure attachment scanning on the Content Server side.

1. On Content Server, edit the following configuration variables for Oracle Distributed Document Capture, if you have not already done so, and restart Content Server. See "Configuring the Preferences.hda File" on page 2-26.

   - `ODDCURLPath=http://`*`ODDC_host/ODDC_webcapture_address`*
   - `ODDCScanAction=`*`ODDC Scan Action`*
   - `AdapterAppScanBtnVisible=true`

2. On Content Server, configure document classification and scan types.

   - From the Administration tray in Content Server, click the **Admin Applets** link.
   - Select the Configuration Manager applet. The Configuration Manager is displayed.
   - Click the Views tab, select the appropriate document classification view from the alphabetical list (**EBSDocClassView** for E-Business Suite or **PSFTDocClassView** for PeopleSoft), and click **Edit Values**.



3. In the Edit Values screen, click **Add** and add document classifications and their corresponding scan profile. Note that documentClassification entries must be unique, but a scan profile can be used multiple times. Click **Close** when done.
4. From the Options menu, select **Publish schema** to publish the data.

2.9.4 Testing the Oracle Distributed Document Capture Via Adapter Configuration

Follow these steps to test the configuration as an end-user. For details, see "Scanning Via Oracle Distributed Document Capture" on page 3-6.

1. Refresh the Managed Attachments results page. You should see a Scan button beside the New button.
2. Click the **Scan** button. In the Scan Document page, select a document classification and security group, and click **Scan Document**. The Oracle Distributed Document Capture client launches.

   Notice that the URL reflects the settings you specified to run the client. It also passes the scan profile, scan action (1 = Scan and 2 = Import), and index data containing the E-Business Suite or PeopleSoft entity values.
3. Within the Oracle Distributed Document Capture client, review, index, and send the document.
4. Return to the Managed Attachments screen and click **Refresh**. The newly scanned document or imported scanned image file should be displayed in the list. (It may take a few minutes to be displayed.)

2.10 Customizing the Adapter

You can customize the Managed Attachments display in the following ways:

- "Customizing at Global, Application, and Business Entity Levels" on page 2-42
- "Customizing the Document Type Used For New Attachments" on page 2-43

2.10.1 Customizing at Global, Application, and Business Entity Levels

You can customize settings at global, application, and business entity (application+business entity) levels in the preferences.hda file. (For general information, see "Configuring the Preferences.hda File" on page 2-26.) This allows you to set a global value and then customize for specific business entities, as illustrated in Table 2–6.

> **Notes:** You must restart the Content Server after modifying the preferences.hda file.
>
> You can add or delete application and business entity configuration entries as needed, but do NOT delete global configuration entries from the preferences.hda file.

Table 2–6 Global, Application, and Business Entity Level Customization

Level	Customization Parameters	Example

Global	Modify the appropriate resultset setting in the preferences.hda file. Specify:
	`name`
	`value`
		This entry sets the **From Repository** button to display globally for the adapter:
		`AppAdapterRepoAttachBtnVisible`
		`true`

Application	Copy and customize a resultset row, setting dAFApplication for the application. Specify:
	`name`
	`value`
	`dAFApplication`
		This entry hides the **From Repository** button in the EBS_instance application.
		`AppAdapterRepoAttachBtnVisible`
		`false`
		`EBS_Instance`

Business Entity	Copy and customize a resultset row, setting dAFApplication and dAFBusinessObjectType for the business entity. Specify:
	`name`
	`value`
	`dAFApplication`
	`dAFBusinessObjectType`
		This entry displays the **From Repository** button for the ExpenseClaims business entity only.
		`AppAdapterRepoAttachBtnVisible`
		`true`
		`EBS_Instance`
		`ExpenseClaims`

2.10.2 Customizing the Document Type Used For New Attachments

A Content Server document type is selected by default when users click the **New** button to attach and check in a document. Using preferences.hda settings, you can specify a different default document type. In addition, you can specify document types on a global, application, or business entity level. For example, you might want to check in all new documents for an expenses business entity using a custom document type geared toward expense attachments.

Follow these steps.

1. On Content Server, create or modify a document type.

   For more information about document types, see the Content Server documentation.

2. In the preferences.hda file, add a new row in the AFEnvironmentConfiguration resultset. For general information, see "Configuring the Preferences.hda File" on page 2-26.

3. Insert an entry that identifies the document type to use as the default type for a specified business entity, where:

   - name: afDocType
   - value: document type key
   - dAFApplication: Application to be assigned this document type
   - dAFBusinessObjectType: Business entity within application to be assigned document type

   Example 2–2 sets the document type *ExpenseClaimsType* as the default type when users attach documents to the ExpenseClaims business entity (within the PSFT_Instance application).

Example 2–2 Custom Default Document Type For Expenses Business Entity

```
afDocType
ExpenseClaimsType
PSFT_Instance
ExpenseClaims
```

4. Restart the Content Server.

2.10.3 Customizing the Content Server Profile Used

The adapter provides a default Content Server profile for each business application, called *EBSProfile* for E-Business Suite and *PSFTProfile* for PeopleSoft. You can copy and customize the profile, then assign it using one of the methods described below, depending on customization needs. For example, you might want to add metadata fields to the profile.

> **Note:** When custom profiles are used, by default generic error messages are shown instead of application-specific error messages. To display custom error messages, override the resource include - af_custom_error_msg_display. In the overridden resource include, set the error message to afErrorMsg.

2.10.3.1 Changing the Profile Globally

Follow these steps to change the global profile used.

1. From the Content Server Configuration Manager, copy the default profile provided (EBSProfile or PSFTProfile). To view these profiles, navigate to the Profiles tab in Configuration Manager.
2. Add new rules as needed. For example, add new metadata fields.
3. In the UCM_CONNECTION_STR parameter (trigger value) of the AXF_SOLUTION_PARAMETERS table, modify the URL to point to the new profile.

   For more information, see "AXF_SOLUTION_PARAMETERS Table" on page A-5.

2.10.3.2 Specifying a Profile For a Specific Business Entity or Application

Follow these steps to modify the profile for a specific business entity or application.

1. From the Content Server Configuration Manager, copy the default profile provided (EBSProfile or PSFTProfile). To view these profiles, navigate to the Profiles tab in Configuration Manager.
2. Add new rules as needed. For example, add new metadata fields.
3. In the preferences.hda file, add a new row in the AFEnvironmentConfiguration resultset. For general information, see "Configuring the Preferences.hda File" on page 2-26.
4. Insert an entry that identifies the Content Server profile to use for a specified business entity, where:
   - name: dpTriggerValue
   - value: Key of new Content Server profile
   - dAFApplication: Application to be assigned this profile
   - dAFBusinessObjectType: Business entity within application to be assigned the profile

   Example 2–3 sets a profile called *OrderPayableProfile* to be used when users attach or scan documents in the OrderPayables business entity within the EBS_Instance application.

   Example 2–3 Custom Content Server Profile For Expenses Business Entity

   ```
   dpTriggerValue
   OrderPayableProfile
   EBS_Instance
   OrderPayables
   ```

5. Restart the Content Server.

2.10.4 Hiding or Displaying Managed Attachments Screen Buttons

You can choose to disable (hide) or display the buttons listed in Table 2–7 to users on the Managed Attachments screen, by changing their environment variable setting to false. For details about Oracle UCM configuration variables, see "Configuring the Preferences.hda File" on page 2-26.

Table 2–7 Environment Variables For Displaying or Hiding Managed Attachments Buttons

Environment Variable	Description
AppAdapterRepoAttachBtnVisible	Displays or hides the **From Repository** button
AppAdapterRefreshBtnVisible	Displays or hides the **Refresh** button
AppAdapterConfigureBtnVisible	Displays or hides the **Configure** button
AppAdapterDetachBtnVisible	Displays or hides the **Detach** button
AppAdapterCheckinNewBtnVisible	Displays or hides the **New** button
AppAdapterScanBtnVisible	Displays or hides the **Scan** button
AppAdapterAutoVueIconVisible	Displays or hides the **AutoVue** button in the Actions column

Follow these steps to hide or display a button globally, or for a specific business entity or application.

1. In the preferences.hda file, add a new row in the AFEnvironmentConfiguration resultset.
2. Insert an entry that identifies the button from the list in Table 2–7 to be disabled or enabled, and the level.

   Example 2–4 displays the **From Repository** button globally but then hides it for the ExpenseClaims business entity (within the EBS_Instance application).

Example 2–4 Displaying and Hiding the From Repository Button

```
AppAdapterRepoAttachBtnVisible
true

AppAdapterRepoAttachBtnVisible
false
EBS_Instance
ExpenseClaims
```

3. Restart the Content Server.

2.10.5 Customizing Scanning

You can customize scanning functionality using Oracle Distributed Document Capture in the following ways:

- "Enabling or Disabling Scanning" on page 2-45
- "Configuring an Alternate Scan Profile For a Business Entity" on page 2-46
- "Modifying the Document Classification Used" on page 2-46

For information about configuring standard scanning options, see "Configuring Oracle Distributed Document Capture" on page 2-35. For information about preferences.hda, see "Configuring the Preferences.hda File" on page 2-26.

2.10.5.1 Enabling or Disabling Scanning

You can enable or disable scanning at the global, application, or business entity level. In Example 2–5, scanning is disabled globally but enabled for the OrderPayables business entity.

Example 2–5 Customized Scanning in Preferences.hda File

```
AppAdapterScanBtnVisible
false

AppAdapterScanBtnVisible
true
EBS_Instance
OrderPayables
```

2.10.5.2 Configuring an Alternate Scan Profile For a Business Entity

The adapter provides two default business application scan profiles. Each points to an application-specific field:

- *EBSScanProfile* references the EBSAppScanProfiles application field
- *PSFTScanProfile* references the PSFTAppScanProfiles application field

You can customize the scan profile used, by copying the profile appropriate for your business application, modifying it to reference another application field, and configuring it for one or more business entities, as described in the following steps.

1. Copy the scan profile that applies to your business application, saving it with a new name.
2. Create all required schema elements, including the AppScanProfiles application field, table, and view.

   To change the application field reference, log in to Oracle UCM. In Configuration Manager, navigate to the Rules tab. Select **PSFTScanRule** or **EBSScanRule**, click **Edit** on the Side Effects tab, and update the ScanProfileKey field to point to another application field.
3. In the preferences.hda file, add a new row in the AFEnvironmentConfiguration resultset.
4. Insert an entry that includes the afScanProfile setting, identifies the scan profile to be used and the application and business entity in which it will apply.

   Example 2–6 shows a scan profile called *MyPIMScanProfile* enabled for the PIM business entity only.

Example 2–6 Enabling Another Scan Profile for a Business Entity

```
afScanProfile
MyPIMScanProfile
PSFT_Instance
PIM
```

2.10.5.3 Modifying the Document Classification Used

The adapter provides two default business application document classifications for scanning. Each classification includes a set of Oracle UCM application fields, a table, and a view.

- For E-Business Suite, the adapter provides EBSAppScanProfiles (fields), EBSDocClass (table), and EBSDocClassView (view).
- For PeopleSoft, the adapter provides PSFTAppScanProfiles (fields), PSFTDocClass (table), and PSFTDocClassView (view).

To modify the classification, perform the following steps.

1. Log in to Oracle UCM. In Configuration Manager, navigate to the EBSDocClassView or PSFTDocClassView.
2. Edit the document classification and scan type values. For more information, see "Configuring Oracle UCM for Distributed Document Capture Via the Adapter" on page 2-40.

2.10.6 Customizing Managed Attachments Screen Images

The adapter provides standard images for Managed Attachments display, which you can customize. For example, you might change the Oracle blue wave image with one specific to your organization. To change images, override the resource include *af_ebs_define_image_locations*. For sample implementations, see *AppAdapter_JS_resource.htm* for E-Business Suite or *ps_AppAdapter_Js_resource.htm* for PeopleSoft.

> **Note:** Customizing images for Managed Attachments requires advanced knowledge of Content Server configuration and customization. Be sure to back up the appropriate files before making modifications.

2.10.7 Customizing the Managed Attachments Screen Style Sheet (CSS) Used

The adapter provides a standard style sheet for the Managed Attachments screen. You can change it by overriding resource includes. For sample implementations, see *AppAdapter_CSS_resource.htm* for E-Business Suite or *ps_AppAdapter_CSS_resource.htm* for PeopleSoft.

> **Note:** Customizing style sheets for Managed Attachments requires advanced knowledge of Content Server configuration and customization. Be sure to back up the appropriate files before making modifications.

2.10.8 Configuring Relationship Attributes

Relationship attributes allow you to store relationship metadata (information about relationships between a document and its business entity) upon attaching documents using Managed Attachments. For example, suppose you have one document attached to two work order entities (WO1 and WO2), and want to allow the document to be printed from WO1, but not from WO2. In this case, you would create a print attribute as an application field on Content Server, and then specify a print relationship attribute for the WO1 business entity in the preferences.hda file. The print attribute would be displayed on the Update page to end-users for the WO1 entity only, allowing them to print the attached document.

Important Points About Relationship Attributes

- You can configure relationship attribute for new document check-in, but not for documents checked in via scanning.
- At runtime, relationship attribute values are stored in the AFRelationship Attributes table; see "AFRelationshipAttributes Table" on page A-18.

Follow these steps to configure relationship attributes.

1. On Content Server, open Configuration Manager and navigate to the Application Fields tab.

2. Add one or more application fields.
3. Navigate to the Rules tab.
4. Edit the AFRelationshipAttributes rule. Add the application fields you added in step 2 to this rule.
5. Open the preferences.hda file and add a new row in the AFRelationshipAttributes resultset. (For general information, see "Configuring the Preferences.hda File" on page 2-26.)

   Each row in the resultset represents one relationship attribute associated with a business object, where:

   - *dAFApplication* refers to the E-Business Suite or PeopleSoft business application for which the relationship attribute is configured.
   - *dAFBusinessObjectType* refers to the Business Object for which the relationship attribute is being enabled.
   - *attribute* refers to the relationship attribute.

   Example 2–7 shows a relationship attribute (Print) configured for an WO1 business object for a PeopleSoft application.

Example 2–7 AFRelationshipAttributes Customization

```
@ResultSet AFRelationshipAttributes
3
dAFApplication
dAFBusinessObjectType
attribute
PSFT_Instance
WO1
Print
@end
```

6. Save and restart Content Server.

2.10.9 Configuring Revision-Specific Mode

By default, each attachment in the Managed Attachments screen provides access to the *most recent revision* of the document. In certain cases, however, you may want to configure one or more business entities to provide access to the revision that was *attached*, even if the document was later updated on Content Server. In this mode, users can see that a more recent revision exists, and if needed, view it and make it the attached revision.

Follow these steps to configure a business entity to display the attached revision instead of the most recent revision.

1. Open the preferences.hda file, and add a new row in the AFRevisionSpecificEntities resultset. (For general information, see "Configuring the Preferences.hda File" on page 2-26.)

   Each row in the resultset represents one business entity for which to enable revision specific attachments, where:.

   - *dAFApplication* refers to the business application for which the revision feature is being configured.
   - *dAFBusinessObjectType* refers to the Business Object for which the revision feature is being enabled.

Example 2–8 shows revision-specific mode configured for a CallRecords business object for an E-Business Suite application.

Example 2–8 AFRevisionSpecificEntities Customization

```
@ResultSet AFRevisionSpecificEntities
2
dAFApplication
dAFBusinessObjectType
EBS_Instance
CallRecords
@end
```

2.10.10 Changing the Result Count

The Managed Attachments screen displays a specific number of attachment results per page (referred to as *ResultCount*). If the number of results exceeds ResultCount, previous and next page controls are displayed on the screen. By default, ResultCount is set to 5, but it can be changed to another number such as 20. To change it, specify a new ResultCount number in the UCM_CONNECTION_STR parameter of the AXF_SOLUTION_PARAMETERS Table. Also see "Example Implementation" on page A-6.

2.10.11 Changing the Result Template

The Managed Attachments screen uses a result template to determine its display. The Content Server result template specifies the Managed Attachments user interface. The adapter provides two default result templates:

- The E-Business Suite template, *adapter_list_results_template.htm*, is referred to as **EBS_LIST**.
- The PeopleSoft template, *ps_adapter_list_results_template.htm*, is referred to as **PSFT_LIST**.

Follow these steps to identify an alternate result template for an application or business entity.

> **Note:** Customizing the result template requires advanced knowledge of Content Server administration and customization.

1. Create a copy of the E-Business Suite or PeopleSoft default result template and register the template with a new name, preferably in a new component.
   - The E-Business Suite template is located at:

     UCM_HOME/custom/AppAdapterEBS/adapter_list_results_template.htm
   - The PeopleSoft template is located at:

     UCM_HOME/custom/AppAdapterPSFT/ps_adapter_list_results_template.htm
2. In the preferences.hda file, add an entry in the AFEnvironmentConfiguration section as follows:

```
ResultTemplate
<Template Reference>
<Application Name>
<Business Entity>
```

In Example 2–9, all requests to Managed Attachments for the WorkOrder business entity would use the *EBS_WORK_ORDER_LIST* custom result template instead of the default E-Business Suite template.

Example 2–9 Preferences.hda Entry For Specifying a Custom Result Template

```
ResultTemplate
EBS_WORK_ORDER_LIST
EBS_Instance
WorkOrder
```

2.10.12 Setting Default Columns

You can specify the default columns to be displayed to users in the Managed Attachments screen. (When the user clicks **Reset** in the Configure Fields for Display Screen, default columns are listed in the Main Information section of the screen.)

The column defaults are title, type, author, date, and revision as follows:

dDocTitle,dDocType,dDocAuthor,dInDate,dRevision

To set alternate default columns for an application or business entity, follow these steps.

1. In the preferences.hda file, add an entry in the AFEnvironmentConfiguration section.
2. Set the value of the *AppAdapterDefaultDisplayColumns* configuration variable as a comma-separated list containing Oracle UCM metadata field names.

   In Example 2–10, the first entry sets document title, type, author, and date as the default columns for the EBS_Instance application. The second entry overrides this setting for the CallRecords business entity by adding the revision column (dRevision) as a default column.

Example 2–10 Preferences.hda Entries For Specifying Default Columns

```
AppAdapterDefaultDisplayColumns
dDocTitle,dDocType,dDocAuthor,dInDate
EBS_Instance

AppAdapterDefaultDisplayColumns
dDocTitle,dDocType,dDocAuthor,dInDate,dRevision
EBS_Instance
CallRecords
```

2.11 Uninstalling the Adapter

Follow the steps listed in these sections to uninstall the adapter:

- "Uninstalling Adapter Components on Content Server" on page 2-51
- "Uninstalling AXF" on page 2-51
- "Uninstalling AXF from E-Business Suite" on page 2-51
- "Uninstalling AXF from PeopleSoft" on page 2-52

2.11.1 Uninstalling Adapter Components on Content Server

Follow these steps to disable and then uninstall the following adapter components on the Content Server.

- AppAdapterCore
- AppAdapterEBS
- AppAdapterPSFT

For details about these components, see "Installing and Enabling Oracle UCM Components" on page 2-23.

1. Log in to Content Server as an administrator.
2. Select **Admin Server** from the Administration menu.

   The Content Admin Server page is displayed.
3. Click the name of the Content Server instance where the component will be uninstalled.

   The Content Admin Server <*instance_name*> page is displayed.
4. Click **Component Manager**.

   The Component Manager page is displayed.
5. Select an adapter component in the Enabled Components list and click **Disable**.
6. Repeat step 5, selecting and disabling the remaining adapter components.
7. Click **Start/Stop Content Server**.

   The Content Admin Server <*instance_name*> is displayed.
8. Click **Restart**.
9. Click **Component Manager**.

   The Component Manager is displayed.
10. Select an adapter component in the Uninstall Component field and click **Uninstall**. Click **OK** to confirm uninstalling the component.
11. Repeat step 10, uninstalling the remaining adapter components.
12. Select the link to return to the Component Manager.

    The Component Manager page is displayed.
13. Click **Start/Stop Content Server**.

    The Content Admin Server <*instance_name*> page is displayed.
14. Restart Content Server to apply the changes.

2.11.2 Uninstalling AXF

To uninstall AXF from SOA, run `uninstall.sh` (Linux/UNIX) or `uninstall.bat` (Windows) and check `uninstall.out` to verify that the EAR was successfully undeployed and the database tables were successfully removed.

2.11.3 Uninstalling AXF from E-Business Suite

Follow these steps to uninstall AXF from E-Business Suite.

1. Assign the AXF configuration schema user the following privileges:

- Drop table
- Drop sequence
- Drop public synonym

2. As the AXF user, execute the **AXF_DROP_TABLES_SYNONYM** script for your E-Business Suite version, from the applicable location listed below. This script drops all tables, synonyms, and sequences created by the AXF_CREATE_TABLES_SYNONYM script run during installation.

   E-Business Suite 12: AXF_INSTALL_DIR/ebs/R12/AXF_DROP_TABLES_SYNONYM.sql

   E-Business Suite 11: AXF_INSTALL_DIR/ebs/R11/AXF_DROP_TABLES_SYNONYM.sql

   Execute the script by entering:

   @AXF_DROP_TABLES_SYNONYM.sql

3. Remove the AXF database schema user.
4. Remove AXF_CUSTOM.* (AXF_CUSTOM.pll, AXF_CUSTOM.pld, and AXF_CUSTOM.plx) from `FORMS_PATH` (or `FORMS60_PATH` on E-Business Suite 11 systems).
5. Restore the CUSTOM.pll file you backed up in step 7 in "Compiling E-Business Suite Forms" on page 2-14.
6. Open Oracle Forms Builder and connect to the E-Business Suite database as the APPS user. Forms Builder is typically located in the `/bin/` subdirectory of your database's Oracle home.
7. Open the restored `CUSTOM.pll` by selecting **File**, then **Open** and selecting **PL/SQL Libraries** (*.pll) in the Files of Type field.
8. With `CUSTOM.pll` open, select **Program**, then **Compile pl/sql**, then **All** (E-Business Suite 12) or **Program**, then **Compile**, then **All** (E-Business Suite 11).
9. Compile CUSTOM into a module (.plx) by selecting **Program**, then **Compile Module** (E-Business Suite 12) or **File**, then **Administration**, then **Compile File** (E-Business Suite 11).
10. Save all before exiting Forms Builder.

2.11.4 Uninstalling AXF from PeopleSoft

No resources are being used if no AXF solutions are implemented, so there is no harm in leaving AXF objects in the system. If no AXF solutions are implemented, you can remove all AXF objects using Application Designer.

3

Managed Attachments Functionality

This chapter provides information on options available to business application users in the Managed Attachments screen configured via the adapter. It includes the following sections:

3.1 Managed Attachments Procedures

This section describes how to perform the following tasks using the Managed Attachments screens. For more information about Content Server procedures, see the *Content Server User Guide*.

Viewing Attachments

Attaching and Detaching Documents

Editing Attachments

Finding Attachments

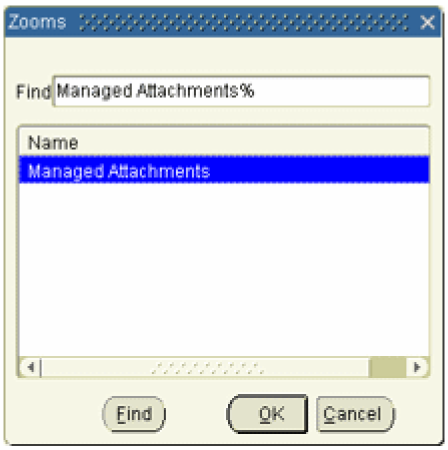
- "Searching for Documents on the Content Server Repository" on page 3-10

3.1.1 Displaying Managed Attachments in E-Business Suite

Follow these steps to display the Managed Attachments screen for an E-Business Suite record.

1. On an E-Business Suite form that supports managed attachments, display a record, and save it, if needed. (For example, create and save an invoice.)
2. From the toolbar, click the Zoom icon shown below.

3. From the Zooms menu, choose **Managed Attachments** and click OK.



Note: You may be prompted to enter a username and password to log in to Oracle UCM, depending on configuration. If prompted, enter the same username that you use to log in to E-Business Suite.

The Managed Attachments Screen is displayed, listing any current attachments for the selected business application record. The line across the top provides key values for the selected business application entity with which the attachment list is associated.

Note: You have access to the Managed Attachments screen for a certain amount of time. After a period of inactivity or total access time is reached, a message is displayed, informing you that your access privileges may have expired. To access the Managed Attachments screen, follow the steps in this section to select the Managed Attachments command again from the Zoom menu.

3.1.2 Displaying Managed Attachments in PeopleSoft

Follow these steps to display the Managed Attachments screen for a PeopleSoft record.

1. On a PeopleSoft page that supports managed attachments, display a record.

2. Activate Managed Attachments.

   Depending on configuration, this might be clicking an **Attachments** button or link.

   Note: You may be prompted to enter a username and password to log in to Oracle UCM, depending on configuration. If prompted, enter the same username that you use to log in to PeopleSoft.

   The Managed Attachments Screen is displayed, listing any current attachments for the selected PeopleSoft record. The line across the top provides key values for the selected PeopleSoft entity with which the attachment list is associated.

   Note: You have access to the Managed Attachments screen for a certain amount of time. After a period of inactivity or total access time is reached, a message is displayed, informing you that your access privileges may have expired. To access the Managed Attachments screen, follow the steps in this section to redisplay the Managed Attachments screen.

3.1.3 Viewing Attached Documents

The Managed Attachments screen provides multiple ways of accessing and viewing documents:

- Click the attachment's link in the **Name** field to open the document in a Web-viewable format or save the document in its native format to a selected location. For more information, see "Opening or Saving a Document" on page 3-8.
- Click the attachment's **Edit** icon under Actions options to make and save changes to the document. See "Editing a Document in its Native Application" on page 3-9.
- Click the **Info** icon to view the attachment's content information, and view the Web-viewable or native version of the document. See "Viewing a Document's Information" on page 3-4.
- Click the **AutoVue** icon (if displayed) to view the document in the AutoVue applet, which provides enhancing options such as annotation and markup. See "Viewing Documents in AutoVue" on page 3-3.

3.1.4 Viewing Documents in AutoVue

Depending on configuration, you may have access to enhanced viewing options in the Managed Attachments screen via AutoVue. If configured, AutoVue allows you to view, print, collaborate, annotate, and mark up non-private (shared) attachments of virtually any document type. For details on shared versus private documents, see "Checking In and Attaching a Document" on page 3-4.

1. In the Managed Attachments screen, click the **View in AutoVue** icon (shown below) for an attachment. When AutoVue is configured, this icon is displayed in the Actions options.

   An AutoVue applet is launched, and the selected document displays in the AutoVue client.

Notes: The AutoVue icon is dimmed (grayed out) for private attachments, which cannot be viewed using AutoVue.

Viewing or annotating a document in AutoVue does not check it out or prevent it from being edited by others. Annotations are contained in a separate layer from their corresponding document.

2. Use AutoVue options to view, annotate, mark up, and print the document. Note that digital markups are saved in the Content Server repository and associated with the attached document.

   For details about AutoVue use, see the *Oracle VueLink 19.3 for Oracle UCM User's Manual* (or higher).

3.1.5 Configuring Fields for Display

Follow these steps to select and order fields for display in the Managed Attachments screen.

1. In the Managed Attachments screen, click the **Configure** icon shown below.

2. On the Configure Fields for Display Screen, specify fields to display by selecting them in the Available Fields area (holding down the Ctrl key to select multiple fields) and clicking the right arrow button to move them to the Main Information area. (Fields selected for display are displayed in dimmed text in the Available Fields area.)
3. Change the order in which fields are displayed by repositioning them in the Main Information area. Move a field by selecting it and clicking the up or down arrow button.

Note: If needed, click the **Reset** button to restore the default field display and order.

4. Click the **Apply** button and view the results of your changes.
5. When done, click the **Save and Exit** button, and close the Configure Fields for Display screen.

3.1.6 Viewing a Document's Information

Follow these steps to view an attached document's metadata values or previous revisions.

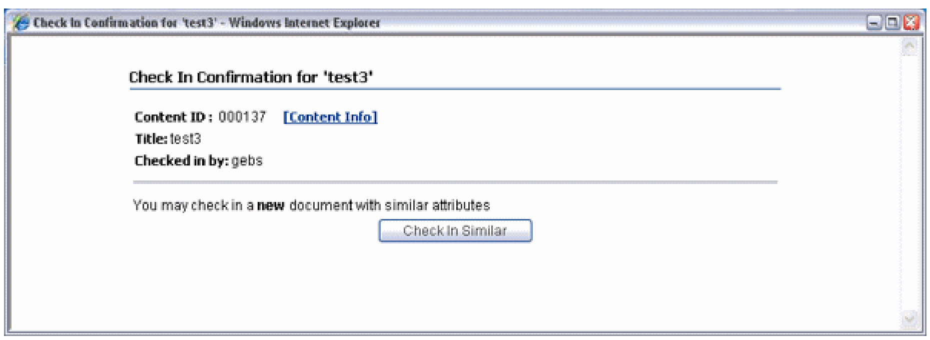
1. In the Managed Attachments screen, click the **Info** icon (displayed in the Info column) for a selected attachment.
2. View details about the document on the Content Information Screen.

3.1.7 Checking In and Attaching a Document

Follow these steps to check in a document and attach it to the selected business application record.

1. In the Managed Attachments Screen, click the **New** button.
2. Complete the fields on the Content Check In Form.
   - In the **Type** field, select a type for the document.
   - In the **Title** field, enter a name for the attached document.
   - Select the **Share Document** field to make the document available to other Oracle UCM users with appropriate access. Leave the field deselected (default) to make the document available when viewed through business application but hidden from the standard Oracle UCM user interface. All users can see private (not shared) attachments when they enter Oracle UCM through business application, regardless of who checked them in.
   - In the **Security Group** field, select a group for the document. If shared, the attachment will be available to users who have permission to this group. (This field is available only if the Share Document field is selected.)
   - Specify the file to attach in the **Primary File** field by clicking the Browse button and selecting a file.
3. Click the **Check In** button.

   Content Server options are displayed and a message confirms that the document was checked in. A button called **Check In Similar** allows you to check in and attach another document using the same metadata values.



4. Close the Check In Confirmation screen.
5. In the Managed Attachments screen, click **Refresh** to display the newly checked in attachment.

3.1.8 Checking Out Documents and Undoing Check-outs

Checking out a document in Oracle UCM makes it temporarily unavailable for other users to save changes to it, until you check it back in, or you or another user undo the check-out.

1. Check out a document by choosing **Checkout** from the Content Actions menu on the Content Information Screen. (Editing a document via the Edit icon also checks out a document.)

Documents Checked Out By You

A green checkmark icon is displayed in the Revision column (if shown) when a document is checked out by you.

1. To undo a check-out by you or check in a revised document, click the **Checked Out By Me** icon to display the Content Information Screen. From its Content Actions menu, choose **Undo Check-out** or **Check-in**.

Documents Checked Out By Another User

A lock icon is displayed in the Revision column (if shown) when a document is checked out by another user.

1. To undo the check-out, click the **Lock** icon to display the Content Information Screen, and choose **Undo Check-out** from its Content Actions menu.

3.1.9 Scanning Via Oracle Distributed Document Capture

The Managed Attachments screen provides a Scan button that, when configured, launches the Oracle Distributed Document Capture application and allows you to either scan a document using a TWAIN compliant scanner or import a scanned image file from disk. After reviewing, editing, and indexing the document, click the **Send** button, which transfers it from Oracle Distributed Document Capture to Oracle UCM and attaches it to the selected business application entity.

Follow these steps to scan or import a document.

1. If scanning documents, place the documents in the feeder tray of the scanner.

   Note: You can attach only one document via scanning or importing at a time.

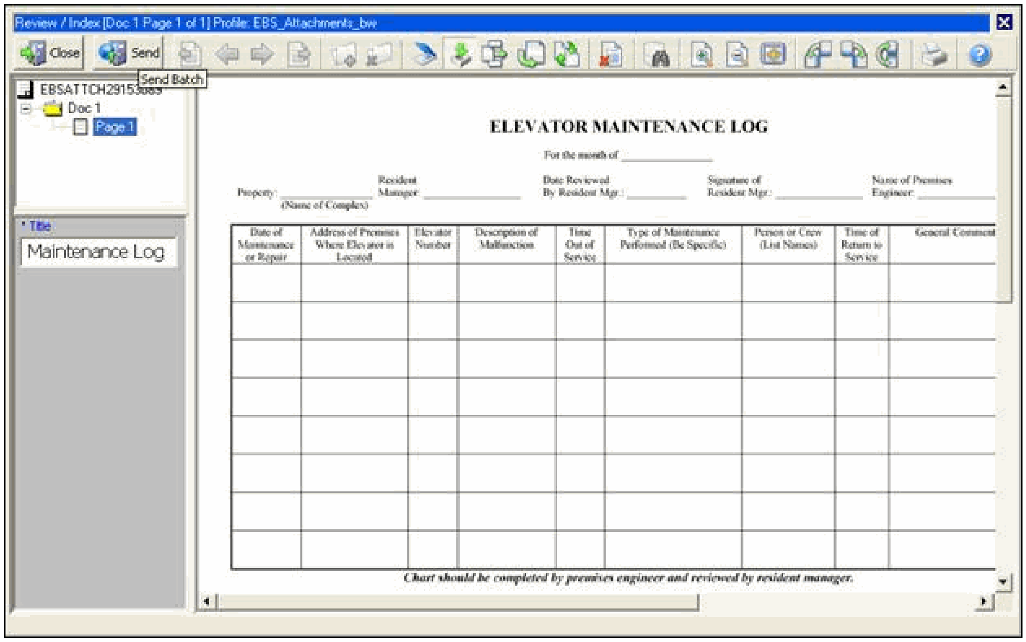
   ---

2. In the Managed Attachments screen, click the **Scan** button. The Scan Document screen is displayed.
3. Select a classification in the **Document Classification** field.

   This identifies the type of document to be scanned or imported. For example, you might choose a document classification of *Identity Documents* to scan a photocopy of a driver's license or passport.
4. Select the **Share Document** field to make the document available to other Oracle UCM users with appropriate access. Leave the field deselected (default) to make the document available when viewed through the business application but hidden from the standard Oracle UCM user interface.
5. In the **Security Group** field, select a group for the document. The attachment will be available only to users who have permission to the group you select. (This field is available only if you chose to share the document in the previous step.)
6. Click the **Scan Document** button. The Oracle Distributed Document Capture client application launches and displays options based on whether the selected document classification is configured for scanning or importing.
   - If set for *scanning*, the scanner scans the pages you placed in the feeder and displays them in the Review/Index screen shown in Figure 3–1, ready for you to review and index them. (All pages are scanned and stored in one document in the batch.)

- If set for *importing*, a File Import screen is displayed, prompting you to select one or more scanned image files to import. After you select files, their pages are displayed in the Review/Index screen shown in Figure 3–1, ready for you to review and index. (All files are imported into a single document in a single batch.)

Figure 3–1 Review/Index Screen in Oracle Distributed Document Capture



7. In the Review/Index screen, review, edit, and index the document. For information, see the *User's Guide for Oracle Distributed Document Capture.* Follow these guidelines:

   - You can add pages to documents, but should not add documents to the batch.
   - Index fields are displayed in the lower side pane. Index fields provide values that are stored as metadata with the Oracle UCM document. An asterisk is displayed before the names of required index fields.
   - All pages in a document have the same index values. Changing the values on one page changes them for all pages in the document.

   Note: If you decide to cancel a document scan or import, you must close the Oracle Distributed Document Capture screen and return to the Managed Attachments screen and perform a new scan or import. This ensures that index values are properly set for attachments.

   ---

8. When done, click **Send** to transfer the document to Oracle UCM and attach it to the business application record. When asked to confirm sending the batch, click **Yes**.

   Note: If required index fields are not complete, you are prompted to complete them in order to send the batch.

The client displays batch send results.

9. Close the Batch Send Results and Oracle Distributed Document Capture screens.
10. In the Managed Attachments screen, click the **Refresh** button to display the newly scanned or imported document now attached to the selected business application record. Note that it may take a few minutes for the generated document to be displayed.

3.1.10 Attaching From the Content Server Repository

Follow these steps to search for and attach documents from the Oracle UCM repository to the selected business application record.

1. In the Managed Attachments screen, click the **From Repository** button. The Expanded Search Form is displayed.
2. Enter search criteria and click **Search**. For example, for the **Title** field, select **Starts** and enter the first few characters of a document's title.

   Search results are displayed, which include documents to which you have security group access.
3. In the **Select** field, select found documents to attach. A grayed out box is displayed if a found document is already attached to the business application record. You can select multiple documents to attach.
4. From the Actions menu above the Select field, choose **Attach to Current Application Entity**. Confirm that you want to attach the selected document(s) to the business application record. A message confirms that the documents were successfully attached.
5. In the Managed Attachments screen, click the **Refresh** button to display the document(s) now attached to the selected business application record.

3.1.11 Detaching a Document

Follow these steps to detach a document from the selected business application record. Detaching a document removes the link to the business application record, but does not delete the document from the Content Server. (Also see "Deleting a Document on Content Server" on page 3-10.)

1. In the Managed Attachments screen, select the row corresponding to the attachment you want to detach from the selected business application record.
2. Click the **Detach** button.
3. A message prompts you to verify that you want to detach the document. Click **OK**.

   A message confirms that the document was successfully detached. After you close the message, the attachment list is automatically refreshed, with the detached document no longer listed.

3.1.12 Opening or Saving a Document

Follow these steps to open a document in a Web-viewable format or save the document in its native format to a selected location such as a local computer. Note that changes you make to a document in this way are not saved on the Content Server; instead, see "Editing a Document in its Native Application" on page 3-9.

1. In the Managed Attachments screen, click a selected document's link in the **Name** field. A File Download dialog box is displayed with options to open or save the file.
2. Click **Open** or **Save**.

3.1.13 Editing a Document in its Native Application

Follow these steps to edit a document on the Content Server. Note that you must have access to the native application.

1. In the Managed Attachments screen, click the **Edit** icon for a selected attachment. (The Edit icon is displayed only for documents that can be edited in this way.)
2. The document opens in its native application. Note that, depending on configuration, you may be prompted to enter a username and password to log in. Make changes and save the document.

   When you open the document using this method, it is automatically checked out. When you save the document in its native application, it is automatically checked back in as a new revision.

3.1.14 Updating a Document's Metadata

Follow these steps to make changes to a selected document's metadata values.

1. In the Managed Attachments screen, click the **Info** icon for a selected attachment.
2. On the Content Information Screen, choose **Update** from the Content Actions menu.
3. Make changes to the document's metadata values on the Info Update Form.
4. Click the **Submit Update** button.

3.1.15 Working With Document Revisions

The Revision column contains useful information about the attachment revision, including:

- the revision number of the attachment.
- if the attachment is checked out by you (green checkmark) or another user (locked icon, hover to view user name).

If *Revision-specific mode* has been configured and a newer revision than the attached revision exists, the **Newer Revision Available** icon (page with green up arrow, shown below) is displayed. To make the newest revision the attached revision, click the icon and choose **Update Attachment to This Revision** from the Content Actions menu in the Content Information Screen.

3.1.16 Deleting a Document on Content Server

Follow these steps to remove a document from the Content Server and also detach it from the business application record. To detach a document only (remove its link to the selected business application record without deleting it from the Content Server), see "Detaching a Document" on page 3-8.

1. In the Managed Attachments screen, click the **Info** icon for a selected attachment.
2. Under Actions options, click the **Delete** link for the revision you want to delete. You will be prompted to confirm the deletion.

3.1.17 Searching for Documents on the Content Server Repository

Follow these steps to search for documents on the Content Server.

> **Note:** Private (not shared) attachments will not be returned in search results when searching in this way from within the business application.

1. In the Managed Attachments screen, click the **From Repository** button.
2. Specify search criteria on the Expanded Search Form.

   For example, to search for a document by its name, select **Starts** in the Title field and enter the first portion of its name in the adjacent field.
3. Click the **Search** button. Search results are listed.

3.2 Managed Attachments Screens

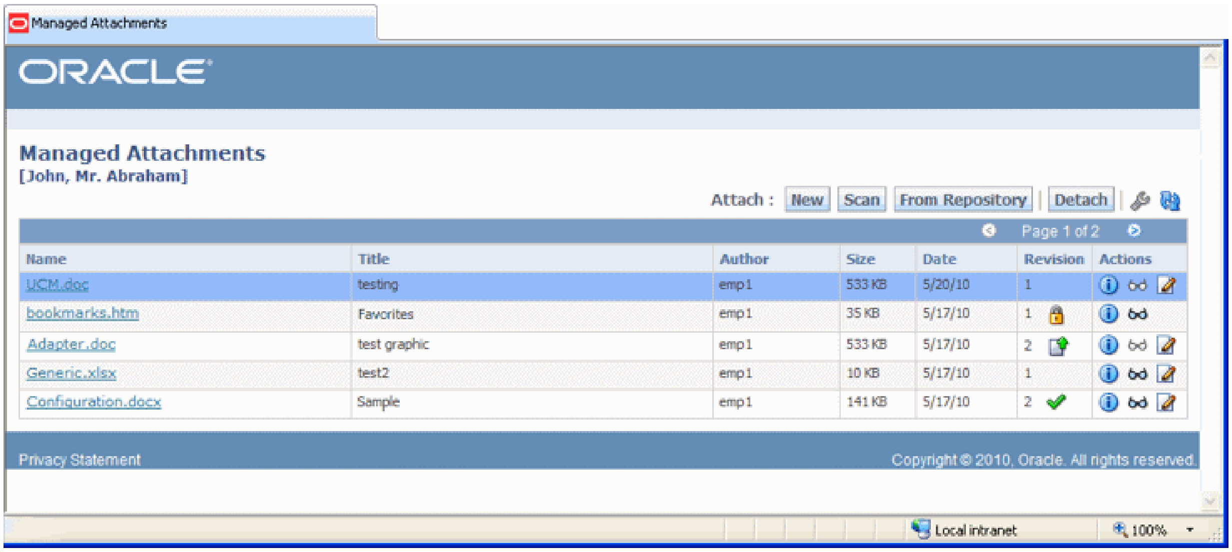
The Managed Attachments screens include:

- "Managed Attachments Screen" on page 3-10
- "Content Check In Form" on page 3-13
- "Configure Fields for Display Screen" on page 3-14
- "Content Information Screen" on page 3-15
- "Info Update Form" on page 3-16
- "Scan Document Screen" on page 3-17
- "Expanded Search Form" on page 3-18
- "Search Results Screen" on page 3-19

3.2.1 Managed Attachments Screen

Use the Managed Attachments screen to view, attach, scan, detach, and edit Oracle UCM documents attached to the selected business application record. You can also use Oracle UCM's search options to locate Oracle UCM documents to which you have access.

The Managed Attachments screen lists all Oracle UCM documents attached to the selected business application record, and provides the options listed in Table 3–1.



About the Managed Attachments Screen

- Metadata fields and values for the selected business application record are displayed in the screen surrounded by square bracket [ ] characters. For example, a managed attachments list for an employee record might display the employee name and/or employee ID.
- The default columns are described in Table 3–1, although users can customize the columns displayed, as described in "Configuring Fields for Display" on page 3-4.
- If the list of attachments is long, page controls and arrows for displaying previous and next pages are displayed.
- You can resize the columns by hovering the cursor over the line between column headings; when it changes to a two-headed arrow, click and drag to increase or decrease the column's size. Column contents wrap to the next line.
- To sort the attachments list, click a column heading. A triangle is displayed after sorting to indicate ascending (right side up) or descending (inverted) order.
- Depending on customization settings, some of the functionality described in this section may not be available. For example, some buttons may not be displayed or some of the icons may be grayed out.
- The Managed Attachments screen is available for a certain amount of time. A message is displayed if your access expires, requiring you to activate Managed Attachments again for the selected business application record.

Table 3–1 Managed Attachments Screen Options

Elements	Icon or Button	Description
Name		Lists the native name (including extension) of each Oracle UCM document attached to the business application record. Click the document's link to open or save a Web-viewable rendition of the document.
Title		Displays the title of the attached Oracle UCM document, assigned at check-in.
Author		Identifies the person who last checked in the file.
Size		Displays the size (KB/MB) of the attached Oracle UCM document.

Table 3–1 (Cont.) Managed Attachments Screen Options

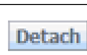
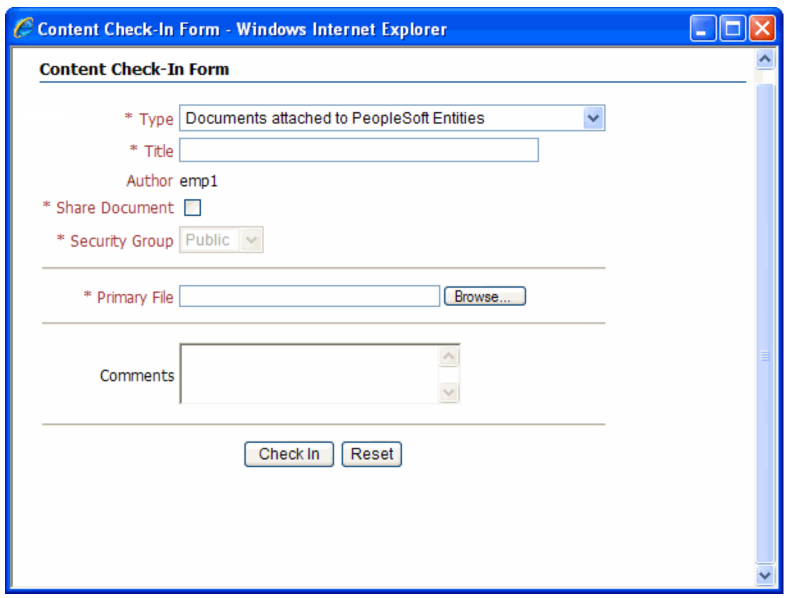
Elements	Icon or Button	Description
Date		Displays the date on which the Oracle UCM document was last checked in to Oracle UCM.
Revision		Displays information about the attached revision. Depending on configuration, some items may not be shown. ▪ **Number:** Indicates the revision number of the attachment. ▪ **Checked Out by Me** icon (checkmark): Indicates that the attachment is checked out by you. Click this icon to display the Content Information Screen, and check in or undo the check-out. ▪ **Checked Out By** icon (lock): Indicates that the attachment is checked out by another user. Hover the cursor over the icon to view the name of the user who checked out the attachment. ▪ **Newer Revision Available** icon (page with up arrow): Indicates that a newer revision exists than the one attached. Click this icon to display the Content Information Screen, and if needed, make the more recent revision the attached revision.
Info		Click this icon to display detailed information and content actions for the selected document on the Content Information Screen. Click this icon to update metadata values for the attached Oracle UCM document on the Info Update Form.
View in AutoVue		Click this icon to view, print, collaborate, annotate, and mark up non-private (shared) attachments of virtually any document type in the AutoVue document viewer, if configured for your system. The AutoVue icon is dimmed (grayed out) for private attachments, which cannot be viewed using AutoVue.
Edit		Click this icon to check out, open, and edit the attached Oracle UCM document in its native application.
New		Click this button to attach an Oracle UCM document to the selected business application record, by completing fields on the Content Check In Form.
Scan		Click this button to scan or import a document and attach it to the business application record, as described in "Scanning Via Oracle Distributed Document Capture" on page 3-6.
From Repository		Click this button to search for files on the Content Server and attach them to the business application record.
Detach		Click this button to detach the selected Oracle UCM document. Detaching removes the Oracle UCM document from the business application entity, but not from Oracle UCM.

Table 3–1 (Cont.) Managed Attachments Screen Options

Elements	Icon or Button	Description
Configure		Click this button to select and order fields for display in the Managed Attachments screen on the Configure Fields for Display Screen.
Refresh		Click this button to update the Managed Attachments display.

3.2.2 Content Check In Form

Use the Content Check In Form to check in documents to Content Server, assign them metadata values, and attach them to the selected business application record.



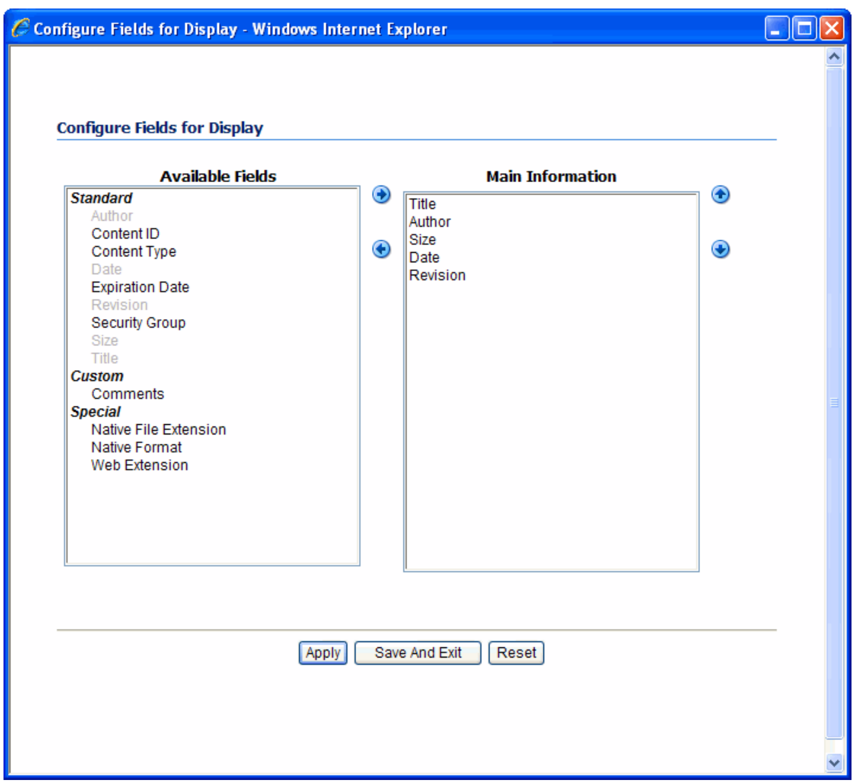
To display this form, click the **New** button in the Managed Attachments Screen.

Elements	Description
Type	Select the option that best describes the type of file to be attached. The default document type is displayed. This field is required.
Title	Enter a descriptive title for the document. This field is required.
Author	Identifies the person who checked in the file. This field is required.
Share Document	Select this field to make the document available to other Oracle UCM users with appropriate access. Leave the field deselected (default) to make the document available when viewed through the business application but hidden from the standard Oracle UCM user interface.

Elements	Description
Security Group	Select a security group for the file. Keep in mind that this file, if shared, will be available to users who have permission to the specified security group. This field is required.
Primary File	Specify a primary file using one of these methods: ■ Click **Browse** next to the Primary File field. Navigate to and select the native file, and then click **Open**. ■ Enter the complete path name and file name of the native file in the Primary File field (for example, c:/My Documents/ABC Project/MyFile.doc). This field is required.
Comments	Enter any notes about the file.
Check In	Click this button to check in the specified document using the settings selected on this screen.
Reset	Click this button to cancel any entries and restore the default settings in this screen.

3.2.3 Configure Fields for Display Screen

The Configure Fields for Display screen allows business application users to specify the attachment information to display in the Managed Attachments screen.

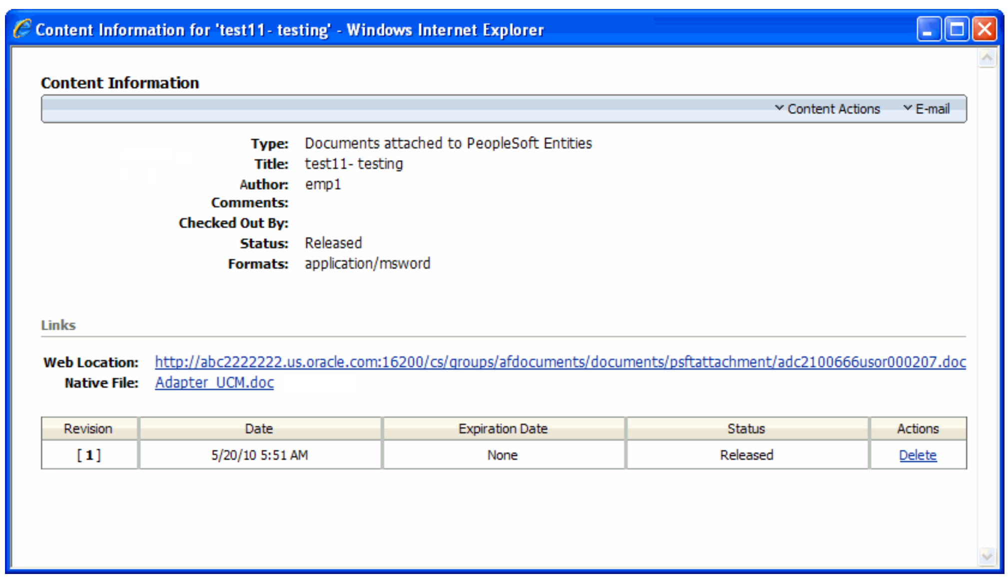


Users display this screen by clicking the **Configure** button in the Managed Attachments Screen.

Elements	Description
Available Fields	Lists fields available for display in the Managed Attachments screen. Click the right arrow to move a selected field to the Main Information area. Fields selected for display are shown in dimmed characters.
Main Information	Lists fields selected for display in the Managed Attachments screen. Fields are displayed left to right in the order in which they are listed in this area. Click the up or down arrow button to reposition a selected field.
Apply	Click this button to preview your changes in the Managed Attachments screen. (You may need to temporarily reposition the Configure Fields for Display screen to view screen changes.)
Save And Exit	Click this button to save changes to the display configuration and return to the Managed Attachments screen.
Reset	Click this button to cancel any changes and restore the default system field display.

3.2.4 Content Information Screen

Use the Content Information screen to view details about the attached file, view its web-viewable or native version, and if needed, delete the document.



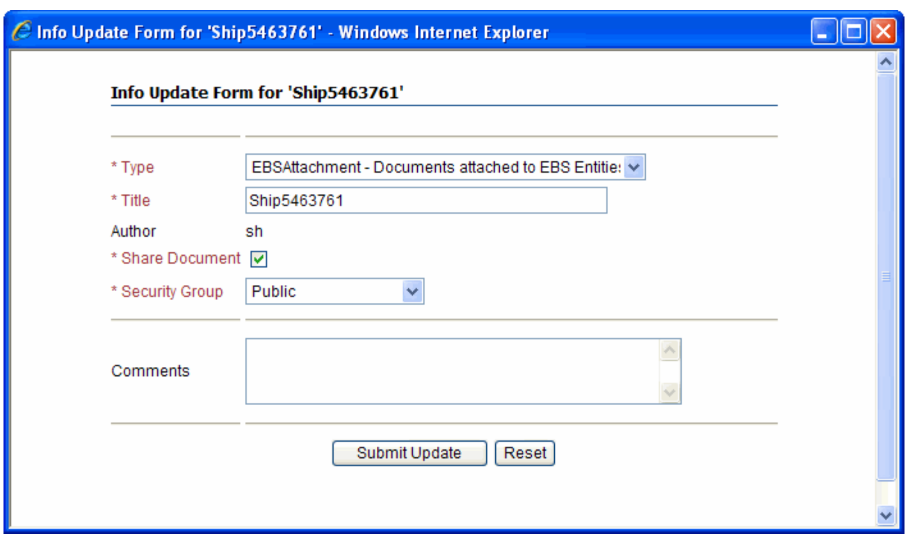
Users display this screen by clicking the **Info** button for a selected document in the Managed Attachments Screen.

Elements	Description
Type	Displays the type that best describes the file.
Title	Displays the title of the attached Oracle UCM file, assigned at checkin.
Author	Identifies the person who checked in the file.
Comments	Displays additional notes about the file.

Elements	Description
Security Group	An identifier that specifies access permission to the file.
Checked Out By	Identifies the user who has the file checked out.
Status	Identifies the file's current status. A status of Released indicates that the revision is available in the Content Server.
Formats	Identifies formats for the file.
Web Location	Click this link to view a web-viewable rendition of the attached file.
Native File	Click this link to either save a copy of the file or open it in its native application.
Table	Lists revisions of the file, along with their release date, expiration date, and status. Click the Delete link to remove the corresponding revision.
Content Actions	Provides options for checking out the file, updating it, checking in a similar file, subscribing to the file, or checking out and opening the file. If viewing this screen after clicking the **Newer Revision Available** icon on the Managed Attachments screen, an additional command is available: Choose **Update Attachment to This Revision** to make the newer revision the attached version.
E-mail	The **Send Link by E-mail** link opens a new e-mail message that contains a URL to the selected file.

3.2.5 Info Update Form

Use the Update Info Form to make changes to a selected document's metadata values. Users search for documents on the Content Server by their metadata values, as described in "Searching for Documents on the Content Server Repository" on page 3-10.

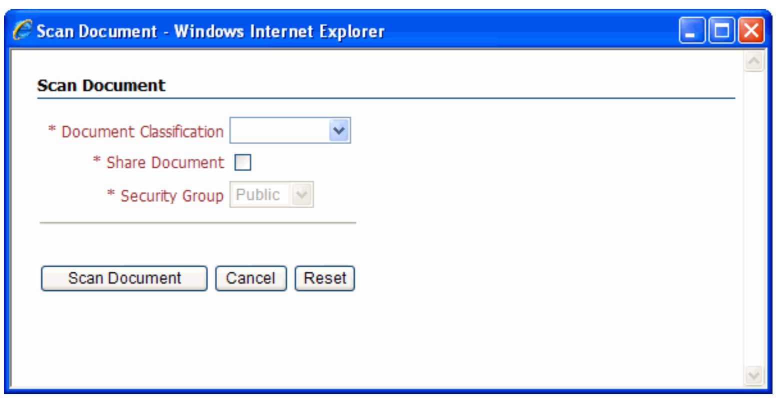


Users display this form by clicking the **Info** icon for a selected attachment in the Managed Attachments Screen, then choosing **Update** from the **Content Actions** menu on the Content Information Screen.

Elements	Description
Type	Select the option that best describes the file.
Title	Enter a descriptive title for the document.
Author	Identifies the user who checked in the current file revision.
Share Document	Select this field to make the document available to other Oracle UCM users with appropriate access. Leave the field deselected (default) to make the document available when viewed through the business application but hidden from the standard Oracle UCM user interface.
Security Group	Specifies access permission to the file. You can enter text or select from the list of predefined values.
Comments	Enter any notes about the file.
Submit Update	Click this button to save the metadata changes to the attached file.
Reset	Click this button to cancel metadata changes and restore them to their values upon entering this form.

3.2.6 Scan Document Screen

Use the Scan Document screen to specify the type of document you want to scan or import, and then attach to the business application entity.



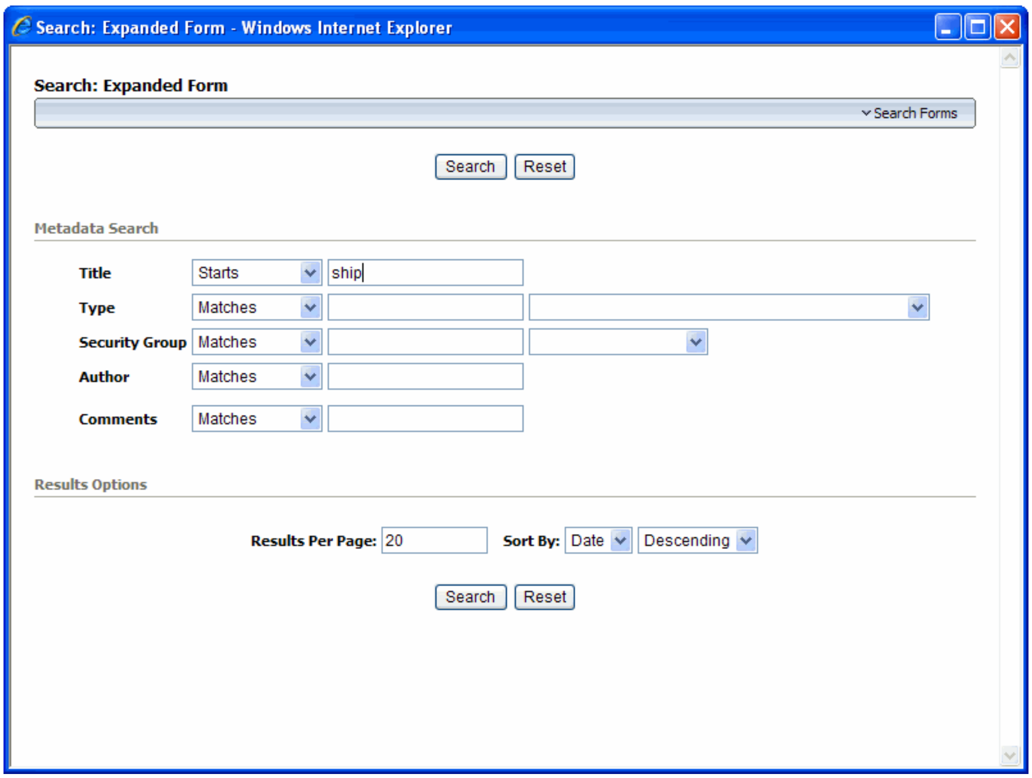
Users display this screen by clicking the **Scan** button in the Managed Attachments Screen.

Element	Description
Document Classification	Identify the type of document to be scanned or imported.
Share Document	Select this field to make the document available to other Oracle UCM users with appropriate access. Leave the field deselected (default) to make the document available when viewed through the business application but hidden from the standard Oracle UCM user interface.
Security Group	Select a group for the document. ▪ If you selected **Share Document**, the document will be available to users who have permission to this group. ▪ If you left **Share Document** deselected, you do not need to select a security group; this field is grayed out.
Scan Document	Click to begin scanning or importing the document.

Element	Description
Cancel	Click to exit without scanning or importing.
Reset	Click this button to cancel any selections and restore the default settings in this screen.

3.2.7 Expanded Search Form

This search screen enables you to search the Content Server for content. After specifying search criteria and clicking **Search**, the results are listed. From the Search Results Screen, you can attach selected documents to the selected business application record.



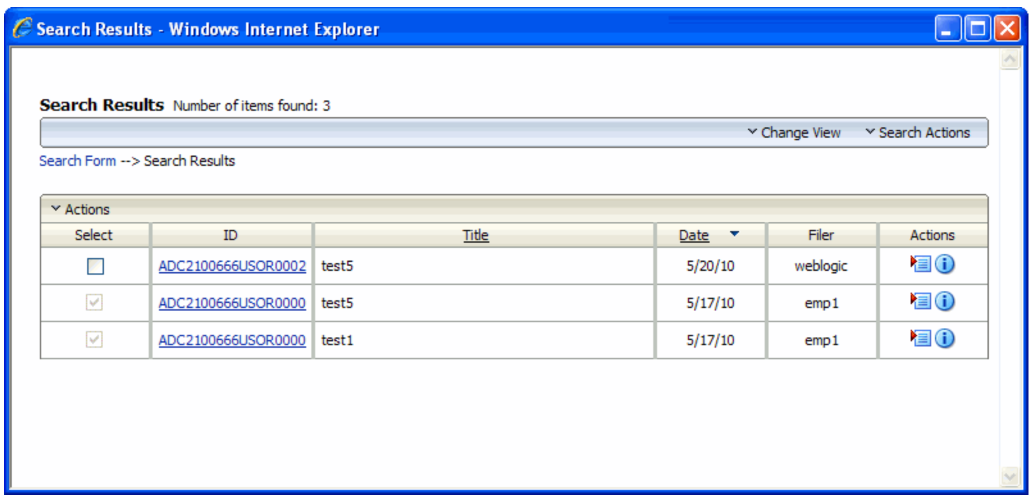
Users display this form by clicking the **From Repository** button in the Managed Attachments Screen.

Elements	Description
Title	Select an operator and search for the file's title.
Type	Select an operator and search for the file's type.
Security Group	Select an operator and search for the file's security group. (To search for private documents, select AFDocuments as the security group.)
Author	Select an operator and search for the person who checked in the file.
Comments	Specify an operator and search for files by their comments.
Results Per Page	Determines the number of results that are displayed on the search results page.

Elements	Description
Sort By	Determines which of the following options are used to sort the targeted search results, and whether or not those results are listed in ascending or descending (default) order: ■ Release Date (default) ■ Title
Search	Click this button to perform the search after specifying search criteria.
Reset	Resets the form.

3.2.8 Search Results Screen

This screen displays the results of your Content Server repository search and allows you to attach one or more selected documents to the selected business application record. You can also save or restrict your search using standard Oracle UCM query actions.



Users display this form by clicking the **From Repository** button in the Managed Attachments Screen, specifying a search in the Expanded Search Form and clicking **Search**.

Elements	Description
Select	Select one or more documents to attach. A grayed out box is displayed if a document is already attached to the business application record. You can select multiple documents to attach.
Actions	From this menu, choose **Attach to current Application Entity** to attach the selected documents to the business application record.
Change View	Select another Content Server results view.
Search Actions	Optionally save the search for future use.

A

Managed Attachments Solution Tables

The Oracle Enterprise Content Management Application Adapters (Managed Attachments Solution) utilizes the following types of database tables, each configured for this solution:

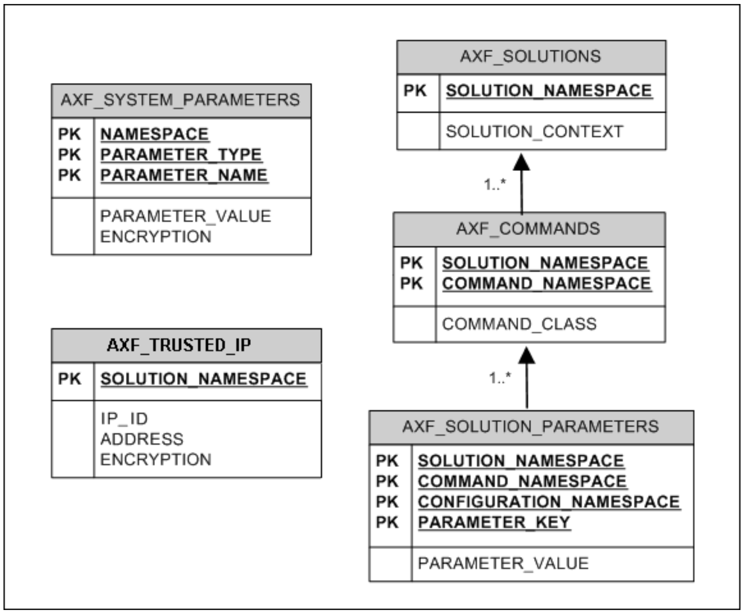
- **Application Extension Framework** (AXF) tables define the solution, its system parameters, and the GrantAccess command used. See "AXF Database Tables" on page A-1.
- **E-Business Suite** tables define how the Managed Attachments screen is activated via the Zoom menu on selected E-Business Suite forms. See "E-Business Suite Database Tables" on page A-7.
- **PeopleSoft** tables define how the Managed Attachments screen is activated via a button, link, or menu on selected PeopleSoft forms. See "PeopleSoft Tables" on page A-13.
- **Content Server** tables define how Content Server documents are mapped to E-Business Suite or PeopleSoft business objects and how users are temporarily granted access to documents associated with a particular business object. See "Content Server Tables" on page A-17.

These tables are automatically populated using database scripts (E-Business Suite) or via Integration Broker (PeopleSoft), as explained in "Installation and Configuration" on page 2-1. However, this appendix describes how the tables are configured, in case you need to modify them.

A.1 AXF Database Tables

Note: If modifying AXF table values in a running system, either execute Clear DB Cache from the Driver page or restart the AXF application within the Application Server for the changes to take effect.

The diagram that follows displays the AXF configuration tables used for the Managed Attachments solution and their relationships.



AXF Table	Description
AXF_SYSTEM_PARAMETERS Table	Define general parameters for infrastructure, services, and solutions.
AXF_TRUSTED_IP Table	Optionally secure the integration by specifying business application server trusted IP addresses.
AXF_SOLUTIONS Table	Define AXF solutions.
AXF_COMMANDS Table	Define AXF commands within solutions.
AXF_SOLUTION_PARAMETERS Table	Define parameters for AXF commands and AXF web tools.

A.1.1 AXF_SYSTEM_PARAMETERS Table

This table defines general system parameters for use by infrastructure, services, or solutions.

A.1.1.1 Column Description

Table A–1 Column Description for AXF_SYSTEM_PARAMETERS Table

Column	Description
NAMESPACE	Specifies the functional area that utilizes the parameter.
PARAMETER_TYPE	Name used to differentiate between parameters. Can be used to define custom types within a namespace. Additional parameters may be added as type *database*.

Table A–1 (Cont.) Column Description for AXF_SYSTEM_PARAMETERS Table

Column	Description
PARAMETER_NAME	Name of the parameter. Used when retrieving the parameter value from the database. Parameters related to this adapter include: ▪ securityClass: Specifies the class name of a security provider for AXF. Options applicable for this adapter include: *NullSecurityCheck*: Bypasses any additional security check. *IpSecurityCheck:* Specifies that the AXF security plug-in accepts requests only from E-Business Suite or PeopleSoft servers set to be trusted, as configured in "AXF_TRUSTED_IP Table" on page A-3. For this adapter, this column must be set to *securityClass*.
PARAMETER_VALUE	Value of the parameter. For this adapter, this column must be set to one of the following: ▪ *oracle.imaging.bai.axf.security.NullSecurityCheck* ▪ *oracle.imaging.bai.axf.security.IpSecurityCheck*
ENCRYPTION	Allows for the encryption of parameter values such as passwords. Possible values for this column include: ▪ ENCRYPT: Causes the value in the parameter value column to be encrypted after the first time the configuration is loaded. After the encryption takes place, the column's value changes to ENCRYPTED. ▪ ENCRYPTED: Denotes that the value in the PARAMETER_VALUE column is encrypted. ▪ PLAIN_TEXT: Denotes that the value in the PARAMETER_VALUE column is in plain text.

A.1.1.2 Example Implementation

This example displays system parameter settings for the adapter solution.

Table A–2 Example AXF_SYSTEM_PARAMETERS Table

NAMESPACE	PARAMETER_TYPE	PARAMETER_NAME	PARAMETER_VALUE	ENCRYPTION
UCM_Managed_Attachments	system	securityClass	oracle.imaging.bai.axf.security.IpSecurityCheck	PLAIN_TEXT

A.1.2 AXF_TRUSTED_IP Table

Use this optional table to configure the AXF security plug-in to accept requests only from business application servers set to be trusted, based on IP address and solution namespace.

In addition to configuring the AXF_TRUSTED_IP table, implementing trusted IP addresses also requires that you set the PARAMETER_VALUE in the AXF_SYSTEM_PARAMETERS table to use *IpSecurityCheck*. See "Example Implementation" on page A-3.

A.1.2.1 Column Description

Table A–3 Column Description for AXF_TRUSTED_IP Table

Column	Description
IP_ID	A sequence represented by AXF_TRUSTED_IP_SEQ.NEXTVAL.
SOLUTION_NAMESPACE	Defines the AXF solution name.

Table A–3 (Cont.) Column Description for AXF_TRUSTED_IP Table

Column	Description
ADDRESS	IP address of the E-Business Suite Forms or PeopleSoft server you want to trust.
ENCRYPTION	Allows for the encryption of parameter values such as passwords. Possible values for this column include: ENCRYPT: Causes the value in the parameter value column to be encrypted after the first time the configuration is loaded. After the encryption takes place, the column's value changes to ENCRYPTED. ENCRYPTED: Denotes that the value in the PARAMETER_VALUE column is encrypted. PLAIN_TEXT: Denotes that the value in the PARAMETER_VALUE column is in plain text. Note that PLAIN_TEXT must be used for the UCM_Managed_Attachments solution.

A.1.2.2 Example Implementation

This example sets a business application server, identified by its IP address, to be trusted for the UCM_Managed_Attachments solution.

Table A–4 Example AXF_TRUSTED_IP Table

IP_ID	SOLUTION_NAMESPACE	ADDRESS	ENCRYPTION
1	UCM_Managed_Attachments	127.0.0.1	PLAIN_TEXT

A.1.3 AXF_SOLUTIONS Table

The AXF_SOLUTIONS table defines the solutions used by AXF. It links to the AXF_COMMANDS Table via the SOLUTION_NAMESPACE column.

A.1.3.1 Column Description

Table A–5 Column Description for AXF_SOLUTIONS Table

Column	Description
SOLUTION_CONTEXT	Defines the JNDI name of the AXF solution implementation. (Currently, AxfCommandMediator is the only solution implementation.)
SOLUTION_NAMESPACE	Defines the AXF solution name.

A.1.3.2 Example Implementation

This example shows the Managed Attachments solution defined, using AxfCommandMediator as its solution implementation.

Table A–6 Example AXF_SOLUTIONS Table

SOLUTION_NAMESPACE	SOLUTION_CONTEXT
UCM_Managed_Attachments	AxfCommandMediator

A.1.4 AXF_COMMANDS Table

This table defines AXF commands and their java classes for the solution. Each command's parameters are configured in the AXF_SOLUTION_PARAMETERS Table.

A.1.4.1 Column Description

Table A–7 Column Description for AXF_COMMANDS Table

Column	Description
SOLUTION_NAMESPACE	The name of the solution, as defined in the AXF_SOLUTIONS Table.
COMMAND_NAMESPACE	Defines the unique name of the command within the solution.
COMMAND_CLASS	The fully qualified class name in which the command is defined. This class will be loaded and the execute() method representing the command will be executed.

A.1.4.2 Example Implementation

This example shows the Oracle UCM Managed Attachments command defined for the Managed Attachments solution.

Table A–8 Example AXF_COMMANDS Table

SOLUTION_NAMESPACE	COMMAND_CLASS	COMMAND_NAMESPACE
UCM_Managed_Attachments	oracle.imaging.axf.commands.ucm.AfGrantAccessCommand	UCM_Managed_Attachments

A.1.5 AXF_SOLUTION_PARAMETERS Table

This table defines command parameters for the solution and AXF command.

A.1.5.1 Column Description

Table A–9 Column Description for AXF_SOLUTION_PARAMETERS Table

Column	Description
SOLUTION_NAMESPACE	Identifies the solution namespace, as defined in the AXF_SOLUTIONS Table.
COMMAND_NAMESPACE	Specifies the command name, as defined in the AXF_COMMANDS Table.

Table A–9 (Cont.) Column Description for AXF_SOLUTION_PARAMETERS Table

Column	Description
CONFIGURATION_NAMESPACE	Used to implement the command. Specify the complete package name of the implementation class. This namespace path provides the physical Java class to be instantiated. The namespace also differentiates commands within the same solution namespace.
PARAMETER_KEY	Specifies the parameter key to be used in the AXF command. Parameters include: ■ RIDC_CONNECTION_STR: Specifies the RIDC connection string used to execute the AF_GRANT_ACCESS Oracle UCM service. Includes the hostname or IP address of the system on which Content Server is running, and the Oracle UCM server port that receives RIDC calls. (To find the value for the Oracle UCM server port, locate the IntradocServerPort config value in config.cfg.) ■ UCM_CONNECTION_STR: Specifies the base URL that executes the Oracle UCM attachments framework search, which lists associated documents. This parameter also sets the following values: Hostname or IP address of the system on which Content Server is running Port on which the web server is listening. The `/idc/` portion of the url should be changed to match your Oracle UCM installation's web root (*`/ucm_web_root/`*) Content Server profile (default profile is EBSProfile or PSFTProfile) GET_SEARCH_RESULTS_FORCELOGIN service ResultCount (default is 5) ResultTemplate (default template is EBS_LIST or PSFT_LIST). DATABASE.METADATA.AFLIST search engine ■ UCM_ADMIN_USER: Specifies the administrative Oracle UCM user that executes the AF_GRANT_ACCESS service for the user logged into the business application.
PARAMETER_VALUE	Specifies the value of the parameter key.

A.1.5.2 Example Implementation

These examples define the UCM_Managed_Attachments command for the UCM_Managed_Attachments solution. Table A–10 provides an E-Business Suite example and Table A–11 provides a PeopleSoft example.

- The first row specifies the RIDC connection string that executes the AF_GRANT_ACCESS Oracle UCM service.
- The second row specifies the Managed Attachments URL that invokes the Oracle UCM attachments framework search.
- The third row specifies the Oracle UCM administrative user who runs the AF_GRANT_ACCESS service; this username is dynamically retrieved.

Fields not shown: SOLUTION_NAMESPACE=UCM_Managed_Attachments

Table A–10 Example AXF_SOLUTION_PARAMETERS Table for E-Business Suite Managed Attachments Solution

COMMAND_ NAMESPACE	CONFIGURATION_NAMESPACE	PARAMETER_KEY	PARAMETER_VALUE
UCM_Managed_ Attachments	oracle.imaging.axf.commands.ucm. AfGrantAccessCommand	RIDC_CONNECTION_STR	idc://*UCM hostname or IP address*:*UCM server port*
UCM_Managed_ Attachments	oracle.imaging.axf.commands.ucm. AfGrantAccessCommand	UCM_CONNECTION_STR	http://*UCM hostname or IP address*:*WebServerPort*/*ucm web root*/idcplg/_p/min/af/ trigger-EBSProfile? IdcService=GET_SEARCH_RESULTS_ FORCELOGIN&ResultCount=20& ResultTemplate=EBS_LIST& SearchEngineName= DATABASE.METADATA.AFLIST
UCM_Managed_ Attachments	oracle.imaging.axf.commands.ucm. AfGrantAccessCommand	UCM_ADMIN_USER	*UCM admin user*

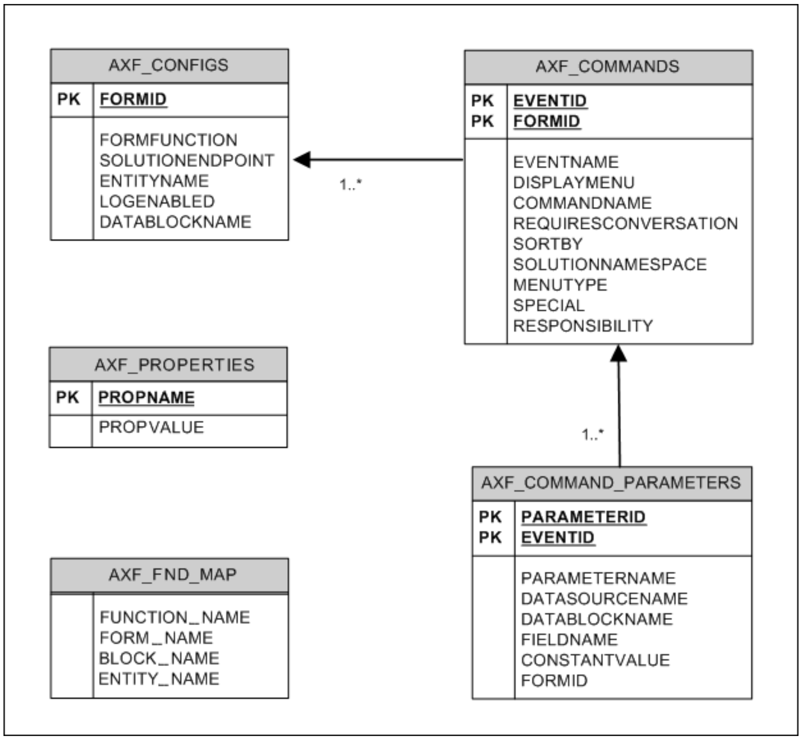
Table A–11 Example AXF_SOLUTION_PARAMETERS Table for PeopleSoft Managed Attachments Solution

COMMAND_ NAMESPACE	CONFIGURATION_NAMESPACE	PARAMETER_KEY	PARAMETER_VALUE
UCM_Managed_ Attachments	oracle.imaging.axf.commands.ucm. AfGrantAccessCommand	RIDC_CONNECTION_STR	idc://*UCM hostname or IP address*:*UCM server port*
UCM_Managed_ Attachments	oracle.imaging.axf.commands.ucm. AfGrantAccessCommand	UCM_CONNECTION_STR	http://*UCM hostname or IP address*:*WebServerPort*/*ucm web root*/idcplg/_p/min/af/ trigger-PSFTProfile? IdcService=GET_SEARCH_RESULTS_ FORCELOGIN&ResultCount=20& ResultTemplate=PSFT_LIST& SearchEngineName= DATABASE.METADATA.AFLIST
UCM_Managed_ Attachments	oracle.imaging.axf.commands.ucm. AfGrantAccessCommand	UCM_ADMIN_USER	*UCM admin user*

A.2 E-Business Suite Database Tables

Each E-Business Suite form enabled for the AF integration requires an AXF E-Business Suite configuration that defines a Zoom Menu item with the label Managed Attachments and a set of parameters that include the E-Business Suite instance name, business object type, business object key(s), and user friendly description of the business object instance.

The diagram that follows displays the E-Business Suite configuration tables used for the Managed Attachments solution and their relationships.



E-Business Suite Table	Description
AXF_CONFIGS Table (E-Business Suite)	Enables the AXF solution on various E-Business Suite Forms.
AXF_COMMANDS Table (E-Business Suite)	Describes the actions to be taken based on user activity.
AXF_COMMAND_PARAMETERS Table (E-Business Suite)	Defines the information sent for the AfGrantAccess command.
AXF_FND_MAP Table (E-Business Suite)	Defines E-Business Suite form values to pass to the AfGrantAccessCommand when a user activates the Managed Attachments functionality from an E-Business Suite form.
AXF_PROPERTIES Table (E-Business Suite)	Defines properties for AXF integration for E-Business Suite.

A.2.1 AXF_CONFIGS Table (E-Business Suite)

Use the AXF_CONFIGS table to enable the AXF solution on various E-Business Suite Forms. This table allows a fine level of granularity when selecting which forms are AXF-enabled.

When an action occurs, the customized code launches the specified solution and command configured for the event. When configured for the E-Business Suite adapter for Oracle UCM, this table invokes the AfGrantAccess command.

A.2.1.1 Column Description

Table A–12 Column Description for AXF_CONFIGS Table

Column Name	Description	Data Type
FORMID	Specifies the primary key of the table.	Number
FORMFUNCTION	Distinguishes each E-Business Suite Form based on the form's functionality.	Varchar2 (100 byte)
SOLUTIONENDPOINT	Specifies a URL to AXF.	Varchar2 (1000 byte)
ENTITYNAME	Used by the attachment functionality as a unique name, which links attachments to the correct Forms.	Varchar2 (100 byte)
LOGENABLED	Enables or disables the log for the specified form. See "Configuring E-Business Suite Logging" on page 2-17. Specify one of the following: ■ 1/TRUE/YES ■ 0/FALSE/NO	Varchar2 (10 byte)
DATABLOCKNAME	Specify the data block on the form to be enabled. Note that you can also specify `AXF_DEFAULT` to enable all data blocks on the form. A Form may be reused by E-Business Suite (for example, Invoice Entry and Invoice Query); the FORMFUNCTION and DATABLOCKNAME together uniquely identify each form.	Varchar2 (100 byte)

A.2.1.2 Example Implementation

This example defines the AfGrantAccess command in the AXF_CONFIGS table for the Invoice Entry form.

Table A–13 Example AXF_CONFIGS Table

FORMID	FORMFUNCTION	SOLUTIONENDPOINT	ENTITY NAME	LOG ENABLED	DATA BLOCKNAME
1	AXF_MANAGED_ATTACHMENTS	`http://axf hostname or ip address:axf port/imaging-bai-axf/AxfSolutionMediator`	(null)	YES	(null)

A.2.2 AXF_COMMANDS Table (E-Business Suite)

Use the AXF_COMMANDS table to describe the actions to be taken based on user activity. This table works in conjunction with the AXF_CONFIGS Table (E-Business Suite).

A.2.2.1 Column Description

Table A–14 Column Description for AXF_COMMANDS Table

Column Name	Description	Data Type	Nullable
FORMID	Links to the AXF_CONFIGS Table (E-Business Suite).	Number	No
EVENTID	Primary key of the table.	Number	Yes

Table A–14 (Cont.) Column Description for AXF_COMMANDS Table

Column Name	Description	Data Type	Nullable
EVENTNAME	Name of the Event command to be invoked (ZOOM for this adapter).	Varchar2(100 byte)	Yes
DISPLAYMENU	Displays text of the menu for the command.	Varchar2(100 byte)	Yes
COMMANDNAMESPACE	Request command to be passed to the back-end when the menu is selected.	Varchar2(100 byte)	Yes
REQUIRESCONVERSATION	Indicates if the command requires a valid conversation or not. For this adapter, this value must be NO.	Varchar2(10 byte)	Yes
SORTBY	Order in which the menu is displayed.	Number	Yes
SOLUTIONNAMESPACE	Name of the solution.	Varchar2(100 byte)	Yes
MENUTYPE	Specify the menu type to display to users in E-Business Suite. ZOOM displays a Zoom menu in the toolbar.	Varchar2(25 byte)	Yes
SPECIAL	Create new menu entries by entering a unique number for the Special type menu. (Not applicable for this adapter.)	Varchar2(10 byte)	Yes
RESPONSIBILITY	Use this column to filter the menu options based on user responsibility. Enter a value to display the menu only to end users with responsibilities associated with that value. (Not applicable for this adapter.)	Varchar2(100 byte)	Yes

A.2.2.2 Example Implementation

The example AXF_COMMANDS table that follows displays fields for an AfGrantAccess command configuration for the Invoice Entry form.

Fields not shown: SPECIAL=(null), RESPONSIBILITY=(null)

Table A–15 Example AXF_COMMANDS Table for Invoice Entry Form

EVENT ID	FORM ID	EVENT NAME	DISPLAYMENU	COMMAND NAMESPACE	REQUIRESCO NVERSATION	SORT BY	SOLUTION NAMESPACE	MENU TYPE
8	1	ZOOM	Managed Attachments	UCM_Managed_ Attachment	NO	3	UCM_Managed_ Attachments	ZOOM

A.2.3 AXF_COMMAND_PARAMETERS Table (E-Business Suite)

Use the AXF_COMMAND_PARAMETERS table to define the information sent for each defined command. Each command may require or omit a different set of parameters.

A.2.3.1 Column Description

Table A–16 Column Description for AXF_COMMAND_PARAMETERS Table

Column	Description
PARAMETERID	Defines a unique ID for the parameter.
EVENTID	Defines a unique ID for the event. Comes from the AXF_ COMMANDS Table (E-Business Suite).

Table A–16 (Cont.) Column Description for AXF_COMMAND_PARAMETERS Table

Column	Description
PARAMETERNAME	The name of the parameter to be passed. For this adapter, this value must be set to: ■ Application: Value assigned to dAFApplication, a required Oracle UCM parameter key. This name/value pair is passed as a configuration parameter to the Oracle UCM AF_GRANT_ACCESS service and attachments framework search.
DATASOURCENAME	Data Source for the parameter value. You can specify *Data* or *Constant*.
DATABLOCKNAME	Data Block of the Form from which the value is fetched
FIELDNAME	Field Name in the form from which the value is fetched.
CONSTANTVALUE	Must be set to a value that uniquely identifies the E-Business Suite instance.

A.2.3.2 Example Implementation

The AXF_COMMAND_PARAMETERS example that follows displays fields configured for the AfGrantAccess command for the Invoice Entry form.

Table A–17 Example AXF_COMMAND_PARAMETERS Table

PARAMETER ID	EVENT ID	PARAMETERNAME	DATASOURCE NAME	DATABLOCKNAME	FIELDNAME	CONSTANTVALUE
1	8	application	CONSTANT	(null)	(null)	EBS_instanceA

A.2.4 AXF_FND_MAP Table (E-Business Suite)

This table relates to an E-Business Suite form's values passed to the AfGrantAccessCommand when a user activates the Managed Attachments functionality from an E-Business Suite form. The adapter looks up values for the E-Business Suite form in this table and passes them to the AfGrantAccessCommand for executing the Oracle UCM AF_GRANT_ACCESS service and attachments framework search.

A.2.4.1 Column Description

Table A–18 Column Description for AXF_FND_MAP Table

Column	Description
FUNCTION_NAME	Defines the E-Business Suite Form based on its functionality.
FORM_NAME	Defines the name of the E-Business Suite form to be enabled.
BLOCK_NAME	Defines the data block on the form to be enabled.
ENTITY_NAME	Used by the attachment functionality as a unique name, which links attachments to the correct forms.

A.2.4.2 Example Implementation

The AXF_FND_MAP example that follows displays fields configured for the AfGrantAccess command for the Invoice Entry form.

Table A–19 Example Implementation for AXF_FND_MAP Table

FUNCTION_NAME	FORM_NAME	BLOCK_NAME	ENTITY_NAME
AP_APXINWKB	APXINWKB	INV_SUM_FOLDER	AP_INVOICES

A.2.5 AXF_PROPERTIES Table (E-Business Suite)

Use the AXF_PROPERTIES table to define properties for AXF integration for E-Business Suite. You can also use its AXF_PAPERCLIP property to enable or disable the paperclip (display attached document) feature, as described in "Enabling or Disabling the Paperclip Attachments Option" on page 2-16.

A.2.5.1 Column Description

Table A–20 Column Description for AXF_PROPERTIES Table (E-Business Suite)

Column	Description
PROPNAME	Specifies properties to be used. Properties include: ■ SecureMode: To enable SSL, set this property to ON, and set values for AXFWalletPath and AXFWalletPwd properties. ■ AXFWalletPath: Certificate location (path). ■ AXFWalletPwd: Password for Wallet Manager. ■ AXF_VERSION: Specify `1` (default) for AXF 10g. ■ AXF_SOAP_SECURITY: Does not apply to the Managed Attachments solution. ■ AXF_SOAP_USER: Does not apply to the Managed Attachments solution. ■ AXF_SOAP_POLICY: Does not apply to the Managed Attachments solution. ■ AXF_PAPERCLIP: Set to TRUE to enable the E-Business Suite native attachments paperclip option, or FALSE (default) to disable it. See "Enabling or Disabling the Paperclip Attachments Option" on page 2-16.
PROPVALUE	Specifies the property's value.

A.2.5.2 Example Implementation

This example table shows the default properties values.

Table A–21 Example AXF_PROPERTIES Table

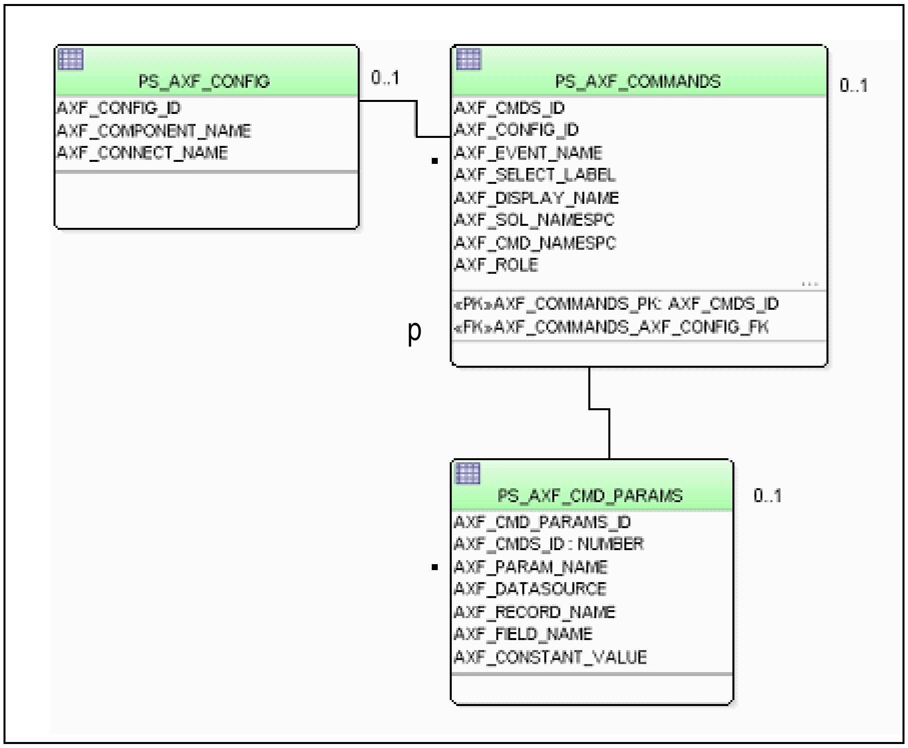
PROPNAME	PROPVALUE
SecureMode	OFF
AXFWalletPath	file:*walletpath*
AXFWalletPwd	walletpassword
AXF_VERSION	1
AXF_SOAP_POLICY	(null)
AXF_SOAP_SECURITY	(null)
AXF_SOAP_USER	(null)
AXF_PAPERCLIP	false

A.3 PeopleSoft Tables

Configuring AXF for PeopleSoft requires configuring these AXF-related tables in PeopleSoft:

- "PS_AXF_CONFIG Table (PeopleSoft)" on page A-13
- "PS_AXF_COMMANDS Table (PeopleSoft)" on page A-14
- "PS_AXF_CMD_PARAMS Table (PeopleSoft)" on page A-15

The following diagram shows how the tables used by the PeopleSoft system in AXF solutions are related.



Note: All AXF table fields require non-null values. You can include a space for fields that are not applicable.

A.3.1 PS_AXF_CONFIG Table (PeopleSoft)

Use the PS_AXF_CONFIG table to enable the AXF solution on various PeopleSoft components. This table allows a fine level of granularity when selecting which pages and components are AXF-enabled.

Events are invoked automatically when an action is performed on a PeopleSoft page. The AXF_PS_Integration project component catches PRE- and POST- save events and makes them available for customization. You can decide which events to use and how and when to use them.

A.3.1.1 Column Description

Table A–22 Column Description for PS_AXF_CONFIG Table

Column	Description
AXF_CONFIG_ID	Specifies the primary key of the table.
AXF_COMPONENT_NAME	Specifies the name of the PeopleSoft component being enabled.
AXF_CONNECT_NAME	Specifies the PeopleSoft Integration Broker Connection name (service operation to call), as defined in the PeopleSoft Integration Broker administration interface. The default service operation is AXF_EXECUTE. You can set up and use other connections.
AXF_VERSION	Specifies the AXF version of the connection. This value should be set to `10g`.

A.3.1.2 Example Implementation

This example defines that the WM_WO (work order) component is AXF-enabled.

Table A–23 Example PS_AXF_CONFIG Table

AXF_CONFIG_ID	AXF_COMPONENT_NAME	AXF_CONNECT_NAME	AXF_VERSION
1	WM_WO	AXF_EXECUTE	10g

A.3.2 PS_AXF_COMMANDS Table (PeopleSoft)

Use the PS_AXF_COMMANDS table to describe the actions to be taken based on user activity. This table works in conjunction with the PS_AXF_CONFIG Table (PeopleSoft).

A.3.2.1 Column Description

Table A–24 Column Description for PS_AXF_COMMANDS Table

Column	Description
AXF_CMDS_ID	Specifies the primary key of the table, used to identify the unique command.
AXF_CONFIG_ID	Specifies the foreign key to the PS_AXF_CONFIG Table (PeopleSoft), which associates this unique command with a particular page and component.
AXF_EVENT_NAME	Specifies the event being executed. The AXF_EVENT_NAME corresponds to the subpage incorporated into an existing PeopleSoft page, such as a button, link, or menu added to a PeopleSoft page to invoke AXF functionality such as the Image Viewer or Task List. Available options include: ▪ AXF_BUTTON_1, …, AXF_BUTTON_5 ▪ AXF_LINK_1, ..., AXF_LINK5 ▪ AXF_COMBO_1, ..., AXF_COMBO_5 ▪ AXF_PRE_SAVE_SBP ▪ AXF_POST_SAVE_SBP
AXF_SELECT_LABEL	Represents the label that for display if using a drop-down component (for example, AXF_COMBO_1).

Table A–24 (Cont.) Column Description for PS_AXF_COMMANDS Table

Column	Description
AXF_DISPLAY_NAME	Defines the name of the button or link to display on the PeopleSoft screen.
AXF_SOL_NAMESPC	Identifies the solution namespace for the command to execute.
AXF_CMD_NAMESPC	Identifies the command namespace for the command to execute.
AXF_PSFT_ROLE	Identifies the PeopleSoft roles with access to the command. Include roles in a comma-delimited list with each role enclosed in single quotes (for example, 'Role1','Role2','Role3')
AXF_SORT_ORDER	Specifies the order of items displayed in a selection field. Sort order applies to selection fields only.
AXF_REQ_CONV	Specifies if a conversation is required for this command before execution. For example, execution of the UpdateTask command requires a conversation to be running in order for the user to select a current task.

A.3.2.2 Example Implementation

This example shows the UCM_Managed_Attachments command added as a link to a PeopleSoft page.

You must specify a PeopleSoft Role in the AXF_PSFT_ROLE field in order to give permissions to use the commands. If a person does not have proper permissions to use the commands, the commands are not displayed. If the commands are displayed but not functioning, this indicates that the commands are not configured properly.

Table A–25 Example PS_AXF_COMMANDS Table

AXF_ CMDS_ ID	AXF_ CONFIG_ ID	AXF_ EVENT_ NAME	AXF_ SELECT_ LABEL	AXF_ DISPLAY_ NAME	AXF_SOL_ NAMESPC	AXF_CMD_ NAMESPC	AXF_PSFT_ ROLE	AXF_ SORT_ ORDER	AXF_ REQ_ CONV
2	1	AXF_LINK_1	(null)	Managed Attachments	UCM_ Managed_ Attachments	UCM_ Managed_ Attachments	'Employee'	1	N

A.3.3 PS_AXF_CMD_PARAMS Table (PeopleSoft)

Use the PS_AXF_COMMAND_PARAMS table to specify the information sent for each defined command. Each command may require or omit a different set of parameters.

A.3.3.1 Column Description

Table A–26 Column Description for PS_AXF_CMD_PARAMS Table

Column	Description
AXF_CMD_PARAM_ID	Specifies the primary key of the table.
AXF_CMD_ID	Specifies the foreign key to the PS_AXF_COMMANDS Table (PeopleSoft), which associates the unique parameter with a specific command.

Table A–26 (Cont.) Column Description for PS_AXF_CMD_PARAMS Table

Column	Description
AXF_PARAM_NAME	Defines the parameter name, where: ■ Application: Specifies the business application, as defined in "AFObjects Table" on page A-17. ■ businessObjectType: Specifies the business application's object type, as defined in "AFObjects Table" on page A-17. ■ businessObjectKey1...5: Represents the primary key name for the document. ■ businessObjectValue1...5: Represents the primary key value for the document. ■ labelValue1...5: Labels displayed on Managed Attachments user interface for displaying key values for the attachments integration.
AXF_DATASOURCE	Specifies where the parameter value is retrieved. ■ DATA: Retrieves the value in PeopleSoft defined by the AXF_RECORD_NAME and AXF_FIELD_NAME fields. ■ CONSTANT: Uses the value defined in the AXF_ CONSTANT_VALUE field.
AXF_RECORD_NAME	Identifies the record of the field in the PeopleSoft page to use as the target value to retrieve when AXF_DATASOURCE is set to DATA.
AXF_FIELD_NAME	Used as the constant value when AXF_DATASOURCE is set to DATA.
AXF_CONSTANT_VALUE	Used as the constant value when AXF_DATASOURCE is set to CONSTANT.

A.3.3.2 Example Implementation

This example shows the information sent for the UCM_Managed_Attachments command, including its application and business object type. The labelValue entries are configured to display key labels/values for the attachment. For example, the labelValues configuration in this table might display the following on the Managed Attachments screen:

[Business Unit], [US001], [Work Order], [123456]

Table A–27 Example PS_AXF_CMD_PARAMS Table

AXF_CMD_ PARAM_ID	AXF_ CMD_ID	AXF_PARAM_NAME	AXF_ DATASOURCE	AXF_RECORD_ NAME	AXF_FIELD_ NAME	AXF_CONSTANT_ VALUE
3	2	application	CONSTANT			PSFT_INSTANCE_A
4	2	businessObjectType	CONSTANT			WM_WO_HDR
5	2	businessObjectKey1	CONSTANT			BUSINESS_UNIT
6	2	businessObjectValue1	DATA	WM_WO_HDR	BUSINESS_UNIT	
7	2	businessObjectKey2	CONSTANT			WO_ID
8	2	businessObjectValue2	DATA	WM_WO_HDR	WO_ID	
9	2	labelValue1	CONSTANT			Business Unit
10	2	labelValue2	DATA	WM_WO_HDR	BUSINESS_UNIT	
11	2	labelValue3	CONSTANT			Work Order
12	2	labelValue4	DATA	WM_WO_HDR	WO_ID	

A.4 Content Server Tables

The adapter utilizes the following additional database tables:

- "AFGrants Table" on page A-17
- "AFObjects Table" on page A-17
- "AFRelationshipAttributes Table" on page A-18
- "AFKeys Table" on page A-18

These tables are automatically populated at runtime. AFGrants is initially populated when the user accesses Oracle UCM from the business application and the AF_GRANT_ACCESS service is run. AFObjects is populated when the user checks in a document to Oracle UCM from the Managed Attachments screen.

A.4.1 AFGrants Table

This table stores the grants given to users, allowing them to temporarily access documents associated with a particular business object.

A.4.1.1 Column Description

Table A–28 Column Description for AFGrants Table

Columns	Description
dUserName	Stores the name of the user.
dAFApplication	Stores the business application’s instance name (for example, PSFT_Instance1).
dAFBusinessObject	Stores the business application’s object
dAFBusinessObjectType	Stores the business application’s object type
dPrivilege	Stores the privilege to grant to the user: R (read), W (write), D (delete), or A (admin). This parameter is optional. If not specified, the access level specified for the AppAdapterGrantPrivilege configuration variable is used, as described in "Configuring the Preferences.hda File" on page 2-26.
dExpirationDate	Stores the date and time at which to expire this grant.
dMaxExpiration	Stores the time at which the maximum access period (in hours) expires.

A.4.2 AFObjects Table

This table maps Content Server documents to AF business objects, in an N-to-N relationship, which allows multiple content items to be associated with a single business object and multiple business objects to contain the same content item.

Each time a user attaches or detaches a document, a record is added or updated in this table.

A.4.2.1 Column Description

Table A–29 Column Description for AFObjects Table

Column	Description
dAFID	Stores the unique ID of each attachment.
dAFApplication	Stores the business application's instance name (for example, PSFT_Instance or EBS_Instance).
dAFBusinessObjectType	Stores the business application's object type (for example, CallRecords or HRMS).
dAFBusinessObject	Stores the business object's ID in the business application instance.
dDocName	Stores a content item's ID associated with the business object.
DID	Stores the ID of the document associated with the business entity. In revision-specific attachments mode, this ID is used in returning a specific version of the document. For more information, see "Configuring Revision-Specific Mode" on page 2-48.

A.4.3 AFRelationshipAttributes Table

This table stores relationship attributes associated with an attachment. For more information, see "Configuring Relationship Attributes" on page 2-47. Depending on the configuration of relationship attributes, a document can have zero or more relationship attributes.

A.4.3.1 Column Description

Table A–30 Column Description for AFRelationshipAttributes Table

Columns	Description
dAFID	Stores the unique ID of each attachment.
attribute	Stores the relationship attribute name.
value	Stores the value of the relationship attribute the user selected.

A.4.4 AFKeys Table

This table stores individual key values for later reference.

The business applications support up to five primary key/value combinations, which can be used instead of dAFBusinessObject to represent a business entity. In a Managed Attachments solution, these keys are mapped to dAFBusinessObject by concatenating the PK_Value fields separated by a | (pipe) character. The original PK_Key and PK_Values are logged to the AFKeys table before performing the mapping operation.

A.4.4.1 Column Description

Table A–31 Column Description for AFKeys Table

Columns	Description
dAFApplication	Stores the business application's instance name.
dAFBusinessObjectType	Stores the business application's object type.

Table A–31 (Cont.) Column Description for AFKeys Table

Columns	Description
dAFBusinessObject	Stores the business object's ID in the business application instance.
PK1_Key ... PK5_Key	Stores up to five key/value combinations.
PK1_Value ... PK5_Value	Stores up to five key/value combinations.

Index

A

L

M

N

O

P

R

S