

IBM Content
Manager for Multiplatforms/IBM Information
Integrator for Content



Installing, Configuring, and Managing the eClient

Version 8 Release 2

IBM Content
Manager for Multiplatforms/IBM Information
Integrator for Content



Installing, Configuring, and Managing the eClient

Version 8 Release 2

Contents

Chapter 1. Overview	1	Starting the eClient on WebSphere 5	87
Third-party application integration overview	2	Stopping the eClient	88
PeopleSoft Integration for IBM Content Manager overview	2	Stopping the eClient on WebSphere 4.	88
Siebel Integration for IBM Content Manager overview	2	Stopping the eClient on WebSphere 5.	88
Documentation conventions	3		
Chapter 2. Requirements	5	Chapter 6. Customizing your eClient application	89
eClient requirements.	5	eClient JavaServer Pages	89
Hardware	5	Customizing eClient graphics	92
Software.	6	Customizing eClient help.	94
Network.	7	Customizing the viewer applet	94
Skill	7		
Information to collect	7		
Third-party application integration requirements	9	 	
PeopleSoft Integration for IBM Content Manager requirements	9	Chapter 7. Managing your eClient application	95
Siebel Integration for IBM Content Manager requirements	10	Setting and changing your configuration parameters	95
		Setting the caching directory.	95
		Setting the maximum number of search results displayed on a page	95
		Setting the maximum number off search results returned from the content server	95
		Setting the maximum file size allowed during import	96
		Setting the property daemon	96
		Setting the EIP INI files	96
		Setting the connection type	96
		Setting the Content Manager Version 8 connector	96
		Enabling launching content files	97
		Setting the e-mail properties.	97
		Enabling EIP advanced workflow	97
		Setting the service connection type	97
		Enabling the viewer applet	97
		Enabling federated folders	98
		Defining how the eClient handles content types	98
		Content types	98
		Configuring parameters for a customized client	99
		Defining server connections	100
		Defining an OnDemand server connection.	100
		Defining an ImagePlus for OS/390 server connection	101
		Chapter 8. Troubleshooting	103
		Troubleshooting the eClient	103
		Troubleshooting scenarios	103
		Configuration problems	109
		Trace information	111
		Miscellaneous tips	111
		Tip 1: Updating annotations	112
		Tip 2: Setting WebSphere in the correct state	112
		Tip 3: DB2 Version 8 Support	112
		Troubleshooting third-party application integration	112
		Troubleshooting PeopleSoft Integration for IBM Content Manager	112
		Troubleshooting Siebel Integration for IBM Content Manager	117
Chapter 3. Installing	13		
Installing the eClient	13		
Installing the eClient on a Windows application server	13		
Installing the eClient on an AIX or Solaris server	14		
Installing third-party application integration	15		
Installing PeopleSoft Integration for IBM Content Manager	15		
Installing Siebel Integration for IBM Content Manager	16		
Chapter 4. Configuring	19		
Configuring the eClient	19		
Configuring the eClient to use IBM WebSphere 5 Java 2 Security	19		
Configuring the eClient with WebSphere Application Server	19		
Configuring to use IBM WebSphere 4 connection pooling with the eClient	23		
Configuring to use IBM WebSphere 5 connection pooling with the eClient	27		
Selecting eClient languages	28		
Verifying the eClient installation and configuration	29		
Configuring third-party application integration	31		
Configuring PeopleSoft Integration for IBM Content Manager	31		
Configuring Siebel Integration for IBM Content Manager	53		
Chapter 5. Starting and stopping the eClient.	87		
Starting the eClient.	87		
Starting the eClient on WebSphere 4	87		

Chapter 9. Removing	121	Chapter 11. Sample properties files	127
Removing the eClient	121	A sample IDMdefault.properties file	127
Removing third-party application integration.	122	A sample IP file used by Siebel Integration	136
Removing PeopleSoft Integration for IBM		Chapter 12. Accessibility information	139
Content Manager	122	Index	141
Removing Siebel Integration for IBM Content		Notices	149
Manager	122	Trademarks	151
 Chapter 10. Getting more information	123		
eClient	123		
Third-party business applications and integration	123		
Getting more information about PeopleSoft			
Integration for IBM Content Manager	123		
Getting more information about Siebel			
Integration for IBM Content Manager	124		

Chapter 1. Overview

The IBM® Content Manager eClient is a Web application that enables your users to search for and retrieve documents from content servers. The content servers that the eClient can access include:

- IBM Content Manager for Multiplatforms
- IBM Content Manager OnDemand
- IBM Content Manager ImagePlus® for OS/390®
- Other content servers

With the eClient, you can connect to Enterprise Information Portal (EIP) and perform searches across a variety of data sources simultaneously. You can also use the eClient to connect directly to content servers. The eClient supports Enterprise Information Portal Version 8.2 workflow and Content Manager Version 8.2 document routing.

The eClient Web application consists of JavaServer Pages (JSP), servlets, and a viewer applet that run on WebSphere® Application Server. You can customize the eClient to meet the needs of your organization.

This document is written primarily for Web administrators who use WebSphere Application Server or have knowledge of Java™ 2 Platform, Enterprise Edition (J2EE) application servers, and who are familiar with Enterprise Information Portal.

Recommendation: Thoroughly review Chapter 2, “Requirements”, on page 5 before you proceed.

Related Reference:

- Chapter 10, “Getting more information”, on page 123
- “Hardware” on page 5
- “Information to collect” on page 7
- “Network” on page 7
- “Skill” on page 7
- “Software” on page 6

Related Tasks:

- Chapter 3, “Installing”, on page 13
- Chapter 4, “Configuring”, on page 19
- Chapter 5, “Starting and stopping the eClient”, on page 87
- Chapter 7, “Managing your eClient application”, on page 95
- Chapter 6, “Customizing your eClient application”, on page 89
- Chapter 8, “Troubleshooting”, on page 103
- Chapter 9, “Removing”, on page 121

Third-party application integration overview

IBM Content Manager eClient Version 8.2 provides integration with the following third-party business applications:

- PeopleSoft Enterprise Portal Version 8.40
- Siebel 7.0.4 and 7.5.2

With the integration, end-users of these third-party business applications can access documents from a variety of content servers.

PeopleSoft Integration for IBM Content Manager overview

PeopleSoft customers need a way to access and manage data in Content Manager from the PeopleSoft portal. PeopleSoft Integration for IBM Content Manager allows PeopleSoft users to move from one product to the other. For example, users no longer have to treat the products separately by going through two login processes.

If you use PeopleSoft with IBM Content Manager system and want to provide a seamless connection from PeopleSoft Enterprise Portal Version 8.40 to Content Manager Version 8.2, then you must have installed:

- Content Manager Version 8.2
- Enterprise Information Portal Version 8.2
- eClient 8.2
- PeopleSoft Enterprise Portal 8.40
- PeopleTools 8.40.09

Recommendation: Review the requirements for these products before proceeding.

Related reference:

“Getting more information about PeopleSoft Integration for IBM Content Manager” on page 123

“Hardware” on page 9

“Network” on page 10

“Skill” on page 10

“Software” on page 9

Related tasks:

“Installing PeopleSoft Integration for IBM Content Manager” on page 15

“Configuring PeopleSoft and the eClient to work together” on page 31

“Troubleshooting PeopleSoft Integration for IBM Content Manager” on page 112

“Removing PeopleSoft Integration for IBM Content Manager” on page 122

Siebel Integration for IBM Content Manager overview

Siebel Integration for IBM Content Manager integrates the capabilities of the IBM Content Manager portfolio of products with those of Siebel eBusiness applications. It accomplishes this goal by utilizing IBM Enterprise Information Portal (EIP) and the IBM Content Manager eClient.

With Siebel Integration for IBM Content Manager, a Siebel end user is able to:

- Search for and retrieve documents that are associated with a Siebel entity (for example, a service request). The documents may be stored in content servers managed by any of the following products:

- Content Manager Version 7.1
- Content Manager Version 8.1
- Content Manager Version 8.2
- Content Manager OnDemand for Multiplatforms Version 7.1
- Content Manager OnDemand for OS/390 Version 2.1, Version 7.1
- Content Manager OnDemand for iSeries™ Version 4.5, Version 5.1
- Content Manager ImagePlus for OS/390 Version 3.1
- Use an eClient viewer to view individual documents.
- While viewing a document, toggle on and off document annotations that were previously created; zoom in and out; rotate the current page; and print the document if the system is configured to enable the print function.

Siebel Integration for IBM Content Manager is available on Windows®, AIX®, and Sun Solaris Operating Environment (hereafter referred to as Solaris).

Recommendation: Review the requirements for these products before proceeding.

Related reference:

“Getting more information about Siebel Integration for IBM Content Manager” on page 124

“Configuring WebSphere Application Server to run the eClient” on page 54

“Network” on page 12

“Skill” on page 12

“Software” on page 11

Related tasks:

“Installing Siebel Integration for IBM Content Manager on Windows, AIX, or Solaris” on page 16

“Configuring WebSphere Application Server to run the eClient” on page 54

“Troubleshooting Scenarios” on page 117

Documentation conventions

Windows-based operating systems use back slashes (\) to delimit directories in a directory path. UNIX®-based operating systems, including AIX, use forward slashes (/). In this information, back slashes (\) are used to delimit directories in directory paths that apply to all operating systems; depending on your operating system, you might need to enter these directory paths differently than shown in the information.

Chapter 2. Requirements

This section provides information about the hardware, software, network, skill, and information requirements for the eClient and third-party application integration.

Related reference:

“eClient requirements”

“Third-party application integration requirements” on page 9

eClient requirements

This section covers information about the hardware, software, network, and skill that are required to install, configure, and manage the eClient. It also discusses the information that you should collect depending on your content server before installing the eClient.

Related reference:

“Hardware”

“Software” on page 6

“Network” on page 7

“Skill” on page 7

“Information to collect” on page 7

Hardware

Server

Follow the requirements for IBM WebSphere Application Server. The eClient requires 25 MB of additional disk space.

Client

You need the hardware that is required to support a browser with support for frames and JavaScript™, for example, Netscape Navigator 4.76 or Microsoft® Internet Explorer 5.5 Service Pack 2 or later.

Related Reference:

Chapter 10, “Getting more information”, on page 123

“Software” on page 6

Software

Table 1. Minimum software requirements for the eClient

System	Software requirements
Application server and Web server	<ul style="list-style-type: none">• One of the following IBM WebSphere Application Server products:<ul style="list-style-type: none">– IBM WebSphere Application Server 4.0.5 AE– IBM WebSphere Application Server 4.0.5 AES– IBM WebSphere Application Server 5– IBM WebSphere Application Server Network Deployment 5• Web server (IBM HTTP Server is included with WebSphere Application Server.)
IBM Enterprise Information Portal	IBM Enterprise Information Portal Version 8.2 and its minimum software requirements Tip: If you want to install the VisualInfo for AS/400 connector, select Version 4.3 or Version 5.1 of the connector.
End-user client	Browser with support for frame and JavaScript (Netscape Navigator 4.76 or higher or Microsoft Internet Explorer 5.5 Service Pack 2 or later). Other versions of browsers might be supported. Java Run-time Environment 1.4.1

Browser Restriction:

- The eClient does not support Netscape Navigator 6.x or 7.x browsers.
- Unpredictable results might occur if you use multiple Netscape browsers to access the eClient simultaneously.
- You might need to refresh a Netscape browser to view the eClient installation documentation correctly.

Java 2 Runtime Environment (JRE) Tips:

- When downloading JRE from the Web Site <http://java.sun.com/j2se/1.4>, download the "Windows (all languages, including English)" version. If you download the "Windows (U.S. English only)" version and set the OS Regional Language to another language on Windows 2000, your browser closes all open windows when you try to view an item using the viewer applet. In this case, your browser does not return an error message.

WebSphere Tips:

- In the WebSphere administrative console GUI for AE, after you update any environment or JVM setting and click **Apply**, check if the environment settings that the eClient set when it was installed are still restored after you made the change.
- If you use WebSphere Application Server Advanced Single Server Edition (AES) and install a resource manager and the eClient on the same machine, both applications use a commonly generated XML file, `IDM_ICM.xml`. This file is different from the default XML file, `server-cfg.xml`, which is provided by

WebSphere AES. For any custom applications to be used along with the eClient and the resource manager on the single server node, these applications need to be deployed on the IDM_ICM.xml file. You can start or stop the ICM_Server using the scripts provided in the save directory of CMeClient.

Related Reference:

Chapter 10, “Getting more information”, on page 123
 “Hardware” on page 5

Network

Servers require that you use TCP/IP. Usually, your operating system automatically installs the necessary TCP/IP software. If you do not have TCP/IP on your system, see your operating system information for instructions about how to install the software.

Related Reference:

“Software” on page 6
 “Information to collect”

Skill

This document assumes that you know how to install and configure:

- Your Content Manager portfolio product
- Enterprise Information Portal Version 8.2
- Databases (primarily IBM DB2 Universal Database)

You should also know how to install and manage:

- WebSphere Application Server
- Web applications on WebSphere Application Server

Related Reference:

“Network”
 “Information to collect”

Information to collect

Before installing the eClient, collect the following information based on the content server that you are connecting to:

Table 2. Information to collect

If you plan to connect to	You must provide this information
Content Manager Version 8 server	<ul style="list-style-type: none"> • server type • location of the directory where the cmbicmsvrs.ini file can be found <p>Note: cmbicmsvrs.ini contains the Content Manager Version 8 server names.</p>
Content Manager OnDemand server	<ul style="list-style-type: none"> • host name • port number • alias name

Table 2. Information to collect (continued)

If you plan to connect to	You must provide this information
ImagePlus for OS/390 server	<p><i>Alias name</i> An alternate name for the server; this is the name that appears in the list of servers your users see. Use a name that is familiar to your users. The alias name can contain blanks or special characters, but it cannot contain a colon.</p> <p><i>Application ID</i> The identifier for the Folder Application Facility.</p> <p><i>FAF IP address</i> The IP address for the Folder Application Facility.</p> <p><i>FAF Port</i> The TCP/IP port for the Folder Application Facility.</p> <p><i>FAF Protocol</i> The communication protocol of the Folder Application Facility Host.</p> <p><i>FAF Symbolic ID</i> The 4-character identifier for the Folder Application Facility that owns and catalogs the documents associated with this datastore. This parameter is required for locking, adding, updating, or deleting annotations, and for locking folders and documents.</p> <p><i>ODM IP address</i> The IP address of the Object Distribution Manager.</p> <p><i>ODM Port</i> The port number for the Object Distribution Manager.</p> <p><i>ODM Terminal ID</i> The terminal identifier for the object distribution manager; if not specified the user ID is used.</p> <p><i>ODM Collection class</i> The collection class where all form overlays are stored. If not specified, forms are searched for in the collection class where the last document was retrieved.</p> <p><i>ODM Protocol</i> The communication protocol of the object distribution manager host.</p> <p><i>ODM Storage Location Control</i> The document storage location control. You can set this to DASD to retrieve documents from DASD only, OPTICAL to retrieve documents from DASD or OPTICAL only, or SHELF to retrieve documents from DASD, OPTICAL, or SHELF.</p>
Content Manager Version server or earlier	Verify that the <code>frnolint.tbl</code> file lists the server correctly.

Related Reference:
“Skill” on page 7

Third-party application integration requirements

This section covers information about the hardware, software, network, and skill that are required to install and configure third-party application integration.

Related reference:

“PeopleSoft Integration for IBM Content Manager requirements”

“Siebel Integration for IBM Content Manager requirements” on page 10

PeopleSoft Integration for IBM Content Manager requirements

This section covers information about hardware, software, network, and skill requirements.

Hardware

This product is installed with Content Manager eClient. If you meet the requirements for the Content Manager eClient, then you meet the hardware requirements for this product. If you have problems meeting the hardware requirements, see the Content Manager and PeopleSoft documentation, or you can go to the technical support web sites for Content Manager at www.ibm.com/support/us/ and for PeopleSoft at www.peoplesoft.com/corp/en/support/index.asp.

Related reference:

“Getting more information about PeopleSoft Integration for IBM Content Manager” on page 123

“Software”

Software

Integration with the Content Manager products requires that the minimum software be installed. Table 3 contains a list of required products, operating systems, and browsers required for implementing PeopleSoft associations (both loose and optimized) with eClient.

Table 3. Minimum software requirements for implementing PeopleSoft associations with IBM Content Manager eClient.

System	Minimum software requirements
IBM Content Manager products	All of the following products: <ul style="list-style-type: none">• IBM Content Manager Version 8.2• IBM Enterprise Information Portal Version 8.2• IBM Content Manager eClient Version 8.2
IBM Content Manager eClient operating systems and browsers	One of the following operating systems and browser combinations: <ul style="list-style-type: none">• Windows 98, Windows 2000, and Windows NT running:<ul style="list-style-type: none">– Microsoft Internet Explorer 5.5– Microsoft Internet Explorer 6.0– Netscape Navigator 4.7x– Netscape Navigator 6.2x• Windows XP running:<ul style="list-style-type: none">– Microsoft Internet Explorer 6.0– Netscape Navigator 6.2x• AIX running Netscape Navigator 4.7• Macintosh running Microsoft Internet Explorer 5.0

Table 3. Minimum software requirements for implementing PeopleSoft associations with IBM Content Manager eClient. (continued)

System	Minimum software requirements
PeopleSoft system	<ul style="list-style-type: none"> • PeopleSoft Enterprise Portal 8.4 or higher • PeopleTools 8.40.09 <p>See <i>PeopleTools 8.4 Hardware and Software Requirements</i> for other hardware and software requirements. Technical support is available at: www.peoplesoft.com/corp/en/support/index.asp</p>

Related reference:

“Hardware” on page 9

“Getting more information about PeopleSoft Integration for IBM Content Manager” on page 123

Network

Servers require that you use TCP/IP. Usually, your operating system automatically installs the necessary TCP/IP software. If you do not have TCP/IP on your system, see your operating system information for instructions about how to install the software.

Related reference:

“Hardware” on page 9

“Software” on page 9

Skill

This document assumes that you know how to configure:

- Databases (primarily DB2 Universal Database)
- Content Manager Version 8.2
- Enterprise Information Portal Version 8.2
- Content Manager eClient Version 8.2
- PeopleSoft Enterprise Portal Version 8.4 (or higher) with PeopleTools 8.40.09 or PeopleTools 8.41.07

You should know how to install and manage:

- An application server
- Web applications on an application server

You should also have sufficient knowledge to develop iScript pagelets and configure the PeopleSoft portal.

Siebel Integration for IBM Content Manager requirements

This section covers information about Siebel Integration for IBM Content Manager hardware, software, network, and skill requirements.

Hardware

Hardware requirements are listed in the WebSphere, Content Manager, and Siebel documentation. This product is installed with the Content Manager eClient. If you meet the requirements for the Content Manager eClient, you meet the hardware requirements for this product. If you have problems meeting the hardware requirements, see the Content Manager and Siebel documentation, or you can go

to the technical support Web sites for Content Manager at www.ibm.com/support/us/ and for Siebel at <http://ebusiness.siebel.com/supportweb>.

Related reference:

“Getting more information about Siebel Integration for IBM Content Manager” on page 124
 “Software”

Software

Table 4 lists the minimum software requirements for Siebel Integration for IBM Content Manager.

Table 4. Minimum software requirements

System	Software requirements
IBM Content Manager content servers	Minimum software required to install one of the following Content Manager servers: <ul style="list-style-type: none"> • IBM Content Manager for Multiplatforms Version 7.1 • IBM Content Manager for Multiplatforms Version 8.1 • IBM Content Manager for Multiplatforms Version 8.2 • IBM Content Manager OnDemand for Multiplatforms Version 7.1 • IBM Content Manager OnDemand for OS/390 Version 2.1 • IBM Content Manager OnDemand for OS/390 Version 7.1 • IBM Content Manager OnDemand for iSeries Version 4.5 • IBM Content Manager OnDemand for iSeries Version 5.1 • IBM Content Manager ImagePlus for OS/390 Version 3.1
IBM Enterprise Information Portal	IBM Enterprise Information Portal Version 8.2 IBM Content Manager eClient Version 8.2
End-user client	<p>For Siebel 7.0.4, use one of the following operating systems:</p> <ul style="list-style-type: none"> • Windows 95 OSR2 • Windows 98 SE • Windows NT® Workstation 4.0 with Service Pack 6a • Windows 2000 with Service Pack 2 • Windows XP Professional <p>For Siebel 7.5.2, use one of the following operating systems:</p> <ul style="list-style-type: none"> • Windows NT Workstation 4.0 with Service Pack 6a • Windows 2000 Professional with Service Pack 2 • Windows XP Professional <p>One of the following browsers:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 5.5 Service Pack 2 or later • Microsoft Internet Explorer 6.0 <p>Restriction:</p> <ul style="list-style-type: none"> • Microsoft Internet Explorer 6.0 must be used with Microsoft Windows XP Professional. • Microsoft Internet Explorer 5.5 must be used with Microsoft Windows 95.

Table 4. Minimum software requirements (continued)

System	Software requirements
Siebel System	For Siebel 7.0.4, see <i>Siebel System Requirements and Supported Platforms, Siebel 7, Version 7.0.4</i> at http://ebusiness.siebel.com/supportweb for information on software requirements. For Siebel 7.5.2, see <i>Siebel System Requirements and Supported Platforms, Siebel 7, Version 7.5.2</i> at http://ebusiness.siebel.com/supportweb for information on software requirements.

Related reference:

“Getting more information about Siebel Integration for IBM Content Manager” on page 124

“Hardware” on page 10

Network

Servers require that you use TCP/IP. Usually, your operating system automatically installs the necessary TCP/IP software. If you do not have TCP/IP on your system, see your operating system information for instructions about how to install the software.

Related reference:

“Hardware” on page 10

“Software” on page 11

Skill

This document assumes that you know how to install and configure:

- Your Content Manager portfolio product
- Enterprise Information Portal Version 8.2
- Content Manager eClient Version 8.2
- Siebel 7.0.4 or Siebel 7.5.2
- Databases (primarily IBM DB2 Universal Database™)

You should know how to install and manage:

- WebSphere Application Server
- Web applications on WebSphere Application Server

Chapter 3. Installing

This section provides information on how to install the eClient and third-party application integration.

Related tasks:

“Installing the eClient”

“Installing third-party application integration” on page 15

Installing the eClient

This section provides instructions on installing the eClient on Windows, AIX, and Solaris.

Note: If you are reinstalling the eClient, you must remove it before reinstalling.

Related Tasks:

Chapter 4, “Configuring”, on page 19

“Configuring the eClient with WebSphere Application Server” on page 19

Installing the eClient on a Windows application server

Prerequisites:

1. If you are using WebSphere Application Server (WAS) AES, stop any server that is already running on WAS. For example, if the default server is running, run `stopServer.bat` located in the `/bin` subdirectory of WebSphere. If you do not stop, then restart the IBM HTTP server, the eClient Web application cannot be installed correctly.
2. If you are using WebSphere Application Server AE, make sure that the WebSphere Application Server administration server (AE) is running before starting the eClient installation.
3. If you are using WebSphere Application Server 5, the application server server 1 must be started. To start server 1, select **Start -> Programs -> IBM WebSphere -> Application Server v5.0 -> Start the Server.**

Procedure:

To install the eClient on your Windows application server:

1. Insert the eClient CD into the CD drive. The launchpad starts automatically. If the launchpad does not start automatically, execute `launchpad.bat` from the launchpad directory.
2. In the launchpad, click **Install** to start the eClient installation program.
3. Follow the instructions in the installation windows. The default directory for the eClient is `C:\Program Files\IBM\CMeClient`. If you are connecting to Content Manager Version 8, the default local file location of the data server list file is:
`C:\Program Files\IBM\CMgmt\cmbicmsrvs.ini`
4. After you install the eClient files, the installation program checks for WebSphere. If the installation program detects WebSphere, you can continue with the automatic configuration of the Web application for the eClient. You

can choose to exit without automatically configuring the application with WebSphere. If you choose to exit, the installation program ends, and you need to manually deploy the eClient on your Web application server.

5. **Optional:** If you choose not to perform the automatic configuration, set up and configure the eClient as a Web application.

Related Tasks:

Chapter 4, “Configuring”, on page 19

“Configuring the eClient with WebSphere Application Server” on page 19

Installing the eClient on an AIX or Solaris server

Prerequisites:

If you are using WebSphere Application Server (WAS) AES, stop any server that is already running on WAS. However, if you are using WAS AE, make sure that the WebSphere Application Server administration server (AE) is running before starting the eClient installation.

If you are using WebSphere Application Server 5, make sure that you have started the application server. To start the application server:

1. Change to *WASROOT/bin* subdirectory, where *WASROOT* is the root directory where WebSphere is installed.
2. Execute
`./startServer.sh server1`

Procedure:

To install the eClient on your application server on AIX or Sun Solaris:

1. Insert the eClient CD into the CD drive.
2. **Optional:** If you are installing on AIX or Sun Solaris using an X window session (for example, Exceed), enter this command:

```
export DISPLAY=hostname:0.0
```

where *hostname* is the host name or IP address where you want to be able to view the install panels.

3. From the launchpad directory, enter this Java command to manually run the launchpad:

```
java com.ibm.cm.install1.launchpad.LaunchPad
```

Note: You must have root or sudo privileges to run the launchpad.

4. Follow the instructions in the installation windows. The default directory to install the eClient is */opt/CMClient*.
5. If you are connecting to Content Manager Version 8, the default local file location of the data server list file is */usr/lpp/cmb/cmgt/cmbicmsrvs.ini* on AIX and */opt/ibm/cmb/cmgt/cmbicmsrvs.ini* on Solaris.

After you install the eClient files, the installation program checks for WebSphere Application Server (WAS). If the installation program detects WAS, you can continue with the automatic configuration of the Web application for the eClient. You can choose to exit without automatically configuring the application with WebSphere.

6. **Optional:** If you choose not to perform the automatic configuration, you must set up and configure the eClient as a Web application.

Related Tasks:

“Installing the eClient on a Windows application server” on page 13

Chapter 4, “Configuring”, on page 19

“Configuring the eClient with WebSphere Application Server” on page 19

Installing third-party application integration

This section provides instructions on installing third-party application integration on Windows, AIX, and Solaris.

Related tasks:

“Installing PeopleSoft Integration for IBM Content Manager”

“Installing Siebel Integration for IBM Content Manager” on page 16

Installing PeopleSoft Integration for IBM Content Manager

This section outlines any installation procedures that you must complete before using PeopleSoft Integration for IBM Content Manager.

Installing PeopleSoft Integration for IBM Content Manager

PeopleSoft Integration for IBM Content Manager is automatically installed when you install the eClient and IBM Content Manager products. You need to configure the PeopleSoft portal and the eClient to work together.

Attention: If EIP is installed on a machine without sharing a Content Manager library server database, you need to install the ICMXLSLG.DLL file on the EIP system. Copy the following file from the Content Manager server to the EIP system:

ICMROOT\integration\peoplesoft\ICMXLSLG.DLL

If the EIP DLL directory does not exist, create that directory now, and then copy the ICMXLSLG.DLL file into it:

- For Windows EIP servers, copy this file to the Windows EIP DLL directory: *CMBROOT\database name\DLL*
- For UNIX EIP servers, copy this file to the UNIX EIP DLL directory: *PATHICMDLL\database name\DLL*

Where:

PATHICMDLL

path specified for the DLLs in the column PATHICMDLL in the ICMSTSYSCONTROL table

database name

name of the EIP database

Related tasks:

“Configuring PeopleSoft and the eClient to work together” on page 31

“Configuring PeopleSoft for a loose association with IBM Content Manager” on page 32

“Configuring for optimized association of PeopleSoft and IBM Content Manager” on page 32

Installing Siebel Integration for IBM Content Manager

This section outlines any installation procedures that you must complete before using Siebel Integration for IBM Content Manager and provides steps to upgrade from Version 7 to Version 8.

Installing Siebel Integration for IBM Content Manager on Windows, AIX, or Solaris

Siebel Integration for IBM Content Manager automatically installs when you install the IBM Content Manager eClient. The IBM Content Manager eClient installation software installs several servlets, JavaServer Pages (JSP), icons, one cascading style sheet, two Siebel Web templates, and a sample Integration Properties (IP) file required for the Siebel Integration for IBM Content Manager.

Two new Web templates (EIP81Applet.swt and EIP81Body.swt) are stored in the *ECLIENROOT*\integration\siebel directory (*ECLIENROOT*/integration/siebel directory for AIX and Solaris), where *ECLIENROOT* is the directory where the eClient is installed. You must copy them into each of the following three directories, where *SIEBELROOT* is the directory where Siebel is installed.

SIEBELROOT\siebsrvr\WEBTEMPL

SIEBELROOT\client\WEBTEMPL

SIEBELROOT\tools\WEBTEMPL

An Integration Properties file (hereafter referred to as IP file) specifies property values that configure your environment for integration with Siebel. A sample IP file named Siebel.properties is stored in the *ECLIENROOT* directory where *ECLIENROOT* is the directory where the eClient is installed. If needed, you can change the file name.

Related task:

“Configuring Siebel Integration for IBM Content Manager” on page 53

Upgrading from Siebel Integration for IBM Content Manager Version 7 to Version 8

You automatically upgrade from Siebel Integration for IBM Content Manager Version 7 to Version 8 when you upgrade from the eClient Version 7 to Version 8.

When configuring Siebel Integration for IBM Content Manager Version 7, you must specify values for the server, userid, and password properties in the IP file.

When configuring Siebel Integration for IBM Content Manager Version 8, you can specify the three properties in either the IP file, the URL, or both places. If you specify them in both the IP file and the URL, the values in the URL take precedence over the values in the IP file.

Two new Web templates (EIP81Applet.swt and EIP81Body.swt) are stored in the *ECLIENROOT*\integration\siebel directory (*ECLIENROOT*/integration/siebel directory for AIX and Solaris) where *ECLIENROOT* is the directory where the eClient is installed. You must:

1. Copy them into each of the following three directories, where *SIEBELROOT* is the directory where Siebel is installed.

SIEBELROOT\siebsrvr\WEBTEMPL

SIEBELROOT\client\WEBTEMPL

SIEBELROOT\tools\WEBTEMPL

2. Change the Siebel configuration to refer to the new files.

| 3. Re-compile the Siebel project.

| **Related reference:**

| "Upgrading from eClient Version 7.1 to eClient Version 8.1" in *Installing, Configuring, and Managing the eClient*.

| **Related task:**

| "Configuring Siebel Integration for IBM Content Manager" on page 53

Chapter 4. Configuring

Read this section for information about configuring the eClient and third-party application integration.

Related tasks:

- “Configuring the eClient”
- “Configuring third-party application integration” on page 31

Configuring the eClient

This section provides steps that you must complete to configure the eClient.

Related tasks:

- “Configuring the eClient to use IBM WebSphere 5 Java 2 Security”
- “Configuring the eClient with WebSphere Application Server”
- “Configuring to use IBM WebSphere 4 connection pooling with the eClient” on page 23
- “Configuring to use IBM WebSphere 5 connection pooling with the eClient” on page 27
- “Selecting eClient languages” on page 28

Configuring the eClient to use IBM WebSphere 5 Java 2 Security

If Java 2 Security is enabled for WebSphere Application Server, You must grant permission to Enterprise Information Portal to perform operations request by the eClient. To grant permission:

1. Use the Java policy tool to open `x:\WebSphere\appserver\config\cells\“cell name”\nodes\“node name”\app.policy`.
2. Give the EIP library directory `java.security.AllPermission`.

Below is an example of the permissions that should be added to the `app.policy` file:

```
grant codeBase "file:/c:/cmbroot/lib/-"{
permission java.security.AllPermission; };
```

There is also a sample `app.policy` file in the `CMeClient` directory.

Configuring the eClient with WebSphere Application Server

This section provides information on how to configure the eClient with WebSphere Application Server on Windows, AIX, and Solaris.

Configuring the eClient with WebSphere Application Server 4.0.5 AE or AES

To manually configure the eClient with WebSphere Application Server 4.0.5 AE or AES on Windows, follow these steps:

1. Open the `idmwas.bat` file located in the `\CMeClient\save` directory.
2. In the Java Virtual Machine (JVM) of the Web server, set the following token values for `CLASSPATH`:

```
CLASSPATH=$sqlpath$$dsep$java\db2java.zip;$proddest$;$cmcommon$;$eipath
$$dsep$lib$dsep$cmbfn81.jar;$eipath$$dsep$lib$dsep$cmbstdk81.jar;$eipath
$$dsep$lib$dsep$cmbview81.jar;$eipath$$dsep$lib$dsep$cmb81.jar;$eipath
$$dsep$lib$dsep$;$eipath$$dsep$lib$dsep$cmbstdk81.jar;$eipath$$dsep$lib
$dsep$xerces.jar;$eipath$$dsep$lib$dsep$cmblog4j81.jar;$eipath$$dsep
$lib$dsep$log4j.jar;$wasroot$$dsep$lib$dsep$j2ee.jar;$eipath$$dsep
$lib$dsep$cmbwas81.jar
```

Explanation of token values:

\$sqlpath\$

Path to the DB2 home directory

\$proddest\$

Path to the eClient home directory

\$cmcommon\$

Path to the location of the EIP INI files

\$eipath\$

Path to the EIP home directory

\$frnpath\$

Path to the folder manager API of EIP home directory

\$wasroot\$

Path to the WebSphere home directory or the home directory of the Web server that you use

\$dsep\$

The file separator based on operating system

3. In the JVM of the Web server, set the following token values for PATH:

```
PATH=$cmcommon$;$eipath$$dsep$;$eipath$$dsep$dll;$sqlpath$$dsep$bin;
$frnpath$$dsep$dllFRNADDRON=YES
```

To manually configure the eClient with WebSphere Application Server AE or AES on AIX, follow these steps:

1. Open the `idmwas.sh` file located in the `/opt/CMClient/Save` directory, where `/opt/CMClient` is the root directory where the eClient is installed.
2. In the Java Virtual Machine (JVM) of the Web server, set the following token values for CLASSPATH:

```
CLASSPATH=.:$proddest$:$cmcommon$:$eipath$/lib/cmbwas81.jar:
$wasroot$/lib/j2ee.jar:$eipath$/lib/cmb81.jar:$eipath$/lib/cmbcm81.jar:
$eipath$/lib/cmbdb281.jar:$eipath$/lib/cmbdb2c81.jar:$eipath$/lib
/cmbddc81.jar:$eipath$/lib/cmbdesc81.jar:$eipath$/lib/cmbdj81.jar:
$eipath$/lib/cmbdj81.jar:$eipath$/lib/cmbdl81.jar:$eipath$/lib/
cmbdlc81.jar:$eipath$/lib/cmbfed81.jar:$eipath$/lib/cmbfedc81.jar:
$eipath$/lib/cmbic81.jar:$eipath$/lib/cmbicc81.jar:$eipath$/lib/
cmbicm81.jar:$eipath$/lib/cmbicmup.jar:$eipath$/lib/cmbipc81.jar:
$eipath$/lib/cmbjdb81.jar:$eipath$/lib/cmbjdbcc81.jar:$eipath$/lib/
cmblog4j81.jar:$eipath$/lib/cmbod81.jar:$eipath$/lib/cmbodc81.jar:
$eipath$/lib/cmbv4c81.jar:$eipath$/lib/cmbview81.jar:$eipath$/lib/
esclisrv.jar:$eipath$/lib/essrv.jar:$eipath$/lib/jaas.jar:$eipath
$/lib/log4j.jar:$eipath$/lib/sguide.jar:$eipath$/lib/xerces.jar:
$eipath$/lib/cmbstdk81.jar:$eipath$/lib:$frnpath$/lib:$sqlpath$/
java12/db2java.zip:$sqlpath$/lib:$sqlpath$/java12:$CLASSPATH
```

Explanation of token values:

\$sqlpath\$

Path to the DB2 home directory

\$proddest\$

Path to the eClient home directory

\$cmcommon\$

Path to the location of the EIP INI files

\$eippath\$

Path to the EIP home directory

\$frnpath\$

Path to the folder manager API of EIP home directory

\$wasroot\$

Path to the WebSphere home directory or the home directory of the Web server that you use

\$dsep\$

The file separator based on operating system

3. In the JVM of the Web server, set the following token values for PATH:

```

PATH=.:$proddest:${WAS_ROOT}/java/sh:${WAS_ROOT}/java/jre/sh:$cmcommon
$: $eippath$/bin:$frnpath$/bin:$eippath$: $frnpath$: $frnpath$/lib:/lib:
/usr/lib:$PATH</entry>
FRNLEVEL=frn
FRNDEFLANG=ENU
FRNDBNAME=
FRNDBCFG=
FRNCOMP=CLIENT
FRNINST=$frnpath$
FRNSHARED=/var/frn
FRNHEAPSIZE=2048
FRNHEAPID=DAEMON
FRNCOMPID=ROOT
FRNLOCAL=$proddest$
FRNROOT=/usr/lpp/frn/bin
FRNLIB=/usr/lpp/frn/lib
CMBROOT=$cmcommon$
FRNADDRON=YES
LD_LIBRARY_PATH=.:/lib:/usr/lib:$eippath$/lib:$LD_LIBRARY_PATH
NLSPATH=/usr/lib/nls/msg/%L/%N:/usr/lib/nls/%L/%N.cat:${NLSPATH}:$eippath
$/msg/en_US/%N
LDR_CNTRL=MAXDATA=0x30000000

```

Note:

The LDR_CNTRL=MAXDATA setting can impact the performance and stability of your Java application on AIX. Set the value of this variable based on the heap size that you expect your application to acquire. You can find more details at: www.ibm.com/servers/esdd/articles/aix4java/index.html.

To manually configure the eClient with WebSphere Application Server AE or AES on Sun Solaris, follow these steps:

1. Open the idmwas.sh file located in the /opt/CMClient/Save directory, where /opt/CMClient is the root directory where the eClient is installed.
2. In the JVM of the Web server, set the following token values for CLASSPATH:

```

CLASSPATH=.:$proddest:$wasroot$/lib/j2ee.jar:$eippath$/lib/cmbwas81.jar:
$eippath$/lib/cmb81.jar:$eippath$/lib/cmbcm81.jar:$eippath$/lib/
cmbdb281.jar:$eippath$/lib/cmbdb2c81.jar:$eippath$/lib/cmbddc81.jar:
$eippath$/lib/cmbdesc81.jar:$eippath$/lib/cmbdj81.jar:$eippath$/lib/
cmbdjc81.jar:$eippath$/lib/cmbdl81.jar:$eippath$/lib/cmbdlc81.jar:
$eippath$/lib/cmbfed81.jar:$eippath$/lib/cmbfedc81.jar:$eippath$/lib/
cmbic81.jar:$eippath$/lib/cmbicc81.jar:$eippath$/lib/cmbicm81.jar:
$eippath$/lib/cmbicmup.jar:$eippath$/lib/cmbipc81.jar:$eippath$/lib/

```

```
cmbjdbc81.jar:$eippath$/lib/cmbjdbc81.jar:$eippath$/lib/cmblog4j81.jar:
$eippath$/lib/cmbod81.jar:$eippath$/lib/cmbodc81.jar:$eippath$/lib/
cmbv4c81.jar:$eippath$/lib/cmbview81.jar:$eippath$/lib/esclisrv.jar:
$eippath$/lib/essrv.jar:$eippath$/lib/jaas.jar:$eippath$/lib/log4j.jar:
$eippath$/lib/sguide.jar:$eippath$/lib/xerces.jar:$eippath$/lib/
cmbjdk81.jar:$eippath$/lib:$eippath$/cmgmt:$sqlpath$/java12/db2java.zip:
$sqlpath$/lib:$sqlpath$/java12:$CLASSPATH
```

Explanation of token values:

\$sqlpath\$

Path to the DB2 home directory

\$proddest\$

Path to the eClient home directory

\$cmcommon\$

Path to the location of the EIP INI files

\$eippath\$

Path to the EIP home directory

\$frnpath\$

Path to the folder manager API of EIP home directory

\$wasroot\$

Path to the WebSphere home directory or the home directory of the Web server that you use

\$dsep\$

The file separator based on operating system

3. In the JVM of the Web server, set the following token values for PATH:

```
PATH=.:$proddest$: $cmcommon$: $eippath$/bin: $eippath$/lib:/usr/lib:
${WAS_ROOT}/java/sh: ${WAS_ROOT}/java/jre/sh: $PATH
```

4. Set the following token values for LD_LIBRARY_PATH:

```
LD_LIBRARY_PATH=.:/lib:/usr/lib: $eippath$/lib: $LD_LIBRARY_PATH
```

5. Set the following token values for NLSPATH:

```
NLSPATH=/usr/lib/nls/msg/%L/%N:/usr/lib/nls/%L/%N.cat: $NLSPATH:
$eippath$/msg/en_US/%N
```

6. Set CMBROOT to \$cmcommon\$.

7. Set the following token values for LDR_CNTRL:

```
LDR_CNTRL=MAXDATA=0x30000000
```

Related tasks:

Chapter 3, “Installing”, on page 13

“Configuring to use IBM WebSphere 4 connection pooling with the eClient” on page 23

Related reference:

Single sign-on is supported on WebSphere Application Server AE for Content Manager Version 8 servers. For more information about configuring WebSphere Application Server for single sign-on, see the WebSphere documentation at: www.ibm.com/software/webservers/appserv/support.html.

Configuring the eClient with WebSphere Application Server 5

To manually configure the eClient with WebSphere Application Server 5 on Windows, follow these steps:

1. Open the Websphere Administrative Console.

2. Under Servers in the tree view of the WebSphere Administrative Console, select **Application Servers**.
3. Click **New** to add a new Application Server with name eClient_Server.
4. Under Applications, select **Enterprise Applications**.
5. Click **Install** to add the eClient Application:
 - a. Add the path to the eClient82.ear file and click **Next**.
 - b. Click **Next**.
 - c. Click **Next**.
 - d. Select eClient82 Web Module and Virtual Host default_host, then click **Next**.
 - e. Select eClient82 Module and the eClient_Server application server that was created for the eClient and click **Apply**.
 - f. Click **Next**.
 - g. Click **Next**.
 - h. Click **Finish**.
6. In the tree view of the WebSphere Administrative Console, under Servers, select **Application Servers**.
7. Select the eClient application server.
8. Click **Process Definition**.
9. Click **Java Virtual Machine**.
10. Add the classpath to the classpath property.
11. Click **Apply**.
12. Under the Environment folder in the WebSphere Administrative Console, Click **Update Web Server Plugin**.
13. Restart the HTTP server.
14. Start the eClient Application Server.

Configuring to use IBM WebSphere 4 connection pooling with the eClient

With the eClient, you can configure to use IBM WebSphere 4 connection pooling.

Prerequisite:

Before you configure to use IBM WebSphere 4 connection pooling with the eClient, you must update the cmbpool.ini file to enable WebSphere connection pooling.

The default location for this file is in %CMCOMMON%:

- C:\Program Files\ibm\CMgmt on Windows servers
- /opt/IBMcmb/cmgt on Solaris
- /usr/lpp/cmb/cmgt on AIX

In this file, set the keyword JavaPool to JavaPool=DKPoolWAS, and set the keyword JDBCPrefix to JDBCPrefix=jdbc/.

You must add the Content Manager Version 8 databases to WebSphere, and verify that WebSphere connection pooling is operating in this new environment.

Restriction:

The eClient supports connection pooling only for direct Content Manager connections.

Recommendation:

Stop the eClient Web application server before starting this setup process.

Procedure:

To accomplish this task, complete these steps:

1. Add a database driver for the eClient application:
 - a. In the WebSphere Advanced Administration Console, expand the Resources folder.
 - b. Expand the JDBC Providers folder and add a new provider. To add a new provider, right-click the JDBC Providers folder, and click **New** to open the JDBC Provider Properties window.
 - c. As shown in Figure 1, in the **Name** field, enter **eClient** as the provider name.
 - d. From the list, select **COM.ibm.db2.jdbc.DB2ConnectionPoolDataSource** as the implementation class.

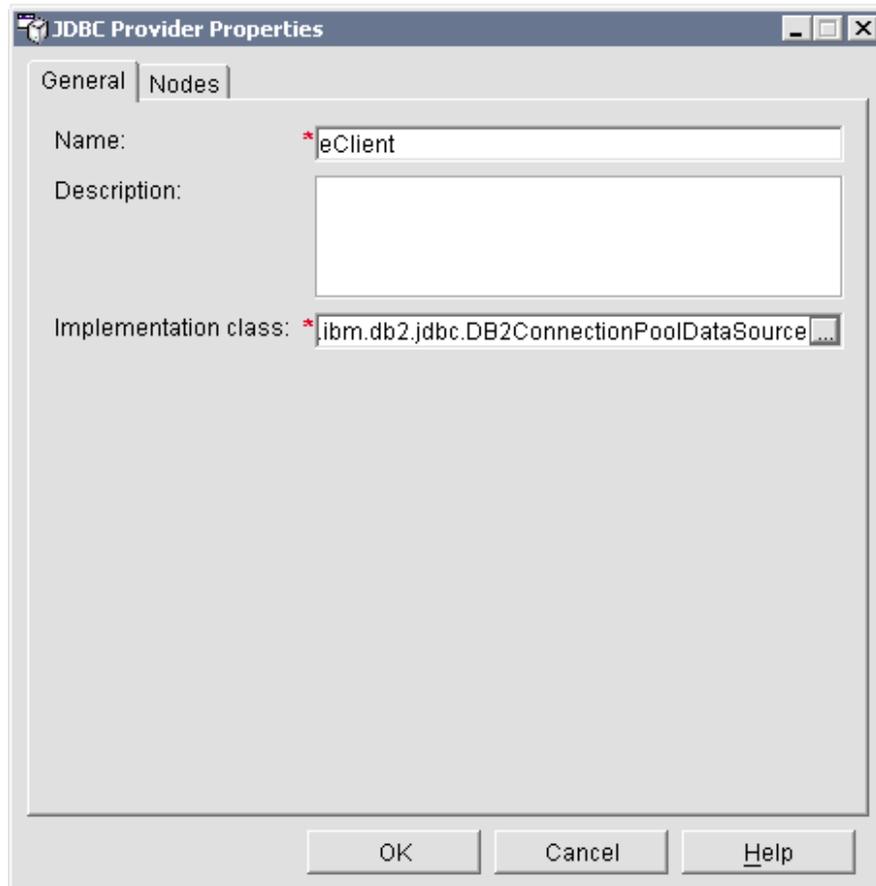


Figure 1. JDBC Provider Properties window

- e. On the Nodes page, click **Install New...** and select the node on which you want to install the driver. The default node is the local node of the WebSphere server.
 - f. After selecting the node, click **Specify Driver** and add the driver. The driver name should be the full path name where db2java.zip is located, such as e:\SQLLIB\java\db2java.zip.
 - g. After adding the driver, click **Install** to install the driver.
2. Add the data sources to the database driver:
 - a. Expand **JDBC Providers** in the tree.
 - b. Expand **eClient**. This name might be different; it is based on the provider name that you previously defined in the Name field of the JDBC Provider Properties window.
 - c. Right-click the Data Sources folder and click **New** to open the Data Source Properties window. You can add the Content Manager Version 8 databases. In the example shown in Figure 2, CM8390 is the database name.

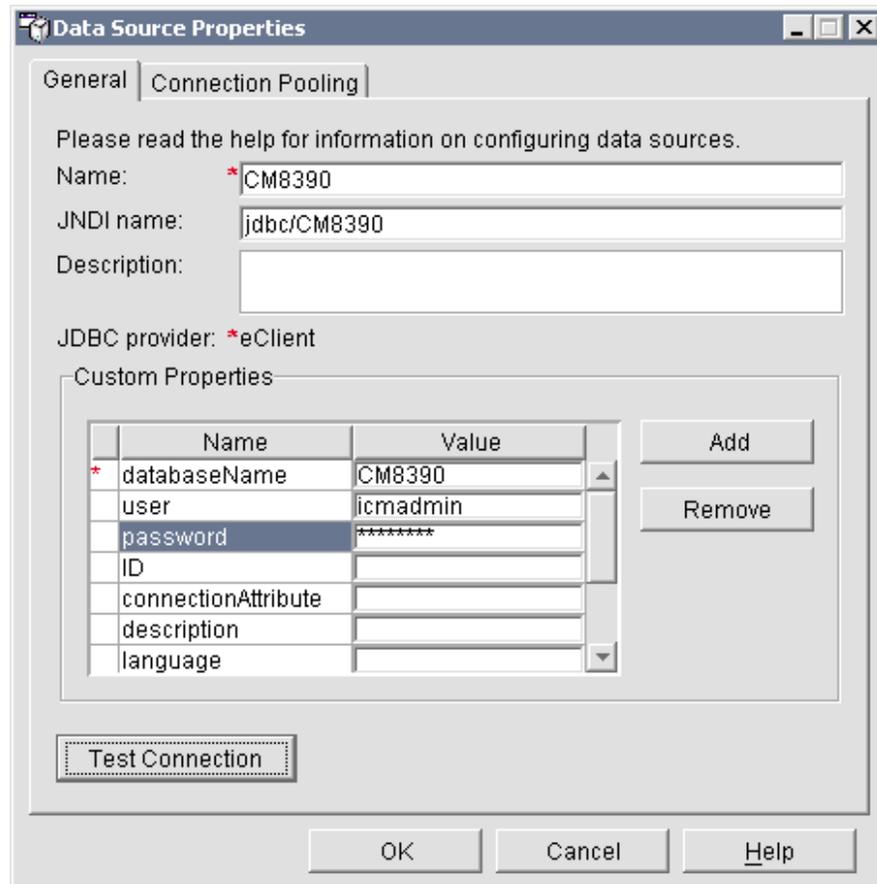


Figure 2. Data Source Properties window

Note:

In the JNDI name field, the prefix jdbc/ with the database name is how the Content Manager Version 8 connection pooling connects to the Content Manager Version 8 database. The JDBC Prefix keyword in cmbpool.ini is concatenated with the database name to obtain the JNDI name. These entries are case-sensitive.

If you specify `icmadmin` as the value for the user property, you can use only the `icmadmin` user ID to log in. As shown in Figure 3, if you want to create other user IDs like `USER1` and `USER2`, you must change the user property to `icmconct` or the DB2 connect user ID specified during Content Manager Version 8 or EIP Version 8 installation. You do not need to restart the WebSphere Application Server to change the WebSphere user and password fields. After changing WebSphere to use a different user and password, click **Apply**. If you specify `icmconct` as the user, you can log in with `USER1` or `USER2`, but not with `icmadmin`.

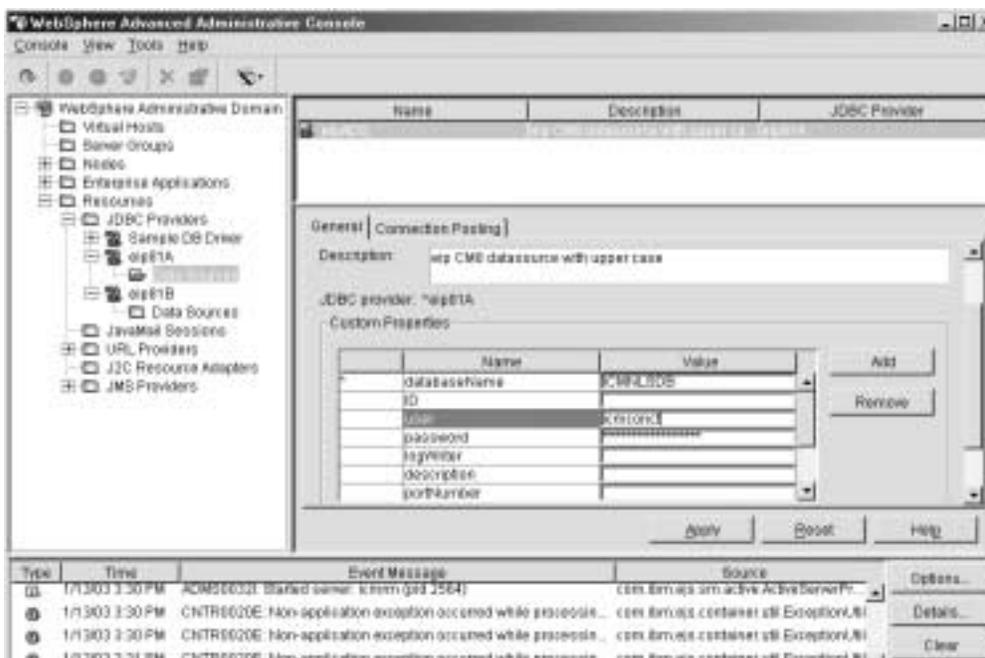


Figure 3. User with `icmconct` value

- Use the WebSphere Resource Analyzer to verify that connection pooling is in use for the eClient application server. In the WebSphere Advanced Administrative Console, select **Tools --> Resource Analyzer**. As shown in Figure 4 on page 27, Database Connection Pooling appears in the tree.

The screenshot shows the Resource Analyzer window with a tree view on the left and a data table on the right. The tree view shows the hierarchy: WebSphere Administrative Domain > Nodes > Default Server > eClient Server > Resources. The data table has columns for Time, Num Creates, Num Destroys, and Num Allocated. The data shows a steady increase in allocated resources over time, with no creates or destroys recorded.

Time	Num Creates	Num Destroys	Num Allocated
Jun 12, 2012 10:51:33	0	0	2
Jun 12, 2012 10:51:38	0	0	1
Jun 12, 2012 10:51:43	0	0	1
Jun 12, 2012 10:51:48	0	0	1
Jun 12, 2012 10:50:53	0	0	1
Jun 12, 2012 10:50:48	0	0	1
Jun 12, 2012 10:50:33	0	0	1
Jun 12, 2012 10:50:27	0	0	1

Figure 4. Resource Analyzer window

Related Tasks:

“Configuring the eClient with WebSphere Application Server” on page 19

“Selecting eClient languages” on page 28

Configuring to use IBM WebSphere 5 connection pooling with the eClient

With the eClient, you can configure to use IBM WebSphere 5 connection pooling.

Procedure:

1. Add a database driver for the eClient application:
 - a. In the WebSphere Advanced Administration Console, expand the resources folder.
 - b. Select the Node to create the JDBC Provider, and click **New** to open the JDBC Provider Properties window.
 - c. Select DB2® JDBC Provider for the JDBC Providers option and click **Apply**.
 - d. In the General Properties screen, add eClient for the name property.
 - e. Click **Apply**.
 - f. Click **Save** to save changes to local configuration.
 - g. Click **Save** to save changes to master configuration.
2. Add the data sources to the database driver:
 - a. In the tree under Resources, click the JDBC Providers link.
 - b. Click on the eClient JDBC Provider. This name might be different; it is based on the provider name that you previously defined in the name field of the JDBC Provider Properties window.
 - c. Under Additional Properties, click **Data Sources**.
 - d. Click **New**. Add the name of the Content Manager or EIP federated database in the name field.
 - e. Select **Apply**.
 - f. Save changes to the local configuration.
 - g. Save changes to the master configuration.
3. Configure the data source driver:

- a. In the tree under Resources, click the JDBC Providers link.
- b. Click on the eClient JDBC Provider. This name might be different; it is based on the provider name that you previously defined in the name field of the JDBC Provider Properties window.
- c. Under Additional Properties, click **Data Sources**.
- d. Select the data source name that was created in Step 2.
- e. In the Related Items section, select J2C Authentication Data Entries.
- f. Click **New** to create new J2C Authentication Data Entries.
- g. Add eClient for the Alias property.
- h. Add the Database user ID. **Note:** If you specify `icmadmin` as the value for the user ID property, you can use only the `icmadmin` user ID to log in. To logon to the eClient with an ID other than `icmadmin`, you must change the user property to `icmconct` or the DB2 connect user ID specified during Content Manager or EIP installation.
- i. Add the password for the user ID specified.
- j. Click **Apply**.
- k. Save changes to local configuration.
- l. Save changes to master configuration.
- m. Navigate to and click on the eClient data source.
- n. Add the alias eClient to Component-managed Authentication Alias.
- o. Add the alias eClient to Container-managed Authentication Alias.
- p. Click **Apply**.
- q. Save changes to local configuration.
- r. Save changes to master configuration.

Selecting eClient languages

The IBM Content Manager eClient is available in the following languages:

- Brazilian Portuguese
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Hebrew
- Hungarian
- Italian
- Japanese
- Norwegian
- Polish
- Portuguese
- Russian
- Simplified Chinese
- Slovak
- Slovenian

- Spanish
- Swedish
- Traditional Chinese
- Turkish

The eClient works with the National Language Support (NLS) of the library server and the operating system. If the library server supports Unicode, the eClient allows you to save and view all language texts when the operating system supports this language. If the library server supports only a specific code page, you must ensure that the code page of the operating system on which the eClient server is running matches the code page of the library server.

The eClient uses UTF-8 for character encoding. You need to set the encoding entry for the language to UTF-8 in the `encoding.properties` file. This file resides in the `\appserver\properties` folder of WebSphere. As an example, to support the simplified Chinese language, set `zh=UTF-8` in the `encoding.properties` file.

For most browsers, you must also specify the language setting. Follow these steps to specify the language settings in your browser:

In Microsoft Internet Explorer 5.5

Select **Tools** -> **Internet Options**, and click **Languages** to view the current language settings. In the Language Preference window, click **Add** to add more languages.

In Netscape Navigator 4.78

Select **Edit** -> **Preferences**. In the left frame of the Preferences window, click **Languages** to view the current language settings. Click **Add** to add more languages.

In Netscape Navigator 6.1

From the **View** menu, select the character coding and the language.

Verifying the eClient installation and configuration

After you installed and configured the eClient as a Web application, you can verify your installation and configuration following these steps:

1. Verify that the eClient application has been deployed successfully on your WebSphere Application Server.

For WebSphere 4.0.5 AE and WebSphere 5

- a. Open the WebSphere Application Server Administrative Console.
- b. Verify that the `eClient_Server` Application Server was created under Servers.
- c. Verify that the IBM eClient 82 Application is installed under Enterprise Applications.

For WebSphere 4.0.5 AES

- a. Open the WebSphere Application Server Administrative Console by clicking **Start** -> **Programs** -> **IBM WebSphere Application Server AE(s) V4.0** -> **Administrator's Console**.
- b. Select **Open a configuration file to edit with the console**.
- c. Select the option, Enter full path to file on server, and enter the path to the `IDM_ICM.xml` configuration file located in your Content Manager Common directory (for example, `C:\Program Files\IBM\CMgmt`).

- d. In the left-hand topology frame, expand **WebSphere Administrative Domain** -> **Nodes** -> *hostname* -> **Application Servers** to find the ICM_Server application server.
 - e. Expand **WebSphere Administrative Domain** -> **Nodes** -> *hostname* -> **Enterprise applications** to find the IBM eClient 82 Web application.
2. Start the eClient Web application, and point your browser to
`http://hostname/Web application name/IDMInit`

where

hostname

Name or IP address of the server machine

Web application name

Name of the eClient Web application

IDMInit

Initial connection servlet

An example of the eClient Web application address is

`http://hostname/eClient82/IDMInit`

If you installed the eClient correctly and the address is correct, the following Logon window should open.



Figure 5. Content Manager eClient Logon window

If you configured the eClient correctly, you should be able to access the content servers that you defined. The content servers that the eClient supports include:

- IBM Content Manager for Multiplatforms Version 7.1
- IBM Content Manager for Multiplatforms Version 8.1
- IBM Content Manager for Multiplatforms Version 8.2
- IBM Content Manager OnDemand for Multiplatforms Version 7.1
- IBM Content Manager OnDemand for OS/390 Version 2.1
- IBM Content Manager OnDemand for OS/390 Version 7.1
- IBM Content Manager OnDemand for iSeries Version 4.5
- IBM Content Manager OnDemand for iSeries Version 5.1
- IBM Content Manager ImagePlus for OS/390 Version 3.1
- IBM VisualInfo for AS/400 Version 4.3 or Version 5.1

If the Logon window does not open, or you cannot access the servers that you defined during installation, see “Configuration problems” on page 109.

Related Tasks:

“Installing the eClient on a Windows application server” on page 13

“Installing the eClient on an AIX or Solaris server” on page 14

Chapter 4, “Configuring”, on page 19

“Configuring the eClient with WebSphere Application Server” on page 19

Configuring third-party application integration

This section provides information about configuring third-party application integration.

Related tasks:

“Configuring PeopleSoft Integration for IBM Content Manager”

“Configuring Siebel Integration for IBM Content Manager” on page 53

Configuring PeopleSoft Integration for IBM Content Manager

This section provides steps that you must complete to allow PeopleSoft and the Content Manager eClient to work together.

Configuring PeopleSoft and the eClient to work together

You can configure PeopleSoft to work with the eClient in two ways. The first way is a loose association. The second way is a closer integration that allows for single sign-on and a more optimized user interface path from the PeopleSoft portal to the IBM Content Manager eClient.

The easiest way to associate PeopleSoft and IBM Content Manager is to provide a loose association between the two products. The purpose of the loose association is to provide a very simple method for a PeopleSoft user to navigate from somewhere in the PeopleSoft portal to the Content Manager eClient Logon page. Although the integration is simpler to establish, providing loose association requires your PeopleSoft users to do additional steps, because it forces them to perform the normal logon steps required for the Content Manager eClient. Loose association requires that users provide their user ID, password, and choose a server.

The second way to accomplish integration is to establish an optimized association, which allows for single sign-on and a more optimized user interface path from the PeopleSoft portal to the IBM Content Manager eClient. The benefit of single

sign-on for PeopleSoft users is that they are only required to enter a user ID and password once: when signing on to the PeopleSoft portal. When PeopleSoft users navigate to the link for Content Manager eClient, they only need to click that link. They do not need to re-enter a user ID and password to use the eClient.

To provide an optimized association, you must complete a few extra steps beyond setting up a loose association. Not only do you setup single sign-on, you can also decide whether or not users are required to choose a server.

You can provide either or both of these integration points. Using the PeopleSoft Security features allows you to control access to pagelets on the PeopleSoft portal. Therefore, you can provide both types of links to IBM Content Manager and restrict user access to those links by setting the appropriate security for each pagelet that contains a link.

Related tasks:

“Configuring PeopleSoft for a loose association with IBM Content Manager”

“Configuring for optimized association of PeopleSoft and IBM Content Manager”

“Installing PeopleSoft Integration for IBM Content Manager” on page 15

Configuring PeopleSoft for a loose association with IBM Content Manager

Loose association is a very quick way to integrate your PeopleSoft portal and IBM Content Manager. To do so, you define a link from the PeopleSoft portal to the IBM Content Manager eClient Web application. Your users need to click the Content Manager eClient link and the eClient will launch in a new browser window, opening to the eClient Logon page.

In order to launch the eClient Logon page from the PeopleSoft portal, you need to develop an iScript pagelet with PeopleCode. You will insert the pagelet in the PeopleSoft portal. This pagelet loads the iScript code and creates the hyperlink text, allowing users to link to the IBM eClient Logon page from the PeopleSoft portal. This process requires that you customize the PeopleSoft portal. The process includes three tasks:

1. “Creating an iScript for loose association in the PeopleSoft Application Designer” on page 43
2. “Enabling security for the iScript code for loose association” on page 48
3. “Creating the IBM Content Manager login pagelet for loose association” on page 50

Related task:

“Before you begin pagelet configuration” on page 43

Configuring for optimized association of PeopleSoft and IBM Content Manager

Optimized association allows for single sign-on. The user’s navigation steps from the PeopleSoft portal to the IBM Content Manager eClient are optimized: PeopleSoft users log in to the PeopleSoft portal as they do normally. Then, they can link directly to the Content Manager eClient; they do not need to re-enter a user ID and password at the eClient Logon page.

To establish optimized association, you must complete the following tasks in the following order:

1. You configure the PeopleSoft Internet Architecture so that the PeopleSoft cookie is passed to the eClient browser session. See “Task 1: Configuring PeopleSoft Internet Architecture”.
2. You specify that the PeopleSoft user ID be passed to the Content Manager eClient by the pagelet. See “Task 2: Configuring pagelet specifications” on page 34.
3. You ensure that the name of the PeopleSoft authentication cookie is properly specified in the integration properties (IP) file and rename the file to be consistent with the IPFile request parameter that is specified in the eClient URL that is used by the PeopleSoft pagelet. See “Task 3: Configuring the integration properties file” on page 36.
4. You synchronize user IDs between PeopleSoft and Content Manager. See “Task 4: Synchronizing user IDs” on page 36.
5. You define an additional PeopleSoft user ID with access to the PeopleSoft portal single sign-on component interface (PRTL_SS_CI). See “Task 5: Defining PeopleSoft component interface ID” on page 37.
6. You copy one file to a specific directory on the Content Manager machine. See “Task 6: Copying the logon user exit routine file” on page 38.
7. You generate the PeopleSoft Portal Single Sign-on Component Interface (PRTL_SS_CI) using PeopleSoft Application Designer. See “Task 7: Generating the PeopleSoft portal single sign-on component interface” on page 39.
8. You specify PeopleSoft configuration parameters in a file for use by Content Manager to authenticate the PeopleSoft users. See “Task 8: Specifying PeopleSoft configuration parameters for Content Manager” on page 41.
9. You make the PeopleSoft run-time environment available to the eClient. See “Task 9: Accessing PeopleSoft run-time” on page 42.

Task 1: Configuring PeopleSoft Internet Architecture: You complete this task during the PeopleSoft server installation.

You must configure the PeopleSoft Internet Architecture (PIA) so that the PeopleSoft cookie is passed to the eClient browser session. The PeopleSoft cookie contains the user’s credentials, which are passed to the Content Manager eClient for authentication. PeopleSoft browser cookies are used for enabling PeopleSoft single sign-on and for restricting user access to, for example, resources, Web pages, controls, and databases.

Because PeopleSoft uses its cookie for user access permissions and for PeopleSoft single sign-on, the PeopleSoft cookie must always be available to the browser session. For the PeopleSoft cookie to be passed to the eClient browser session, you must specify one authentication domain that contains both application servers (PeopleSoft portal and the Content Manager eClient) when you install the PIA. PeopleSoft calls this the authentication domain (authTokenDomain).

Requirement: When you specify the authentication domain during installation of the PIA, you must start the domain name with a period (.). Do not use imbedded blanks. For example, if the domain to which both these application servers belong is abc.def.ghi.com, your domain specification must be .abc.def.ghi.com. Later, users must supply the fully qualified host name in the URL used to access the PeopleSoft portal. If you do not make these changes, users cannot open the PeopleSoft portal home page.

Ensure that the browsers used to access the PeopleSoft portal and the eClient have the browser’s security set up to handle cookies appropriately. For Microsoft

Internet Explorer, you need to set the Internet Options for Security to enable the per-session cookies. If per-session cookies are disabled, then you cannot access these pages. For Netscape Navigator, you need to either accept all cookies or accept only cookies that get sent back to the originating server. If all cookies are disabled, then you cannot access these pages. Before you proceed, verify that cookies are enabled.

Related concept:

“Configuring for optimized association of PeopleSoft and IBM Content Manager” on page 32

Related tasks:

“Task 2: Configuring pagelet specifications”
“Enabling browsers to accept cookies” on page 114

Task 2: Configuring pagelet specifications: This task assumes that you have already configured the PeopleSoft Internet Architecture (PIA), placing both the PeopleSoft portal and the eClient in the same domain. You complete this task on the PeopleSoft Enterprise Portal.

For this task, you need to construct a pagelet that links the Content Manager eClient to the PeopleSoft portal. You must create a pagelet that points to the PeopleSoft Internet Script (iScript) code that contains the Content Manager eClient URL, a PeopleSoft user ID, and, depending what iType that you choose, the server name and server type. To create a pagelet, you must create an iScript. The iScript contains a URL pointing to the location of either the eClient Logon window or a specific Content Manager database.

The steps to build the pagelet for loose association and optimized association are similar except for the construction of the URL. For loose association, you need to point to the Content Manager eClient Logon Window, which might look like the following URL:

```
http://host.abc.def.ghi.com/eClient82/IDMInit
```

While a URL for an optimized association might look like this link:

```
http://host.abc.def.ghi.com/eClient82/IDMIntegrator?  
&ReleaseLevel=PEOPLESOFTV840&IPFile=PeopleSoft  
&iType=logon&userid=PS
```

Or it could look like this link:

```
http://host.abc.def.ghi.com/eClient82/IDMIntegrator?  
&ReleaseLevel=PEOPLESOFTV840&IPFile=PeopleSoft  
&iType=connection&server=ICMNLSD&serverType=Fed&userid=PS
```

A URL statement must specify the host name (*host name*), the location of the eClient application (*eClient application name*), the servlet name (*servlet name*), and the argument properties (*argument properties*), for example, `http://host name/eClient application name/servlet name?argument properties`.

A valid URL for single sign-on contains the servlet specification (IDMIntegrator to invoke optimized association), four required parameters (the release level argument, the integrator properties file name, the iType, and the user ID) and two optional parameters (the server and serverType arguments).

A URL contains the following argument properties:

ReleaseLevel

This property indicates the release level of the PeopleTools application. The acceptable valid values are `ReleaseLevel=PEOPLESOFTV840` or `ReleaseLevel=PEOPLESOFTV841`.

IPFile This property specifies the name of the integration properties file. The IP File has a file extension of `.properties`, however, you do not include `.properties` when you specify the IPFile value in the URL. The case sensitivity of the IPFile property varies by platform. For more on the integration properties file, see “Task 3: Configuring the integration properties file” on page 36.

iType This property specifies the type of integration to use. For PeopleSoft, you specify either `iType=logon` or `iType=connection`. Use `iType=logon` when you do not want to specify the server and `serverType` properties. This setting allows the PeopleSoft user to manually select the server. If the eClient has only one backend server defined to it, then the eClient takes the user directly to the home page for this server. When you use `iType=connection`, you must specify the server parameter. If you do not specify a `serverType`, then a `serverType` of `Fed` is assumed. If you want users to log on to another `serverType` other than `Fed`, like `ICM`, then, you must specify the `serverType` either in the URL or in the integration properties file. The `iType=connection` setting enables users to link straight to the home page of a server.

server This property is the name of the Content Manager server database to which the eClient connects. The server must be specified when `iType=connection` is used. An example specification is `server=ICMNLSDDB`. If this value is also specified in the integration properties file, then the value specified in the URL takes precedence.

serverType

This property is the type of Content Manager server to which the eClient connects. The valid specifications are `serverType=ICM` or `serverType=Fed`. When the `iType=connection`, then the `serverType` is automatically assumed to be `serverType=Fed`. If you want users to log on to another `serverType`, like `ICM`, then, you must specify the `serverType=ICM` in the URL or the integration properties file. When you specify the `serverType` property, it must be specified in the same location as the `server` property. For example, either you specify `server` and `serverType` in the URL or the integration properties file. If the `serverType` value is also specified in the integration properties file, then the value specified in the URL takes precedence.

userid This property specifies the user ID that was used to sign on to the PeopleSoft portal and will be used to log on to the Content Manager library server database.

Related concept:

“Configuring for optimized association of PeopleSoft and IBM Content Manager” on page 32

Related tasks:

“Task 1: Configuring PeopleSoft Internet Architecture” on page 33

“Task 3: Configuring the integration properties file” on page 36

“Before you begin pagelet configuration” on page 43

“Creating the IBM Content Manager login pagelet for optimized association” on page 51

Task 3: Configuring the integration properties file: This task assumes that you have already created the PeopleSoft pagelet for optimized association. You complete this task on the eClient server.

A sample integration properties file called `PeopleSoft.properties` is installed with the eClient. You can find it in the `ECLIENTROOT\CMeClient` directory, where `ECLIENTROOT` is the location where you installed Content Manager eClient. Rename the file to be consistent with the `IPFile` request parameter specified in the eClient URL used by the PeopleSoft pagelet. The properties that are specified in this file are:

authCookie

This property specifies the name of the authentication cookie that PeopleSoft uses for single sign-on. The property should be `authCookie=PS_TOKEN`.

server This property is the name of the Content Manager server database to which the eClient connects. The server must be specified when `iType=connection` is used. An example specification is `server=ICMNLSDDB`. If this value is also specified in the URL, then the value specified in the URL takes precedence.

serverType

This property is the type of Content Manager server to which the eClient connects. The valid specifications are `serverType=ICM` or `serverType=Fed`. When the `iType=connection`, then the `serverType` is automatically assumed to be `serverType=Fed`. If you want users to log on to another `serverType`, like `ICM`, then, you must specify the `serverType=ICM` in the URL or the integration properties file. When you specify the `serverType` property, it must be specified in the same location as the `server` property. For example, either you specify `server` and `serverType` in the URL or the integration properties file. If the `serverType` value is also specified in the integration properties file, then the value specified in the URL takes precedence.

type This property specifies the presentation type: it specifies what objects and capabilities to include in the eClient Web pages. For PeopleSoft, you must specify `type=3`.

Related concept:

“Configuring for optimized association of PeopleSoft and IBM Content Manager” on page 32

Related task:

“Task 2: Configuring pagelet specifications” on page 34

“Task 4: Synchronizing user IDs”

Task 4: Synchronizing user IDs: This task assumes that you have already configured the integration properties file and pagelet specifications. You complete this task on the PeopleSoft server and the Content Manager System Administration client.

You must synchronize user IDs between PeopleSoft and Content Manager to successfully implement the single sign-on feature. The users that you want to have single sign-on access to Content Manager need to have the same user information on both PeopleSoft and Content Manager.

After you synchronize user IDs, you must configure PeopleSoft to authenticate users from PeopleSoft to Content Manager. **You cannot use LDAP user authentication and PeopleSoft Integration for IBM Content Manager at the same time.** You must choose to use either one or the other to authenticate users, not both.

After users log on to the IBM Content Manager eClient through PeopleSoft single sign-on, user status does not synchronize across the PeopleSoft portal and the IBM Content Manager eClient. Users can log in to the IBM Content Manager eClient through PeopleSoft single sign-on, and then they can log off of the Content Manager eClient without affecting their sign-on status in the PeopleSoft portal. Conversely, users can sign-off of the PeopleSoft portal without affecting their login status on the IBM Content Manager eClient.

Related concept:

“Configuring for optimized association of PeopleSoft and IBM Content Manager” on page 32

Related tasks:

“Task 3: Configuring the integration properties file” on page 36

“Task 5: Defining PeopleSoft component interface ID”

Task 5: Defining PeopleSoft component interface ID: This task assumes that you have already synchronized user IDs for single sign-on. You complete this task on the PeopleSoft Enterprise Portal.

You must define a special PeopleSoft user ID that has access to the PeopleSoft portal single sign-on component interface (PRTL_SS_CI). The PRTL_SS_CI identifies the PeopleSoft portal to Content Manager, allowing sign-on to occur. When the PeopleSoft user ID connects to Content Manager, Content Manager uses the PRTL_SS_CI to authenticate the user ID as a valid user ID in Content Manager. You need to define and use a unique user ID that has full access to the PRTL_SS_CI in its permission list. This unique user ID that you define must not be used to sign-on to the PeopleSoft portal. To eliminate the security exposure, do not grant permissions to this user ID beyond those described in the following steps:

1. Create a permission list:
 - a. In the Enterprise Menu on the PeopleSoft portal, select **PeopleTools --> Security --> Permissions & Roles --> Permission Lists**.
 - b. Click the **Add a New Value** tab and type the name of the permission list. In this example, it is named PERMISSION_PRTL_SS_CI. You can name it what you want.
 - c. When you have named the new permission list, click **Add**. The Permission Lists page displays.
 - d. Click the **Component Interfaces** tab. You might have to click the right arrow to see this tab.
 - e. Type PRTL_SS_CI in the **Name** field and click **Edit**.
 - f. Specify that the methods **Authenticate**, **Get**, and **Get_UserID** have **Full Access** and then click **OK**.
 - g. Complete the rest of the Permission Lists page fields as needed. Asterisks (*) indicate a required field.
 - h. When you have completed the Permission Lists page, click **Save**.
2. Create a role:

- a. In the Enterprise Menu on the PeopleSoft portal, select **PeopleTools --> Security --> Permission & Roles --> Roles**.
 - b. Click the **Add a New Value** tab and enter the name of the role. In this example, it is named ROLE_PRTL_SS_CI. You can name it what you want.
 - c. When you have named the new role, click **Add**. The Roles page displays.
 - d. Click the **General** tab and enter a description for this role.
 - e. Click the **Permission Lists** tab.
 - f. Type the name of the permission list that you defined in step 1 on page 33, for example, PERMISSION_PRTL_SS_CI. If you do not know the exact name of the permission list that you want to use, click the magnifying glass next to the **Permission List** field. The permission list that you select from the returned results is placed in the **Permission List** field.
 - g. Complete the rest of the Roles page fields as needed. Asterisks (*) indicate a required field.
 - h. When you have completed the Roles page, click **Save**.
3. Create a user:
- a. In the Enterprise Menu on the PeopleSoft portal, select: **PeopleTools --> Security --> User Profiles --> User Profiles**.
 - b. Click the **Add a New Value** tab and type the name of the user. In this example, it is named USER_PRTL_SS_CI. You can name it what you want.
 - c. When you have named the new user, click **Add**. The User Profiles page displays.
 - d. Click the **General** tab. Type a password and then confirm the password by typing it in again.
 - e. Click the **ID** tab and choose **None** for the **ID type**.
 - f. Click the **Roles** tab and type ROLE_PRTL_SS_CI for the **Role Name**. If you do not know the exact name of the role name that you want, click the magnifying glass next to the **Role Name** field. The role name that you select from the returned results is placed in the **Role Name** field.
 - g. Click **Save**. If you do not specify a value for the **Symbolic ID**, a warning message displays. A symbolic ID is used as a search key for an AccessID. For more information about the symbolic ID, see the PeopleSoft documentation.
 - h. Click **OK** to accept the message.

Now, the user account has been created and is ready to be used by the single sign-on user exit routine: logon user exit routine.

Related concept:

“Configuring for optimized association of PeopleSoft and IBM Content Manager” on page 32

Related tasks:

“Task 4: Synchronizing user IDs” on page 36

“Task 6: Copying the logon user exit routine file”

Task 6: Copying the logon user exit routine file: This task assumes that you have created a unique user ID with full access to the PeopleSoft portal single sign-on component interface (PRTL_SS_CI). You complete this task on the Content Manager library server database.

A user exit is a predefined place in the code where a user exit routine can be given control. The user exit routine acts like a plug-in and it must adhere to the interface defined by the user exit. The logon user exit routine provides the interface to validate with PeopleSoft authentication. To allow single sign-on, you must configure the user interface routine appropriately.

Single sign-on under PeopleSoft requires changes to the Content Manager stack. You need to copy a file to a specific directory on the Content Manager machine. The PeopleSoft portal and the Content Manager eClient can be on different machines and application server types, but they must be able to communicate with each other. In fact, the eClient uses the PeopleSoft single sign-on component interface (PTRL_SS_CI) to authenticate the credentials. The eClient sends the results of that authentication step to the logon user exit routine, which completes the authentication process.

The backend server connectors supported by logon user exit routines are the IBM Content Manager (ICM) version 8 Connector, and the Enterprise Information Portal version 8 Federated Connector. You must copy the file named ICMXLSLG.DLL to the directory *ICMROOT\database name\DLL* from the directory *ICMROOT\integration\peoplesoft* for Windows, or *ICMDLL/database name/DLL/* on Unix-based operating system, where *ICMROOT* is the location where you installed Content Manager, *ICMDLL* is the value of the *ICMDLL* environment variable, and *database name* is the name of the Content Manager library server database. This step is not automatically done for you because customers who do not integrate with PeopleSoft can experience a performance penalty and copying this file overwrites the LDAP logon user exit routine file, replacing user authentication using LDAP.

Restriction: You cannot use LDAP authentication and PeopleSoft single sign-on at the same time. You can specify only one logon user exit routine at any given time.

Related concept:

“Configuring for optimized association of PeopleSoft and IBM Content Manager” on page 32

Related tasks:

“Task 5: Defining PeopleSoft component interface ID” on page 37

“Task 7: Generating the PeopleSoft portal single sign-on component interface”

Task 7: Generating the PeopleSoft portal single sign-on component interface:

This task assumes that you have already copied ICMXLSLG.DLL to its appropriate location. You complete this task on the PeopleSoft server and the eClient server.

You need to generate the PeopleSoft portal single sign-on component interface (PTRL_SS_CI) using the PeopleSoft Application Designer. Using the Application Designer, you must:

- Create and compile the packages needed by ICMPSSS0.java.
- Compile ICMPSSS0.java.
- Install all of these class files in the appropriate directories.

The file ICMPSSS0.java is on the eClient server machine, in a directory called *ECLIENTROOT\integration\peoplesoft*, where *ECLIENTROOT* is the location where you installed eClient.

The PeopleSoft portal single sign-on component interface, PRTL_SS_CI, allows integration of a single sign-on solution with the PeopleSoft portal. Use the PeopleSoft Application Designer to build the classes supporting the PRTL_SS_CI API. To enable this API, complete the following steps:

1. Generate the PeopleSoft portal single sign-on component interface (PRTL_SS_CI) API to allow the logon user exit routine to communicate to PeopleSoft. To generate the pre-required PeopleSoft Java classes that support the component interface, complete the following steps:
 - a. Open the PeopleSoft Application Designer and sign-on.
 - b. In the Application Designer, select **File --> Open**. The Open Definition window opens.
 - c. In the Open Definition window, click **Definition --> Component Interface**.
 - d. In the **Selection Criteria** group, type PRTL_SS_CI in the **Name** field and click **Open**. The PRTL_SS_CI (Component Interface) window opens.
 - e. In the Application Designer main window, select **Build --> PeopleSoft APIs**. The Build PeopleSoft API Bindings window opens.
 - f. In the Build PeopleSoft API Bindings window, the **Build** check boxes for the **COM Type Library** group and the **Java Classes** group are selected by default. Clear the **COM Type Library** group check box.
 - g. In the **Java Classes** group, enter the name of the target directory. For example, you can use the directory C:\CM_SS0.
 - h. In the same window, there is a list of APIs to build. Click **All** to select all of the APIs to build and then click **OK**.
 - i. Close the PeopleSoft Application Designer.
2. Compile the PeopleSoft Java code generated in the previous steps. The full path of psjoa.jar must either be set in the CLASSPATH or specified as a command line parameter. To complete this step, you can run the following commands in a command window (note that the following steps assume that you specified C:\CM_SS0 as the target directory in the **Java Classes** group in the previous step):
 - a. Enter C:
 - b. Enter CD \CM_SS0\PeopleSoft\Generated\CompIntfc
 - c. Enter javac -classpath PS_HOME\class\psjoa.jar *.java, where PS_HOME is the location where you installed PeopleSoft.
 - d. Enter CD \CM_SS0\PeopleSoft\Generated\PeopleSoft
 - e. Enter javac -classpath PS_HOME\class\psjoa.jar *.java, where PS_HOME is the location where you installed PeopleSoft.
 - f. The classes from the two PeopleSoft packages (PeopleSoft.Generated.CompIntfc and PeopleSoft.Generated.PeopleSoft) must be available to the eClient. Therefore, depending on the PeopleSoft license agreement, you might be permitted to copy the classes to the eClient server. For example, WebSphere Application Server Advanced Edition for Windows uses the following directory locations for the generated classes:

```
ECLIENTROOT\installedApp\eClient82.ear\eClient82.war\WEB-INF\classes\PeopleSoft\Generated\CompIntfc\
```

and

```
ECLIENTROOT\installedApp\eClient82.ear\eClient82.war\  
WEB-INF\classes\PeopleSoft\Generated\PeopleSoft\
```

If your PeopleSoft license agreement does not allow you to copy the class files, then you must configure WebSphere Application Server to access them on the PeopleSoft server.

3. You must add the location of the directories where the two PeopleSoft packages (PeopleSoft.Generated.CompIntfc and PeopleSoft.Generated.PeopleSoft) reside to the CLASSPATH in order to compile ICMPSSSO.java in the next step. The class files in these two packages must remain in the CLASSPATH so that the run-time code can access them.
4. Compile the ICMPSSSO.java file installed with the eClient. The full path of psjoa.jar must either be set in the CLASSPATH or specified as a command line parameter. To complete this step, run the following command in a command window:
 - a. Enter `CD ECLIENROOT\integration\peoplesoft`, where *ECLIENROOT* is the location where you installed the eClient.
 - b. Enter `javac -classpath PS_HOME\class\psjoa.jar ICMPSSSO.java`, where *PS_HOME* is the location where you installed PeopleSoft.
 - c. Copy the class file to the eClient server. For example, WebSphere Application Server Advanced Edition for Windows uses the following directory location for the class:
`ECLIENROOT\installedApp\eClient82.ear\eClient82.war\WEB-INF\classes\`

Important: The file ICMPSSSO.class must be available to the eClient.

Related concept:

“Configuring for optimized association of PeopleSoft and IBM Content Manager” on page 32

Related tasks:

“Task 6: Copying the logon user exit routine file” on page 38

“Task 8: Specifying PeopleSoft configuration parameters for Content Manager”

Task 8: Specifying PeopleSoft configuration parameters for Content Manager:

This task assumes that you have already enabled the PeopleSoft portal single sign-on component interface API. You complete this task on the eClient server.

Specify the PeopleSoft configuration parameters in the ICMPSSSO.properties file for use by eClient to authenticate the PeopleSoft users. These configuration parameters include the name of the PeopleSoft server, the port on which the PeopleSoft server is listening, and a user ID and password for connection. The user ID and password values are those that you added according to instructions in “Task 5: Defining PeopleSoft component interface ID” on page 37.

For the eClient to communicate with the PeopleSoft component interface, it must know where the PeopleSoft software is installed. To configure the eClient, you must edit the file named ICMPSSSO.properties, located in the following directory:
 ECLIENROOT\integration\peoplesoft\

Copy the ICMPSSSO.properties file to the same directory where you put the ICMPSSSO.class file. Open the ICMPSSSO.properties file in an editor and modify the following name-value pairs:

ServerName=PSServer

Name of the PeopleSoft server providing the authentication

ServerPort=PSPort

Port number on which the PeopleSoft server is listening

UserID=*USER_PRTL_SS_CI*

User ID authorized to execute the PRTL_SS_CI component interface functions

Password=*UserIDpassword*

Password for UserID

After you modify the `ICMPSSSO.properties`, save it.

Related concept:

“Configuring for optimized association of PeopleSoft and IBM Content Manager” on page 32

Related tasks:

“Task 7: Generating the PeopleSoft portal single sign-on component interface” on page 39

“Task 9: Accessing PeopleSoft run-time”

Task 9: Accessing PeopleSoft run-time: This task assumes that you already have a modified copy of the `ICMPSSSO.properties` file in the same directory as the `ICMPSSSO.class` file. You complete this task on the eClient server.

Note: The eClient must have access to the PeopleSoft run-time file in the WebSphere Application Server’s CLASSPATH. The run-time file is a JAR file named `psjoa.jar`. In a default PeopleSoft 8.4 installation, `psjoa.jar` is in: `PS_HOME\web\psjoa\psjoa.jar`. For example, WebSphere Application Server Advanced Edition uses the following directory location: `ECLIENTROOT\installedApps\eClient82.ear\eClient82.war\WEB_INF\lib\psjoa.jar`. Depending on the PeopleSoft license agreement, you might be permitted to copy the PeopleSoft run-time file to the eClient server. If the PeopleSoft license agreement does not permit copying of the run-time file, you must configure the WebSphere Application Server to access the run-time file on the PeopleSoft server.

If you have not configured the `ICMPSSSO.properties` correctly, Content Manager does not allow you to log on. If you have a problem when you initially test the single sign-on path, check the log file on the Content Manager machine for one of the following return codes. The default log file name is `ICMSERVER.LOG`. If you have logging and tracing set, the log file records the return codes. Depending on what failed, you can receive one of the following return codes:

7123 RC_INVALID_PARAMETER: You have an invalid pointer or value.

7006 RC_DLL_LOAD_ERROR: Content Manager could not load a DLL.

7011 RC_GET_PROC_ADDRESS_ERROR: Content Manager could not obtain a procedure.

If you configured the `ICMPSSSO.properties` correctly, the log file lists a return code of 0.

You can turn on the logging and tracing in the Content Manager System Administration Library Server Configuration Log and Trace window in the system administration client.

Related concept:

“Configuring for optimized association of PeopleSoft and IBM Content Manager” on page 32

Related task:

“Task 8: Specifying PeopleSoft configuration parameters for Content Manager” on page 41

Related reference:

“Getting more information about PeopleSoft Integration for IBM Content Manager” on page 123

Before you begin pagelet configuration

Before you begin configuring the pagelet, you must delete the cache from the browser so your browser settings use the changes that you make to the pagelet that you need to modify. If you do not delete what is in the cache, changes that you make to the pagelet are ignored.

To delete the cache, complete the following steps:

1. Stop the WebSphere application server.
2. Stop the PeopleSoft application server. For instructions on stopping the PeopleSoft application server, see the PeopleSoft documentation.
3. Delete the PeopleSoft application server cache: *PS_HOME*\appserv\PSEP\cache, where *PS_HOME* is the location where you installed the PeopleSoft files and *PSEP* is the name of the PeopleSoft version that you use, for example, PeopleSoft 8.40 would be PSEP84.
4. Delete the WebSphere PeopleSoft server cache: *WebSphere*\AppServer\installedApps\peoplesoft\portal\ps\cache, where *WebSphere* is where you installed the WebSphere files.
5. Start the PeopleSoft application server. For instructions on starting the PeopleSoft application server, see the PeopleSoft documentation.
6. Start the WebSphere application server.

Related tasks:

“Creating an iScript for loose association in the PeopleSoft Application Designer”

“Creating an iScript for optimized integration in the PeopleSoft Application Designer” on page 45

Creating an iScript in the PeopleSoft Application Designer**Creating an iScript for loose association in the PeopleSoft Application Designer:**

This task assumes that you have already completed all steps in “Before you begin pagelet configuration”.

An iScript defines the location of the eClient Logon window. You develop the iScript with the understanding of the following rules:

- The eClient URL must be an HTML definition.
- The HTML definition must be in a FieldFormula, namely, the iScript.
- The FieldFormula must be in a Field.
- The Field must be in a Record.
- The flexibility of the PeopleSoft portal gives you the liberty to create pagelets using your own preferred method without using the PeopleSoft Application Designer. This information only describes how to create pagelets using the PeopleSoft Application Designer.

1. Open the PeopleSoft Application Designer. In a default PeopleTools 8.4 installation, the Application Designer is at `PS_HOME\bin\client\winx86\pside.exe`, where `PS_HOME` is where you installed the PeopleSoft files.
When you sign on to the PeopleSoft Application, the Application Server Name is the server where PeopleTools is installed. Use a user ID and password that has definition authority, for example a system administrator ID. **Important:** In PeopleSoft, user IDs, and passwords are case sensitive.
2. Create an HTML definition:
 - a. In the Application Designer, select **File --> New**. The New Definition window opens.
 - b. Select **HTML** and click **OK**. A window to compose HTML opens.
 - c. Type an HTML statement, for example, `Click here` to log in to the IBM CM eClient.
 - d. Replace the host name, for example `host.abc.def.ghi.com`, with the DNS name of the host where your Content Manager eClient resides. You must modify `eClient82` if you did not accept the default eClient installation path. The sample link says, Click here to login to the IBM Content Manager eClient. Choose whatever prompt words that you want. With the English version of PeopleSoft, use only the portable ASCII character set.
 - e. Now select **File --> Save As** to save this new file. In this example, the HTML file is saved as `LOOSEHTML`. You can name it what you want.
3. Create a field definition:
 - a. In the Application Designer, select **File --> New**. The New Definition window opens.
 - b. Select **Field** and then click **OK**. The Field window opens.
 - c. Complete the **Label ID**, the **Long Name**, and the **Short Name**. The **Def** check box is automatically selected for you. You can leave everything else to the default values.
 - d. Select **File --> Save As** to save this new field. In this example, the field definition is saved as `LOOSEFIELD`. You can name it what you want, but do not use a name that has already been used.
4. Create a record definition:
 - a. In the Application Designer, select **File --> New**. The New Definition window opens.
 - b. Select **Record**, and then click **OK**. The Record window opens.
 - c. From the PeopleSoft Application Designer main window, select **Insert --> Field**. The Insert Field window opens.
 - d. Type a name in the **Selection Criteria Name** field. Use the same name that you specified in step 3, for example, `LOOSEFIELD`.
 - e. Click **Insert**. This action inserts the field that you created into the Record window and becomes a part of the record that you are creating.
 - f. Close the Insert Field window.
 - g. In the Record window, click the **Record Type** tab.
 - h. Select the **Derived/Work** radio button as the record type.
 - i. Select **File --> Save As** and type the record name. In this example, the name is `WEBLIB_LOOSEREC`. **Requirement:** The record name must begin with `WEBLIB_` to work.
5. Edit the iScript PeopleCode:

- a. In the Record window, click the **Record Fields** tab.
 - b. Right-click the row that represents the field that you just inserted (in this example, that field is called LOOSEFIELD) and click **View PeopleCode**. The Record PeopleCode window opens. The title of this window has a string with the following values separated by periods (.):
 - Record definition name (for example, WEBLIB_LOOSEREC)
 - Field definition name (for example, LOOSEFIELD)
 - PeopleSoft event name, FieldFormula
 - c. Verify that the left list shows the field name that you specified, for example, LOOSEFIELD.
 - d. Verify that the right list shows FieldFormula. In the large editable part of this window, enter the following code:


```
Function IScript_CMLOOSELOG()
    %Response.Write(GetHTMLText(HTML.LOOSEHTML));
End-Function;
```

Where:

 - CMLOOSELOG is the name for your IScript function.
 - LOOSEHTML is the HTML file that you created in step 2 on page 44.
 - e. When you finish editing the script, select **File --> Save** to save it.
6. After you are finished with the PeopleSoft Application Designer, you can close the tool.

After you create an iScript, you need to restrict access to it. Begin this task by going to “Enabling security for the iScript code for loose association” on page 48.

Creating an iScript for optimized integration in the PeopleSoft Application

Designer: This task assumes that you have already completed all steps in “Before you begin pagelet configuration” on page 43.

An iScript defines the location of the eClient Logon window. You develop the iScript with the understanding of the following rules:

- The eClient URL must be an HTML definition.
- The HTML definition must be in a FieldFormula, namely, the iScript.
- The FieldFormula must be in a Field.
- The Field must be in a Record.
- The flexibility of the PeopleSoft portal gives you the liberty to create pagelets using your own preferred method without using the PeopleSoft Application Designer. This information only describes how to create pagelets using the PeopleSoft Application Designer.

In the case of optimized integration, you must create three HTML definitions. In these steps, choose the prompt words that you want. With the English version of PeopleSoft, use only the portable ASCII character set.

1. Open the PeopleSoft Application Designer. In a default PeopleTools 8.4 installation, the Application Designer is found at `PS_HOME\bin\client\winx86\pside.exe`, where `PS_HOME` is where you installed the PeopleSoft files.

When you sign on to the PeopleSoft Application, the Application Server Name is the server where PeopleTools is installed. Use a user ID and password that has definition authority, for example a system administrator ID. **Important:** In PeopleSoft, user IDs and passwords are case sensitive.

2. Create an HTML definition:
 - a. In the PeopleSoft Application Designer, select **File --> New**. The New Definition window opens.
 - b. Scroll down, select **HTML**, and click **OK**. A window to compose HTML opens.
 - c. Type the first part of a three-part HTML statement. For example, if you want the pagelet to read Click here to automatically log in to the IBM CM eClient., then your leading portion of HTML should say Click. Select **File --> Save As** to save this new file. Specify a name that indicates that this file is the first part of the HTML statement for optimized association, for example, HTML_CM_LEAD.
 - d. Create a second HTML definition. Select **File --> New**. The New Definition window opens. Scroll down, select **HTML**, and click **OK**. A window to compose HTML opens. Type the middle part of a three-part HTML statement. In this example, the pagelet reads, Click here to automatically log in to the IBM CM eClient.. The middle portion of HTML should say here. Select **File --> Save As** to save this new file. Specify a name that indicates that this file contains the link of the HTML statement for optimized association, for example, HTML_CM_LINK.
 - e. Create a third HTML definition. Select **File --> New**. The New Definition window opens. Scroll down, select **HTML**, and click **OK**. A window to compose HTML opens. Type the last part of a three-part HTML statement. In this example, the pagelet reads, Click here to automatically log in to the IBM CM eClient.. Your last portion of HTML should say to automatically log in to the IBM CM eClient.. Select **File --> Save As** to save this new file. Specify a name that indicates that this is the last file of the HTML statement for optimized association, for example, HTML_CM_TRAIL.
3. Create a field definition:
 - a. In the Application Designer, select **File --> New**. The New Definition window opens.
 - b. Select **Field** and then click **OK**. The Field window opens.
 - c. Complete the **Label ID**, the **Long Name**, and the **Short Name**. The **Def** check box is automatically selected for you. You can leave everything else to the default values.
 - d. Select **File --> Save As** to save this new field. In this example, the Field definition is saved as OPT_FIELD. You can name it what you want, but do not use a name that has already been used.
4. Create a record definition:
 - a. In the PeopleSoft Application Designer, select **File --> New**. The New Definition window opens.
 - b. Select **Record**, and then click **OK**. The Record window opens.
 - c. From the PeopleSoft Application Designer main window, select **Insert --> Field**. The Insert Field window opens.
 - d. Type a name in the **Selection Criteria Name** field. Use the same name that you specified in step 3, for example, OPT_FIELD.
 - e. Click **Insert**. This action inserts the field that you created into the record that you are creating.
 - f. Close the Insert Field window.
 - g. In the Record window, click the **Record Type** tab.
 - h. Select the **Derived/Work** radio button as the record type.

- i. Select **File** --> **Save As** and type the record name. In this example, the name is WEBLIB_OPT_REC. **Requirement:** The record name must begin with WEBLIB_ to work.
5. Edit the iScript PeopleCode:
 - a. In the Record window, click the **Record Fields** tab.
 - b. Right-click the row that represents the field that you just inserted (in this example, that field is called OPT_FIELD), and click **View PeopleCode**. The Record PeopleCode window opens. The title of this window has a string with the following values separated by periods (.):
 - Record definition name (for example, WEBLIB_OPT_REC)
 - Field definition name (for example, OPT_FIELD)
 - PeopleSoft event name, FieldFormula
 - c. Verify that the left list shows the field name that you specified, for example, OPT_FIELD.
 - d. Verify that the right list shows FieldFormula. In the large editable part of this window, enter one of the following codes:
 - For simple logon integration type:


```
Function IScript_CMOPTLOG1()
    %Response.Write(GetHTMLText(HTML.HTML_CM_LEAD));
    %Response.Write(" <a ");
    %Response.Write("href=");
    %Response.Write("http://host.abc.def.ghi.com/");
    %Response.Write("eClient82/IDMIntegrator");
    %Response.Write("?&ReleaseLevel=PEOPLESOFTV840");
    %Response.Write("&IPFile=PeopleSoft");
    %Response.Write("&iType=logon");
    %Response.Write("&userid=");
    %Response.Write(%UserId);
    %Response.Write(">");
    %Response.Write(GetHTMLText(HTML.HTML_CM_LINK));
    %Response.Write("</a> ");
    %Response.Write(GetHTMLText(HTML.HTML_CM_TRAIL));
End-Function;
```
 - For when you specify the iType=connection, where server and serverType are specified in the integration properties file (IP File):


```
Function IScript_CMOPTLOG2()
    %Response.Write(GetHTMLText(HTML.HTML_CM_LEAD));
    %Response.Write(" <a ");
    %Response.Write("href=");
    %Response.Write("http://host.abc.def.ghi.com/");
    %Response.Write("eClient82/IDMIntegrator");
    %Response.Write("?&ReleaseLevel=PEOPLESOFTV840");
    %Response.Write("&IPFile=PeopleSoft");
    %Response.Write("&iType=connection");
    %Response.Write("&userid=");
    %Response.Write(%UserId);
    %Response.Write(">");
    %Response.Write(GetHTMLText(HTML.HTML_CM_LINK));
    %Response.Write("</a> ");
    %Response.Write(GetHTMLText(HTML.HTML_CM_TRAIL));
End-Function;
```
 - For when you specify iType=connection, where server and serverType are specified on the URL:


```
Function IScript_CMOPTLOG3()
    %Response.Write(GetHTMLText(HTML.HTML_CM_LEAD));
    %Response.Write(" <a ");
    %Response.Write("href=");
    %Response.Write("http://host.abc.def.ghi.com/");
    %Response.Write("eClient82/IDMIntegrator");
```

```

%Response.Write("&ReleaseLevel=PEOPLESOFTV840");
%Response.Write("&IPFile=PeopleSoft");
%Response.Write("&iType=connection");
%Response.Write("&server=ICMNLSD&serverType=Fed");
%Response.Write("&userid=");
%Response.Write(%UserId);
%Response.Write("<>");
%Response.Write(GetHTMLText(HTML.HTML_CM_LINK));
%Response.Write("</a> ");
%Response.Write(GetHTMLText(HTML.HTML_CM_TRAIL));
End-Function;

```

Where:

- CMOPTLOG1, CMOPTLOG2, CMOPTLOG3 are the names for your iScript functions.
 - HTML_CM_LEAD, HTML_CM_LINK, HTML_CM_TRAIL are the HTML files that you created in step 2 on page 46.
 - host.abc.def.ghi.com is the actual fully qualified host name where your Content Manager eClient resides.
 - eClient82 is the path where you installed the eClient.
 - &ReleaseLevel=PEOPLESOFTV840 gives the version of PeopleTools that you use, either PEOPLESOFTV840 or PEOPLESOFTV841.
 - &IPFile=PeopleSoft reflects the name of the integration properties file used on the eClient machine. Notice that the extension .properties does not occur in the specification.
 - &server=ICMNLSD specifies the name of the server to which you need to connect.
 - &serverType=Fed specifies use of either the Enterprise Information Portal Federated connector (Fed) or the Content Manager version 8 connector (ICM).
- e. When you finish editing the script, select **File --> Save** to save it.

After you create an iScript, you need to restrict access to it. Begin this task by going to “Enabling security for the iScript code for optimized association” on page 49.

Enabling security for the iScript code

Enabling security for the iScript code for loose association: This task assumes that you have already created an iScript.

After you define an iScript, you must secure access to it. Because the iScript is buried within a record, you must enable security for the record. To enable security for a record, complete the following steps:

1. Sign on to PeopleSoft Enterprise Portal with a user ID that has Definition permission, for example a system administration ID.
2. In the Enterprise Menu on the left side of the portal, select **PeopleTools --> Security --> Permissions and Roles --> Permission Lists**.
3. Click **Search by --> Permission List** and then click **Search**.
4. Select **ALLPORTL** from the returned search results, and then select the **Web Libraries** tab of the **ALLPORTL** permission list. You might have to click the right arrow to see this tab.
5. Type the name of the record that you defined in the PeopleSoft Application Designer, and then click the magnifying glass to search. If you do not see a search field or button, click the plus sign (+) and a search field displays. This

example uses the record name WEBLIB_LOOSEREC. **Requirement:** Web library records must begin with the prefix WEBLIB_.

6. After the search completes, click your Web library record name, for example, WEBLIB_LOOSEREC, in the list of results. This action places the Web library record into the **ALLPORTL** permission list.
7. Click **Edit**. The Web Library Permissions window opens.
8. Select **Full Access** from the **Access Permissions** list for your function, for example, LOOSEFIELD.FieldFormula.iScript_CMLOOSELOG.
9. Click **OK**. You return to the **ALLPORTL** permission list window.
10. Click **Save** to complete security enablement for your iScript.

Related tasks:

“Creating an iScript for loose association in the PeopleSoft Application Designer” on page 43

“Creating the IBM Content Manager login pagelet for loose association” on page 50

Enabling security for the iScript code for optimized association: This task assumes that you have already created an iScript.

After you define an iScript, you must secure access to it. Because the iScript is buried within a record, you must enable security for the record. To enable security for a record, complete the following steps:

1. Sign on to PeopleSoft Enterprise Portal with a user ID that has Definition permission, for example a system administration ID.
2. In the Enterprise Menu on the left side of the portal, select **PeopleTools --> Security --> Permissions and Roles --> Permission Lists**.
3. Click **Search by --> Permission List** and then click **Search**.
4. Select **ALLPORTL** from the returned search results, and then select the **Web Libraries** tab of the **ALLPORTL** permission list. You might have to click the right arrow to see this tab.
5. Type the name of the record that you defined in the PeopleSoft Application Designer, and then click the magnifying glass to search. If you do not see a search field or button, click the plus sign (+) and a search field displays. This example uses the record name WEBLIB_OPT_REC. **Requirement:** Web library records must begin with the prefix WEBLIB_.
6. After the search completes, click your Web library record name, for example, WEBLIB_OPT_REC, in the list of results. This action places the Web library record into the **ALLPORTL** permission list.
7. Click **Edit**. The Web Library Permissions window opens.
8. Select **Full Access** from the **Access Permissions** list for your function, for example, OPT_FIELD.FieldFormula.iScript_CMLOPTLOG.
9. Click **OK**. You return to the **ALLPORTL** permission list window.
10. Click **Save** to complete security enablement for your iScript.

Related tasks:

“Creating an iScript for optimized integration in the PeopleSoft Application Designer” on page 45

“Creating the IBM Content Manager login pagelet for optimized association” on page 51

Creating the IBM Content Manager login pagelet

Creating the IBM Content Manager login pagelet for loose association: This task assumes that you have already created an iScript and a record and have enabled security for the record.

To create a pagelet, complete the following steps:

1. In the Enterprise Menu on the left side of the portal, select **PeopleTools** --> **Portal** --> **Structure and Content**. The Structure and Content window opens.
2. In the list of folders, click **Portal Objects**.
3. Click **Pagelets** in the list of folders.
4. Click **Demo** in the list of folders. The current page defines the structure and content for demonstration pagelets. From this page, click **Add Content Reference** to define a new pagelet. You might have to scroll down to see **Add Content Reference**. The Content Ref Administration form displays.
5. Complete the Content Ref Administration form by supplying the values for the following fields (asterisks (*) indicate a required field):

***Name**

Type the internal name of your pagelet, for example, IBM_CM_LOOSE_LOGIN.

***Label** Specify the label for the pagelet title, for example, Loose Association. This label also appears in the list of content references of pagelets.

Usage Type

Select **Pagelet**.

***Node Name**

Select **Always use local**.

URL Type

Select **PeopleSoft Script**.

***Record (Table) Name**

Specify the name of your Web library record, for example, WEBLIB_LOOSEREC.

***Field Name**

Specify the name of your field, for example, LOOSEFIELD.

***PeopleCode Event Name**

Select **FieldFormula**.

***PeopleCode Function Name**

Select the name of your iScript, for example, IScript_CMLOOSELOG.

Attention: Some of the fields above might be hidden to you until you choose the appropriate values.

6. Set the security level for the pagelet:
 - a. On the top of this Content Ref Administration form, click the **Security** tab.
 - b. Select **Public** as the **Access Type**.
7. Click **Save**. If you want to add this pagelet to a tab, continue with step 8. Otherwise, the pagelet configuration on this portal is completed. Skip to step 9 on page 51.
8. **Optional:** Add the pagelet to a new tab:

- a. In the Enterprise Menu on the left side of the portal, select **PeopleTools --> Portal --> Structure and Content**. The Structure and Content window opens.
- b. In the list of folders, click **Portal Objects**.
- c. Click **Homepage** from the list of folders. On the next window, click the **Tabs** folder. The page that you now see defines the structure and content for tabs on the PeopleSoft portal home page. From this page, click **Add Content Reference** to define a new tab.
- d. Complete the Content Ref Administration form by supplying the values for the following fields (asterisks (*) indicate a required field):

***Name**

Type the internal name of your tab, for example, IBM_CM_TAB.

***Label** Specify the label for the tab title, for example, IBM CM. This label also appears in the list of content references of tabs.

Sequence Number

Specify a number that positions your tab on the portal. On the page that represents the structure and content for tabs (back one page), you can see the sequence numbers of the other tabs. The first tab will be at 0 and the second tab will be at 10. Choose a sequence number that is not already in use. For example, if you want your tab to be third, specify 20.

Usage Type

Select **Homepage tab**.

Attention: Some of the fields above might be hidden to you until you choose the appropriate values.

- e. On the top of this Content Ref Administration form, click the **Security** tab.
 - f. Select **Public** as the **Access Type**.
 - g. On the top of this Content Ref Administration form, click the **Tab Content** tab.
 - h. Find the **Demo** section, select the check box that corresponds to the label of the pagelet, for example, Loose Association, and select **Required**.
 - i. Click **Save**.
9. Close the Web browser.

Related tasks:

“Creating an iScript for loose association in the PeopleSoft Application Designer” on page 43

“Enabling security for the iScript code for loose association” on page 48

“Post pagelet configuration clean up” on page 53

Creating the IBM Content Manager login pagelet for optimized association:

This task assumes that you have already created an iScript and a record and have enabled security for the record.

To create a pagelet, complete the following steps:

1. In the Enterprise Menu on the left side of the portal, select **PeopleTools --> Portal --> Structure and Content**. The Structure and Content window opens.
2. In the list of folders, click **Portal Objects**.
3. Click **Pagelets** in the list of folders.

4. Click **Demo** in the list of folders. The current page defines the structure and content for demonstration pagelets. From this page, click **Add Content Reference** to define a new pagelet. You might have to scroll down to see **Add Content Reference**. The Content Ref Administration form displays.
5. Complete the Content Ref Administration form by supplying the values for the following fields (asterisks (*) indicate a required field):

***Name**

Type the internal name of your pagelet, for example, IBM_CM_OPT_LOGIN.

***Label** Specify the label to appear in the list of content references of pagelets. If you intend to define several pagelets for different servers, you might want to specify the server name and server type as the label, for example ICMNLSDB (FED).

Usage Type

Select **Pagelet**.

***Node Name**

Select **Always use local**.

URL Type

Select **PeopleSoft Script**.

***Record (Table) Name**

Specify the name of your Web library record, for example, WEBLIB_OPT_REC.

***Field Name**

Specify the name of your field, for example, OPT_FIELD.

***PeopleCode Event Name**

Select **FieldFormula**.

***PeopleCode Function Name**

Select the name of your iScript, for example, IScript_CM_OPTLOG1.

6. Set the security level for the pagelet:
 - a. On the top of this Content Ref Administration form, click the **Security** tab.
 - b. Select **Public** as the **Access Type**.
7. Click **Save**. If you want to add this pagelet to a tab, continue with step 8 on page 50. Otherwise, the pagelet configuration on this portal is completed. Skip to step 9 on page 51.
8. **Optional:** Add the pagelet to a new tab:
 - a. In the Enterprise Menu on the left side of the portal, select **PeopleTools --> Portal --> Structure and Content**. The Structure and Content window opens.
 - b. In the list of folders, click **Portal Objects**.
 - c. Click **Homepage** from the list of folders. On the next window, click the **Tabs** folder. The page that you now see defines the structure and content for tabs on the PeopleSoft portal home page. From this page, click **Add Content Reference** to define a new tab.
 - d. Complete the Content Ref Administration form by supplying the values for the following fields (asterisks (*) indicate a required field):

***Name**

Type the internal name of your tab, for example, IBM_CM_TAB.

***Label** Specify the label for the tab title, for example IBM CM. This label also appears in the list of content references of tabs.

Sequence Number

Specify a number that positions your tab on the portal. On the page that represents the structure and content for tabs (back one page), you can see the sequence numbers of the other tabs. The first tab will be at 0 and the second tab will be at 10. Choose a sequence number that is not already in use. For example, if you want your tab to be third, specify 20.

Usage Type

Select **Homepage tab**.

- e. On the top of this Content Ref Administration form, click the **Security tab**.
 - f. Select **Public** as the **Access Type**.
 - g. On the top of this Content Ref Administration form, click the **Tab Content tab**.
 - h. Find the **Demo** section, select the check box that corresponds to the label of the pagelet, for example, ICMNLSDB (FED), and select **Required**.
 - i. Click **Save**.
9. Close the Web browser.

Related tasks:

“Creating an iScript for optimized integration in the PeopleSoft Application Designer” on page 45

“Enabling security for the iScript code for optimized association” on page 49

“Post pagelet configuration clean up”

Post pagelet configuration clean up

This task assumes that you have created a pagelet and that you are ready to use it.

You need to clear the browser cache to prevent it from using old information and begin using your new settings.

1. Stop the WebSphere application server.
2. Stop the PeopleSoft application server.
3. Delete the PeopleSoft application server cache: *PS_HOME*\appserv*PSEP*\cache, where *PS_HOME* is the location where you installed the PeopleSoft files and *PSEP* is the name of the PeopleSoft version that you use, for example, PeopleSoft 8.40 would be PSEP84.
4. Delete the WebSphere PeopleSoft server cache:
WebSphere\AppServer\installedApps\peoplesoft\portal\ps\cache, where *WebSphere* is where you installed the WebSphere files.
5. Start the PeopleSoft application server.
6. Start the WebSphere application server.

Related tasks:

“Creating the IBM Content Manager login pagelet for loose association” on page 50

“Creating the IBM Content Manager login pagelet for optimized association” on page 51

Configuring Siebel Integration for IBM Content Manager

This section provides steps that you must complete to allow Siebel to work together with the Content Manager eClient.

Configuring WebSphere Application Server to run the eClient

You need to ensure that the WebSphere Application Server (WAS) session timeout value is appropriately set for the Siebel user community. Start WAS and set the session timeout value before running the eClient.

Procedure:

Step 1: Launching WebSphere Administrator's Console

To launch WebSphere Administrator's Console on Windows, select **Start --> Programs --> IBM WebSphere --> Application Server V4.0 --> Administrator's Console**.

To launch WebSphere Administrator's Console on AIX and Sun Solaris, follow these steps:

1. Open a new terminal.
2. At the prompt, enter `WebSphere/AppServer/bin`, where *WebSphere* is the root directory where your WebSphere application server is installed.
3. Enter: `./adminclient.sh host_name portnumber` (for example, `./adminclient.sh localhost 900`).

Step 2: Set Session Timeout Value for WebSphere

1. Select **WebSphere Administrative Domain --> Nodes --> Host Name --> Application Servers --> eClient_server**.
2. When the application server properties are displayed in the Properties View window, click **Services**.
3. From the list of services, select **Session Manager Service**, and click **Edit Properties**.
4. In the Session Manager Service window, click the **Advanced** tab.
5. Select **Set Timeout**, and set the value for **Invalidation Timeout** in minutes. This value must be at least two minutes.
6. Click **OK**.
7. Click **General**.
8. Click **Environment**.
9. Click **OK**.
10. Click **Apply**.
11. Restart the eClient application server to ensure that the change becomes effective immediately.

After you configure WebSphere application server, you can proceed to "Configuring the eClient".

Related task:

"Configuring the eClient"

Configuring the eClient

To configure the eClient, you need to specify values for the properties in the IP file.

Procedure:

1. Use a text editor to open the IP file.
2. Specify values for four required properties in the IP file.

eClientToken

Specify an eClientToken property value to control access to the content servers. This value is provided in a URL by the Siebel application when it attempts to access any supported content servers. The Siebel Integration for IBM Content Manager then compares the token provided in the URL with the token in the IP file. Content Manager permits access only to unstructured data when these two tokens match. This ensures that the URL originated from a Siebel server intended to have access to the Content Manager datastore.

The eClientToken property is case-sensitive. Valid characters are any of the ISO8859-1 Latin 1 characters with the exception of the following characters, which are reserved for use within the query string of a URL:

;
/
?
:
@
&
=
+
,
\$

Example:

eClientToken=integrator

type The type property specifies the look and feel of the Web pages that are produced by the JavaServer Pages. For Siebel Integration for IBM Content Manager, set type to 1. If you specify any other value, the Web pages produced by the JavaServer Pages will not have the look and feel of the Siebel user interface.

cssPrefix

The cssPrefix property specifies a file name prefix for the cascading style sheet file used by the JavaServer Pages for integration with Siebel. For Siebel Integration for IBM Content Manager, set the cssPrefix property to alt1.

iconPrefix

The iconPrefix property specifies a file name prefix for the icon files used by the JavaServer Pages for integration with Siebel. For Siebel Integration for IBM Content Manager, set the iconPrefix property to alt1.

3. **Optional:** Specify the value for the printEnabled property. The printEnabled property specifies whether a print capability is included in the toolbar of the document viewers. It can be set to true or false. The default value is true.
4. Specify values for three optional properties--server, userid, and password. You can either specify them as properties in the IP file or specify them as arguments in the URL within the calculated field of a business component. If you specify them in both places, the values in the calculated field take precedence over the values in the IP file.

server

The server property specifies the name of the federated server database that is accessed by the Siebel Integration for IBM Content Manager servlet.

Example:

```
server=icm1sdb
```

userid

By setting the userid property, you specify the user ID that is used to access the federated server database.

Example:

```
userid=newuser
```

password

The password property specifies the password for the user ID that is used to access the federated server database.

Example:

```
password=password
```

5. **Optional:** If you plan to use the eClient viewer applet, follow these steps to configure your browser environment:
 - a. Ensure that JRE 1.4 is installed properly:
 - 1) Install the Java 2 Runtime Environment SE v 1.4.0_02 on your browser machine.
 - 2) Designate the Java plug-in as the default Java run-time for Microsoft Internet Explorer.
 - b. Ensure that Microsoft Internet Explorer is configured properly:
 - 1) Select **Tools --> Internet Options --> Advanced**.
 - 2) In the Settings list, find the section with heading Java (Sun), and un-check the check box titled "Use Java 2 v 1.4.0_02 for <applet>" (requires restart).

Note: The IP file name is included within the calculated field values specified when you configure Siebel. Therefore, if you change the IP file name, make sure that you also change the IPFile argument values in the calculated fields as needed. If you use the symbolic URL to configure Siebel 7.5.2, make sure that you change the IPFile argument values in the symbolic URLs.

Related tasks:

"Configuring WebSphere Application Server to run the eClient" on page 54

"Customizing and configuring Siebel 7.0.4"

"Task 1: Customizing the business objects layer" on page 58

"Customizing and configuring Siebel 7.5.2" on page 69

"Task 1: Configuring a business component to handle external data using a symbolic URL" on page 70

Customizing and configuring Siebel 7.0.4

Introduction to customizing and configuring Siebel 7.0.4: If you are using Siebel 7.0.4, you must specify a URL within the calculated field of a Siebel business component. Configuration of Siebel 7.0.4 consists of three tasks: customizing the business objects layer, customizing the user interface layer, and configuring the Siebel application.

Prerequisites:

To successfully configure Siebel 7.0.4, verify that you have:

- Created an Enterprise Information Portal federated server
- Set up a Content Manager server (Content Manager Version 7, Content Manager Version 8, Content Manager OnDemand for Multiplatforms Version 7.1, Content Manager OnDemand for OS/390 Version 2.1, Version 7.1, Content Manager OnDemand for OS/400 Version 4.5, Version 5.1, or ImagePlus for OS/390 Version 7.1) using the EIP system administration client or equivalent application
- Created item types
- Imported data into your Content Manager server(s)
- Created federated entities and search templates in EIP
- Created Siebel users on Windows

Recommendation:

Archive the Siebel repository objects that you plan to change. If you need to remove the Siebel Integration for IBM Content Manager later, you can import these archived object definitions to restore your Siebel application environment to the level that existed prior to this configuration.

During the configuration process, you need to set values for multiple objects (such as the applet name and the value of the calculated field). On several occasions, you need to use a value that you previously set to define a new object. Therefore, it is highly recommended that you keep a record of all the values that you set.

This document includes an example to help you understand the process of configuring Siebel 7.0.4 to access unstructured data that is stored in Content Manager. This example provides specific values for field settings within each step of each task. For example, within Step 1 of Task 2:

Name Provide a meaningful name (in our example, Applet Web Page Calc Value).

This example assumes that you set the following values to the arguments in the calculated field during the configuration process:

host name

eipserver

port number

80

eClient application name

eClient82

eClientToken

token

IPFile Siebel

search template

2k_DriverLicense

This example also assumes that you have set up a user John Smith in Siebel, and set the language to English in all applications and services.

Related tasks:

“Configuring the eClient” on page 54

“Validating your configured environment” on page 85

“Task 1: Customizing the business objects layer”

Task 1: Customizing the business objects layer: In order to associate unstructured data managed by IBM Content Manager with a Siebel entity, you must add a calculated field to a business component for that entity.

Follow these steps to add a calculated field to a business component:

1. Launch **Siebel Tools**.
2. In Object Explorer, select **Siebel Objects --> Business Component**.
3. In the Business Components window, select a business component (in our example, Service Request). This record is highlighted after you select it.
4. From the menu, select **Tools --> Lock Project**.
5. In Object Explorer, select **Business Component --> Field**. The Fields window opens, and all fields in the selected business component (in our example, Service Request) are displayed.
6. In the Fields window, right-click and select **New Record**. A blank new record displays above all existing records.
7. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide a meaningful name (in our example, Archived Content).

Calculated

TRUE

Note: The value TRUE is represented as a checkmark in the interface. This applies to all occurrences of TRUE.

Calculated Value

Provide a valid calculated value (in our example, "<iframe height=300 width=960 frameborder=0 src='http://eipserver:80/eClient82/IDMIntegrator? eClientToken=token&IPFile=Siebel&Entity= 2k_DriverLicense &Lastname="[Contact Last Name]"+&ReleaseLevel=SIEBELV704'> </iframe>"). See “Calculated value property” for more information on how to define a calculated value for a calculated field.

Type DTYPE_TEXT

Use Default Sensitivity

TRUE

8. Move your cursor off of this record to commit it.

Calculated value property: This calculated value property contains an IFRAME HTML tag with an src attribute that contains a URL for invoking the integration servlet. The calculated value property is generally in this form:

```
<iframe height=height width=width frameborder=0
src='http://hostname:port/eClientApp/IDMIntegrator?
eClientToken=eClientToken&IPFile=IPFilename&
Entity=Entity&SearchCriterionName=SearchCriterionValue&
ReleaseLevel=SIEBELV704&server=Server&userid=UserID
&password=Password'>
Sorry your browser does not support IFRAMES.</iframe>
```

Explanation of variables used in the above syntax:

height The value of the height attribute for the IFRAME

width The value of the width attribute for the IFRAME

hostname:port

The hostname and port to use for access to the eClient application server

eClientApp

eClient application name

eClientToken

The value of the eClientToken property specified in the IP file

IPFilename

Name of the IP file

Entity Name of the search template

SearchCriterionName=SearchCriterionValue

Name value pair of search criterion name and search criterion value

Server Name of federated server database

UserID

User ID to be used to access the federated server database

Password

Password to be used to access the federated server database

The following arguments are required in the calculated field:

eClientToken

A Siebel application must provide the eClientToken value in a URL when attempting to access Content Manager. The Siebel Integration for IBM Content Manager compares the token provided in the URL with the token specified in the IP file to control access to the data managed by the content servers. The value that you specify for the eClientToken is case-sensitive.

IPFile The value for IPFile argument specifies the name of the IP file.

Entity The value for the Entity argument specifies the name of the search template for the federated search. Search template names are case-sensitive.

search criterion name=search criterion value

Each search criterion consists of a name value pair. The search criterion name is any valid name defined for the specified search template. The search criterion value is any valid value for that search criterion name.

Typically, the search criterion value is the name of a field within the business component record that contains the calculated field. The name of the field is specified using the following syntax: "+[field_name]+" where *field_name* is the name of the field within the business component record. When the calculated field value is determined, the value of the field within the current business component record is used for the search criterion value.

The search criterion value need not be the name of a field within the business component record that contains the calculated field. It may be an expression built from field names, standard functions, and string, numeric, and logical operations. Refer to the Siebel Tools Reference for additional details.

An evaluated search criterion value must be a federated attribute value.

Note: In the syntax of search criterion name--"search criterion name=search criterion value", only the equal (=) operator is supported. Search criteria are case-sensitive.

ReleaseLevel

The value for ReleaseLevel argument specifies the release level of the Siebel application. When using Siebel 7.0.4, the ReleaseLevel value is SIEBELV704.

The following arguments are optional if you specified the server, userid, and password properties in the IP file. If you specify them in both the calculated field and the IP file, the values in the calculated field take precedence over the values in the IP file.

server The server argument specifies the name of the federated server database to be accessed.

userid The userid argument specifies the user ID that is to be used to access the federated server database.

password

The password argument specifies the password that is to be used to access the federated server database.

The maximum length of the calculated value property of a calculated field within a business component is 255 bytes. To specify an expression that is longer than 255 bytes, you must define the calculated value property as a concatenation of other calculated value properties each having a length that is less than or equal to 255.

Example: Consider the following example of a calculated value property for a field named Archived Content of a business component named Service Request, which references the SR Number field of the Service Request business component. This calculated value property exceeds 255 bytes, and cannot be entered into the **Calculated Value** field within the calculated field. Therefore, you should specify it as [AC1] + [SR Number] + [AC3], where AC1 and AC3 are the names of other calculated fields within the Service Request business component.

- Calculated value property for calculated field AC1:

```
"<iframe height=300 width=960 frameborder=0 src='http://ec82fvt:80/eClient82/IDMIntegrator?eClientToken=token&IPFile=Siebel&Entity=SRST&RN="
```

- Calculated value property for calculated field AC3:

```
"&ReleaseLevel=SIEBELV704&server=eipserver&userid=newuser&password=password">Sorry your browser does not support IFRAMES.</iframe>"
```

Related concept:

"Introduction to customizing and configuring Siebel 7.0.4" on page 56

Related tasks:

"Task 2: Customizing the user interface layer"

"Step 1: Creating a Web template object" on page 61

Task 2: Customizing the user interface layer:

Task overview: After you customize the business object layer, you must customize the user interface layer, so that the unstructured data that the eClient retrieves from content servers can be displayed to Siebel end users.

This task consists of 11 steps:

- “Step 1: Creating a Web template object”
- “Step 2: Creating a Web template file object”
- “Step 3: Creating an applet” on page 62
- “Step 4: Creating an applet control” on page 62
- “Step 5: Creating an applet Web template” on page 63
- “Step 6: Creating an applet Web template item” on page 64
- “Step 7: Creating a view” on page 64
- “Step 8: Creating a view Web template” on page 65
- “Step 9: Creating view Web template items” on page 65
- “Step 10: Updating the screen object” on page 66
- “Step 11: Compiling” on page 67

Step 1: Creating a Web template object:

1. In Object Explorer, select **Siebel Objects --> Web Template**. The Web Templates window opens.
2. Right-click and select **New Record**. A blank new record appears above all existing records.
3. Scroll over this record to set values for the following fields and keep the default values for all other fields:
 - Name** Provide a meaningful name (in our example, Applet Web Page Calc Value).
 - Project** Provide the name of the project for the business component being modified (in our example, Service).
 - Type** Applet Template - Form
4. Move off of this record to commit it.

Related concept:

“Task overview” on page 60

Related task:

“Step 2: Creating a Web template file object”

Step 2: Creating a Web template file object:

1. Select the Web template object that you created in “Step 1: Creating a Web template object”.
2. In Object Explorer, select **Siebel Objects --> Web Template --> Web Template File**. The Web Template Files window opens.
3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:
 - Name** Provide the same name as the name of the Web template created in “Step 1: Creating a Web template object” (in our example, Applet Web Page Calc Value).
 - File Name** EIP81Applet.swt
5. Move off of this record to commit it.

Related concept:

“Task overview” on page 60

Related task:

“Step 1: Creating a Web template object” on page 61

“Step 3: Creating an applet”

Step 3: Creating an applet:

1. In Object Explorer, select **Siebel Objects** --> **Applet**. The Applets window opens.
2. Right-click and select **New Record**. A blank new record appears above all existing records.
3. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide a meaningful name (in our example, Service Request Archived Content Applet).

Project

Provide the project name for the business component being modified (in our example, Service).

Business Component

Provide the name of the business component to which you added the calculated field in “Task 1: Customizing the business objects layer” on page 58 (in our example, Service Request).

Class CSSFrameBase

Title Provide a meaningful name. This can be the same name as the calculated field (in our example, Archived Content).

Type Standard

4. Move off of this record to commit it.

Related concept:

“Task overview” on page 60

Related tasks:

“Step 2: Creating a Web template file object” on page 61

“Step 4: Creating an applet control”

Step 4: Creating an applet control:

1. Select the applet that you created in “Step 3: Creating an applet”.
2. In Object Explorer, select **Siebel Objects** --> **Applet** --> **Control**. The Controls window opens.
3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide the same name as the name of the calculated field (in our example, Archived Content).

Display Format

HTML Text

Field Provide the same name as the name of the calculated field (in our example, Archived Content).

HTML Display Mode
DontEncodeData

HTML Only
TRUE

HTML Row Sensitive
TRUE

HTML Type
Field

Read Only
TRUE

Sort TRUE

Text Alignment
Left

Visible
TRUE

5. Move off of this record to commit it.

Related concept:

“Task overview” on page 60

Related tasks:

“Step 3: Creating an applet” on page 62

“Step 5: Creating an applet Web template”

Step 5: Creating an applet Web template:

1. Select the applet that you created in “Step 3: Creating an applet” on page 62.
2. In Object Explorer, select **Siebel Objects --> Applet --> Applet Web Template**. The Applet Web Templates window opens.
3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Base

Type Base

Web Template

Provide the name of the Web Template Object created in “Step 1: Creating a Web template object” on page 61 (in our example, Applet Web Page Calc Value).

5. Move off of this record to commit it.

Related concept:

“Task overview” on page 60

Related tasks:

“Step 4: Creating an applet control” on page 62

“Step 6: Creating an applet Web template item” on page 64

Step 6: Creating an applet Web template item:

1. Select the applet Web template that you created in “Step 5: Creating an applet Web template” on page 63.
2. In Object Explorer, select **Siebel Objects --> Applet --> Applet Web Template --> Applet Web Template Item**. The Applet Web Template Items window opens.
3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide the same name as the calculated field created in “Task 1: Customizing the business objects layer” on page 58 (in our example, Archived Content).

Control

Select the applet control created in “Step 4: Creating an applet control” on page 62 (in our example, Archived Content).

Item Identifier

1301

Type Control

5. Move off of this record to commit it.

Related concept:

“Task overview” on page 60

Related tasks:

“Step 5: Creating an applet Web template” on page 63

“Step 7: Creating a view”

Step 7: Creating a view:

1. In Object Explorer, select **Siebel Objects --> View**. The Views window opens.
2. Right-click and select **New Record**. A blank new record appears above all existing records.
3. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide a meaningful name (in our example, Service Request Detail Archived Content View).

Project

Provide the name of the business component you are modifying (in our example, Service).

Business Object

Select the business object that corresponds to the screen where this view will be placed. This is typically the business object for the business component that was modified in “Task 1: Customizing the business objects layer” on page 58 (in our example, Service Request).

Screen Menu

TRUE

Title Provide a meaningful title (in our example, Service Request Archived Content).

Thread Applet

Provide the name of the applet that provides the data value for the thread field (in our example, Service Request Detail Applet).

Thread Field

Provide the name of the field whose data value is included in the arrow box, following the Thread Title (in our example, SR Number).

Thread Title

Provide the text used in the thread to identify the view (in our example, SR#:).

4. Move off of this record to commit it.

Related concept:

“Task overview” on page 60

Related tasks:

“Step 6: Creating an applet Web template item” on page 64

“Step 8: Creating a view Web template”

Step 8: Creating a view Web template:

1. Select the view that you created in “Step 7: Creating a view” on page 64.
2. In Object Explorer, select **Siebel Objects --> View --> View Web Template**. The View Web Templates window opens.
3. In the View Web Templates window, right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Base

Web Template

View Detail

5. Move off of this record to commit it.

Related concept:

“Task overview” on page 60

Related tasks:

“Step 7: Creating a view” on page 64

“Step 9: Creating view Web template items”

Step 9: Creating view Web template items: You must create a view Web template item for each applet being displayed in the view. In our example, we are adding the Service Request Detail Applet and our new applet, the Service Request Archived Content Applet, to our view. Therefore, we are creating two view Web template items for the two applets being displayed in our view.

Follow these steps to create each view Web template item:

1. Select the view Web template that you created in “Step 8: Creating a view Web template”.
2. In Object Explorer, select **Siebel Objects --> View --> View Web Template --> View Web Template Item**. The View Web Template Items window opens.

3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide a meaningful name (in our example, Service Request Detail Applet for the first view Web template item and Service Request Archived Content Applet for the second view Web template item).

Item Identifier

An item identifier provides the mapping to a control within a Siebel Web template (.swt) file (in our example, 1 for the first view Web template item and 2 for the second view Web template item).

Applet

Provide the name of the applet being included in this view (in our example, Service Request Detail Applet for the first view Web template item and Service Request Archived Content Applet, the name of the applet created in “Step 3: Creating an applet” on page 62 for the second view Web template item).

Applet Mode

Provide the mode to be used for the applet when rendering the view (in our example, Edit for the first view Web template item and Base for the second view Web template item).

5. Move off of this record to commit it.

Related concept:

“Task overview” on page 60

Related tasks:

“Step 8: Creating a view Web template” on page 65

“Step 10: Updating the screen object”

Step 10: Updating the screen object:

1. In Object Explorer, select **Siebel Objects --> Screen**. The Screens window opens.
2. Select the screen into which you want to add the view created in “Step 7: Creating a view” on page 64 (in our example, Service Request Screen).
3. Select **Tools --> Lock Project**.
4. Expand **Screen** and select **Screen View**. The Screen Views window opens.
5. Right-click and select **New Record**. A blank new record appears above all existing records.
6. Scroll over this record to set values for the following fields and keep the default values for all other fields:

View Provide the name of the view that you created in “Step 7: Creating a view” on page 64 (in our example, Service Request Detail Archived Content View).

Category Menu Text

Provide the text that you want to display in the **category** menu in Siebel (in our example, Archived Content).

Category Viewbar Text

Provide the text that you want to display in the category viewbar in Siebel (in our example, Archived Content).

Menu Text

Provide the text that you want to display in the menu in Siebel (in our example, Archived Content).

Viewbar Text

Provide the text that you want to display on the viewbar tab in Siebel (in our example, Archived Content).

Sequence

Provide a number that places the view tab in the desired location in the screen of the Siebel application (in our example, 292).

7. Move off of this record to commit it.

Related concept:

“Task overview” on page 60

Related tasks:

“Step 9: Creating view Web template items” on page 65

“Step 11: Compiling”

Step 11: Compiling:

1. Select **Tools** --> **Compile Project**. The Object Compiler window opens.
2. Under **Projects**, select **Locked Projects**.
3. In the text field to the left of **Browse**, specify the path to the target directory for the SRF file (in our example, C:\sea703\client\OBJECTS\ENU\).
4. Click **Compile**.
5. Select **Tools** --> **Unlock Project** to unlock the locked projects.
6. Exit **Siebel Tools**.

Related concepts:

“Introduction to customizing and configuring Siebel 7.0.4” on page 56

“Task overview” on page 60

Related task:

“Step 10: Updating the screen object” on page 66

Task 3: Configuring the Siebel application:

Task overview: After you configure the user interface layer, you must configure the Siebel application for the integration with the IBM Content Manager portfolio product.

This task consists of 3 steps:

- “Step 1: Logging on to the Siebel Call Center as an administrator”
- “Step 2: Setting up a new view in the Siebel Call Center” on page 68
- “Step 3: Creating a responsibility” on page 68

Step 1: Logging on to the Siebel Call Center as an administrator: Follow these steps to log on to the Siebel Call Center as an administrator:

1. Select **Start** --> **Programs** --> **Siebel Client 7.0.4** --> **Siebel Call Center-ENU**.
2. Enter your administrator user ID and password.
3. Select **Connect to** --> **Server**.

Related concept:

“Task overview” on page 67

Related task:

“Step 2: Setting up a new view in the Siebel Call Center”

Step 2: Setting up a new view in the Siebel Call Center: Follow these steps to set up a new view in the Siebel Call Center:

1. Select **View --> Site Map --> Application Administration**.
2. Select **Views**.
3. Click **New**.
4. Set values for the following fields:

Name Provide the name of the view that you created in “Step 7: Creating a view” on page 64 (in our example, Service Request Detail Archived Content View).

Description

Provide a description for this view (in our example, View for Siebel Integration for IBM Content Manager).

5. Move off of this view to commit it.

Related concept:

“Task overview” on page 67

Related task:

“Step 1: Logging on to the Siebel Call Center as an administrator” on page 67

“Step 3: Creating a responsibility”

Step 3: Creating a responsibility:

1. Select **View --> Site Map --> Application Administration --> Responsibilities**.
2. Click **New**.
3. Provide the following information:

Responsibility

Provide a name for the responsibility (in our example, Call Center Manager for Content Manager).

Description

Provide a description for this responsibility.

Organization

Default Organization

4. Move off of this record to commit it.
5. From the User window, select a user (in our example, John Smith).
6. From the View window, select **Service Request Detail Archived Content View**.
7. Move off this record to commit it.
8. Log off of the Siebel Call Center.

Related concepts:

“Introduction to customizing and configuring Siebel 7.0.4” on page 56

“Task overview” on page 67

Related task:

“Step 2: Setting up a new view in the Siebel Call Center” on page 68

After completing all above tasks, proceed to “Validating your configured environment” on page 85.

Customizing and configuring Siebel 7.5.2

Introduction to customizing and configuring Siebel 7.5.2: You can customize and configure Siebel 7.5.2 in two ways:

- Use the same approach as the one used for Siebel 7.0.4--specify a URL within the calculated field of a Siebel business component. If you choose this option, follow the instructions in “Customizing and configuring Siebel 7.0.4” on page 56.
Note: When creating the Calculated Value field value, use SIEBELV75 for the ReleaseLevel argument value.
- Use the Siebel 7.5.2 portal framework to define a symbolic URL within the calculated field of a Siebel business component.

This section describes how to use the portal framework to configure Siebel 7.5.2.

Siebel 7.5.2 provides portal agents that allow you to integrate external data (for example, unstructured data that are managed by Content Manager) into the Siebel user interface. You use a symbolic URL to configure a calculated field in the business component to handle external data. Then, you configure an applet to display the external HTML content inside of the applet container within a view.

Configuration of Siebel 7.5.2 consists of three tasks: Configuring a business component to handle external data using a symbolic URL, displaying external content within an applet, and configuring the Siebel application.

Prerequisites:

To successfully configure Siebel 7.5.2, verify that you have:

- Created an Enterprise Information Portal federated server
- Set up a Content Manager server (Content Manager Version 7, Content Manager Version 8, Content Manager OnDemand for OS/390 Version 2.1, Version 7.1, Content Manager OnDemand for Multiplatforms Version 7.1, Content Manager OnDemand for iSeries Version 4.5, Version 5.1, or ImagePlus for OS/390 Version 7.1) using the EIP system administration client or equivalent application
- Created item types
- Imported data into your Content Manager server(s)
- Created federated entities and search templates in EIP
- Created Siebel users on Windows

Recommendation:

Archive the Siebel repository objects that you plan to change. If you need to remove the Siebel Integration for IBM Content Manager later, you can import these archived object definitions to restore your Siebel application environment to the level that existed prior to this configuration.

During this process, you need to set values for multiple objects (such as the applet name and the value of the calculated field). On several occasions, you need to use a value that you previously set to define a new object. Therefore, it is highly recommended that you keep a record of all the values that you set.

This document includes an example to help you understand how to configure Siebel 7.5.2 to access unstructured data that are stored in a content server. This example provides specific values for field settings within each step of each task. For example, within Step 1 of Task 2:

Name Provide a meaningful name (in our example, Applet Web Page Calc Value)

This example assumes that you have set the following values for the arguments in the calculated field during the configuration process:

host name

eipserver

port number

80

eClient application name

eClient82

eClientToken

token

IPFile Siebel

search template

2k_DriverLicense

This example also assumes that you have set up a user John Smith in Siebel, and set the language to English in all applications and services.

Related tasks:

“Configuring the eClient” on page 54

“Validating your configured environment” on page 85

“Task 1: Configuring a business component to handle external data using a symbolic URL”

Task 1: Configuring a business component to handle external data using a symbolic URL: To configure business components to handle external data using a symbolic URL, you need to create a new calculated field in the business component. Rather than representing structured content such as records in a database, this field represents the HTML content sent from an external host.

Follow these steps to create a calculated field in the business component:

1. Launch **Siebel Tools**.
2. In Object Explorer, select **Siebel Objects --> Business Component**.
3. In the Business Components window, select a business component (in our example, Service Request).
4. From the menu, select **Tools --> Lock Project**.
5. In Object Explorer, select **Business Component --> Field**. The Fields window opens, displaying all of the fields in the selected business component (in our example, Service Request).
6. In the Fields window, right-click and select **New Record**. A blank new record appears above all existing records.
7. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide a meaningful name (in our example, Archived Content).

Calculated

TRUE

Note: The value TRUE is represented as a checkmark in the interface. This applies to all occurrences of TRUE.

Calculated Value

Enter the name of the symbolic URL (enclosed in double quotes) that you want to use to submit the HTTP request (in our example, "SRSU").

Type DTYPE_TEXT**Use Default Sensitivity**

TRUE

Related concept:

"Introduction to customizing and configuring Siebel 7.5.2" on page 69

Related tasks:

"Task 2: Displaying external content within an applet"

"Step 1: Creating a Web template object"

Task 2: Displaying external content within an applet:

Task Overview: After you create the calculated field for the business component, you use a control in a form applet to expose it in the user interface.

This task consists of 11 steps:

"Step 1: Creating a Web template object"

"Step 2: Creating a Web template file object" on page 72

"Step 3: Creating an applet" on page 72

"Step 4: Creating an applet control" on page 73

"Step 5: Creating an applet Web template" on page 74

"Step 6: Creating an applet Web template item" on page 74

"Step 7: Creating a view" on page 75

"Step 8: Creating a view Web template" on page 75

"Step 9: Creating view Web template items" on page 76

"Step 10: Updating the screen object" on page 77

"Step 11: Compiling" on page 77

Step 1: Creating a Web template object:

1. In Object Explorer, select **Siebel Objects** --> **Web Template**. The Web Templates window opens.
2. Right-click and select **New Record**. A blank new record appears above all existing records.
3. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide a meaningful name (in our example, Applet Web Page Calc Value).

Project

Provide the name of the project for the business component being modified (in our example, Service).

Type Applet Template - Form

4. Move off of this record to commit it.

Related concept:

“Task Overview” on page 71

Related task:

“Step 2: Creating a Web template file object”

Step 2: Creating a Web template file object:

1. Select the Web template object that you created in “Step 1: Creating a Web template object” on page 71.
2. In Object Explorer, select **Siebel Objects --> Web Template --> Web Template File**. The Web Template Files window opens.
3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide the same name as the name of the Web template created in “Step 1: Creating a Web template object” on page 71 (in our example, Applet Web Page Calc Value).

File Name

EIP81Applet.swt

5. Move off of this record to commit it.

Related concept:

“Task Overview” on page 71

Related tasks:

“Step 1: Creating a Web template object” on page 71

“Step 3: Creating an applet”

Step 3: Creating an applet:

1. In Object Explorer, select **Siebel Objects --> Applet**. The Applets window opens.
2. Right-click and select **New Record**. A blank new record appears above all existing records.
3. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide a meaningful name (in our example, Service Request Archived Content Applet).

Project

Provide the project name for the business component being modified (in our example, Service).

Business Component

Provide the name of the business component to which you added the calculated field in “Task 1: Configuring a business component to handle external data using a symbolic URL” on page 70 (in our example, Service Request).

Class CSSFrameBase

Title Provide a meaningful name. This can be the same name as the calculated field (in our example, Archived Content).

Type Standard

4. Move off of this record to commit it.

Related concept:

“Task Overview” on page 71

Related tasks:

“Step 2: Creating a Web template file object” on page 72

“Step 4: Creating an applet control”

Step 4: Creating an applet control:

1. Select the applet that you created in “Step 3: Creating an applet” on page 72.
2. In Object Explorer, select **Siebel Objects --> Applet --> Control**. The Controls window opens.
3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide the same name as the name of the calculated field (in our example, Archived Content).

Display Format

HTML Text

Field Provide the same name as the name of the calculated field (in our example, Archived Content).

Field Retrieval Type

Symbolic URL

HTML Display Mode

DontEncodeData

HTML Only

TRUE

HTML Row Sensitive

TRUE

HTML Type

Field

Read Only

TRUE

Sort

TRUE

Text Alignment

Left

Visible

TRUE

5. Move off of this record to commit it.

Related concept:

“Task Overview” on page 71

Related tasks:

“Step 3: Creating an applet” on page 72

“Step 5: Creating an applet Web template”

Step 5: Creating an applet Web template:

1. Select the applet that you created in “Step 3: Creating an applet” on page 72.
2. In Object Explorer, select **Siebel Objects --> Applet --> Applet Web Template**. The Applet Web Templates window opens.
3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Base

Type Base

Web Template

Provide the name of the Web Template Object created in “Step 1: Creating a Web template object” on page 71 (in our example, Applet Web Page Calc Value).

5. Move off of this record to commit it.

Related concept:

“Task Overview” on page 71

Related tasks:

“Step 4: Creating an applet control” on page 73

“Step 6: Creating an applet Web template item”

Step 6: Creating an applet Web template item:

1. Select the applet Web template that you created in “Step 5: Creating an applet Web template”.
2. In Object Explorer, select **Siebel Objects --> Applet --> Applet Web Template --> Applet Web Template Item**. The Applet Web Template Items window opens.
3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide the same name as the calculated field created in “Task 1: Configuring a business component to handle external data using a symbolic URL” on page 70 (in our example, Archived Content).

Control

Select the applet control created in “Step 4: Creating an applet control” on page 73 (in our example, Archived Content).

Item Identifier

1301

Type Control

5. Move off of this record to commit it.

Related concept:

“Task Overview” on page 71

Related tasks:

“Step 5: Creating an applet Web template” on page 74

“Step 7: Creating a view”

Step 7: Creating a view:

1. In Object Explorer, select **Siebel Objects --> View**. The Views window opens.
2. Right-click and select **New Record**. A blank new record appears above all existing records.
3. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide a meaningful name (in our example, Service Request Detail Archived Content View).

Project

Provide the name of the business component you are modifying (in our example, Service).

Business Object

Select the business object that corresponds to the screen where this view will be placed. This is typically the business object for the business component that was modified in “Task 1: Configuring a business component to handle external data using a symbolic URL” on page 70 (in our example, Service Request).

Screen Menu

TRUE

Title Provide a meaningful title (in our example, Service Request Archived Content).

Thread Applet

Provide the name of the applet that provides the data value for the thread field (in our example, Service Request Detail Applet).

Thread Field

Provide the name of the field whose data value is included in the arrow box, following the Thread Title (in our example, SR Number).

Thread Title

Provide the text used in the thread to identify the view (in our example, SR#:).

4. Move off of this record to commit it.

Related concept:

“Task Overview” on page 71

Related tasks:

“Step 6: Creating an applet Web template item” on page 74

“Step 8: Creating a view Web template”

Step 8: Creating a view Web template:

1. Select the view that you created in “Step 7: Creating a view”.
2. In Object Explorer, select **Siebel Objects --> View --> View Web Template**. The View Web Templates window opens.

3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Base

Web Template

View Detail

5. Move your cursor off of this record to commit it.

Related concept:

“Task Overview” on page 71

Related tasks:

“Step 7: Creating a view” on page 75

“Step 9: Creating view Web template items”

Step 9: Creating view Web template items: You must create a view Web template item for each applet that is displayed in the view. In our example, we are adding the Service Request Detail Applet and our new applet, the Service Request Archived Content Applet, to our view. Therefore, we are creating two view Web template items for the two applets that are displayed in our view.

Follow these steps to create each view Web template item:

1. Select the view Web template that you created in “Step 8: Creating a view Web template” on page 75.
2. In Object Explorer, select **Siebel Objects --> View --> View Web Template --> View Web Template Item**. The View Web Template Items window opens.
3. Right-click and select **New Record**. A blank new record appears above all existing records.
4. Scroll over this record to set values for the following fields and keep the default values for all other fields:

Name Provide a meaningful name (in our example, Service Request Detail Applet for the first view Web template item and Service Request Archived Content Applet for the second view Web template item).

Item Identifier

An item identifier provides the mapping to a control within a Siebel Web template (.swt) file (in our example, 1 for the first view Web template item and 2 for the second view Web template item).

Applet

Provide the name of the applet being included in this view (in our example, Service Request Detail Applet for the first view Web template item and Service Request Archived Content Applet, the name of the applet created in “Step 3: Creating an applet” on page 72 for the second view Web template item).

Applet Mode

Provide the mode to be used for the applet when rendering the view (in our example, Edit for the first view Web template item and Base for the second view Web template item).

5. Move off of this record to commit it.

Related concept:

“Task Overview” on page 71

Related tasks:

“Step 8: Creating a view Web template” on page 75

“Step 10: Updating the screen object”

Step 10: Updating the screen object:

1. In Object Explorer, select **Siebel Objects** --> **Screen**. The Screens window opens.
2. Select the screen into which you want to add the view created in “Step 7: Creating a view” on page 75 (in our example, Service Request Screen).
3. Select **Tools** --> **Lock Project**.
4. Expand **Screen** and select **Screen View**. The Screen Views window opens.
5. Right-click and select **New Record**. A blank new record appears above all existing records.
6. Scroll over this record to set values for the following fields and keep the default values for all other fields:

View Provide the name of the view that you created in “Step 7: Creating a view” on page 75 (in our example, Service Request Detail Archived Content View).

Category Menu Text

Provide the text you want to display in the **category** menu in Siebel (in our example, Archived Content).

Category Viewbar Text

Provide the text you want to display in the category tab in Siebel (in our example, Archived Content).

Menu Text

Provide the text you want to display in the menu in Siebel (in our example, Archived Content).

Viewbar Text

Provide the text you want to display on the viewbar tab in Siebel (in our example, Archived Content).

Sequence

Provide a number that places the view tab in the desired location in the screen of the Siebel application (in our example, 292).

7. Move off of this record to commit it.

Related concept:

“Task Overview” on page 71

Related tasks:

“Step 11: Compiling”

“Step 9: Creating view Web template items” on page 76

Step 11: Compiling:

1. Select **Tools** --> **Compile Project**. The Object Compiler window opens.
2. Under **Projects**, select **Locked Projects**.
3. In the text field to the left of **Browse**, specify the path to the target directory for the SRF file (in our example, C:\sea705\client\OBJECTS\ENU\).

4. Click **Compile**.
5. Select **Tools --> Unlock Project** to unlock the locked projects.
6. Exit **Siebel Tools**.

Related concept:

“Task Overview” on page 71

Related task:

“Step 10: Updating the screen object” on page 77

Task 3: Configuring the Siebel application:

Task overview: After you configure the user interface layer, you must configure the Siebel application for integration with IBM Content Manager server.

This task consists of eight steps:

- “Step 1: Logging on to the Siebel Call Center as an administrator”
- “Step 2: Defining the external data host”
- “Step 3: Defining a symbolic URL” on page 79
- “Step 4: Defining required symbolic URL arguments” on page 79
- “Step 5: Defining symbolic URL arguments (Optional)” on page 82
- “Step 6: Specifying an external Web application and defining login credentials (Optional)” on page 83
- “Step 7: Setting up a new view in the Siebel Call Center” on page 84
- “Step 8: Creating a responsibility” on page 84

Step 1: Logging on to the Siebel Call Center as an administrator: Follow these steps to log on to the Siebel Call Center as an administrator:

1. Select **Start --> Programs --> Siebel Client 7.5 --> Siebel Call Center-ENU**.
2. Enter your administrator user ID and password.
3. Select **Connect to --> Server**.

Related concept:

“Task overview”

Related task:

“Step 2: Defining the external data host”

Step 2: Defining the external data host: In this step, you define the external data host in the Host Administration view:

1. Launch **Siebel Call Center 7.5**.
2. From the menu, select **View --> Site Map --> Integration Administration --> Host Administration**.
3. Click **New**.
4. Provide the following information:

Name Specify the host name for the system where the eClient is installed. The host name should include the domain suffix (in our example, server.mycompany.com).

Virtual Name

Provide a user-defined name for the host (in our example, "eipserver").

Authentication Type

Leave this field blank.

Authentication Value

Leave this field blank.

Related concept:

"Task overview" on page 78

Related task:

"Step 1: Logging on to the Siebel Call Center as an administrator" on page 78

"Step 3: Defining a symbolic URL"

Step 3: Defining a symbolic URL: In this step, you define the symbolic URLs referenced in the calculated value fields of "Task 1: Configuring a business component to handle external data using a symbolic URL" on page 70.

1. From the menu, select **View --> Site Map --> Integration Administration --> Symbolic URL Administration**.
2. In the Symbolic URL Administration view, click **New**.
3. Provide the following information:

Name Provide the name of the symbolic URL (in our example, "SRSU").

URL Provide the URL for invoking the eClient Integration servlet. This URL has the following format: *URL scheme://virtual host name/eClient application name/IDMIntegrator* (in our example, `http://eipserver:80/eClient82/IDMIntegrator`).

Host Name

Provide the virtual name of the host defined in the Host Administration view in step 4 of "Step 2: Defining the external data host" on page 78 (in our example, `server.mycompany.com`).

Fixup Name

Default

Multivalued Treatment

Leave this field blank.

SSO Disposition

IFrame

Web Application

Leave this field blank.

Related concept:

"Task overview" on page 78

Related tasks:

"Step 2: Defining the external data host" on page 78

"Step 4: Defining required symbolic URL arguments"

Step 4: Defining required symbolic URL arguments: In this step, you define the arguments for the symbolic URL:

1. From the menu, select **Site Map --> Integration Administration --> Symbolic URL Administration**. The Symbolic URL Administration window opens.
2. Select the symbolic URL that you want to configure.
3. In the Symbolic URL Arguments applet, click **New**.
4. Provide the following information:

Name method

Required

Yes

Argument Type

Command

Argument Value

The Siebel Symbolic URL Administration offers two Argument value fields. Enter `PostRequest` in the first Argument value field, and leave the second value field blank.

Append as Argument

Yes

Sequence

1

5. Click **New**.
6. Provide the following information:

Name eClientToken

Required

Yes

Argument Type

Constant

Argument Value

Same as the `eClientToken` property value specified in the IP file (in our example, `token`). Siebel Integration for IBM Content Manager compares the token provided in the URL with the token specified in the IP file to control access to the data managed by the content servers. The `eClientToken` value is case-sensitive.

Append as Argument

Yes

Sequence

2

7. Click **New**.
8. Provide the following information:

Name IPFile

Required

Yes

Argument Type

Constant

Argument Value

Provide the name of your IP file (in our example, `Siebel`).

Append as Argument

Yes

Sequence

3

9. Click **New**.

10. Provide the following information:

Name ReleaseLevel

Required

Yes

Argument Type

Constant

Argument Value

Specify the release level of Siebel application server (in our example, SIEBELV75).

Append as Argument

Yes

Sequence

4

11. Click **New**.

12. Provide the following information:

Name Entity

Required

Yes

Argument Type

Constant

Argument Value

Provide the name of the federated search template that you defined using EIP system administration client (in our example, 2k_DriverLicense).

Append as Argument

Yes

Sequence

5

13. Define search criteria. For each search criterion, click **New**, and provide the following information:

Name Provide the search criterion name.

Required

Yes

Argument Type

Field or Constant

Use an argument type value of `Field` if the argument value is a field in the record for the Siebel entity. Use an argument type value of `Constant` if the argument value is a constant.

Argument Value

Provide the search criterion value (in our example, Contact Last Name).

Append as Argument

Yes

Sequence

<next sequence number>

Related concept:

“Task overview” on page 78

Related tasks:

“Step 3: Defining a symbolic URL” on page 79

“Step 5: Defining symbolic URL arguments (Optional)”

Step 5: Defining symbolic URL arguments (Optional): There are three optional symbolic URL arguments: server, userid, and password. You do not need to define them in the symbolic URL if you specified the server, userid, and password properties in the IP file. If you specify them in both the symbolic URL and the IP file, the values in the symbolic URL take precedence over the values in the IP file.

Follow these steps to define symbolic URL arguments:

1. In the Symbolic URL Administration window, click **New**.
2. Provide the following information:

Name server

Required

Yes

Argument Type

Constant

Argument Value

Provide the name of the server database to be accessed.

Append as Argument

Yes

Sequence

<next sequence number>

3. Click **New**.
4. Provide the following information:

Name userid

Required

Yes

Argument Type

If you are using the single sign-on capability of Siebel, set Argument Type to Command, otherwise, set Argument Type to Constant.

Argument Value

If Argument Type is Command, specify UserLoginID. If Argument Type is Constant, specify the user ID that is to be used to access the server database.

Append as Argument

Yes

Sequence

<next sequence number>

5. Click **New**.
6. Provide the following information:

Name password

Required

Yes

Argument Type

If you are using the single sign-on capability of Siebel, set Argument Type to Command, otherwise, set Argument Type to Constant.

Argument Value

If Argument Type is Command, specify UserLoginPassword. If Argument Type is Constant, specify the password that is to be used to access the server database.

Append as Argument

Yes

Sequence

<next sequence number>

Related concept:

“Task overview” on page 78

Related tasks:

“Step 4: Defining required symbolic URL arguments” on page 79

“Step 6: Specifying an external Web application and defining login credentials (Optional)”

Step 6: Specifying an external Web application and defining login credentials (Optional): Siebel 7.5.2 also provides a single sign-on capability. The benefit of single sign-on for Siebel users is that they are only required to enter a user ID and password once when using a Siebel eBusiness application that accesses unstructured data managed by IBM Content Manager. You do not need to perform this step unless you are using the Siebel single sign-on capability.

In this step, you specify an external Web application and define login credentials:

1. Select an existing Siebel user or create a Siebel user.
2. From the menu, select **Site Map --> Integration Administration --> SSO Systems Administration --> Set the SSO System Value**.
 - a. Specify a value for **System Name** (in our example, SSO).
 - b. From the **Symbolic URL Name** list box, select the name of the symbolic URL (in our example, SRSU).
3. From the menu, select **Site Map --> Integration Administration --> SSO Systems Administration --> Set the SSO System Users**.
 - a. From the Siebel **Login Name** list box, select your Siebel login name (in our example, siebel_user).
 - 1) Set Login Name to the user name that you use to log on to the server database (in our example, newuser).
 - 2) Set Password to the password that you use to log on to the server database (in our example, password).

Related concept:

“Task overview” on page 78

Related tasks:

“Step 5: Defining symbolic URL arguments (Optional)” on page 82

“Step 7: Setting up a new view in the Siebel Call Center”

Step 7: Setting up a new view in the Siebel Call Center: Follow these steps to set up a new view in the Siebel Call Center:

1. Select **View --> Site Map --> Application Administration**.
2. Select **Views**.
3. Click **New**.
4. Set values for the following fields:

Name Provide the name of the view that you created in “Step 7: Creating a view” on page 64 (in our example, Service Request Detail Archived Content View).

Description

Provide a description for this view (in our example, View for Siebel Integration for IBM Content Manager).

5. Move off of this view to commit it.

Related concept:

“Task overview” on page 78

Related task:

“Step 6: Specifying an external Web application and defining login credentials (Optional)” on page 83

“Step 8: Creating a responsibility”

Step 8: Creating a responsibility: Follow these steps to create a responsibility:

1. Select **View --> Site Map --> Application Administration --> Responsibilities**.
2. Click **New**.
3. Provide the following information:

Responsibility

Provide a name for the responsibility (in our example, Call Center Manager for Content Manager).

Description

Provide a description for this responsibility.

Organization

Default Organization

4. Move off of this record to commit it.
5. From the User window, select a user (in our example, John Smith).
6. From the View window, select **Service Request Detail Archived Content View**.
7. Move off this record to commit it.
8. Log off of the Siebel Call Center.

Related concept:

“Task overview” on page 78

Related task:

“Step 7: Setting up a new view in the Siebel Call Center”

After completing all above tasks, proceed to “Validating your configured environment”.

Validating your configured environment

After you finish installation and configuration of Siebel Integration for IBM Content Manager, it is highly recommended that you validate your configured environment.

Log on to the Siebel Call Center using the user ID and password that you set up (in our example, the user ID and password for John Smith).

Follow these steps to validate your configured environment:

1. During configuration, you modified a business component (in our example, Service Request) for a Siebel entity (in our example, Service Request) and created a view (in our example, the Service Request Detail Archived Content View) that permits the display of unstructured data associated with that entity. Click the screen tab for a screen that contains the view you created (in our example, service).
2. Click **New** to create a new record for the Siebel entity.
3. Specify values for each of the fields within the record that are referenced in the search criterion within the calculated field or by symbolic URL arguments (in our example, Last Name).
4. Click the view tab that initiates the search for the unstructured data (in our example, archived content).
5. Verify whether the expected unstructured data is displayed in the search results.

Chapter 5. Starting and stopping the eClient

This section provides you with information on starting and stopping the eClient on WebSphere 4 and WebSphere 5 on Windows, AIX, and Solaris.

Starting the eClient

This section describes how to start the eClient on WebSphere 4 and WebSphere 5 on Windows, AIX, and Solaris.

Starting the eClient on WebSphere 4

You can start the eClient on WebSphere 4 by either executing the .bat files (.sh files for AIX and Solaris) or using the WebSphere Administrative Console.

To start the eClient by executing the .bat files (.sh files for AIX and Solaris):

1. If on Windows, change to the \Save subdirectory; if on AIX or Solaris, change to the /Save subdirectory.
- 2.

On Windows:

For WebSphere Application Server 4.0.5 AE, open the startIDMAE.bat file; for WebSphere Application Server 4.0.5 AES, open the startIDMAES.bat file.

On AIX or Solaris

For WebSphere Application Server 4.0.5 AE, enter startIDMAE.sh; for WebSphere Application Server 4.0.5 AES, enter startIDMAES.sh.

To start the eClient by using the WebSphere Administrative Console:

1. Navigate to the eClient application server entry for your application server machine within the WebSphere Administrative Domain.
2. If you have not started the eClient, right-click and select **Start**. If you have started the eClient already, and you want to restart it, right-click and select **Stop**. After the Stop command completes, right-click and select **Start**.

Starting the eClient on WebSphere 5

You can start the eClient on WebSphere 5 by executing the .bat files (.sh files for AIX and Solaris).

To start the eClient by executing the .bat file (.sh files for AIX and Solaris):

1. If on Windows, change to the \Save subdirectory; if on AIX or Solaris, change to the /Save subdirectory.
- 2.

On Windows

Open the startIDMServer.bat file.

On AIX and Solaris

Enter startIDMServer.sh.

Related Tasks:

Chapter 4, “Configuring”, on page 19

Stopping the eClient

This section describes how to stop the eClient on WebSphere 4 and WebSphere 5 on Windows, AIX, and Solaris.

Stopping the eClient on WebSphere 4

You can stop the eClient on WebSphere 4 by executing the .bat files (.sh files for AIX and Solaris):

1. If on Windows, change to the \Save subdirectory; if on AIX or Solaris, change to the /Save subdirectory.
- 2.

On Windows

For WebSphere Application Server 4.0.5 AE, open the stopIDMAE.bat file; for WebSphere Application Server 4.0.5 AES, open the stopIDMAES.bat file.

On AIX or Solaris

For WebSphere Application Server 4.0.5 AE, enter stopIDMAE.sh; for WebSphere Application Server 4.0.5 AES, enter stopIDMAES.sh.

Stopping the eClient on WebSphere 5

You can stop the eClient on WebSphere 4 by executing the .bat file (.sh files for AIX and Solaris):

1. If on Windows, change to the \Save subdirectory; if on AIX or Solaris, change to the /Save subdirectory.
- 2.

On Windows

Open the stopIDMServer.bat file.

On AIX or Solaris

Enter stopIDMServer.sh.

Related Tasks:

Chapter 4, “Configuring”, on page 19

Chapter 7, “Managing your eClient application”, on page 95

Chapter 6. Customizing your eClient application

You can customize your eClient application to meet the needs of your organization.

Related tasks:

“eClient JavaServer Pages”

“Customizing eClient graphics” on page 92

“Customizing eClient help” on page 94

eClient JavaServer Pages

The eClient is implemented using a set of JSP. These JSP are located in the directory where you installed the eClient. To customize the eClient, you can modify these JSP or substitute JSP of your own.

The eClient includes the following JSP:

eClient JSP related to individual items

Blank.jsp	Displays a blank page
IDMActionPage.jsp	Opens the eClient home page, where your user can start to use the eClient functions.
IDMAddedItem.jsp	Confirms that an item has been added to a folder or worklist
IDMAddItemtoFolder.jsp	Allows a document or folder to be added to a folder
IDMChangePassword.jsp	Displayed when the user wants to change the password.
IDMCloseWindow.jsp	Closes a window
IDMDeleteItem.jsp	Allows an item to be deleted from the database.
IDMDeletedItem.jsp	Verifies that an item was deleted.
IDMClipboard.jsp	Allows items to be viewed in the clipboard.
IDMEditAttributes.jsp	Displays the item attributes and allows for updating the attributes. Used to change how an item is indexed.
IDMEmail.jsp	Displayed when the user wants to create an e-mail message with an object attached.
IDMLogon.jsp	Displays when the user firsts accesses the eClient and for logging on to the server. This page displays the banner graphic (banner.gif). To customize the banner, you can supply a different graphic and call it from this page.
IDMLogon2.jsp	Displays the Logon page
IDMLogonNewPassword.jsp	Displays the Change Password page, where your users can change their passwords.
mail.jsp	Enables e-mailing of a document.
IDMMessageBox.jsp	Displays a message box
IDMItemTypeList.jsp	Lists requested type of item.
IDMItemTypeListFrame.jsp	Displays the item type list and item type list title bar.
IDMItemTypeListTitlebar.jsp	Displays the title of the item type.
IDMItemTypeList.jsp	Displays the list of item types, index classes or search templates. This JSP is a part of the IDMItemTypeListFrame frameset
IDMItemTypeListFrame.jsp	Displays the frameset that contains IDMItemTypeListFrame and IDMItemTypeListTitlebar

IDMItemTypeListTitlebar.jsp	The title bar that displays the information in the frameset for displaying the list of item types, index classes, OnDemand folders or search templates.
IDMItemVersions.jsp	Displays a list of all of the versions of an item
IDMNoteLog.jsp	Displays the window where a user can view or add to the Notelog from a Content Manager Version 8 server
IDMResultsFrameBottom.jsp	Displays the search results panel in the lower frame of the IDMSearchFrame page.
IDMQueryBuilder.jsp	Displays the query builder.
Heading.jsp	Displays heading of the search result page.
ItemTable.jsp	Displays a collection of items.
ItemTableHeader.jsp	Displays table headers for a collection of items.
ItemTabs.jsp	Displays item type tabs for a collection of items.
IDMItemVersions.jsp	Displays versions of an item.
ControlPrt.jsp	Allows the user to print HTML-based content from their browser.
ErrorPage.jsp	Displays when an error is encountered.
LocalPrintFrameset.jsp	Displays the print options.
IDMUserIDMapping.jsp	Provides user with a logon window to modify stored user ID and password mapped into the EIP administrative database for a federated server.
IDMProcessing.jsp	Displays the "Processing" or "Please Wait" graphic when there is an ongoing process
IDMProgressIndicator.jsp	Displays the progress indicator
IDMUserIDMapping.jsp	Enables your users to map their user IDs to access various content servers via the federated server

eClient JSP related to search

IDMAdvancedSearch.jsp	Displays the advanced search page in a frame controlled by IDMSearchFrame.jsp.
IDMBasicSearch.jsp	Displays the basic search page in a frame controlled by IDMSearchFrame.
IDMSearchFrame.jsp	Displays the main search page frameset.
IDMSearchResults.jsp	Displays the search results.
IDMSearchTemplate.jsp	Displays the page that contains the list of valid search templates or item types that a user can use for searching.
IDMSearchToolbar.jsp	Displays the toolbar for the search.
IDMViewApplet.jsp	Opens the HTML page embedded with the viewer applet.
IDMViewFrames.jsp	Displays the View page; when the entire item is sent to the browser, this page writes the item to the browser.
IDMViewPage.jsp	Displays the pane containing the current page of the selected item in the View page; this page is displayed in the lower frame of IDMViewFrame using the current settings for size, rotations, and other parameters.
IDMViewToolbar.jsp	When an item type is viewed, displays the toolbar in the upper frame of IDMViewFrame.
IDMResultsFrameBottom.jsp	Displays the bottom frameset of the search results.

eClient JSP related to folders

IDMAddItem.jsp	Displays the Import Document, Create Folder, and Create Federated Folder pages
----------------	--

IDMFolderContents.jsp	Displays the contents of a directory from the search results.
IDMFolderDeleteItem.jsp	Displayed when the user wants to remove an item from a folder.
IDMFolderContents.jsp	Displays the contents in a folder. This is within a worklist or search results. This is displayed within the same frame as the worklist of search results.
IDMFolderDeleteItem.jsp	Delete an item or multiple items from a folder

eClient JSP related to annotations

IDMODAnnotationsBB.jsp	Displays the lower button set for annotations in a frame of IDMODAnnotationsFrame.
IDMODAnnotationsBS.jsp	Displays the border title for annotations in a frame of IDMODAnnotationsFrame.
IDMODAnnotationsBT.jsp	Displays the upper button set for finding an annotation in a frame of IDMODAnnotationsFrame.
IDMODAnnotationsFrame.jsp	Displays the View Annotations page; this file contains the frameset for the page.
IDMODAnnotationsList.jsp	Displays the list of annotations for the selected document in a frame of IDMODAnnotationsFrame.
IDMODAnnotationsView.jsp	Displays the annotation in a frame of IDMODAnnotationsFrame.
IDMODAnnotationsBB.jsp	Displays the bottom area of the OnDemand annotations interface
IDMODAnnotationsBS.jsp	Displays the frame for the search area of the OnDemand annotations interface
IDMODAnnotationsBT.jsp	Displays the top area of the OnDemand annotations interface
IDMODAnnotationsFrame.jsp	Displays the frameset for the OnDemand annotations interface
IDMODAnnotationsEntry.jsp	Displays a framed interface made up of several frames
IDMODAnnotationsList.jsp	Displays a framed interface made up of several frames
IDMODAnnotationsView.jsp	Displays the annotation content for the selected annotation within the OnDemand annotations interface

eClient JSP related to workflow and document routing

IDMWorkLists.jsp	Lists worklists that the user can retrieve.
IDMWorkItems.jsp	Displays work items in a worklist.
IDMWorkflowCheckIn.jsp	Checks in work items.
IDMWorkflowFrames.jsp	Contains IDMWorkflowToolBar.jsp and IDMWorkItems.jsp.
IDMWorkflowNotifications.jsp	Displays work notifications.
IDMWorkflowStartOnFolder.jsp	Starts workflows for multiple items.
IDMWorkflowToolBar.jsp	Toolbar for IDMWorkItems.jsp
IDMWorkflowChange.jsp	Moves selected item from current workflow to another workflow.
IDMWorkflowInfo.jsp	Displays the workflow or document routing information.
IDMWorkflowStart.jsp	Starts an item on an EIP workflow or Content Manager document routing process

IDMWorkflowStrings.jsp	Displays workflows variables for the work item. Each item on an EIP workflow has up to 5 variables that can be displayed or edited.
IDMWorkflowSuspend.jsp	Allows the user to suspend the workflow on a chosen document for a specified time.
IDMWorkflowDelNotif.jsp	Deletes a workflow notification list
WFPageHeading.jsp	Displays the column headers for the worklist
WFPageItemTable.jsp	Displays a general list of items such as documents and folders
WFPageItemTableHeader.jsp	Builds the table headers, or column headers.
WFPageItemTabs.jsp	Builds the tabs for items from different item types or index classes.

eClient JSP related to document routing

IDMDocRoutingConfirmWindow.jsp	Opens a window and displays a page that confirms an item has been put on a document routing process
IDMDocRoutingGetWork.jsp	Internal JSP that retrieves items from a document routing process or workflow and populates a worklist
IDMDocRoutingInfo.jsp	Displays the document routing information for an individual item from the search results
IDMDocRoutingPriority.jsp	Changes priority of an item on a document routing process
IDMDocRoutingSelectUser.jsp	Displays a window to select a user to assign the work to from a worklist
IDMDocRoutingSetOwner.jsp	Set the owner for a document routing process

If you substitute your own JSP, or if you place your modified pages in a different directory, you must update the Servlet JSP in the `IDM.properties` file. For information about setting up the eClient to use your customized JSP, see “Configuring parameters for a customized client” on page 99

Customizing eClient graphics

All of the graphics (including the icons) that are used by the JSP and the help are located in the `\CMeClient\installedApp\eClient82.ear\eClient82.war\icons` directory in Windows and in the `/opt/CMeClient/installedApp/eClient82.ear/eClient82.war/icons` on AIX and Solaris, where `/opt/CMeClient` is the directory where the eClient is installed.

The most common graphics to change are the background graphics. Four different background graphics are used in the eClient and each is specified with an individual CSS class. Replacing these background graphics with files of the same name will change the background of those pages that use the related CSS class. Consult the table below to determine which files and class to modify. All of the backgrounds can be specified to use the same graphic, or not use any graphics, but 4 different classes and backgrounds are used by default to provide flexibility within the interface.

Table 5. CSS classes and background graphics

CSS class or element	Background graphic	Description
BODYLOGON	icons/logon_bk.jpg	Used for the Logon and Change Password pages within the eClient
BODYHOME	icons/home_bk.jpg	Used for the Home page within the eClient. This is the first page that is displayed after the Logon page.
BODYMINI	icons/mini_bk.jpg	Used for framed pages within the eClient. The Basic Search, Advanced Search, and Search Template viewer pages use this class.
BODYDIALOG	icons/dialog_bk.jpg	Used for windows within the eClient. The Import, Edit Attributes, E-mail and many other windows use this class.
BODY	N/A	For all other pages in the eClient, the element within the cascading style sheet sets the appearance. The BODY element does not by default specify a background graphic, but specifies the background color = white.

You can replace the artwork with your own to customize the graphics for your eClient. You can set the font, colors, and background colors of the eClient in the `eclient81.css` cascading style sheet file. If the default location for the icons or graphics are changed, the CSS style which specify a background image may also need to be modified. Below are the CSS classes that are specified in the cascading style sheet file used by the eClient:

```

/* main body - plain white background */
BODY {
background : White;
padding-top : 0px;
padding-left : 0px;
/*background-image : url(icons/background.jpg);
*/
}/* body - For Logon screen */
.BODYLOGON {
background : White;
padding-top : 0px;
padding-left : 0px;
background-image : url(icons/logon_bk.jpg);
}
/* body - Home page or Action Page */
.BODYHOME {
background : White;
padding-top : 0px;
padding-left : 0px;
background-image : url(icons/home_bk.jpg);
}
/* body - For Frame pages background */
.BODYMINI {
background : White;
padding-top : 0px;
padding-left : 0px;

```

```
background-image : url(icons/mini_bk.jpg);
background-repeat : no-repeat;
}
/* body - background for Dialog windows */
.BODYDIALOG {
background : White;
padding-top : 0px;
padding-left : 0px;
background-image : url(icons/dialog_bk.jpg);
}
```

Customizing eClient help

As part of customizing the eClient for your users, you can provide customized online help or add your own. The help files are written in Hypertext Markup Language (HTML) and reside in the directory where the eClient is installed.

The help files use a cascading style sheet, (`eclient81.css`) and a JavaScript file, (`generalFunctionsIDM.js`). Both reside in the directory where the eClient is installed. If you use your own style sheet or script file, change the links in the help files.

The help files use a graphic for the background, `bkgrd.gif`, located in the `icons` directory. If you supply your own graphic, change the style sheet to identify it.

If you add your own help topics, you must modify the JSP for the pages or panels from which you want to display the new help topics. Specify the new HTML files that you supply in the calls to help.

Customizing the viewer applet

You can customize the viewer applet by modifying the default configuration file, `CMBViewerConfiguration.properties`, located in the `cmbviewer81.jar` file or creating a new configuration file. See "Working with the Java document viewer toolkit" in *Workstation Application Programming Guide*.

Chapter 7. Managing your eClient application

This section discusses how to manage your eClient application.

Related tasks:

“Setting and changing your configuration parameters”

“Defining how the eClient handles content types” on page 98

“Configuring parameters for a customized client” on page 99

Setting and changing your configuration parameters

After installation, the eClient uses default configuration properties that you can edit in the `IDM.properties` file. The `IDM.properties` file resides in the root directory where the eClient is installed. Most aspects of managing the eClient application are controlled by these basic parameters in this file.

To change the properties, open `IDM.properties` in a text editor, make the changes, and save it. The changes you make to the properties file take effect the next time the eClient property daemon checks the properties. If you have disabled the property daemon, you must restart the application server for the eClient to use the changes.

The `IDMdefault.properties` file contains the default values for the parameters in the `IDM.properties` file.

Setting the caching directory

You can set where the eClient caches documents to help manage your system resources. Specify the directory that you want to use for document caching on the `CacheDir` parameter.

Setting the maximum number of search results displayed on a page

You can specify the maximum number of search results that are displayed on a page on the `MaxResults` parameter. For example, if you set this parameter to 50 and receive 200 results from a search, you will view four pages of results. However, as servers might have their own maximum results values, make sure that the values that you specify do not exceed the servers' own maximum values. This parameter does not affect the number of results that are returned by a federated search for the Enterprise Information Portal. You control this number in Enterprise Information Portal.

Setting the maximum number of search results returned from the content server

You can limit the number of items that are returned from a particular content server on the `TotalMaxResults` parameter. This limit improves performance on the middle-tier and prevents the browser from timing out when it processes a large number of hits that are found for a query. If you set this parameter to 100, the eClient returns the 100 most recent items even if there are more search results. If you set the parameter to the default value of -1, the eClient returns all search results.

Setting the maximum file size allowed during import

You can specify the maximum size of a file in bytes that can be imported on the `max_import_file_size` parameter.

Setting the property daemon

The eClient property daemon periodically checks for updates to the `IDM.properties` file. You can enable the daemon and set its frequency on the `PropertyDaemonInterval` parameter.

Set the parameter to an integer greater than 0 to enable the property daemon; the integer indicates the frequency of checks in minutes. For example, if you enter 10, the property daemon checks whether you have made changes to the file every 10 minutes. Set the parameter to 0 to disable the daemon. If you enter an invalid value, then the default value 1 is used.

Setting the EIP INI files

The eClient checks several Enterprise Information Portal configuration files.

You must set the location of the Enterprise Information Portal INI files as Uniform Resource Locators (URLs), for example, `file:///c:/cmbroot/cmbcs.ini`. You must correctly set the location of the EIP files here, otherwise the eClient will not work.

CMBCC2MimeURL

Specify the location of the `cmbcc2mime.ini` file that contains the MIME (Multipurpose Internet Mail Extension) type associations.

CsIniURL

Specify the location of the `cmbcs.ini` file that defines whether the content server run-time environments are local or remote. The setting of the `ConnectionType` parameter affects this setting.

ClientIniURL

Specify the location of the `cmbclient.ini` file that specifies the RMI (Remote Method Invocation) server. The setting of the `ConnectionType` parameter affects this setting.

Setting the connection type

You can specify whether the Enterprise Information Portal administration database and content server run-time environments are local to this server or remote by setting the `ConnectionType` parameter. Values for this parameter are:

- 0** To use local versions; the settings in `ClientIniURL` are ignored.
- 1** To use remote versions; the settings in `ClientIniURL` are used to locate `cmbclient.ini`; `CsIniURL` is ignored.
- 2** To dynamically set the location; `ClientIniURL` is used for locating `cmbclient.ini`, and `CsIniURL` is used to locate the Enterprise Information Portal `cmbcs.ini` file.

Setting the Content Manager Version 8 connector

Specify the location of the server initialization file for Content Manager Version 8 servers on the `ICMServersURL` parameter by using this format:

`ICMServersURL=[fully qualified URL]`. For example,

`ICMServersURL=file:///C:\Program Files\IBM\CMgmt\cmbicmsrvs.ini`

Note: This value should be a fully qualified URL giving the location of the `cmbicmsrvs.ini` file. Use the name of your Content Manager Version 8 server ini file if it has a different name.

Enabling launching content files

With a `display-defaults` file, you can specify which file types to convert on the server for viewing in your user's browser. You can also specify which file types to send to the browser to launch. Set `adminDefined=true` to use the defaults file. Use the `adminDefaultsFile` parameter to specify the name and location of this file. For more information about the `display-defaults` file, see "Defining how the eClient handles content types" on page 98.

Setting the e-mail properties

You must set several parameters to use e-mail with the eClient:

emailenabled

Set to true to enable e-mail and false to disable it.

mailUser

Set to a valid user ID on the mail server; returned mail goes to the user ID.

mailHost

Set to the IP address of the mail server.

The eClient sends e-mail with UTF-8 encoding.

Enabling EIP advanced workflow

Set the `workFlowEnabled` parameter to true to enable workflow.

Setting the service connection type

You can set the `serviceconnectiontype` parameter to specify the location of the EIP workflow server. Values for this parameter are:

- 0 To use a local configuration; workflow is installed on the same machine as your application server.
- 1 To use a remote configuration; workflow is installed on an RMI server.
- 2 To use a dynamic configuration.

Enabling the viewer applet

You can use a viewer applet to allow users to perform actions on retrieved files such as annotation editing, rotation, zooming, and printing more easily. To enable the viewer applet, set the `viewerAppletEnabled` parameter to true, and use the `IDAdminDefaults.properties` `display-defaults` file to indicate the formats that the viewer applet supports. See "Defining how the eClient handles content types" on page 98 for information about formats.

You need to have a Java plug-in to run the viewer applet. The plug-in might not be installed on a user's machine. For Windows, you can specify the location from which the plug-in is automatically installed by Microsoft Internet Explorer or Netscape Navigator in the `plugin_exe` and `plugin_page` parameters, respectively. The default values for these parameters point to a JavaSoft Web site. You can change these default values for performance reasons, or to prevent your users from retrieving this plug-in from outside your firewall. For AIX and Solaris, you should install the Java plug-in Version 1.3.1 prior to running the eClient.

Enabling federated folders

A federated folder enables you to store related documents from different content servers in a single collection, and save search results persistently in EIP databases. For example, an insurance claim consists of documents from a Content Manager server, a DMV record from a DB2 relational table, and a voice or video of the claim from a VideoCharger server. Using a federated folder, you can group these documents in an EIP database. Federated folders perform like native folders from other content servers. You can create, retrieve, update, and delete a federated folder like a native folder. To enable the federated folder capability, set the `createFedFolderEnabled` parameter to `true`. To disable the federated folder capability, set the `createFedFolderEnabled` parameter to `false`.

Defining how the eClient handles content types

With a display-defaults file, you can specify which file types to convert on the server for viewing in your users' browser. You can also specify which file types to send to the browser to launch and specify whether to use the viewer to view the files. This file is `IDMAdminDefaults.properties`, which resides in the directory in which the eClient was installed.

Attention: If you have a pre-existing copy of this file, it is not overwritten if you install again.

Content types

In the eClient display-defaults file, you can specify:

- MIME types that are converted at your server and displayed to your users' eClient
- MIME types that are downloaded and launched in a plug-in or other application at the client machine
- Which files are viewed with the viewer applet

The display-defaults file contains entries for MIME types in the form:

type/subtype=launch_indicator

The *launch_indicator* must be either:

don't launch

To perform conversion before sending the content to the client browser for display.

Restriction:

- Thai text cannot be rendered Left to right HTML, MSWord or RTF files are not supported.
- Turkish HTML documents coded as `CHARSET=iso-8859-9` are not supported.
- The eClient does not support HTML documents through version 3.0. Do not set Javascript or XML documents to don't launch.

launch To download the content for the client machine to launch. The eClient converts any MIME types that are not explicitly specified in this file with launch. With this setting, the appropriate browser plug-in or external application is launched if the display defaults are correctly set.

applet To view the file with the viewer applet.

The viewer applet supports TIFF (image/tiff), GIF (image/gif), JPEG (image/jpeg), Bitmap (image/bmp), PCX (image/pcx), MO:DCA-P (Mixed Object Document Content Architecture-Presentation), IOCA (Image Object Content Architecture), and PTOCA (Presentation Text Object Content Architecture with form overlays) files. If the eClient viewer applet identifies an unsupported file type, it terminates this process, and returns to the page that launches a document.

Restriction: The applet might fail if the users' browser is configured with a socks proxy. Specify the IP address for the proxy server in the browser settings instead of the host name.

Example:

If Acrobat Reader is installed on the end-users' system, the following lines send PDF files to the browser because the browser can display that format. MO:DCA-P files are converted at the server to a displayable format.

```
application/pdf=launch  
application/vnd.ibm.modcap=don't launch
```

The following line enables the viewer applet to view TIFF content files.

```
image/tiff=applet
```

You can use the display-defaults file provided with the eClient or create your own. If you create your own file, you must:

- Specify its location and file name in the `adminDefaultsFile` parameter in the `IDM.properties` file.
- Store the file in a directory in your `CLASSPATH` variable
- Set the `adminDefined` parameter in the `IDM.properties` file.

Configuring parameters for a customized client

If you have customized your eClient, you can set certain configuration parameters to work with your customized application. These parameters are in the `IDM.properties` file.

To set the location of graphic files:

You set the location for the graphic files used by the eClient application on the `ImageURL` parameter. Specify the path for the images.

To set the error page:

You specify the JavaServer Pages (JSP) to use when encountering an error on the `ErrorPage` parameter. The default is `Errorpage.jsp`. If you want to use a custom error page with a different file name, specify it on this parameter.

To specify different servlets:

The servlet JSP parameters specify the JSP to use for the various eClient servlets. The `IDM.properties` file supplied with the eClient contains the full list of servlet parameters and the JSP that are supplied with the eClient. The specification takes the following form:

```
Output.servlet_name=JSP
```

If you write your own JSP to customize the eClient, you specify them in the servlet JSP parameters. If, for example, you write your own JSP named `MySearch.jsp` to let users perform searches and view the results, you can specify it like this:

Output.IDMSearch=/MySearch.jsp

You can specify your own JSP for any of the servlets.

To set the application name:

If you want to use a different name for the application, specify it on the WebAppName parameter. The name you specify and the Web application name that you specified for your J2EE server need to match.

Defining server connections

For most servers, the eClient uses the server definitions from the Enterprise Information Portal. During installation of the eClient, you can define a direct connection for a single IBM Content Manager OnDemand server or IBM Content Manager ImagePlus for OS/390 server. You can make changes to the server definitions, or you can add an additional IBM Content Manager OnDemand server or IBM Content Manager ImagePlus for OS/390 server that your users access using the eClient in the `IDM.properties` file.

On AIX, to list and connect to the Content Manager Version 7 servers and OnDemand content server in the eClient Logon window, enter `export LIBPATH=/usr/lpp/cmb/lib:/usr/lpp/frn/lib:$LIBPATH` before starting WebSphere AE or AES. Start WebSphere from the same environment where you have exported `LIBPATH`. You can specify this command in the profile file of the user who starts WebSphere so that it is not necessary to export the path again.

On Solaris, to list and connect to the Content Manager Version 7 servers and OnDemand content server in the eClient Logon window, enter `export LD_LIBRARY_PATH=/usr/lpp/cmb/lib:$LIBPATH` before starting WebSphere AE or AES. Start WebSphere from the same environment where you have exported `LD_LIBRARY_PATH`. You can specify this command in the profile file of the user who starts WebSphere so that it is not necessary to export the path again.

Restriction:

The eClient does not support the EIP Domino.Doc connector, the EIP Information Catalog connector, the EIP Rational Database connector, the EIP Extended Search connector either directly or through a federated connection.

When you add a new library server to the eClient server list, you must update the `cmbicmsrvs.ini` and `cmbicmenv.ini` files. When you add a federated database, you must update the `cmbds.ini` and `cmbfedenv.ini` files. Instructions for updating these files is in the "Generating configuration files" section of *Planning and Installing Your Content Management System*.

Defining an OnDemand server connection

You define a connection for an OnDemand server on the `Datastore.OD.x` parameter. Each OnDemand server connection that you define is numbered; the parameter for the first is `Datastore.OD.0`, for the second is `Datastore.OD.1`, and so forth. Number the connections in order and do not skip a number. The specification takes the following form:

`Datastore.OD.X=alias:IP address or host name:port`

where:

alias An alternate name for the server; this is the name that appears in the list of servers your users see. Use a name that is familiar to your users.

IP address or host name

The IP (Internet Protocol) address or host name of the server.

port The port to use; specify the port if the OnDemand server requires a port. A port of 0 is ignored. This attribute is optional.

The following example specifies connections for two OnDemand servers:

```
Datastore.OD.0=AcmeOD:serv1.acme.com:1009  
Datastore.OD.1=Jones'OD:9.71.23.110:3219
```

The OnDemand Advanced Function Presentation (AFP) plug-in now supports Microsoft Internet Explorer Version 5.5 Service Pack 2 and Internet Explorer Version 6.0. This support is in AFP Plugin 7.1.0.5 and above, available from: <ftp://service.software.ibm.com/software/ondemand/fixes/v71/>.

Defining an ImagePlus for OS/390 server connection

You define a connection for ImagePlus for OS/390 server in the `Datastore.IP390.x` parameter. Each ImagePlus for OS/390 server connection that you define is numbered; the parameter for the first is `Datastore.IP390.0`, for the second is `Datastore.IP390.1`, and so forth. Number the connections in order and do not skip a number. The specification takes the following form:

```
Datastore.IP390.X=ALIAS=ALIAS;APPL=APPL;  
FAFIP=FAFIP;IODMIP=IODMIP;FAFPORT=FAFPORT;IODMPORT=IODMPORT  
;FAFPROT=FAFPROT;IODMPROT=IODMPROT;TERMID=TERMID;FAFSITE=FAFSITE;  
OVERLAYS=OVERLAYS;IODMCNTL=IODMCNTL
```

where:

ALIAS An alternate name for the server; this is the name that appears in the list of servers your users see. Use a name that is familiar to your users. The alias name can contain blanks or special characters, but it cannot contain a colon. For example: IP390

APPL The identifier for the folder application facility (FAF). For example: 01

FAFIP The IP address for FAF. For example, 9.25.176.23

IODMIP

The IP address for the object distribution manager. For example, 9.67.43.83

FAFPORT

The TCP/IP port for the folder application facility used by ImagePlus for OS/390. For example, 3061

IODMPORT

The port number for the object distribution manager. For example, 3082

FAFPROT

The communication protocol of the FAF host; use 4000 for FAF CICS® and 4500 for TCP/IP on IMS™.

IODMPROT

The communication protocol for the object distribution manager host; use 4000 for TCP/IP on CICS and 4500 for TCP/IP on IMS.

TERMID

The terminal identifier for the object distribution manager; if not specified the user ID is used.

FAFSITE

The 4-character identifier for the FAF that owns and catalogs the documents for this server. For example, CS61

OVERLAYS

OVERLAYS is an optional parameter. The IODM collection class where all form overlays are stored. If not specified, forms are searched for in the collection class where the last document was retrieved.

IODMCNTL

IODMCNTL is an optional parameter. The IODM document storage location control; the document must be in the specified location to be retrieved. You can set this to:

DASD Retrieves documents from DASD only.

OPTICAL

Retrieves documents from DASD or OPTICAL only.

SHELF

Retrieves documents from DASD, OPTICAL, or SHELF.

For example, to define an ImagePlus for OS/390 connection to a host with an IP address of 9.88.123.67:

```
Datastore.IP390.0=ALIAS=Acme IP390;APPL=03;  
FAFIP=9.88.123.673;IODMIP=9.88.123.67;  
FAFPORT=1061;IODMPORT=3080;FAFPROT=400;  
IODMPROT=4000;FAFSITE=CS61
```

Chapter 8. Troubleshooting

This section provides you with scenarios, tips and trace information for troubleshooting the eClient and third-party application integration.

Related tasks:

“Troubleshooting the eClient”

“Troubleshooting third-party application integration” on page 112

Troubleshooting the eClient

Information in this section can help you understand and fix possible problems that you might encounter when installing, configuring, and managing the eClient.

Related reference:

“Troubleshooting scenarios”

“Configuration problems” on page 109

“Trace information” on page 111

Troubleshooting scenarios

If you encounter problems, review the following scenarios for help:

Scenario 1: Corrupted international characters

Problem:

Certain international characters appear corrupted on some of the install panels.

Explanation and Solution:

A possible cause of this problem is that the Sun Java Runtime Environment (JREs) do not include font property files for the following languages. To implement support for these languages in the eClient, locate and copy the following files to the lib subdirectory of your JRE installation directory:

- font.properties.ru
- font.properties.pl
- font.properties.cs
- font.properties.hu
- font.properties.CP1250

Scenario 2: Cannot launch document

Problem:

The eClient cannot launch a document. Microsoft Internet Explorer might show a blank page. Netscape Navigator launches the plug-in, but does not show the document. For example, Adobe Acrobat provides this message The file is damaged and could not be repaired.

Explanation and Solution:

IBM HTTP Server for Windows cannot launch in the plug-in application documents over 64K that are handled by a browser.

At this time, there is no permanent fix for this problem in the IBM HTTP Server for Windows. A workaround is to disable the HTTP cache-Afpa and the AfpCache keywords. To accomplish this without using the HTTP GUI administrator:

1. Open the `http.conf` file located in the `\IBM HTTP SERVER\conf\` directory. In this file, you see two keywords: `AfpaEnable AfpaCache on`
2. Comment out these keywords by using the pound sign: `#AfpaEnable #AfpCache on`
3. Restart the HTTP server to set these changes.

Scenario 3: Warning message in the final install panel

Problem:

A warning message is displayed in the final install panel.

Explanation and Solution:

You received this message because automount was running during the installation process. This warning is the result of an installation program defect, and does not affect performance or functionality. You can ignore it.

Scenario 4: Persistent blank window during the eClient deployment

Problem:

While deploying the eClient into a WebSphere application server during installation, a blank window appears longer than 5 minutes.

Explanation and Solution:

It is possible that the eClient deployment phase has stopped due to a running WebSphere Java process. Terminate the eClient installation program and then terminate the WebSphere Java processes. On Windows, examine Task Manager to ensure that you terminated all Java processes. On AIX and Solaris, use the command `ps -ef | grep java` to verify that the WebSphere application Java processes are not running. After terminating all running WebSphere Java processes, run the eClient installation program again.

Scenario 5: Cannot display Visio documents

Problem:

The eClient cannot display Visio documents.

Explanation and Solution:

You need to have the Visio viewer to view Visio documents. You can download the Visio viewer from www.microsoft.com/office/visio/default.asp. Also, the Visio viewer cannot launch the documents directly; you must download the Visio documents to view them correctly.

Scenario 6: Cannot view documents of MIME type *multipart/mixed*

Problem:

The eClient cannot display documents of MIME type *multipart/mixed*.

Explanation and Solution:

This problem occurred because EIP is installed on a Solaris or AIX machine. On AIX or Solaris, you can only view the first part of a document of MIME type *multipart/mixed* in the default browser.

Scenario 7: Browser timeout during an OnDemand search

Problem:

A browser timeout occurred during an OnDemand search.

Explanation and Solution:

A possible cause of this problem is that a query results in a large quantity of returned items, for example, 1000 or more. To prevent this problem, in the *IDM.properties* file, set the *TotalMaxResults* parameter to a lower value so OnDemand sends back fewer results to the eClient.

Scenario 8: Cannot view OnDemand AFP files

Problem:

The eClient cannot display some OnDemand AFP files.

Explanation and Solution:

This problem occurred because these OnDemand AFP files are created using certain fonts or special code pages, but you do not have those fonts or the code pages configured on the client system where the AFP files are viewed. To fix this problem, you need to map AFP fonts or code page files. For instructions about mapping AFP fonts and code page files, see "Mapping AFP Fonts" in *OnDemand Windows Client Customization Guide*, which is available at www-3.ibm.com/software/data/ondemand/mp/library.html.

Scenario 9: Java Virtual Machine (JVM) crashes

Problem:

The Java Virtual Machine (JVM) crashed.

Explanation and Solution:

A possible cause is that when multiple users connect to an OnDemand content server and log in and out at a rapid rate, the system does not have enough time to clean up the *TIME_WAIT* sockets. Eventually, the ports numbers between 1024 and 5000 for those *TIME_WAIT* socks run out and the JVM crashes.

To fix this problem, complete the follow steps based on platform:

For Windows:

Add *TcpTimedWaitDelay* and *MaxUserPort* registry values as a workaround. You can set these values through *REGEDIT* command.

1. Set *TcpTimedWaitDelay* to 30:
 - a. Click **Start** -> **Run**.
 - b. In the available field, enter *regedit*.

- c. Go to the key directory file:
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/TcpTimedWaitDelay. The value type is REG_DWORD.
- d. Double-click **TcpTimedWaitDelay**.
- e. Select **Decimal**.
- f. Type 30 in the **Value data** field. The default value for this field is 0xF0 (240 decimal). The valid range is 30-300 (decimal).

Description: This parameter determines the length of time that a connection stays in the TIME_WAIT state when it is closed. When a connection is in the TIME_WAIT state, the socket pair cannot be reused. This is also known as the 2MSL state because the value should be twice the maximum segment lifetime on the network. See RFC 793 for further details.

2. Set the MaxUserPort to 65534:
 - a. Click **Start** -> **Run**.
 - b. In the available field, enter regedit.
 - c. Go to the key directory file:
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/MaxUserPort. The value type is REG_DWORD.
 - d. Double-click **MaxUserPort**.
 - e. Select **Decimal**.
 - f. Type 30 in the **Value data** field. The default value for this field is 0x1388 (5000 decimal). The valid range is 5000 - 65534(decimal).

Description: This parameter controls the maximum port number used when an application requests any available user port from the system. Normally, short-lived ports are allocated in the range from 1024 through 5000. Setting this parameter to a value outside of the valid range causes the nearest valid value to be used (5000 or 65534).

For Solaris:

The tuning changes noted below do not remain across reboots. Add the following changes to a runtime commands file, so they are enacted at each boot. The runtime commands file is /etc/init.d/inetinit.

1. Make more sockets available:
 - a. At the command prompt, enter:

```
#/usr/sbin/ndd -set /dev/tcp tcp_conn_req_max_q 65534
```

The q queue holds sockets awaiting an accept() call from the application.

- b. At the command prompt, enter:

```
#/usr/sbin/ndd -set /dev/tcp tcp_conn_req_max_q0 65534
```

The q0 queue contains half-open sockets.

2. Decrease the time wait before closing the sockets by entering:

```
#/usr/sbin/ndd -set /dev/tcp tcp_time_wait_interval 60000
```

For AIX:

The tuning changes noted below do not remain across reboots. Add the following changes to a runtime commands file, so they are enacted at each boot. The runtime commands file is /etc/rc.net.

1. To make more sockets available, enter at the command prompt:

```
/usr/sbin/no -o clean_partial_conns=1
```

This setting will instruct the kernel to randomly remove half-open sockets from the q0 queue to make room for new sockets.

The default range is sufficient, but you can change it using the no command. Here is an example that sets the TCP ephemeral port range to 49152 through 65535:

```
# /usr/sbin/no -o tcp_ephemeral_low=49152  
# /usr/sbin/no -o tcp_ephemeral_high=65535
```

2. Decrease the time wait before closing the sockets:

```
# no -o tcp_timewait=5
```

On AIX 4.3.2, the default TIME_WAIT seems to be set to 15 seconds, which translates in AIX terms to tcp_timewait = 1, as each tcp_timewait is about 15 seconds. So you need to use the no command to set the tcp_timewait to 5 to make the TIME_WAIT just over 60 seconds (using a value of 4 will leave TIME_WAIT less than 60 seconds)

Scenario 10: Multiple cursors

Problem:

Multiple cursors are displayed pages with multiple text fields.

Explanation and Solution:

This occurred because you are using Netscape Navigator 4.76 on AIX or Sun Solaris. This does not impact the function of the eClient.

Scenario 11: Cannot view double-byte character sets

Problem:

Documents in double-byte languages (Simplified Chinese, Traditional Chinese, Japanese, and Korean) cannot be viewed.

Explanation and Solution:

The English version of Netscape Navigator 4.7 browser does not support viewing of the double-byte character set. If you want to use a Netscape Navigator 4.7 browser to view one of these language versions using the eClient, you need the corresponding language version of Netscape. Also, Netscape Navigator 4.7 does not support flyover texts for double-byte character set. To view flyover texts in these languages, use Microsoft Internet Explorer.

Scenario 12: Cannot reload a page

Problem:

A page cannot be loaded in the browser.

Explanation and Solution:

The browser's default toolbar is disabled when the eClient is used. To perform a browser reload of a screen in Netscape Navigator, right-click anywhere within the browser's viewer window, and select **Reload** or press **Ctrl+R**. To perform a browser reload of a screen in Microsoft Internet Explorer, click right-click anywhere within the browser's viewer window, and select **Refresh** or press **F5**.

Scenario 13: Viewer applet hover help appears corrupted

Problem:

The viewer applet hover help appears corrupted in double byte languages (Simplified Chinese, Traditional Chinese, Japanese, and Korean).

Explanation and Solution:

This problem occurred most probably because that you are using the Java2 Runtime Environment (JRE), Standard Edition, Version 1.3.1_01. Install the Java2 Runtime Environment (JRE), Standard Edition, Version 1.4.0 "International for Windows" version to avoid this problem.

Scenario 14: The eClient environment settings disappear

Problem:

The eClient environment settings disappear intermittently.

Explanation and Solution:

This is caused by a known WebSphere GUI problem. Stop and remove the eClient from WebSphere, and use the `idmwas` file located in the `Save` directory of the eClient. To avoid this problem, install WebSphere eFix PQ63508.

Scenario 15: Directed to an incorrect address to install the Java plug-in by Netscape

Problem:

While attempting to use the viewer applet, Netscape directed me to install the plug-in from an incorrect address.

Explanation and Solution:

If you use Netscape on Solaris, and want to use the viewer applet, you must download and configure the Java plug-in to run the applet. Install and configure the Java plug-in before using the viewer applet. You can download the Java 2 Runtime Environment (JRE), Standard Edition, Version 1.4.0 from:
<http://java.sun.com/j2se/1.4>.

Scenario 16: Cannot use the viewer applet

Problem:

The viewer applet cannot be launched.

Explanation and Solution:

If you configured the eClient to use the viewer applet, and used WebSphere Application Server Version 4.0.3 AE or AES, you must install WebSphere efix "PQ54572 4.0.x: Deploying signed jar file problem", or complete these steps after you install the eClient and before you use the applet:

1. Execute `mkdir /temp` to create a temporary directory.
2. Move to `cd /temp`.
3. Execute
`jar -xvf [installed eClient directory]/eClient82.ear`

to extract the eClient82 EAR archive into the temporary directory eClient82. EAR currently resides in the directory where the eClient is installed.

4. Execute

```
jar -xvf eClient82.war viewerApplet.jar cmbview82.jar
```

to extract viewerApplet.jar and cmbview82.jar from the eClient82 EAR archive.

5. Execute

```
move viewerApplet.jar [installed WebSphere directory]/installedApps/  
eClient82.ear/eClient82.war
```

and

```
move cmbview81.jar [installed WebSphere directory]/installedApps/eClient82.ear/  
/eClient82.war
```

to overwrite both of the JAR files in the directory where WebSphere is installed.

Note: If you do not overwrite the JAR files in the directory where WebSphere is installed, the applet fails to pass the Java security check and cannot be loaded into your browser.

Error when resizing the browser window

Problem:

While resizing the browser window in Netscape Navigator 4.75, this error message is displayed:

Data Missing

This document resulted from a POST operation and has expired from the cache. If you wish you can repost the form data to recreate the document by pressing the reload button.

Explanation and solution:

Click **Reload** to repost the data.

Configuration problems

Figure 6 on page 110 shows the eClient Logon window. After installing and configuring your eClient, you can access the Logon window at the following address: `http://hostname/Web application name/IDMInit`. In the address, `hostname` is the name or IP address of the server machine, `Web application` is the name of the eClient Web application (eClient82 is the default name), and `IDMInit` is the initial connection servlet.



Figure 6. Content Manager eClient Logon window

If the Logon window does not display and you receive HTTP 404 - File not found or The page cannot be found error:

- Verify that you entered the correct address. The default name of the eClient web application, eClient82, might have been changed in the IDM.properties file by another administrator.
- Verify that the eClient Web application is started or running.
- If you are using WebSphere Application Server Advanced Edition on AIX or Solaris, verify that it is started. Enter `ps -ef|grep WebSphere`. If WebSphere is not running, enter `StartupServer.sh` to start it.
- Verify that the HTTP server is started.

If the Logon window opens, but there are no servers listed in the **Server** list:

- If you are trying to connect to an EIP server, verify that your host name, port number, RMI server configuration (if connecting remotely), and connection strings for the EIP server is correct.
- If you are trying to connect to IBM Content Manager Version 7 or an earlier version, verify that the `Frnolint.tbl` file lists the servers correctly.
- If you are trying to connect to an ImagePlus for OS/390 server or a Content Manager OnDemand server, verify that the values for the server are set correctly in the `IDM.properties` file. To connect to more than one ImagePlus for OS/390 or OnDemand server, add connection strings for each one and specify their values in the `IDM.properties` file.
- On AIX, to list the Content Manager Version 7 servers in the eClient Logon window, enter `export LIBPATH=/usr/lpp/cmb/lib:$LIBPATH` before starting

WebSphere AE or AES. Start WebSphere from the same environment where you have exported LIBPATH. You can specify this in the .profile of the user who starts WebSphere so that it is not necessary to export the path again.

If you had problems installing on AIX, delete everything that was created by the eClient installation in the /tmp directory before attempting the installation process again.

Trace information

The eClient can produce trace information. You can set the location, information level, and size for these files. You manage these files by setting parameters in the IDM.properties file.

To set the location of the trace files:

The WorkingDir parameter determines the location of the trace files. Set this parameter to the full path for the directory that you want to contain the trace files.

Example:

```
WorkingDir=d:\\Program Files\\CMeClient\\IBM\\TRACE
```

for Windows or

```
/opt/CMeClient/TRACE
```

for AIX or Solaris.

To set the tracing level:

You can set the trace level to one of the following values:

- 0** Tracing is off
- 1** Tracing is on for exceptions and errors
- 2** Level 1 with the addition of general information, method entry, and exit points
- 3** Level 2 with the addition of API calls
- 4** Level 3 with the addition of Enterprise Information Portal non-visual bean tracing

Set the tracing level on the TraceLevel parameter. If the trace level is set to 3 or 4, you might see an error in the dklog.log file when you log on. This error is not fatal, and the eClient functions normally. See *Messages and Codes* for information about configuring this file.

To set the trace file size:

Trace information is written to a series of files, named TraceX.txt. When the file size reaches a maximum, a new trace file is started, and incrementing X renames the previous one. For example, when the current trace file reaches the maximum size, it is named Trace1.txt, and the new file is Trace.txt.

Set the maximum size in kilobytes (KB) for trace files on the MaxTraceSize parameter.

Miscellaneous tips

This section provides miscellaneous tips about updating annotations, setting WebSphere in the correct state, and DB2 Version 8 support.

Tip 1: Updating annotations

If you update annotations of a document in the document viewer applet, and the library server is configured for optional versioning, the eClient always replaces the current version of the annotations with the updated annotations.

Tip 2: Setting WebSphere in the correct state

If you installed the eClient without putting WebSphere in the correct state, you need to uninstall the eClient, start and stop the servers as appropriate, and then install again.

If you leave the WebSphere Application Server Administrative Console open, the eClient display cannot be refreshed, and you need to close the Administrative Console and reopen it after the installation to see the eClient Web application.

Tip 3: DB2 Version 8 Support

If the eClient is installed on a system with DB2 Version 8, it can only access content servers that are installed on DB2 Version 8.

If you use the eClient to access a DB2 Version 8 federated server, it can only access federated entities that are mapped to content servers that are installed on DB2 Version 8. You can only use federated search templates that are defined on those federated entities for search.

Troubleshooting third-party application integration

Information in this section can help you understand and fix possible problems that you might encounter when installing, configuring, and managing third-party application integration.

Related tasks:

“Troubleshooting PeopleSoft Integration for IBM Content Manager”

“Troubleshooting Siebel Integration for IBM Content Manager” on page 117

Troubleshooting PeopleSoft Integration for IBM Content Manager

The following references and tasks include troubleshooting information that might help you install, configure, and administrate the integration of PeopleSoft and IBM Content Manager.

Related tasks:

“Fixing a corrupted WebSphere server configuration file” on page 113

“Enabling browsers to accept cookies” on page 114

Related reference:

“Correct domain name for the PeopleSoft Internet Architecture” on page 113

“Host name” on page 113

“License codes” on page 113

Host name

Some prerequisite products installed in the process of providing this solution do not accept a host name that contains an underscore character (_). To prevent errors with the host name, limit the characters used for a host name to a small subset of the ASCII portable character set.

License codes

When installing the PeopleTools, use the correct license code. The PeopleSoft Portal Solutions Suite comes bundled with PeopleTools, but each product has its own unique license code. You might discover, after installation, that you used the wrong license code. When you enter an incorrect license code, an error occurs while loading the database with the PeopleSoft Database Configuration Wizard or Data Mover utility.

Attention: The PeopleTools System Database requires a separate license than your regular PeopleTools license. Therefore, when installing PeopleTools, enter the individual product license code, not the regular PeopleTools license.

Fixing a corrupted WebSphere server configuration file

You might encounter one of two different corruptions to the WebSphere server configuration file, either with a duplicated web module ID or a corrupted XML statement.

Problem 1: When PeopleSoft installs its web application into WebSphere application server, the web module IDs are hard coded as WebModuleRef_9, WebModuleRef_10, and WebModuleRef_11. If you have installed other web applications prior to PeopleSoft, such as the Content Manager resource manager or Content Manager eClient, the WebSphere Application Server configuration file might become corrupted. You can manually edit the file, `server-cfg.xml`, to fix the problem.

Problem 2: If the configuration file is corrupted, then you cannot start WebSphere Application Server Advanced Edition Single Server (WAS AES). Look for a CLASSPATH specification in the middle of the XML file and remove the extra characters that are corrupting the file. For example, you might find the following corrupted XML statement in the middle of the server configuration file:

```
<properties xmi:id;${WAS_ROOT}/installedApps/peoplesoft/PORTAL/WEB-INF/lib/entapplethttp.jar;${WAS_ROOT}/installedApps/peoplesoft/PORTAL/WEB-INF/lib/entappletp10.jar;${WAS_ROOT}/installedApps/peoplesoft/PORTAL/WEB-INF/lib/entappletp12.jar;${WAS_ROOT}/installedApps/peoplesoft/PORTAL/WEB-INF/lib/entappletp5.jar;${WAS_ROOT}/installedApps/peoplesoft/PORTAL/WEB-INF/lib/entappletp7.jar;${WAS_ROOT}/installedApps/peoplesoft/PORTAL/WEB-INF/lib/entappletp1.jar"SystemProperty_4" name="MaxConnectBacklog" value="511"/>
```

Replace the corrupted XML statement with this XML statement:

```
<properties xmi:id="SystemProperty_4" name="MaxConnectBacklog" value="511"/>
```

Correct domain name for the PeopleSoft Internet Architecture

When you specify the authentication domain during installation of the PIA, you must start the domain name with a period (.). Do not use imbedded blanks. For example, if the domain to which both these application servers belong is `abc.def.ghi.com`, your domain specification must be `.abc.def.ghi.com`. Later, users must supply the fully qualified host name in the URL used to access the PeopleSoft portal. If you do not make these changes, users cannot open the PeopleSoft portal home page.

Enabling browsers to accept cookies

The browsers used to access the PeopleSoft portal and the eClient must have their browsers set up to enable cookies. If cookies are disabled, you cannot access these pages. In Internet Explorer, you need to enable per-session cookies. In Netscape Navigator, you need to enable cookies that are sent back to the originating server.

To enable cookies:

- For Microsoft Internet Explorer Version 5:
 1. Open the Microsoft Internet Explorer browser.
 2. Select **Tools** --> **Internet Options**. The Internet Options window opens.
 3. Click the **Security** tab and click **Custom Level**. The Security Settings window opens.
 4. Scroll down to the **Cookies** section.
 5. Under the Allow per-session cookies (not stored) subsection, click **Enable**.
- For Microsoft Internet Explorer Version 6:
 1. Open the Microsoft Internet Explorer browser.
 2. Select **Tools** --> **Internet Options** --> **Privacy** --> **Advanced**. The Advanced Privacy Settings window opens.
 3. Click the **Override automatic cookie handling** and **Always allow session cookies** check boxes.
 4. Select any radio buttons in **First-party Cookies** and **Third-party Cookies**. The choices that you make do not affect PeopleSoft's integration with the eClient.
- For Netscape Navigator 4.7:
 1. Open the Netscape Navigator browser.
 2. Select **Edit** --> **Preferences**. The Preferences window opens.
 3. In the **Category** list, click **Advanced**.
 4. Under the Cookies section, select **Accept only cookies that get sent back to the originating server**.
- For Netscape Navigator 6.2:
 1. Open the Netscape Navigator browser.
 2. Select **Edit** --> **Preferences**. The Preferences window opens.
 3. In the Category list, click **Privacy & Security** --> **Cookies**.
 4. Under the Cookies section, select either **Enable cookies for the originating web site only** or **Enable all cookies**.

Using multiple PeopleSoft servers

When an installation has more than one PeopleSoft server and these servers all have the defaults from the original installation, then they have the same message node names. This occurrence might be considered a feature that could be exploited for fail-over purposes. However, one consequence is that when more than one PeopleSoft server has the same user ID defined, any one of those servers can authenticate the user ID used to log on to the eClient. If the Content Manager system administrator considers that this is a security risk, the workaround is to change the MSGNODENAME in all the tables where the default message node name is found. Contact PeopleSoft Global Support Center for the database script needed to modify all instances of MSGNODENAME in your RDBMS.

Using spaces for tab names in PeopleSoft

In PeopleSoft, when the user clicks over to a tabbed page on the portal (or when the browser is automatically directed to a tabbed default homepage), PeopleSoft's

internal name of the tab is part of the URL. If the internal name of a tab has a space in it, then the URL has a space in it. Some versions of Netscape Navigator do not encode the space as %20, but Microsoft Internet Explorer does. Therefore, if you are using Netscape Navigator and you want to create tabbed pages on the PeopleSoft portal, do not use a space in the tab name.

PeopleSoft authentication timeout

If a PeopleSoft user signs on to PeopleSoft and does not click over to the eClient before the PS_TOKEN cookie times out, then the user cannot access Content Manager. The PS_TOKEN cookie is used for PeopleSoft user authentication and the default timeout value is 720 minutes (12 hours). Modification of the PS_TOKEN cookie timeout value affects all users of the PeopleSoft system. To modify the timeout value from the PeopleSoft Portal Enterprise Menu:

1. Select **PeopleTools -> Security -> Security Objects -> Single Signon**.
2. Change the Authentication Token expiration.
3. Click **Save**.

Troubleshooting scenarios

Scenario 1: eClientToken message

Problem:

When a PeopleSoft user performs a search, the following error message appears in the eClient trace log: "Either an eClientToken value or an authCookie value must be provided in the Integration Properties File."

Solution:

Provide an authCookie value in the IP file.

Scenario 2: Blank eClient browser window

Problem:

A PeopleSoft user receives a blank eClient browser window.

Solution:

1. Look in the eClient trace log for more information.
2. Check the URL used to invoke the eClient. Ensure that all required parameters and values have been specified.
3. Check the Integration Properties file specified by the URL. Ensure that all required properties and values have been specified.

Scenario 3: Error report (single sign-on pagelet)

Problem:

A PeopleSoft user encounters the followed error report when attempting to use the single sign-on pagelet to access the eClient: "Your session has expired or you have not logged on." This problem can occur when a browser window for an eClient on server "A" is accidentally superseded by a browser window for an eClient on server "B". This might happen if the user forgets that there is already an active eClient "A" session and then starts a new window for eClient "B" from the same Microsoft Internet Explorer session, without logging off from eClient "A" first.

Solution:

Use the Netscape Communicator browser, or log off before launching a new eClient browser window with Microsoft Internet Explorer.

Scenario 4: Greater or fewer privileges for a second eClient user**Problem:**

A second eClient user is granted greater or fewer privileges than designated. For example, user A is allowed to see user B's search templates. This problem can occur when an eClient window for privilege "A" user is accidentally superseded by a new eClient window for a privilege "B" user. This might happen if the user forgets that there is already an active eClient session (logged on for user with privilege set "A") and then starts a new eClient window, from the same Microsoft Internet Explorer session, and then logs on again for user with privilege set "B" without logging off user "A" first.

Solution:

Use the Netscape Communicator browser, or logoff before launching a new eClient browser window with Microsoft Internet Explorer.

Scenario 5: Error report (document viewer)**Problem:**

When trying to use the document viewer to access content on the eClient, the browser window displays the following error report: "An Error Has Occurred! com.ibm.mm.beans.CMBNoConnectionException: There is no established connection to the server. The connection has been disconnected." This problem can occur when an eClient window is accidentally superseded by a new eClient window. This might happen if the user forgets that there is already an active eClient session and then attempts to start a new eClient window, from the same Microsoft Internet Explorer session, without logging off first.

Solution:

Use the eClient applet viewer to access content, use the Netscape Communicator browser, or logoff before launching a new eClient browser window with Microsoft Internet Explorer.

IBM Content Manager, PeopleSoft and LDAP

Currently, use of both LDAP authentication and PeopleSoft single sign-on is not supported on the same Content Manager library server. If you have configured your Content Manager library server for optimized association you cannot authenticate with LDAP, regardless of whether the user is signing on from PeopleSoft or not. If the library server is configured to perform LDAP authentication, it is still possible to use loose association.

The Content Manager system administration client provides a tool to import users from LDAP into Content Manager. The import facility assumes that you are importing users from LDAP into Content Manager with the intention of using LDAP authentication. However, when a user is imported into Content Manager from LDAP, there are alternative ways to get this user authenticated:

- Enable the PeopleSoft single sign-on feature by configuring for optimized association. After completing this configuration, you can now proceed to use the PeopleSoft single sign-on authentication.
- Define users on the machine where Content Manager resides and configure the pagelets that they access for loose association. Additionally, imported users that intend to use the stand-alone eClient must also be defined locally on the machine where Content Manager resides.

Troubleshooting Siebel Integration for IBM Content Manager

Troubleshooting Scenarios

If you encounter problems, review the following scenarios for help:

Scenario 1: Blank page displayed:

Problem: A blank page is displayed.

Solution:

1. Make sure that your browser supports IFRAMES.
2. Check the IP file to ensure that eClientToken, server, userid, password, type, cssPrefix, iconPrefix, and printEnabled property values are correctly specified.
3. Verify that the search criterion name is spelled correctly and is in proper case. You can find the search criterion name in the calculated field, which you configured using Siebel Tools.
4. Make sure that the search criterion value is valid. You can find the search criterion value in the calculated field or symbolic URL that you configured using Siebel Tools.

Scenario 2: Inconsistent colors and fonts:

Problem: The colors displayed and the sizes of the fonts used by the integration JavaServer Pages appear inconsistent with the standard Siebel application colors and fonts.

Solution:

Verify that type is set to 1 and that cssPrefix is set to alt1 in the IP file.

Scenario 3: Problem of graphical buttons:

Problem: The graphical buttons on the document viewer toolbars do not appear at all, or appear to be inconsistent with the standard Siebel application graphical buttons.

Solution:

Verify that iconPrefix is set to alt1 in the IP file.

Scenario 4: Unexpected session expiration error:

Problem: You encounter this unexpected error message: Your session has expired or you have not logged on.

Solution:

This happens when you are using Microsoft Internet Explorer Version 6 with the Siebel Web client, or your session has timed out. If you are using Microsoft Internet Explorer Version 6, change the browser privacy setting to Low or Accept All Cookies.

Another alternative is to configure a special privacy setting for the eClient Web site. Otherwise, initiate another logon session by clicking on the Web template tab.

Scenario 5: SQL0954C error:

Problem: While performing a search or other action, you encountered this error:

SQL0954C Not enough storage is available in the application heap to process the statement. SQLSTATE=57011.

Solution:

Increase the size of the DB2 application heap. You can use the applheapsz database configuration variable. See the DB2 Universal Database documentation for more information concerning this procedure.

Scenario 6: Search error when adding a new record to a Siebel entity:

This scenario only applies if your calculated field has a calculated value that is an IFRAME containing a URL.

Problem:

When a Siebel end user creates an instance of a Siebel entity (for example, a service request), the following message displays:

An Error has Occurred

No search String specified.

The above error messages typically display because the calculated field for the Siebel entity references a field within the entity that does not yet have a value. For example, these error messages appear for the following calculated field value when a service request is created:

```
<IFRAME height=300 width=960 frameborder=0
src='http://ec82fvt:80/eClient82/IDMIntegrator?eClientToken=token
&IPFile=Siebel&Entity=SRST&L="+[Contact Last Name]+"&ReleaseLevel=SiebelV704'>
Sorry your browser does not support IFRAMES.</IFRAME>
```

Solution:

Replace the existing calculated field value with the following:

```
IIF ([Contact Last Name] is not null,[AC1],[AC2])
```

AC1 is a calculated field with a calculated value property equal to the calculated value property of the existing calculated field and AC2 is another calculated field with the following calculated value property: "<IFRAME height=300 width=960 frameborder=0 src=''>Sorry your browser does not support IFRAMES</IFRAME>"

Note: IIF in the above code sample is not a typo, and must be correctly entered in the calculated field to fix this problem.

Scenario 7: authCookie message:

Problem: When a Siebel user performs a search, the following error message appears in the eClient trace log:

Either an eClientToken value or an authCookie value must be provided in the Integration Properties File.

Solution:

Provide an eClientToken value in the IP file.

Scenario 8: Search not performed when using a symbolic URL:

Problem: When a Siebel user attempts to perform a search, the search request is not sent to the eClient.

Solution:

Verify that each symbolic URL argument has an argument value. If a required argument has no value, the request is not sent, because there is no value to append to the URL.

Scenario 9: Extraneous "WI_UndefinedSymbolicURL:=" error message:

Problem: A Siebel system administrator re-configures the Siebel 7.5.2 application to use an IFRAME with an embedded URL rather than a symbolic URL. Then, when users execute search requests, the displayed search results list is correct, but an extraneous WI_UndefinedSymbolicURL:= error message also appears on the screen.

Solution:

During initial configuration for use of a symbolic URL, the value of the Field Retrieval Type field within the control for the calculated field was set to Symbolic URL. This value is invalid when using an IFRAME with an embedded URL. Change the value of the Field Retrieval Type field to blank.

Scenario 10: Security alert pop-ups with HTTPS:

Problem: The browser displays one or more security alert pop-ups when using HTTPS as the protocol for a URL within a calculated value field or symbolic URL.

Solution:

Use a valid certificate issued from a trusted certificate authority, or install the self-signed certificate in the certificate store. Certificates can be installed directly from the security alert popup dialog by selecting **view certificate** followed by **install certificate**. This action launches the certificate import wizard.

Miscellaneous tips

Tip 1: You might encounter problems when attempting to access the eClient and Siebel using browser windows on the same client system.

Tip 2: After you make changes to the business objects and user interface layers that are visible to users of the Siebel Web client, you must:

1. Compile from within Siebel Tools.
2. Stop the Siebel server service.
3. Copy the Siebel repository (.srf) file to the *SIEBELROOT*\siebsrvr\object\ directory, where *SIEBELROOT* is the root directory where the Siebel application server is installed.
4. Restart the Siebel server service after the copy operation is complete.

Tip 3: If the eClient is configured to use the viewer applet, and your Siebel Integration configuration contains multiple IP files, the `printEnabled` property that is used by the applet viewer corresponds to the search that returned the first document opened in the applet viewer window. This applies every time the viewer applet window is opened.

Tip 4: A user ID that is associated with a Siebel application request must have authorization to access the federated server database containing the Siebel Integration search templates and all content server databases that the request accesses.

Trace information

All error and trace information is recorded in the eClient trace files. You can set the location, information level, and size for these files by setting parameters in the `IDM.properties` file. For detailed information, see "Trace information" in *Installing, Configuring, and Managing the eClient*.

Some of the error and information messages available only in English.

Chapter 9. Removing

This section covers information about how to remove the eClient and third-party application integration.

“Removing the eClient”

“Removing third-party application integration” on page 122

Removing the eClient

Remove the eClient before removing Enterprise Information Portal, because the eClient uninstall program uses Java Virtual Machine (JVM), which might reside in CMBROOT. To remove the eClient from Windows:

1. From the Control Panel, open **Add/Remove Programs**.
2. Select **IBM Content Manager eClient** from the list.
3. Click **Add/Remove**.

All of the installed eClient files and directories are removed from your machine. Any files or directories that you have modified or any files or directories that you have created remain. The properties file is not deleted. To delete these files, delete the root directory where the eClient is installed.

To remove the eClient from AIX:

1. Change to the `/opt/CMeClient/_uninst` directory, where `/opt/CMeClient` is the root directory where the eClient is installed.
2. Enter
`./aixuninstall`
3. Follow the instructions provided.

All of the installed eClient files and directories are removed from your machine. Any files or directories that you have modified or any files or directories that you have created remain. The properties file is not deleted. To delete these files, delete the root directory where the eClient is installed.

To remove the eClient from Solaris:

1. Change to the `/opt/CMeClient/_uninst` directory, where `/opt/CMeClient` is the root directory where the eClient is installed.
2. Enter
`./uninstall.bin`
3. Follow the instructions provided.

All of the installed eClient files and directories are removed from your machine. Any files or directories that you have modified or any files or directories that you have created remain. The properties file is not deleted. To delete these files, delete the root directory where the eClient is installed.

Removing third-party application integration

This section describes the process for removing third-party application integration.

“Removing PeopleSoft Integration for IBM Content Manager”

“Removing Siebel Integration for IBM Content Manager”

Removing PeopleSoft Integration for IBM Content Manager

PeopleSoft Integration for IBM Content Manager is automatically removed when you remove the eClient.

The Content Manager uninstall program automatically removes all of the PeopleSoft Integration for IBM Content Manager files except for ICMXLSLG.DLL file. The ICMXLSLG.DLL file is not part of the typical Content Manager uninstall program because this DLL file has moved from its default installation location to activate PeopleSoft single sign-on.

You can remove the ICMXLSLG.DLL in two ways:

- Type the path to the ICMXLSLG.DLL file when prompted by the Content Manager uninstall program. The file is located in *ICMROOT\database name\DLL*, where *ICMROOT* is the location where you installed Content Manager and *database name* is the name of the library server database.
- Remove the file manually after the Content Manager uninstall program is finished.

Removing Siebel Integration for IBM Content Manager

The Siebel Integration for IBM Content Manager is automatically removed when you remove the eClient.

To restore the Siebel environment, undo all of the steps in “Configuring Siebel Integration for IBM Content Manager” on page 53 or import the SRF file that you archived before configuring Siebel Integration for IBM Content Manager.

Delete the two Web templates (EIP81Applet.swt and EIP81Body.swt) from each of the following directories where *SIEBELROOT* is the root directory where the Siebel application server is installed:

SIEBELROOT\siebsrvr\WEBTEMPL

SIEBELROOT\client\WEBTEMPL

SIEBELROOT\tools\WEBTEMPL

Chapter 10. Getting more information

You can get more information about the eClient and third-party application integration from a variety of resources including books and online support.

Related reference:

“eClient”

“Third-party business applications and integration”

eClient

You can access the latest information about the IBM Content Manager eClient and Enterprise Information Portal from:

www.ibm.com/software/data/eip/support.html

You can access the latest information about the WebSphere Application Server from: www.ibm.com/software/webservers/appserv/support.html

Third-party business applications and integration

You can get more information about third-party business applications and their integration with IBM products from the IBM documentation library and the Web sites of business applications.

Related tasks:

“Getting more information about PeopleSoft Integration for IBM Content Manager”

“Getting more information about Siebel Integration for IBM Content Manager” on page 124

Getting more information about PeopleSoft Integration for IBM Content Manager

This section contains a list of resources that you can use to further educate yourself on Content Manager, Enterprise Information Portal, WebSphere, and PeopleSoft.

IBM Content Manager for Multiplatforms Version 8 Release 2

Table 6 identifies the Content Manager information that helps you to migrate, install, configure, administer, and remove Content Manager. You can access this information from the Information Center if you installed it or from the CDs that came with Content Manager.

Table 6. Information available in the Content Manager library.

Title	File name on documentation CD
<i>Planning and Installing Content Manager</i>	install.pdf
<i>System Administration Guide</i>	sysadmin.pdf
<i>Modeling Your Data in Content Manager Version 8</i>	dtmodmst.pdf

You can also find product support at www.ibm.com/software/data/cm/

IBM Enterprise Information Portal for Multiplatforms Version 8 Release 2

Table 7. Information available in the Enterprise Information Portal library.

Title	File name on documentation CD
<i>Planning and Installing Information Integrator for Content</i>	eipinst.pdf
<i>Managing Information Integrator for Content</i>	eipmanag.pdf
<i>Workstation Application Programming Guide</i>	apgwork.pdf
<i>Messages and Codes</i>	messcode.pdf
Online Application Programming Reference	onlineapr.zip
<i>Installing, Configuring, and Managing the eClient</i>	ecliinst.pdf

You can also find product support at www.ibm.com/software/data/eip

WebSphere Application Server

You can access the latest information about WebSphere Application Server from www.ibm.com/software/webservers/appserv/support.html

PeopleSoft PeopleBooks

You can get the following PeopleSoft PeopleBooks from the PeopleSoft product Web site at www.peoplesoft.com:

- *Using PeopleSoft Applications*
- *Data Management*
- *PeopleCode Developer's Guide*
- *PeopleCode Reference*
- *PeopleSoft Application Designer*
- *PeopleSoft Component Interfaces*
- *PeopleSoft Enterprise Integration*
- *PeopleSoft Internet Architecture Administration*
- *PeopleSoft Portal Technology*
- *Security*

Getting more information about Siebel Integration for IBM Content Manager

This section contains a list of resources that you can use to further educate yourself on Content Manager, Enterprise Information Portal, WebSphere, and Siebel eBusiness applications.

IBM Content Manager for Multiplatforms

Table 6 on page 123 identifies the Content Manager information that helps you to migrate, install, configure, administer, and remove Content Manager. You can access this information from the Information Center if you installed it, or from the CDs that came with Content Manager.

Table 8. Information available in the Content Manager library.

Title	File name on documentation CD
<i>Planning and Installing Content Manager</i>	<i>install.pdf</i>
<i>System Administration Guide</i>	<i>sysadmin.pdf</i>

Table 8. Information available in the Content Manager library. (continued)

Title	File name on documentation CD
<i>Modeling Your Data in Content Manager Version 8</i>	<i>dtmodmst.pdf</i>

You can access the latest information about IBM Content Manager at:
www.ibm.com/software/data/cm/.

IBM Enterprise Information Portal for Multiplatforms Version 8.1

Table 9. Information available in the Enterprise Information Portal library.

Title	File name on documentation CD
<i>Planning and Installing Information Integrator for Content</i>	<i>eipinst.pdf</i>
<i>Managing Information Integrator for Content</i>	<i>eipmanag.pdf</i>
<i>Workstation Application Programming Guide</i>	<i>apgwork.pdf</i>
<i>Messages and Codes</i>	<i>messcode.pdf</i>
<i>Online Application Programming Reference</i>	<i>onlineapr.zip</i>
<i>Installing, Configuring, and Managing the eClient</i>	<i>ecliinst.pdf</i>

You can also access the latest information about IBM Enterprise Information Portal Version 8.1 and the eClient Version 8.1 at: www.ibm.com/software/data/eip

WebSphere Application Server

You can access the latest information about WebSphere Application Server from:
www.ibm.com/software/webservers/appserv/support.html

Bookshelf for Siebel eBusiness Application

You can access the latest information about Siebel eBusiness applications within *Bookshelf for Siebel eBusiness Applications Version 7.0.4* or *Bookshelf for Siebel eBusiness Applications Version 7.5.2* on the Siebel product CD.

Chapter 11. Sample properties files

This section provides a sample `IDMdefault.properties` file that is used by the eClient and a sample Integration Properties file (IP file) that is used by Siebel Integration for IBM Content Manager.

A sample `IDMdefault.properties` file

```
#-----
# Licensed Materials - Property of IBM
# IBM CM eClient
#
# (C) Copyright IBM Corporation 2002,2003. All rights reserved.
#
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM
# Corporation.
#
# DISCLAIMER OF WARRANTIES:
#-----
#
# The version number of this install.
# It is used during installation of this product.
#
# You should NOT edit this property.
#
# Format: ver=XX [where XX = version number, numerals only, no decimals
# -- v 7.12 = 712, -- v 8.1 = 81]
#
# Example:
# ver=82
#
ver=82
#-----
#
# Property Daemon is a daemon thread that monitors application property changes and
# reloads all properties if a change was detected. PropertyDaemonInterval is the
# time interval between checks of changed properties. Values are in minutes.
#
# Valid values are integrals greater than or equal to zero. Any integral value
# less than zero will default to 1. Also, non-integral or a missing value will
# default to 1. A value of 0 disables the daemon.
#
# Note: PropertyDaemonInterval does have an impact on application performance
#
PropertyDaemonInterval=10
#-----
#
# Application level tracing. Trace valid values are (0|1|2|3|4|5).
# 0 = tracing off
# 1 = exceptions, and errors
# 2 = level 1 with the addition of general information, method entry, and
# method exit points
# 3 = level 2 with the addition of API calls
# 4 = level 3 with the addition of EIP non-visual bean Tracing
# 5 = performance tracing
#
#
# You must stop and restart the eClient App Server for changes to Trace
```

```

# to take effect.
#
TraceLevel = 1
#-----
#-----
# Working Directory.
# WorkingDir = logging, tracing, and temp data conversion directory
#
# Example: Windows "C:\\CMeClient\\logs"
# AIX      "/opt/CMeClient/logs"
# Sun      "/opt/CMeClient/logs"
#
WorkingDir=
#-----
#-----
# Cache Directory.
# CacheDir = storage area for document caching
#
# Example: Windows "c:\\CMeClient\\cache"
# AIX      "/opt/CMeClient/Cache"
# Sun      "/opt/CMeClient/Cache"
#
CacheDir=
#-----
#-----
# Image URL
# ImageURL = The path to jsp images
#
ImageURL=/eClient82/icons
#-----
#-----
# Error Page. This page is called in an event of an application error.
# ErrorPage = the name of error reporting jsp.
# ErrorPage=/ErrorPage.jsp
#-----
#-----
# Servlet JSPs
# The JSP to be used to display data from servlets.
# Output.IDMLogon=/IDMLogon.jsp
Output.IDMSearch=/IDMSearchFrame.jsp
Output.IDMConnection_in=/IDMActionPage.jsp
Output.IDMConnection_out=/IDMLogon.jsp
Output.IDMConnection_disc=/IDMLogon2.jsp
Output.IDMSortSearchResults=/IDMSearchResults.jsp
Output.IDMDocViewer=/IDMViewFrames.jsp
Output.IDMOpenFolder=/IDMFoldercontents.jsp
Output.IDMOpenFolderContents=/IDMFoldercontents.jsp
Output.IDMChangePassword_in=/IDMChangePassword.jsp
Output.IDMChangePassword_out=/IDMLogon2.jsp
Output.IDMEmail=/IDMEmail.jsp
Output.IDMDeleteItem_in=/IDMDeleteItem.jsp
Output.IDMDeleteItem_out=/IDMDeletedItem.jsp
Output.IDMAddItem_in=/IDMAddItem.jsp
Output.IDMAddItem_out=/IDMAddedItem.jsp
Output.IDMCreateFolder_in=/IDMAddItem.jsp
Output.IDMCreateFolder_out=/IDMCloseWindow.jsp
Output.IDMAddItemToFolder_in=/IDMAddItemToFolder.jsp
Output.IDMAddItemToFolder_out=/IDMCloseWindow.jsp
Output.IDMRemoveItemFromFolder_in=/IDMFolderDeleteItem.jsp
Output.IDMRemoveItemFromFolder_out=/IDMCloseWindow.jsp
Output.IDMClipboard_in=/IDMClipboard.jsp
Output.IDMClipboard_out=/IDMCloseWindow.jsp
Output.IDMItemVersioning_in=/IDMItemVersions.jsp
Output.IDMItemVersioning_out=/IDMCloseWindow.jsp
Output.IDMEditAttributes_in=/IDMEditAttributes.jsp
Output.IDMEditAttributes_out=/IDMCloseWindow.jsp
Output.IDMODUpdateAnnotations=/IDMODAnnotationsFrame.jsp

```

```

Output.IDMODAnnotationsList_in=/IDMODAnnotationsList.jsp
Output.IDMODAnnotationsList_out=/IDMCloseWindow.jsp
Output.IDMODAnnotationsView_in=/IDMODAnnotationsView.jsp
Output.IDMODAnnotationsView_out=/IDMCloseWindow.jsp
Output.IDMNoteLog_in=/IDMNoteLog.jsp
Output.IDMNoteLog_out=/IDMCloseWindow.jsp
Output.IDMUserMapping_in=/IDMUserIDMapping.jsp
Output.IDMUserMapping_out=/IDMLogon2.jsp
#-----
#
# Web Application Name.
# WebAppName = Web Application Name, default value is /eClient82
#
WebAppName=/eClient82
#-----
#
# Maximum Search Results displayed per screen.
#
#
#-----
MaxResults=10
#-----
# Maximum Search Results retrieved from the server per search criterion.
#
# Values: -1 returns all hits
#
# NOTE: Note this value should be set to value other than -1 if searches begin
# to timeout. Users search criteria should also be refined if the search
# results are larger than the value of TotalMaxResults.
#
#
#
#-----
TotalMaxResults=-1
#-----
# URL for cmbcc2mime.ini file
# The cmbcc2mime.ini file consists of the Content classes associated
# with a MIME type. The different Content Classes defined in this file can
# be associated with a MIME type that the Server will send to the client.
# The client will use that MIME type to launch the application associated
# to that MIME type.
#
# Example: Windows cmbCC2MimeURL=file:///C:
# \\Program Files\IBM\CMgmt\cmbcc2mime.ini
# AIX cmbCC2MimeURL=file:///usr/lpp/cmb/cmgmt/cmbcc2mime.ini
# Sun cmbCC2MimeURL=file:///IBMcmb/cmgmt/cmbcc2mime.ini
#
# NOTE: This URL should not be a file or localhost URL when remote connectors
# are used via RMI (when connectiontype or serviceconnectiontype is 1 or 2).
# This file is shared by the connectors and should be at a URL that is
# accessible to all the RMI servers that are in use. For
# instance, http://cm.ibm.com/eClient82/cmbcc2mime.ini would point
# to a cmbcc2mime.ini file that the administrator has stored with the
# eClient web application for use by all the RMI servers.
#
cmbCC2MimeURL=

#-----
#
# URL for cmbcs.ini file
# The cmbcs.ini file is installed with each client and system administration
# program. In cmbcs.ini, there are variables you must set to remote or local
# to find the content server runtimes
#
# Example: Windows CsIniURL=file:///C:\Program Files\IBM\CMgmt\cmbcs.ini
# AIX CsIniURL=file:///usr/lpp/cmb/cmgmt/cmbcs.ini

```

```

# Sun      CsIniURL=file:///IBMcmb/cmgmt/cmbcs.ini
#
CsIniURL=
#-----
#-----
# The URL of the cmbclient.ini file that defines the RMI server.
#
# Example: Windows ClientIniURL=file:///C:\\ProgramFiles\\IBM
# \\CMgmt\\cmbclient.ini
# AIX      ClientIniURL=file:///usr/lpp/cmb/cmgmt/cmbclient.ini
# Sun      ClientIniURL=file:///IBMcmb/cmgmt/cmbclient.ini
#
ClientIniURL=
#-----
#-----
# URL of the cmbsvcs.ini file that defines how to access workflow. This value is
# used only when the serviceconnectiontype is set to 2 (dynamic).
#
# Default: not specified (null)
#
# Example: Windows cmbsvcs=file:///C:\\Program Files\\IBM\\CMgmt\\cmbsvcs.ini
# AIX      cmbsvcs=file:///usr/lpp/cmb/cmgmt/cmbsvcs.ini
# Sun      cmbsvcs=file:///IBMcmb/cmgmt/cmbsvcs.ini
#
# NOTE: This property is ignored when serviceconnectiontype is set to 0
# (local) or 1 (remote).
# This property is required when serviceconnectiontype is set to 2 (dynamic).
#
cmbsvcs=
#-----
#-----
# The URL of the cmbsvclient.ini file that defines the workflow RMI server.
# Default: not specified (null)
#
# Example: Windows cmbsvclient=file:///C:\\ProgramFiles\\
# IBM\\CMgmt\\cmbsvclient.ini
# AIX      cmbsvclient=file:///usr/lpp/cmb/cmgmt/cmbsvclient.ini
# Sun      cmbsvclient=file:///IBMcmb/cmgmt/cmbsvclient.ini
#
# NOTE: This property is ignored when serviceconnectiontype is set to 0 (local).
# This property is required when
# serviceconnectiontype is set to 1 (remote) or 2 (dynamic).
#
cmbsvclient=
#-----
#-----
#
# Location of the server initialization file for CMv8 servers.
# (note: has same purpose as the v7 file frnolint.tbl)
# Value should be the fully qualified URL giving the location of the file
# cmbicmsrvs.ini.
# (note: If your CMv8 server ini file has a different name, you should use
# it's URL.)
#
# Format: ICMServersURL=[fully qualified URL] (forward slashes escaped)
#
# Example: Windows ICMServersURL=file:C:\\ProgramFiles
# \\IBM\\CMgmt\\cmbicmsrvs.ini
# AIX      ICMServersURL=file:///usr/lpp/cmb/cmgmt/cmbicmsrvs.ini
# Sun      ICMServersURL=file:///IBMcmb/cmgmt/cmbicmsrvs.ini
#
ICMServersURL=
#-----
#-----
# Specifies the location of EIP database and content server runtimes.
# (default type is local)

```

```

#
# 0 = local
# 1 = remote
# 2 = dynamic
#
# If connectionType = local, the ClientIniURL is ignored. All content server
# runtimes will be treated as local, ignoring the values in cmbcs.ini
# If connectionType = remote, ClientIniURL will be used
# to tell the system where to locate the cmbclient.ini
# and CsIniURL will be ignored. All content server runtimes will be
# treated as remote, ignoring the values in cmbcs.ini
# If connectionType = dynamic, ClientIniURL will also be used
# to tell the system where to locate the cmbclient.ini,
# and CsIniURL will be used to tell the system where to
# locate the cmbcs.ini. Content server runtime local or remote will
# be determined from cmbcs.ini
# Note : As ICM servers do not need to use remote runtimes, specifying
# connectiontype = 1 (remote) , will remove ICM servers from the list.
#
ConnectionType=0
#-----
#-----
# Specifies the location of the workflow service. Default: 0 (zero)
#
# Valid input: An integer : 0, 1, 2
#
# Set to 0 if you are using a local configuration. This means workflow
# is installed on your Web server.
#
# Set to 1 if you are using a remote configuration. This means workflow
# is installed on an RMI server as defined in the cmbsvclient attribute.
#
# Set to 2 if you are using a dynamic configuration. This means workflow
# is installed either on your Web server or RMI server, according to the
# cmbsvcs attribute.
#
serviceconnectiontype=0
#-----
#-----
# Specifies whether the cache is enabled for the workflow data.
#
# Default: false
#
# Valid input: Boolean : true, false
#
workflowcache=false
#-----
#-----
# OD Server connection properties [alias:(ip or hostname):port]
# Alias will be used to represent the name of the server to the user.
#
# Example: BigBlue:eserver.ibm.com:80
# BigBlue - will be presented to the user on the logon screen
# eserver.ibm.com - hostname or ip address of the OnDemand server
# 80 - connection port for the OnDemand server
#
# Additional servers can be added by specifying the name-value pair as follows:
#
# Datastore.OD.0 = alias:(ip or hostname):port
# Datastore.OD.1 = alias:(ip or hostname):port
# Datastore.OD.2 = alias:(ip or hostname):port
# . . . . . = alias:(ip or hostname):port
# Datastore.OD.7 = alias:(ip or hostname):port
#
#Datastore.OD.0=OD390:test.ibm.com:3219
#-----
#-----

```

```

# connect_string is a string which supplies all of the specific connection
# parameters to establish and maintain a connection to the IP390 backend
# server.
#
# Additional servers can be added by specifying the name-value pair as follows:
#
# Datastore.IP390.0 = connection string
# Datastore.IP390.1 = connection string
# Datastore.IP390.2 = connection string
# . . . . . = connection string
# Datastore.IP390.7 = connection string
#
# Example: Datastore.IP390.0=ALIAS=IP390;APPL=01;FAFIP=9.67.43.83;IODMIP=9.67.43.83;
# FAFPORT=3061;IODMPORT=3082;FAFPROT=4000;IODMPROT=4000;FAFSITE=CS61
#
# Valid parameters are:
#
# ALIAS =Alias name for the server. This name will be presented to the
#end user for this server.
#This parameter is required
#
# APPL =The Application Id of the FAF Host application to connect.
# This parameter is required.
#
# FAFIP = The TCPIP address of the FAF Host to connect. This
# parameter is required.
#
# IODMIP =The TCPIP address of the IODM Host to connect. This
# parameter is required.
#
# FAFPORT =The TCPIP port number of the FAF Host.This
# parameter is required.
#
# IODMPORT=The TCPIP port number of the IODM Host. This parameter
# is required.
#
# FAFPROT =The communication protocol of the FAF Host. Valid values
# are (4000 for TCPIP on CICS, and 4500 for TCPIP on IMS). This
# parameter is required.
#
# IODMPROT=The communication protocol of the IODM Host. Valid values
# are (4000 for TCPIP on CICS, and 4500 for TCPIP on IMS).This
# parameter is required.
#
# TERMID =This is the IODM Terminal Id for this workstation. If not
# specified, the UserId will be used as the Terminal Id.
#
# FAFSITE =The 4 character symbolic ID of the FAF that owns and catalogs
# the documents associated with this datastore. This parameter
# is required forlocking, adding, updating or deleting annotations,
# and for locking folders and documents.
#
# OVERLAYS=This is the IODM Collection Class where all form overlays are stored.
# If not specified, forms will be searched for from the collection
# class where the last document was retrieved.
#
# IODMCNTL=This is the IODM document storage location control.
# If the document is not located at the specified location, the document
# will not be retrieved. Valid choices for value are:
# DASD
# Retrieve documents from DASD only.
# OPTICAL
# Retrieve documents from DASD or Optical only.
# SHELF
# Retrieve documents from DASD, Optical or shelf.
#
# Datastore.IP390.0=ALIAS=IP390;APPL=01;FAFIP=9.67.43.83;IODMIP=9.67.43.83;

```

```

FAFPOR=3061;IODMPOR=3082;FAFPRO=4000;IODMPRO=4000;FAFSITE=CS61
#-----
#-----
# Thin to Thick Toggle Switch
# adminDefined property allows the admin to create a file containing
# the file types which should be launched or transformed
# adminDefaultsFile property defines the mime types file to use
# or the mode of presentation for the mime type
#
# The default is to transform the document, and allow launching
# if the browser supports the mime type
#
adminDefined=true
adminDefaultsFile=/IDMadminDefaults.properties
#-----
#-----
# Specifies the Button Width to be used by eClient JSPs
#
# Default: 7
#
# Valid input: non-negative number
# jspButtonWidth=7
#-----
#-----
# Specifies the Button Height to be used by eClient JSPs
#
# Default: 18
#
# Valid input: non-negative number
#
jspButtonHeight=18
#-----
#-----
# Specifies the default edit field size
#
# Default: 40
#
# Valid input: non-negative number
# defaultAttributeLength=40
#-----
#-----
# Specifies the maximum file size (in bytes) allowed during import.
# Valid range (0 - 2147483647). This allows the admin to limit the size of
# files that can be imported via the eClient.
#
# Default: 2147483647
#
# Valid input: non-negative number
#
max_import_file_size=2000000
#-----
#-----
# Location of java plugin installation exe for IE.
#
# allows admin to set location from where java plugin should be
# installed by IE.
# plugin_exe=http://java.sun.com/products/plugin/autodl/jinstall-1_4_0-win.cab
# Version=1,4,0,0
# plugin_exe=http://java.sun.com/products/plugin/autodl/jinstall-1_4_0-win.cab
# Version=1,4,0,0
#-----
#-----
# Location of java plugin installation page for NN.
#
# allows admin to set location from where java plugin should be
# installed by NN.
# plugin_page=http://java.sun.com/j2se/1.4/download.html
#-----

```

```

#-----
#version of java plugin.
#
#allows admin to set version of java plugin the browser
#should use when invoking applets.
plugin_version=1.4
#-----
#
# Mail Properties
# mailUser specifies a valid user on the mailHost SMTP server.
# All mail returned will be returned to the mailUser.
mailUser=user@mymailhost.com
mailHost=mail.net
#-----
#
# workflowEnabled allows the administrator to enable or disable the
# workflow functionality of the client
# Valid values: "true" or "false"
#
workflowEnabled=false
#-----
#
# Enable/Disable Features
#
# checkInOutEnabled property allows the admin to "turn off" the Check in/out
# capabilities of the IDM Browser Client
checkInOutEnabled=false
#-----
#
# Enable/Disable Features
#
# emailEnabled property allows the admin to "turn off" the email
# capabilities of the IDM Browser Client
# capabilities of the IDM Browser Client
emailEnabled=false
#-----
#
# Enable/Disable display of server group error messages
#
# Valid input: true or false
# errorDisplayEnabled=false
#-----
#
# Enable/Disable reindexing of documents
#
# reIndexEnabled property allows the admin to turn off or on reindexing
# capabilities of the IDM Browser Client
# reIndexEnabled=true
#-----
#
# Enable/Disable Viewer Applet
#
# The viewerAppletEnabled property allows an admin to enable a viewer applet
# that will do client-based rotation, zooming, and graphical annotations editing.
# If this property is set to "true" the applet is used. If this property is set
# to "false" the applet is not used and rotation, zooming, and other functions
# will be done via JSP/HTML. Graphical annotation editing is only possible using
# the applet.
# NOTE: In addition to setting this property to true, you must specify
# which mime types the applet is to be used for in
# IDMAdminDefaults.properties.
# viewerAppletEnabled=false
#-----
#
# Specifies if import is enabled

```

```

# Default: false
#
# Valid input: true false
# importSupported=false
#-----
# Specifies if create folder is enabled
#
# Default: false
#
# Valid input: true or false
# CreateFolderEnabled=false
#-----
#-----
# Enable/Disable Direct retrieve from V8 Resource Manager
#
# The Viewer Applet can be set to retrieve document data directly from
# the CM V8 resource manager.
# This reduces processor, network, and disk space usage on the application
# server. However, if there are firewalls or other network security
# devices between the user's machine and the resource manager machine,
# this may fail. (The applet request uses HTTP, so normal proxies should
# not cause this failure. The failure is likely to occur when
# the application server is in a DMZ between firewalls and the user's
# machine is outside the firewalls and the resource manager is inside
# the firewalls.) This parameter is set to true in this file by
# default and will default to true if the setting is not present in this file.
directRetrieveEnabled=true
#-----
#-----
# On the logon server list on the logon page, display the server type with the
# server name. ex. "ICMNLSDDB (CM8)"
displayServerType=true
#-----
#-----
# For displaying of stored text like notelog, etc., there needs to be a
# default codepage set for the text to display properly. This value not
# used for CM8 notelogs.

default_char_encoding=Cp858
#-----
#-----
# Set the display resolution for the document. This is the desired display
# device resolution that is appropriate for documents.
default_display_resolution=96
#-----
#-----
# Set the preferred scale for the document.
# Scale of 1.0 represents actual size of 100%;
# Scale of 0.5 represents normal size of 50%.
preferred_scale=0.5
#-----
#-----
# Disable/enable image enhanced mode for the document viewer.
# This value does not apply to the viewer applet.
#
# NOTE: Setting enhance mode to false will reduce memory usage dramatically on
Mid-tier server

enhance_mode=false
#-----
#-----
# Disable/enable image enhanced mode for the document viewer.
# This value does not apply to the viewer applet.
#
# NOTE: Setting enhance mode to false will reduce memory usage
# dramatically on Mid-tier server

```

```

enhance_mode=false
#-----
#-----
# Disable/enable access to backend datastore
#
# A value of false will remove all backend servers of corresponding datastore
# type from the logon screen
#
# CM7 = CM 7.x or lower
# ICM = CM 8.x or higher
# FED = Federated Connections
# VI400 = Visual Info
#
# Valid input: true or false
# Default value: true
#
# NOTE: Setting datastores that are not used to false will boost performance of the
# application.
#-----
CM7=true
ICM=true
FED=true
VI400=true
#-----
# by default search arguments are repopulated on the search jsps
enable_search_arguments=true
#-----
#-----
# Specifies if creation of federated folders is enabled
#
# Default: true
#
# Valid input: true or false
#
createFedFolderEnabled=false
#-----

```

A sample IP file used by Siebel Integration

This section contains a sample IP file. A similar file named `Siebel.properties` is installed in the `ECLIENTROOT` directory, where `ECLIENTROOT` is the root directory where the eClient is installed.

```

#-----
# @copyright(disclaimer)
# Licensed Materials - Property of IBM
# IBM Content Manager for Multiplatforms V8.1 (Program Number 5724-B19)
# (C) Copyright IBM Corp. 1994, 2002 All Rights Reserved.
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM
# Corp.
#
# DISCLAIMER OF WARRANTIES:
#
# Permission is granted to copy and modify this Sample code, and to
# distribute modified versions provided that both the copyright notice
# and this permission notice and warranty disclaimer appear in all
# copies and modified versions.
#
# THIS SAMPLE CODE IS LICENSED TO YOU AS-IS. IBM AND ITS SUPPLIERS AND
# LICENSORS DISCLAIM ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, IN SUCH
# SAMPLE CODE, INCLUDING THE WARRANTY OF NON-INFRINGEMENT AND THE
# IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.
# IN NO EVENT WILL IBM OR ITS LICENSORS OR SUPPLIERS BE LIABLE FOR ANY
# DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE THE SAMPLE

```

```

# CODE, DISTRIBUTION OF THE SAMPLE CODE, OR COMBINATION OF THE SAMPLE CODE
# WITH ANY OTHER CODE.
# IN NO EVENT SHALL IBM OR ITS LICENSORS AND SUPPLIERS BE LIABLE FOR ANY
# LOST REVENUE, LOST PROFITS OR DATA, OR FOR DIRECT, INDIRECT,
# SPECIAL, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED
# AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF IBM OR ITS LICENSORS
# OR SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
#
# @endCopyright
#-----
#
# eClientToken is selected by a system administrator and must be provided in the
# URL by a business partner application that does not require the specification
# of authCookie. When the business partner application request is processed,
# the eClientToken value provided in the URL is compared with the token
# specified in this properties file. Valid characters for the eClientToken are
# any of the ISO 8859-1 Latin 1 characters with the exception of ";", "/", "?",
# ":", "@", "&", "=", "+", ",", and "$", which are reserved characters
# within the query string of a URL.
#
#-----
eClientToken=
#-----
# server specifies the name of the content server database that the
# IDMIntegrator servlet will access.
#
#-----

server=
#-----
# userid specifies the userid that will be used to access the content
# server database.
#
#-----
userid=
#-----
# password specifies the password for the userid that will be used to access
# the content server database.
#
#-----
password=
#-----
# type controls the objects that appear and the capabilities that are
# supported within a web page that is generated by the JavaServer Pages.
#
#-----
type=1
#-----
# cssPrefix specifies a file name prefix for the Cascading Style Sheet file that
# will be used by the JavaServer Pages. The specification determines the text
# fonts, colors, etc. that are used. A value of alt1 specifies the use
# of alt1eclient81.css.
#
#-----
cssPrefix=alt1
#-----
#
# iconPrefix specifies a file name prefix for the icon files that will be used by
# the JavaServer Pages. A value of alt1 specifies the use of gif files with
# names prefixed by the character string alt1. These gif files contain
# graphical buttons for the document viewer toolbar.
#
#-----
iconPrefix=alt1
#-----
#

```

Chapter 12. Accessibility information

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. Because the eClient is a Web application, your browser settings control the accessibility features. For example, through your browser, you can control font size and colors and use the browser's shortcut keys. Special keyboard shortcut keys are associated with the eClient viewer applet, and they are documented in the eClient online help. See the Accessibility page in the online help for more information.

Index

Special characters

- Scmcommon\$
 - for CLASSPATH
 - AIX 21
 - Solaris 22
 - Windows 20
- Sdsep\$
 - for CLASSPATH
 - AIX 21
 - Solaris 22
 - Windows 20
- Seippath\$
 - for CLASSPATH
 - AIX 21
 - Solaris 22
 - Windows 20
- Sfrnpath\$
 - for CLASSPATH 20
 - AIX 21
 - Solaris 22
- Sproddest\$
 - for CLASSPATH
 - AIX 20
 - Solaris 22
 - Windows 20
- Ssqlpath\$
 - for CLASSPATH
 - AIX 20
 - Solaris 22
 - Windows 20
- Swasroot\$
 - for CLASSPATH 20
 - AIX 21
 - Solaris 22

Numerics

- 7006
 - for PeopleSoft 42
- 7011
 - for PeopleSoft 42
- 7123
 - for PeopleSoft 42

A

- accessibility 139
- accessing the PeopleSoft portal 113
- AIX 16
- alias name
 - of ImagePlus for OS/390 server 8
- applet
 - creating
 - for Siebel 7.0.4 62
 - for Siebel 7.5.2 72
- applet control
 - creating
 - for Siebel 7.0.4 62
 - for Siebel 7.5.2 73

- applet Web template
 - creating
 - for Siebel 7.0.4 63
 - for Siebel 7.5.2 74
- applet Web template item
 - creating
 - for Siebel 7.0.4 64
 - for Siebel 7.5.2 74
- application ID
 - of ImagePlus for OS/390 server 8
- application name
 - setting
 - in the eClient 100
- application server properties 54
- application servers for PeopleSoft 33
- appserverproperties file 29
- authCookie
 - for PeopleSoft 36
 - PS_TOKEN 36
- authenticate users
 - for PeopleSoft 37
- authentication
 - domain
 - for PeopleSoft 33
 - domain name requirements for PeopleSoft 33
 - user
 - for PeopleSoft 33
 - user ID
 - for PeopleSoft 37
 - using PeopleSoft 37
- authTokenDomain for PeopleSoft 33
- automatically configuring the eClient
 - on AIX 14
 - on Solaris 14
 - on Windows 13

B

- browser cookies for PeopleSoft 33
- browser restriction
 - for the eClient 6
- browser security for PeopleSoft 33
- browser settings
 - resetting
 - for PeopleSoft 43
- browsers 11
 - supported
 - for PeopleSoft 9
- business component
 - configuring
 - for Siebel 7.5.2 70
- business objects layer
 - customizing
 - for Siebel 7.0.4 58

C

- caching directory
 - setting
 - in the eClient 95
- cascading style sheet files 94
- changing
 - configuration parameters
 - for eClient 95
- character encoding 29
- CLASSPATH token values
 - explanation 20
 - setting 19
- cleaning the cache
 - for PeopleSoft 53
- cmbpool.ini 23
- code page 29
- collect information for the eClient 7
- compiling
 - Siebel 7.0.4 67
 - Siebel 7.5.2 77
- component interface
 - define 37
- configuration parameters
 - changing
 - for eClient 95
 - for PeopleSoft 41
 - setting
 - for eClient 95
 - specify
 - for PeopleSoft 41
- configuration parameters for PeopleSoft 33
- configuration problems
 - eClient 109
- configure
 - pagelet specifications 34
 - PeopleSoft Internet Architecture 33
- configured environment
 - validating
 - for Siebel Integration 85
- configuring 19
 - business component
 - for Siebel 7.5.2 70
 - loose association for PeopleSoft 32
 - optimized association for PeopleSoft 32
 - overview
 - for PeopleSoft 31
 - Siebel 7.5.2 69, 78
 - Siebel application
 - 7.0.4 67
 - for Siebel 7.5.2 69
 - single sign-on for PeopleSoft 32
- configuring for a customized client 99
- configuring Siebel 7.0.4 56
- configuring Siebel Integration for IBM Content Manager 53
- configuring the eClient 19
 - for Siebel Integration 54
 - with WebSphere 4.0.5 AE
 - procedure 19

- configuring the eClient *(continued)*
 - with WebSphere 4.0.5 AES
 - procedure 19
 - with WebSphere 5
 - procedure 22
 - with WebSphere application server 19
- configuring the eClient as a Web application 14
- configuring third-party application integration 31
- configuring WebSphere Application Server
 - for Siebel Integration 54
- connection type
 - setting
 - in the eClient 96
- Content Manager requirements
 - for Siebel Integration 11
- Content Manager Version 7 2
- Content Manager Version 8 2
- Content Manager Version 8 connector
 - setting
 - in the eClient 96
- Content Ref Administration form
 - for PeopleSoft 50, 52
- content servers i
- cookie
 - browser settings
 - for PeopleSoft 114
- copying 16
- creating
 - applet
 - for Siebel 7.0.4 62
 - for Siebel 7.5.2 72
 - applet control
 - for Siebel 7.0.4 62
 - for Siebel 7.5.2 73
 - applet Web template
 - for Siebel 7.0.4 63
 - for Siebel 7.5.2 74
 - applet Web template item
 - for Siebel 7.0.4 64
 - for Siebel 7.5.2 74
 - responsibility
 - for Siebel 7.0.4 68
 - for Siebel 7.5.2 84
 - view
 - for Siebel 7.0.4 64
 - for Siebel 7.5.2 75
 - view Web template
 - for Siebel 7.0.4 65
 - for Siebel 7.5.2 75, 76
 - view Web template items
 - for Siebel 7.0.4 65
 - Web template file object
 - for Siebel 7.5.2 72
 - for Siebel Version 7.0.4 61
 - Web template object
 - for Siebel 7.0.4 61
 - for Siebel 7.5.2 71
- customizing
 - business objects layer
 - for Siebel 7.0.4 58
 - eClient application 89
 - PeopleSoft portal 32

- customizing *(continued)*
 - user interface layer
 - for Siebel 7.0.4 60

D

- data server list file
 - default local file location 13
- data server list file default local file location
 - on AIX 14
 - on Solaris 14
- Data Sources folder 25
- default directory
 - for the eClient 13
- defining
 - external data host
 - for Siebel 7.5.2 78
 - ImagePlus for OS/390 server connection
 - in the eClient 101
 - login credentials
 - for Siebel V7.5.2 83
 - OnDemand server connection
 - in the eClient 100
 - optional symbolic URL arguments
 - for Siebel 7.5.2 82
 - required symbolic URL arguments
 - for Siebel 7.5.2 79
 - server connections
 - in the eClient 100
 - symbolic URL
 - for Siebel 7.5.2 79
- deleting cache
 - for PeopleSoft 43
- different servlets
 - setting
 - in the eClient 99
- displaying external content
 - for Siebel 7.5.2 71
- document routing i
- domain name
 - for PeopleSoft 113

E

- e-mail properties
 - emailenabled 97
 - mailHost 97
 - mailUser 97
 - setting
 - in the eClient 97
- eClient
 - configuring
 - for Siebel Integration 54
 - configuring to use IBM WebSphere 4
 - connection pooling 23
 - prerequisites 23
 - procedure 24
 - recommendation 24
 - restriction 23
 - configuring with WebSphere 4.0.5 AE
 - procedure 19
 - configuring with WebSphere 4.0.5 AES
 - procedure 19

- eClient *(continued)*
 - configuring with WebSphere 5
 - procedure 22
 - configuring with WebSphere application server 19
 - getting more information 123
 - installing 13
 - installing on AIX
 - prerequisites 14
 - installing on AIX or Solaris 14
 - procedure 14
 - installing on Solaris
 - prerequisites 14
 - manually configuring with WebSphere Application Server 20
 - reinstalling 13
 - starting
 - on WebSphere 4 87
 - starting on WebSphere
 - on Windows 13
 - verifying installation 29
- eClient address 29
- eClient application
 - customizing 89
 - managing 94
- eClient application server
 - starting 87
- eClient browser restriction 6
- eClient CD 13, 14
- eClient client requirements 5
- eClient default directory 13
 - on AIX 14
 - on Solaris 14
- eClient graphics
 - customizing 92
- eClient help
 - customizing 94
- eClient JavaServer pages 89
- eClient JRE tips 6
- eClient JSP
 - annotation 91
 - document routing 92
 - folder 90
 - individual items 89
 - search 90
 - workflow 91
- eClient languages
 - selecting 28
- eClient launchpad 13
- eClient network requirements 7
- eClient server requirements 5
- eClient skill requirements 7
- eClient viewer 2
- eClient Web application i
- eClient Web application name 29
- eClient WebSphere tips 6
- EIP INI files
 - setting
 - for the eClient 96
- EIP system administration client 56
- enable security for a record
 - for PeopleSoft 48, 49
- enable security for loose association 48
- enable security for optimized association 49

- enabling
 - federated folder
 - in the eClient 97
 - launching content files
 - in the eClient 97
 - viewer applet
 - in the eClient 97
 - workflow 97
- enabling browsers to accept cookies
 - for PeopleSoft 114
- enabling cookies in Microsoft Internet Explorer
 - for PeopleSoft 114
- enabling cookies in Netscape Navigator 4.7
 - for PeopleSoft 114
- enabling cookies in Netscape Navigator 6.2
 - for PeopleSoft 114
- encoding.properties 29
- end-user client requirements
 - for Siebel Integration 11
- Enterprise Information Portal i, 2
- Enterprise Information Portal federated server 56
- Enterprise Information Portal requirements
 - for Siebel Integration 11
- Enterprise Information Portal version 8 Federated Connector
 - for PeopleSoft 39
- error page
 - setting
 - in the eClient 99
- Exceed 14
- external content
 - displaying
 - for Siebel 7.5.2 71
- external data
 - for Siebel 7.5.2 69
- external data host
 - defining
 - for Siebel 7.5.2 78
 - for Siebel 7.5.2 78
- external Web application
 - specifying
 - for Siebel V7.5.2 83

F

- FAF IP address
 - of ImagePlus for OS/390 server 8
- FAF port
 - of ImagePlus for OS/390 server 8
- FAF protocol
 - of ImagePlus for OS/390 server 8
- FAF symbolic ID
 - of ImagePlus for OS/390 server 8
- federated entities 56
- federated folder 97
 - enabling
 - in the eClient 97
- field definition
 - creating
 - for PeopleSoft 46
 - loose association
 - for PeopleSoft 44

- FieldFormula rule
 - for PeopleSoft 43, 45
- fnolint.tbl
 - for Content Manager Version 7 server or earlier 7, 8

G

- getting more information 123
 - about eClient 123
 - about Siebel Integration for IBM Content Manager 124

H

- hardware requirements
 - for PeopleSoft 9
 - for Siebel Integration 10
 - for the eClient 5
- Hardware requirements
 - for Siebel Integration 10
- host name
 - for PeopleSoft 113
- hostname
 - for PeopleSoft 33
- HTML 94
- HTML definition
 - creating
 - for PeopleSoft 44, 46
- Hypertext Markup Language 94

I

- IBM Content Manager (ICM) version 8 Connector
 - for PeopleSoft 39
- IBM Content Manager mid-tier products 2
- ICMPSSO.java
 - compile 39, 41
 - create packages 39
 - install 39
- ICMPSSO.properties 42
- ICMPSSO.properties file 41
- ICMSERVER.LOG
 - logging and tracing
 - for PeopleSoft 42
- ICMXLSLG.DLL 15, 122
 - for PeopleSoft 39
- IDM.properties file
 - for the eClient 95
- IDMadminDefaults.properties 98
- IDMdefault.properties 95
- IDMIntegrator for PeopleSoft 34
- idmwas.bat
 - eClient 19
- idmwas.sh 20
- ImagePlus for OS/390 server connection
 - defining
 - in the eClient 101
- information
 - about Bookshelf for Siebel Business Application 125
 - about Content Manager 124
 - about Enterprise Information Portal 125

- information (*continued*)
 - about WebSphere Application Server 125
 - Content Manager
 - for PeopleSoft 123
 - Enterprise Information Portal
 - for PeopleSoft 124
 - PeopleBooks 124
 - PeopleSoft 124
- information about Content Manager on the Web
 - for PeopleSoft 123
- information about Enterprise Information Portal on the Web 124, 125
- information about PeopleSoft on the Web 124
- information to collect
 - Content Manager OnDemand 7, 8
 - Content Manager Version 8 7, 8
 - for the eClient 7
 - ImagePlus for OS/390 7, 8
- installing
 - the eClient 13
- installing PeopleSoft 15
- installing Siebel Integration for IBM Content Manager 16
- installing Siebel Integration for IBM Content Manager on Windows, AIX or Solaris 16
- installing the eClient
 - on Windows 13
 - prerequisites 13
 - procedure 13
- installing the eClient on AIX
 - prerequisites 14
- installing the eClient on AIX or Solaris 14
 - procedure 14
- installing the eClient on Solaris
 - prerequisites 14
- installing the eClient on Windows 13
 - prerequisites 13
 - procedure 13
- installing third-party application
 - integration 15
- integration
 - loose
 - for PeopleSoft 31
 - optimized
 - for PeopleSoft 31
- integration properties file
 - for PeopleSoft 35, 36
- Integration Properties file
 - for Siebel Integration 16
- integration properties file for PeopleSoft 33
- Invalidation Timeout 54
- IP file properties
 - userid 56
- IPFile
 - for PeopleSoft 33
- IPFile for PeopleSoft 35, 36
- iScript
 - create
 - for PeopleSoft 34
 - creating 45
 - for PeopleSoft 43

- iScript *(continued)*
 - editing
 - for PeopleSoft 44, 47
 - for PeopleSoft 43, 45, 48, 49
 - loose association
 - for PeopleSoft 43
 - optimized association 45
 - sample for loose association
 - for PeopleSoft 45
 - sample for optimized association 47
- iScript for PeopleSoft 32
- iScript rules
 - for PeopleSoft 43, 45
- item types 56
- iType for PeopleSoft 34
 - connection 35
 - integration type 35
 - logon 35

J

- JavaServer Pages i
 - substituting your own 92
- JDBC Providers folder 24
- JDBC Providers Properties window 24
- JRE tips
 - for the eClient 6

L

- launching content files
 - enabling
 - in the eClient 97
- launchpad
 - for eClient
 - AIX 14
- library server 29
- license codes for PeopleSoft 113
 - troubleshooting 113
- linking
 - loose association for PeopleSoft 31
- location of cmbcc2mime.ini file
 - specifying
 - in the eClient 96
- location of cmbclient.ini file
 - specifying
 - in the eClient 96
- location of cmbcs.ini file
 - specifying
 - in the eClient 96
- location of graphic files
 - setting
 - in the eClient 99
- location of the trace files
 - setting
 - for the eClient 111
- logging and tracing in Content Manager
 - for PeopleSoft 42
- logging on
 - to the Siebel Call Center 7.0.4 67
- logging on to the Siebel Call Center
 - as an administrator 78
- login credentials
 - defining
 - for Siebel V7.5.2 83

- login name
 - for Siebel 7.5.2 83
- login pagelet for loose association
 - creating
 - for PeopleSoft 50
- login pagelet for optimized association
 - creating
 - for PeopleSoft 51
- logon user exit routine
 - copy
 - for PeopleSoft 38
 - for PeopleSoft 38
 - logon user exit routine for PeopleSoft 33
- loose association
 - HTML definition
 - for PeopleSoft 44
 - iScript definition
 - for PeopleSoft 44
 - pagelet definition
 - for PeopleSoft 50
 - pagelet security
 - for PeopleSoft 50
 - record
 - for PeopleSoft 48
 - record definition
 - for PeopleSoft 44
 - security
 - for PeopleSoft 48
 - loose association for PeopleSoft 31
 - loose association URL
 - for PeopleSoft 34

M

- managing
 - eClient application 94
- manually configuring the eClient with
 - WebSphere Application Server 20
- maximum file size allowed during import
 - setting
 - in the eClient 95
- maximum number of search results
 - displayed on a page
 - setting
 - in the eClient 95
 - in the eClient 95
- maximum number of search results
 - returned from the content server
 - setting
 - in the eClient 95
- MIME type files, converting 98
- MIME types 98
- miscellaneous tips
 - for the eClient 111
- Miscellaneous tips
 - for Siebel Integration 119
- multiple PeopleSoft servers 114

N

- National Language Support 29
- network requirements 10
 - for Siebel Integration 12
 - for the eClient 7
- new view
 - setting up in Siebel Call Center
 - for Siebel 7.5.2 84

O

- ODM collection class
 - of ImagePlus for OS/390 server 8
- ODM IP address
 - of ImagePlus for OS/390 server 8
- ODM port
 - of ImagePlus for OS/390 server 8
- ODM protocol
 - of ImagePlus for OS/390 server 8
- ODM storage location control
 - of ImagePlus for OS/390 server 8
- ODM terminal ID
 - of ImagePlus for OS/390 server 8
- OnDemand server connection
 - defining
 - in the eClient 100
- operating system 12
- optimized association
 - field definition
 - for PeopleSoft 46
 - HTML definition
 - for PeopleSoft 46
 - iScript definition
 - for PeopleSoft 47
 - pagelet definition
 - for PeopleSoft 51
 - pagelet security
 - for PeopleSoft 52
 - record
 - for PeopleSoft 49
 - record definition
 - for PeopleSoft 46
 - security
 - for PeopleSoft 49
 - optimized association for PeopleSoft 31, 32, 34
- optional symbolic URL arguments
 - for Siebel 7.5.2 82
- overview 2
 - eClient i
 - PeopleSoft 2
 - Siebel Integration for IBM Content
 - Manager 2
 - third-party application integration 2

P

- pagelet
 - adding to a new tab
 - for PeopleSoft 50, 52
 - clean-up
 - for PeopleSoft 53
 - configuring 34
 - creating
 - for PeopleSoft 34, 50, 51
 - for PeopleSoft 33
 - iScript
 - for PeopleSoft 32
 - loose association for PeopleSoft 32
 - modify
 - for PeopleSoft 43
 - optimized association for
 - PeopleSoft 32
 - security
 - for PeopleSoft 32, 50, 52

- pagelet (*continued*)
 - using
 - for PeopleSoft 53
- pagelet configuration
 - for PeopleSoft 43
- Password 42
- PATH token values
 - setting
 - in Web server JVM 20
- PeopleCode 44, 47
- PeopleSoft Application Designer 33, 39, 40, 43, 45
 - location of 44, 45
- PeopleSoft cookie 33
- PeopleSoft Internet Architecture
 - domain name 113
- PeopleSoft Java code
 - compile 40
- PeopleSoft port
 - access to 33
- PeopleSoft portal single sign-on
 - component interface 33, 37, 39, 40
- PeopleSoft run-time 42
- PeopleSoft single sign-on interface 39
- permission list
 - create
 - for PeopleSoft 37
 - example
 - for PeopleSoft 37
 - for PeopleSoft 37
- platforms
 - supported
 - for PeopleSoft 9
 - for Siebel Version 7.0.4 11
 - for Siebel Version 7.5 11
- portal agents
 - in Siebel 7.5.2 69
- prerequisites
 - Siebel 7.5.2 69
- presentation type 36
- properties in IDM.properties
 - changing
 - for eClient 95
- property daemon
 - setting
 - in the eClient 96
- PRTL_SS_CI
 - enable
 - for PeopleSoft 40
 - for PeopleSoft 37, 39
- PRTL_SS_CI for PeopleSoft 33, 39
- PS_TOKEN
 - for PeopleSoft 36
- psjoa.jar
 - for PeopleSoft 40

R

- RC_DLL_LOAD_ERROR
 - for PeopleSoft 42
- RC_GET_PROC_ADDRESS_ERROR
 - for PeopleSoft 42
- RC_INVALID_PARAMETER
 - for PeopleSoft 42
- record
 - create
 - for PeopleSoft 44

- record (*continued*)
 - for PeopleSoft 48, 49
- record definition
 - creating
 - for PeopleSoft 46
- record rule
 - for PeopleSoft 43, 45
- reinstalling
 - the eClient 13
- ReleaseLevel
 - PeopleSoftTools 35
- removing 120
 - eClient files and directories
 - eClient files and directories 121
 - Siebel Integration 122
 - third-party application integration 121
- removing PeopleSoft 122
- required symbolic URL arguments
 - defining
 - for Siebel 7.5.2 79
- requirements 3
 - for PeopleSoft Integration for IBM Content Manager 9
 - for Siebel Integration for IBM Content Manager 10
 - for the eClient 5
 - for third-party application integration 9
- hardware
 - for PeopleSoft 9
 - for Siebel Integration 10
- network
 - for PeopleSoft 10
- skill
 - for PeopleSoft 10
- software
 - for PeopleSoft 9
 - for Siebel Integration 11
 - for the eClient 6
- responsibility
 - creating
 - for Siebel 7.0.4 68
 - for Siebel 7.5.2 84
- return codes
 - for PeopleSoft 42
- role
 - create 37
 - example 37
- run-time environment for PeopleSoft 33
- running the eClient launchpad
 - on AIX 14
 - on Solaris 14

S

- sample IP file 136
- sample properties file
 - IDMdefault.properties 127
- sample properties files 125
- screen object
 - updating
 - for Siebel 7.0.4 66
 - for Siebel 7.5.2 77
- search templates 56
- security
 - enable 48, 49

- security (*continued*)
 - loose association 48
 - optimized association 49
- record
 - for PeopleSoft 48, 49
- selecting eClient languages 28
- server connections
 - defining
 - in the eClient 100
- server definitions 100
- server IP address 29
- server properties
 - for PeopleSoft 36
- server properties for PeopleSoft 35
- ServerName 41
- ServerPort 41
- serverType for PeopleSoft
 - Fed 35, 36
 - ICM 35, 36
- serverType properties for PeopleSoft 35, 36
- service connection type
 - setting
 - in the eClient 97
- setting
 - application name
 - in the eClient 100
 - caching directory
 - in the eClient 95
 - configuration parameters
 - for eClient 95
 - connection type
 - in the eClient 96
 - Content Manager Version 8 connector
 - in the eClient 96
 - different servlets
 - in the eClient 99
 - e-mail properties
 - in the eClient 97
 - EIP INI files
 - for the eClient 96
 - error page
 - in the eClient 99
 - location of graphic files
 - in the eClient 99
 - location of the trace files
 - for the eClient 111
 - maximum file size allowed during import
 - in the eClient 95
 - maximum number of search results displayed on a page
 - in the eClient 95
 - maximum number of search results returned from the content server
 - in the eClient 95
 - property daemon
 - in the eClient 96
 - service connection type
 - in the eClient 97
 - trace file size
 - for the eClient 111
 - tracing level
 - for the eClient 111
- setting PATH token values 20
- setting token values for CLASSPATH 19

- setting up
 - a new view in the Siebel Call Center
 - for Siebel 7.5.2 84
- Siebel 7.0.4
 - calculated field 58
 - calculated property value 58
 - configuring 56
 - prerequisites 56
- Siebel 7.5.2
 - configuring 69, 78
- Siebel application
 - configuring
 - for Siebel 7.5.2 69
- Siebel Call Center 67
- Siebel Client 67
- Siebel eBusiness applications 2
- Siebel Integration
 - removing 122
- Siebel Integration for IBM Content Manager
 - configuring 53
 - getting more information 124
 - installing 16
 - installing on Windows, AIX or Solaris 16
 - upgrading from Version 7 to Version 8 16
- Siebel Integration IP file properties
 - cssPrefix 55
 - eClientToken 54
 - iconPrefix 55
 - password 56
 - printEnabled 55
 - server 55
 - type 55
- Siebel Integration software
 - requirements 11
- Siebel users 56
- sign-off
 - for PeopleSoft 37
- sign-on
 - for PeopleSoft 37
- single sign-on
 - for PeopleSoft 37, 39, 40, 42
 - implement
 - for PeopleSoft 36
- single sign-on authentication cookie
 - for PeopleSoft 36
- single sign-on for PeopleSoft 31
- single sign-on URL for PeopleSoft 34
- single sign-on user exit routine
 - for PeopleSoft 38
- skill requirements 10
 - for Siebel Integration 12
 - for the eClient 7
- software requirements
 - for PeopleSoft 9
- software requirements for the eClient 6
- Solaris 16
- specifying
 - external Web application
 - for Siebel V7.5.2 83
 - location of cmbcc2mime.ini file
 - in the eClient 96
 - location of cmbclient.ini file
 - in the eClient 96

- specifying (*continued*)
 - location of cmbcs.ini file
 - in the eClient 96
- SRF file
 - in Siebel 7.5.2 69
- startIDMAE.bat 87
- startIDMAES.bat 87
- starting
 - eClient application server 87
- starting the eClient
 - on WebSphere 4 87
- starting the eClient on WebSphere
 - on Windows 13
- stopIDMAE.bat 88
- stopIDMAES.bat 88
- style sheet 94
- sudo privileges 14
- symbolic URL
 - defining
 - for Siebel 7.5.2 79
 - in Siebel 7.5.2 70
- synchronize user IDs
 - for PeopleSoft 37
- synchronize user IDs for PeopleSoft 33
- synchronize user IDs 36

T

- TCP/IP 7, 10, 12
- technical support Web sites
 - for Content Manager 10
 - for Siebel 10
- terminal 54
- third-party application integration
 - configuring 31
 - installing 15
 - removing 121
 - troubleshooting 112
- third-party business applications and integration
 - getting more information
 - getting more information 123
- trace file size
 - setting
 - for the eClient 111
- trace information
 - eClient 111
 - for Siebel Integration 120
- tracing level
 - setting
 - for the eClient 111
- troubleshooting
 - correct domain name
 - for PeopleSoft 113
 - eClient 103
 - for PeopleSoft 112
 - host name
 - for PeopleSoft 113
 - third-party application
 - integration 112
 - WebSphere configuration file
 - for PeopleSoft 113
- troubleshooting scenarios
 - eClient 103
 - for Siebel Integration 117

- type properties
 - behavior
 - for PeopleSoft 36
 - for PeopleSoft 36

U

- Unicode 29
- uninstalling PeopleSoft 122
- updating the screen object
 - for Siebel 7.0.4 66
 - for Siebel 7.5.2 77
- upgrading
 - from Siebel Integration for IBM Content Manager Version 7 to Version 8 16
- URL arguments for PeopleSoft 34
- URL parameters for PeopleSoft 34
- user
 - create 38
 - example 38
- user authentication
 - for PeopleSoft 39
- user exit
 - for PeopleSoft 39
- user interface layer
 - customizing
 - for Siebel 7.0.4 60
- UserID 42
- userid argument for PeopleSoft 35
- UTF-8 29

V

- validating
 - configured environment 85
 - for Siebel Integration 85
- verifying the eClient installation 29
- view
 - creating
 - for Siebel 7.0.4 64
 - for Siebel 7.5.2 75
 - setting up
 - for Siebel 7.0.4 68
- view Web template
 - creating
 - for Siebel 7.0.4 65
 - for Siebel 7.5.2 75
- view Web template items
 - creating
 - for Siebel 7.5.2 76
 - for Siebel 7.0.4 65
- viewer applet i
 - enabling
 - in the eClient 97

W

- Web library
 - for PeopleSoft 48
 - optimized association
 - for PeopleSoft 49
- Web template file object
 - creating
 - for Siebel 7.5.2 72
 - for Siebel Version 7.0.4 61

- Web template object
 - creating
 - for Siebel 7.0.4 61
 - for Siebel 7.5.2 71
- Web templates
 - for Siebel Integration 16
 - for Siebel Integration for IBM Content Manager 16
- WebSphere 4 connection pooling 23
 - prerequisites 23
 - procedure 24
 - recommendation 24
 - restriction 23
- WebSphere 5 Java 2 Security eClient
 - configuring to use WebSphere 5 Java 2 Security 19
- WebSphere Administrator's Console 54
 - launch
 - on AIX 54
 - on Sun Solaris 54
 - on Windows 54
- WebSphere Application Server 54
- WebSphere Resource Analyzer 26
- WebSphere server
 - troubleshooting corrupted configuration file for PeopleSoft 113
- WebSphere server configuration file correction to the XML statement 113
- WebSphere session timeout value set 54
- WebSphere tips
 - for the eClient 6
- workflow i
 - enabling 97

X

- X window session 14

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J74/G4
555 Bailey Avenue
San Jose, CA 95141
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

IBM	DisplayWrite®	PowerPC®
400®	e-business	PTX®
Advanced Peer-to-Peer Networking®	HotMedia®	QBIC®
AIX	Hummingbird®	RS/6000®
AIXwindows®	ImagePlus	SecureWay®
APPN®	IMS	SP™
AS/400®	Micro Channel®	VideoCharger™
C Set ++®	MQSeries®	Visual Warehouse™
CICS	MVS/ESA™	VisualAge®
DATABASE 2	NetView®	VisualInfo™
DataJoiner®	OS/2®	WebSphere
DB2	OS/390	
DB2 Universal Database	PAL®	

Approach®, Domino™, Lotus®, Lotus 1-2-3®, Lotus Notes® and SmartSuite® are trademarks or registered trademarks of the Lotus Development Corporation in the United States, other countries, or both.

Intel and Pentium® are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.



Program Number: 5724-B19
5724-B43

Printed in U.S.A.

SC27-1350-02

