

IBM eDiscovery Manager



# Installing and Configuring your eDiscovery Management System

*Version 2.2.2.0*



IBM eDiscovery Manager



# Installing and Configuring your eDiscovery Management System

*Version 2.2.2.0*

**Note**

Before using this information and the product it supports, read the information in “Notices” on page 209.

This edition applies to version 2.2.2 of IBM eDiscovery Manager (product number 5724-V36) and to all subsequent releases and modifications until otherwise indicated in new editions.

This edition replaces GC19-1278-04.

© **Copyright IBM Corporation 2008, 2014.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# Contents

## ibm.com and related resources . . . . . vii

How to send your comments . . . . .	viii
Contacting IBM. . . . .	viii
Determining the eDiscovery Manager version number . . . . .	viii
Accessibility features of eDiscovery Manager . . . . .	ix

## Chapter 1. eDiscovery Manager overview 1

What's new in eDiscovery Manager V2.2.2? . . . . .	2
Accessibility features of eDiscovery Manager . . . . .	3
eDiscovery Manager architecture overview . . . . .	5
End-to-end scenario: Electronic discovery of documents for legal cases . . . . .	7
Scenario: Prepare a system for the entire lifecycle of records for legal purposes . . . . .	8
Scenario: Organize content with an IBM Enterprise Records and enterprise content management system solution . . . . .	9
Scenario: Preparing the email repository for email analytics . . . . .	10
Scenario: Collecting electronic content for legal cases . . . . .	12
Scenario: Managing a case life cycle . . . . .	13
Scenario: Analyzing collected documents for legal discovery . . . . .	14
Sample configurations . . . . .	16
Planning IBM Content Collector, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with Content Manager EE . . . . .	16
Planning IBM Content Collector, IBM Content Classification, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with Content Manager EE . . . . .	18
Planning IBM Content Collector, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with FileNet P8 . . . . .	19
Planning IBM Content Collector, IBM eDiscovery Manager, IBM eDiscovery Analyzer, and IBM Enterprise Records with FileNet P8 . . . . .	20
Planning IBM Content Collector, IBM Content Classification, IBM Enterprise Records, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with FileNet P8. . . . .	21

## Chapter 2. Installing eDiscovery Manager . . . . . 25

Installing eDiscovery Manager to connect to Content Manager EE . . . . .	25
Before upgrading eDiscovery Manager . . . . .	26
Before installing eDiscovery Manager to connect to Content Manager EE . . . . .	27
Connecting eDiscovery Manager to Content Manager EE using single sign-on . . . . .	30
Installation checklist (Content Manager EE). . . . .	32
Installing WebSphere Application Server. . . . .	33

Installing an IBM Information Integrator for Content connector . . . . .	35
Installing the Lotus Domino server . . . . .	36
Installing or upgrading eDiscovery Manager in a Content Manager EE environment. . . . .	40
Database tuning to improve performance (Content Manager EE). . . . .	43
Installing eDiscovery Manager to connect to FileNet P8 . . . . .	43
Before upgrading eDiscovery Manager . . . . .	44
Before installing eDiscovery Manager to connect to FileNet P8 . . . . .	46
Configuring the IIOP connection between the eDiscovery Manager system and the FileNet P8 server using single sign-on . . . . .	48
Installation checklist (FileNet P8) . . . . .	51
Installing WebSphere Application Server. . . . .	53
Installing the Lotus Domino server . . . . .	55
Installing or upgrading eDiscovery Manager in a FileNet P8 environment . . . . .	60
Database tuning to improve performance (FileNet P8) . . . . .	62
Validating the eDiscovery Manager installation . . . . .	63
Silent installation . . . . .	64
Creating a response file . . . . .	64
Running a silent installation. . . . .	65
Post-installation changes to the configuration files . . . . .	67
Post-upgrade changes to the configuration files . . . . .	67
Restoring email notifications after an upgrade. . . . .	68
Starting and stopping the eDiscovery Manager server . . . . .	68

## Chapter 3. Configuring eDiscovery Manager . . . . . 69

Configuration checklists . . . . .	70
Configuration checklists (FileNet P8) . . . . .	70
Configuration checklists (Content Manager EE) . . . . .	87
Configuring security . . . . .	102
Configuring security in a Content Manager EE environment. . . . .	103
Configuring security in a FileNet P8 environment. . . . .	107
Changing the eDiscovery administrator password. . . . .	109
Customizing the user directory . . . . .	110
User directory file (Lotus Domino) . . . . .	111
User directory file (Microsoft Active Directory) . . . . .	111
Configuring document preview (AIX) . . . . .	112
Configuring viewing . . . . .	113
Configuring Lotus iNotes viewing . . . . .	114
Configuring Lotus Notes viewing . . . . .	115
Configuring the password manager for Lotus iNotes and Lotus Notes viewing . . . . .	116
Configuring export . . . . .	119
Configuring PDF export. . . . .	120

PST export configuration of Exchange emails	120
Configuring Lotus Notes export	121
Disabling the ability to specify a fully qualified export directory	125
Using short names for directories and files	125
EDRM XML plug-in and output compression limitations	126
Configuring email notifications	127
Configuring eDiscovery Manager to connect to FileNet P8 by using the Web Services Interface (WSI) transport method	127
Configuring eDiscovery Manager to use SSL to connect to FileNet P8	128
Enabling secure cookies	130
Configuring IBM eDiscovery Manager to open and save compressed attachments	130
Adding FileNet P8 version 4.5.1 servers	131
Configuring single sign-on support	131
Configuring IBM eDiscovery Manager to access documents in different IBM Content Manager item types	133
Configuring eDiscovery Manager to work with eDiscovery Analyzer	134
Searching and search results	134
Date range searches	134
Searching the Subject or content field of email with non-English language search terms	135
Configuring the style.lex file for nonalphanumeric, special, and wildcard character searches	135
Searching files not encoded in ASCII or UTF-8	135
Saving search results to a folder	135
Limitation in successful item count	136
IBM Legacy Content Search Engine related functionality that affects searching in eDiscovery Manager	136
Using IBM eDiscovery Manager with multi-part SharePoint documents archived by IBM Content Collector	137
Searching SharePoint documents (FileNet P8)	138
Searching SharePoint documents (IBM Content Manager)	140
Using IBM eDiscovery Manager with IBM Connections documents archived by IBM Content Collector	141
Searching IBM Connections documents (FileNet P8)	143
Searching IBM Connections documents (IBM Content Manager)	147

## Chapter 4. Managing cases in eDiscovery Manager . . . . . 151

Allowed tasks during phases of a case	152
Legal holds in eDiscovery Manager	152

## Chapter 5. Monitoring eDiscovery Manager system status . . . . . 155

How the eDiscovery Manager work manager schedules tasks	155
---	-----

## Chapter 6. Troubleshooting eDiscovery Manager . . . . . 157

Troubleshooting installation and uninstallation problems	158
WASX7017E and WASX7116E exceptions when deploying eDiscovery Manager	158
DGL0394A: Cannot instantiate class when installing or uninstalling	159
Installation program not progressing	159
Installation program not progressing during application server deployment in a FileNet P8 environment	164
ERROR: Setup for Microsoft Visual C++ Redistributable Package was not successful	165
Installation completes with errors	166
Where is the installation log file?	168
Uninstallation program not progressing	168
Uninstallation stops due to a DGL3704A error from DB2	172
Silent installation fails to run and an error message is not displayed	172
eDiscovery Manager component could not be removed	173
ACL data and privilege set exceptions when deleting eDiscovery Manager data	175
Some eDiscovery Manager files might not be removed during uninstallation	176
Installation fails because a supported version of IBM Information Integrator for Content was not found	177
Exporting content that has an unsupported MIME type	177
Troubleshooting configuration problems	178
Cannot access eDiscovery Manager (Content Manager EE)	178
Cannot access eDiscovery Manager (FileNet P8)	178
Users and administrators prompted for Lotus Notes password	179
[Servlet Error]-[action]: java.lang.NoClassDefFoundError: lotus.domino.NotesException	179
Configuring the TCP/IP timeout value for Lotus Domino servers	180
Error while searching for senders or recipients by using LDAP from the IBM eDiscovery Manager web client	181
Enabling eDiscovery Manager logging	181
Troubleshooting problems during search or use	182
Opening multiple browser windows or tabs causes unexpected behavior	182
DYRC2004E when accessing a folder	182
DYRC1028E when viewing folder contents	183
Export to NSF file not progressing	184
Export not progressing or Lotus Notes viewing causes eDiscovery Manager application server to crash	184
Invalid password causes Lotus Domino export failure	185
Internal Server Error during export of Lotus Domino Lotus Domino content	185

Lotus Domino Server Not Found error during export . . . . .	186	Tasks fail due to insufficient privileges . . . . .	197
File name issues with the collection definition export . . . . .	186	Export task fails with an REPOSITORY_UNAVAILABLE error . . . . .	197
NSFDbOpenExtended: This database cannot be opened because a consistency check of it is needed . . . . .	187		
Attempt to create duplicate template rejected	188		
Problems occur when EDRM exported files are uncompressed . . . . .	188		
DYRC1029E when exporting documents . . . . .	189		
Internal server error when viewing or exporting content . . . . .	189		
Exporting content that has an unsupported MIME type . . . . .	190		
What are CSN_ERROR files? . . . . .	190		
NO_PERMISSION exception when connecting to a FileNet P8 server . . . . .	191		
Export fails with NOTES ERROR message in the dominoExport.log file . . . . .	192		
Lotus export fails with NSFDbCreateAndCopy error 16643 and a File does not exist message	192		
Web client sessions time out after 30 minutes	193		
Web client session is closed when accessing multiple eDiscovery Manager servers . . . . .	194		
DYRC9999E error when searching and the log file contains DGL5052A: Operand type mismatch in a query string . . . . .	195		
Two views of the same Lotus Notes email have different timestamps . . . . .	195		
Error 404: No target servlet configured for uri: /edmclient or HTTP 404 - File not found . . . . .	196		
Some Microsoft Outlook email attachments cannot be previewed . . . . .	196		
		<b>Chapter 7. Removing and reinstalling eDiscovery Manager . . . . .</b>	<b>199</b>
		Removing and reinstalling eDiscovery Manager (Content Manager EE) . . . . .	199
		Removing eDiscovery Manager with the intent to reinstall this version (Content Manager EE) . . . . .	199
		Removing eDiscovery Manager with the intent to reinstall a previous version (Content Manager EE) . . . . .	200
		Removing and reinstalling eDiscovery Manager (FileNet P8) . . . . .	201
		Removing eDiscovery Manager with the intent to reinstall this version (FileNet P8) . . . . .	201
		Removing eDiscovery Manager with the intent to reinstall a previous version (FileNet P8) . . . . .	202
		<b>Chapter 8. Removing eDiscovery Manager . . . . .</b>	<b>203</b>
		Before removing eDiscovery Manager . . . . .	203
		Removing eDiscovery Manager . . . . .	204
		Running a silent uninstallation . . . . .	206
		<b>Notices . . . . .</b>	<b>209</b>
		<b>Privacy policy considerations . . . . .</b>	<b>213</b>
		<b>Index . . . . .</b>	<b>215</b>





---

## ibm.com and related resources

Product support and documentation are available from [ibm.com](http://www.ibm.com)<sup>®</sup>.

### Support and assistance

Product support is available on the web for IBM<sup>®</sup> eDiscovery Manager and all of its prerequisites. Simply click **Support** from the appropriate product website.

#### IBM eDiscovery Manager

[http://www.ibm.com/support/entry/portal/Software/Information\\_Management/eDiscovery\\_Manager](http://www.ibm.com/support/entry/portal/Software/Information_Management/eDiscovery_Manager)

#### IBM eDiscovery Analyzer

[http://www.ibm.com/support/entry/portal/Software/Information\\_Management/eDiscovery\\_Analyzer](http://www.ibm.com/support/entry/portal/Software/Information_Management/eDiscovery_Analyzer)

#### IBM CommonStore for Exchange Server

[http://www.ibm.com/support/entry/portal/Overview/Software/Information\\_Management/CommonStore\\_for\\_Exchange\\_Server](http://www.ibm.com/support/entry/portal/Overview/Software/Information_Management/CommonStore_for_Exchange_Server)

#### IBM CommonStore for Lotus<sup>®</sup> Domino<sup>®</sup>

[http://www.ibm.com/support/entry/portal/Overview/Software/Information\\_Management/CommonStore\\_for\\_Lotus\\_Domino](http://www.ibm.com/support/entry/portal/Overview/Software/Information_Management/CommonStore_for_Lotus_Domino)

#### IBM Content Collector

[http://www.ibm.com/support/entry/portal/Overview/Software/Information\\_Management/InfoSphere\\_Content\\_Collector/](http://www.ibm.com/support/entry/portal/Overview/Software/Information_Management/InfoSphere_Content_Collector/)

#### IBM Content Manager Enterprise Edition

<http://www.ibm.com/software/data/cm/cmgr/mp/>

#### IBM FileNet<sup>®</sup> P8

[http://www.ibm.com/support/entry/portal/Overview/Software/Information\\_Management/FileNet\\_Product\\_Family](http://www.ibm.com/support/entry/portal/Overview/Software/Information_Management/FileNet_Product_Family)

#### IBM Enterprise Records

[http://www.ibm.com/support/entry/portal/Overview/Software/Information\\_Management/InfoSphere\\_Enterprise\\_Records](http://www.ibm.com/support/entry/portal/Overview/Software/Information_Management/InfoSphere_Enterprise_Records)

#### IBM Records Manager

[http://www.ibm.com/support/entry/portal/Overview/Software/Information\\_Management/Records\\_Manager](http://www.ibm.com/support/entry/portal/Overview/Software/Information_Management/Records_Manager)

#### IBM WebSphere<sup>®</sup> Application Server

[http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere\\_Application\\_Server](http://www.ibm.com/support/entry/portal/Overview/Software/WebSphere/WebSphere_Application_Server)

#### IBM Lotus Notes<sup>®</sup> and IBM Lotus Domino

<http://www.ibm.com/software/lotus/notesanddomino/>

### Information center

You can view the IBM eDiscovery Manager product documentation in an Eclipse-based information center. See the information center at <http://pic.dhe.ibm.com/infocenter/email/v3r0m0/index.jsp>.

## PDF publications

You can view a PDF version of the IBM eDiscovery Manager installation and configuration guide by using the Adobe Acrobat Reader for your operating system. The guide is available from the IBM Publications Center at <http://www.ibm.com/shop/publications/order?CTY=US&FNC=SRX&PBL=GC19-1278-05>. If you do not have the Acrobat Reader installed, you can download it from the Adobe web site at <http://www.adobe.com>.

---

## How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

Send your comments by using the online reader comment form at [https://www14.software.ibm.com/webapp/iwm/web/signup.do?lang=en\\_US&source=swg-rcf](https://www14.software.ibm.com/webapp/iwm/web/signup.do?lang=en_US&source=swg-rcf).

## Consumability survey

You are invited to tell IBM how to improve the consumability of software products. If you want to help IBM make IBM eDiscovery Manager easier to use, take the Consumability Survey at <http://www.ibm.com/software/data/info/consumability-survey/>.

---

## Contacting IBM

To contact IBM customer service in the United States or Canada, call 1-800-IBM-SERV (1-800-426-7378).

To learn about available service options, call one of the following numbers:

- In the United States: 1-888-426-4343
- In Canada: 1-800-465-9600

For more information about how to contact IBM, see the Contact IBM website at <http://www.ibm.com/contact/us/>.

## Determining the eDiscovery Manager version number

When you submit a PMR, your IBM Software Support representative will ask you for the version number of your site's eDiscovery Manager software in order to obtain an accurate picture of your environment.

To determine the version of eDiscovery Manager software that is running, take either of the following actions.

- From the eDiscovery Manager web client, click **About**. The About IBM eDiscovery Manager window displays the version number.
- From the scripts subdirectory of the eDiscovery Manager installation directory, run the script that is appropriate for your operating system.

**AIX®**    `edmlevel.sh`

**Windows**  
          `edmlevel.bat`

---

## Accessibility features of eDiscovery Manager

IBM eDiscovery Manager includes features that make it more accessible for people with disabilities.

**Important:** The accessibility features are supported on Windows operating systems only.

### Keyboard input and navigation

#### Keyboard input

You can use the keyboard instead of a mouse to operate the product. To use any button on the user interface, move to the button and press the spacebar or the Enter key.

#### Keyboard focus

The position of the keyboard focus is outlined, indicating which area of the window is active and where your keystrokes will have an effect.

#### Response time adjustments

By default, the eDiscovery Manager web client times out after 30 minutes. However, you can adjust this behavior on the Session management pane of the WebSphere Application Server administrative console. See “Web client sessions time out after 30 minutes” on page 193 for complete information about preventing eDiscovery Manager from timing out.

#### Silent installation

For an accessible version of the installation, you must use the silent installation feature.

### Keyboard shortcut keys

You can use the keyboard to access all of the functions of the eDiscovery Manager web client.

In general, keyboard access conforms to standard Microsoft Windows guidelines.

Keyboard access differs from standard Microsoft Windows guidelines in the following ways.

#### Access keys, tabbing, and tables

Access keys are provided only for buttons and menu items. Press the Tab key to reach all fields.

Press the Tab key to move the cursor into a table. Press the Tab key again to move the cursor to the next cell in a table. To move out of the table to the next field, hold down the Ctrl key and press Tab. When the cursor is in a table, pressing Enter is not equivalent to clicking **OK** to close the window; you must move out of the table first.

You can switch between tabs by using the Left and Right Arrow keys.

#### Combination boxes

Use the Up and Down Arrow keys to move to an item. Then, press Enter to select it.

#### Tree views

Expand tree view items by using the Right Arrow key and collapse tree

view items by using the Left Arrow key. Move up and down the tree by using the Up Arrow and the Down Arrow keys. Select a tree item by pressing the Enter key.

#### **List boxes, check boxes, and radio buttons**

In a list box, press the Down Arrow and Up Arrow keys to browse items and press the Enter key to select an item.

Within list boxes, the following actions have no effect:

- Pressing the Ctrl key with Page Up, Page Down, Home, or End
- Pressing Shift+F8

You can select individual radio buttons by pressing the Tab key and then the Spacebar key or by using the access keys. Arrow keys do not select radio buttons within a group.

#### **Notebook tabs**

Access keys are not provided for notebook tabs. Move the focus to a page tab by using the Right Arrow and Left Arrow keys or the Tab key, or by pressing Ctrl+Page Down or Ctrl+Page Up.

#### **Status message**

Informational and status messages are displayed at the bottom of the eDiscovery Manager web client. You can use the following shortcut keys for that section:

- Ctrl+m shows the full status message window
- Ctrl+e expands the status message window vertically
- Ctrl+c clears the messages in the status message window

#### **Additional keystrokes**

The following keys have no effect on text fields:

- Alt+Backspace
- Ctrl+Z
- Shift+Delete

### **Features for accessible display**

The eDiscovery Manager web client has the following features that enhance the user interface and improve accessibility for users with low vision.

#### **High-contrast mode**

In Windows systems, the web client supports the high-contrast mode option that is provided by the operating system. This feature supports a higher contrast between background and foreground colors.

#### **Non-dependence on color**

You do not need to distinguish between colors to use any function of this product.

### **Compatibility with assistive technologies**

The eDiscovery Manager web client is compatible with the JAWS screen reader application. The web client has the properties that are required for JAWS to make on-screen information available to visually impaired users.

**Requirement:** You must start the JAWS screen reader by using the **java** command instead of the **javaw** command. If you start the screen reader with the **javaw** command, the screen reader does not work properly.

## **Product documentation**

Documentation for this product is available in accessible formats.

Documentation is available in an accessible Eclipse information center in HTML format. With the HTML format, you can view documentation according to the display preferences set in your browser. It also allows the use of screen readers and other assistive technologies.

Documentation is also available in PDF format.



---

## Chapter 1. eDiscovery Manager overview

IBM eDiscovery Manager assists with legal discovery and helps you handle immediate litigation and investigation matters by enabling you to proactively search, manage, and export electronically stored information (ESI), including email and other business content. This content can reside in either IBM Content Manager Enterprise Edition or IBM FileNet P8 content servers. In addition to their support for basic unstructured content (files), Content Manager EE and FileNet P8 provide more specific support for email archives that were created by IBM Content Collector, IBM CommonStore, or IBM FileNet Email Manager.

eDiscovery Manager supports a variety of content types, for example:

- IBM Lotus Domino content
- Microsoft Exchange content
- SMTP email
- Microsoft SharePoint content
- Files
- SAP artifacts
- Custom content

Refer to the product information for your archive servers to get complete information about the types of content that are supported by those servers.

Each user is assigned one or more *roles* to determine what tasks that user can perform with the eDiscovery Manager content. If the user is assigned the role to view content in its original (or *native*) format, you must install the client applications with which the content was authored on the same machine as eDiscovery Manager. In addition, any workstation on which the eDiscovery Manager web client is running must also have the client application installed. If you do not have the appropriate client application, eDiscovery Manager presents you with a list of available applications.

Because of the volume of content in most enterprise companies, sorting through and finding email, documents, or other files is a time-consuming and resource-intensive task. eDiscovery Manager helps you locate content that is most relevant to a particular legal matter and it ensures that the content is retained until the matter is resolved. This reduced set of potentially relevant content enables more efficient use of expensive legal analysts.

### Finding relevant content

Typically, the first step in the active e-discovery process is for the legal employees or IT staff to produce email and other documents that meet certain criteria in terms of dates, custodians, and content. Using eDiscovery Manager, legal or IT users can find content that might be relevant to the legal matter. The legal or IT users do not need a deep or broad understanding of where various types of data are stored or what types of content and metadata fields might be searchable. For convenience and usability, an eDiscovery Manager administrator sets up one or more search templates that map to various content servers, data types, and fields containing key enterprise data, thereby simplifying the search task for the legal or IT users.

As users perform searches by using the eDiscovery Manager web client, they can preview the retrieved content in an HTML viewer or they can open it in its native form, assuming that the appropriate application is available on their desktop. Previewing helps them validate that the search is returning relevant content. As users refine their searches, they can save their search results for later review and refinement with the goal of obtaining the best set of potentially relevant results.

Sometimes, relevant information in a legal matter might not only exist in the past, but might evolve in the ongoing process of doing business. In those situations, targeted searches can be scheduled to occur on a regular basis, continually adding potentially relevant content.

## **Organizing relevant content**

As users find content that is relevant to a discovery order, they can add their search results to case folders in eDiscovery Manager. Doing so effectively puts a legal hold on the content so that it cannot be deleted from the content server until the legal matter is resolved. The search terms that produced the search results are also stored in the case so that they can be used later. For example, they might be used to defend the results of the e-discovery process. Users can also move and copy content between case folders to consolidate search results and organize them in a way that is most useful for legal counsel.

## **Exporting relevant content**

Ideally, after the legal employees or IT staff finds all potentially relevant content, the legal team further refines the set of truly responsive content by using IBM eDiscovery Analyzer. The legal employees or IT staff can then use eDiscovery Manager to export all or a subset of the content and provide it to a third party or opposing counsel for further processing and analysis.

Content can be exported in its native format or in industry-standard Electronic Discovery Reference Model (EDRM) XML files. eDiscovery Manager also provides options to export the content to HTML and PDF formats. Users can further extend eDiscovery Manager to export content to other formats by creating your own export format plug-ins.

## **Creating audit reports**

eDiscovery Manager provides auditing capabilities that help your organization to execute defensible e-discovery and corporate compliance processes. In addition to tracking the searches that contribute content to cases, eDiscovery Manager can track the movements of users who access cases. Having control of ESI preservation and chain of custody helps your organization to avoid spoliation sanctions.

---

## **What's new in eDiscovery Manager V2.2.2?**

IBM eDiscovery Manager Version 2.2.2 provides the following new features.

### **Column sorting**

By clicking a column header in the search results, the search results are sorted by that column.

### **Location in the search results**

Row numbers were added to search results to assist with navigating the results.



### **XITSuperceded audit record**

An XITSuperceded audit record is created when an eDiscovery Manager folder has multiple versions of the same XIT objects.

### **Renaming a case**

All cases can be renamed. Every time a case you rename a case, a CaseRename audit report is generated.

### **Saving search results or folder content to a CSV file**

You can save search results or folder content to a comma-separated text file (CSV). The fields and values from the search or folder are saved, but not the document contents.

### **Export and save operations support fully qualified paths**

The export operation and the save to a CSV file operation support fully qualified paths to a directory, and the directory does not have to be on the eDiscovery Manager server. For example, you can specify a location on a shared network drive that the eDiscovery Manager server can access. The eDiscovery Manager administrator can optionally turn off support for fully qualified paths.

### **Previewing calendar and appointment documents**

You can preview calendar and appointment documents from the search results or in a folder.

### **Support for journal entries**

Journal recipients that are stored in the ICCVaryindFields field are supported for document previews, export operations, and saving results to a CSV file. The To, Cc, and BCC values can be previewed, exported, and saved to a CSV text file.

### **Support for IBM Connections Version 4.5 documents**

eDiscovery Manager now supports previewing and exporting IBM Connections Version 4.5 documents.

---

## **Accessibility features of eDiscovery Manager**

IBM eDiscovery Manager includes features that make it more accessible for people with disabilities.

**Important:** The accessibility features are supported on Windows operating systems only.

### **Keyboard input and navigation**

#### **Keyboard input**

You can use the keyboard instead of a mouse to operate the product. To use any button on the user interface, move to the button and press the spacebar or the Enter key.

#### **Keyboard focus**

The position of the keyboard focus is outlined, indicating which area of the window is active and where your keystrokes will have an effect.

#### **Response time adjustments**

By default, the eDiscovery Manager web client times out after 30 minutes. However, you can adjust this behavior on the Session management pane of the WebSphere Application Server administrative console. See “Web client sessions time out after 30 minutes” on page 193 for complete information about preventing eDiscovery Manager from timing out.

## **Silent installation**

For an accessible version of the installation, you must use the silent installation feature.

## **Keyboard shortcut keys**

You can use the keyboard to access all of the functions of the eDiscovery Manager web client.

In general, keyboard access conforms to standard Microsoft Windows guidelines.

Keyboard access differs from standard Microsoft Windows guidelines in the following ways.

### **Access keys, tabbing, and tables**

Access keys are provided only for buttons and menu items. Press the Tab key to reach all fields.

Press the Tab key to move the cursor into a table. Press the Tab key again to move the cursor to the next cell in a table. To move out of the table to the next field, hold down the Ctrl key and press Tab. When the cursor is in a table, pressing Enter is not equivalent to clicking **OK** to close the window; you must move out of the table first.

You can switch between tabs by using the Left and Right Arrow keys.

### **Combination boxes**

Use the Up and Down Arrow keys to move to an item. Then, press Enter to select it.

### **Tree views**

Expand tree view items by using the Right Arrow key and collapse tree view items by using the Left Arrow key. Move up and down the tree by using the Up Arrow and the Down Arrow keys. Select a tree item by pressing the Enter key.

### **List boxes, check boxes, and radio buttons**

In a list box, press the Down Arrow and Up Arrow keys to browse items and press the Enter key to select an item.

Within list boxes, the following actions have no effect:

- Pressing the Ctrl key with Page Up, Page Down, Home, or End
- Pressing Shift+F8

You can select individual radio buttons by pressing the Tab key and then the Spacebar key or by using the access keys. Arrow keys do not select radio buttons within a group.

### **Notebook tabs**

Access keys are not provided for notebook tabs. Move the focus to a page tab by using the Right Arrow and Left Arrow keys or the Tab key, or by pressing Ctrl+Page Down or Ctrl+Page Up.

### **Status message**

Informational and status messages are displayed at the bottom of the eDiscovery Manager web client. You can use the following shortcut keys for that section:

- Ctrl+m shows the full status message window
- Ctrl+e expands the status message window vertically
- Ctrl+c clears the messages in the status message window

### Additional keystrokes

The following keys have no effect on text fields:

- Alt+Backspace
- Ctrl+Z
- Shift+Delete

### Features for accessible display

The eDiscovery Manager web client has the following features that enhance the user interface and improve accessibility for users with low vision.

#### High-contrast mode

In Windows systems, the web client supports the high-contrast mode option that is provided by the operating system. This feature supports a higher contrast between background and foreground colors.

#### Non-dependence on color

You do not need to distinguish between colors to use any function of this product.

### Compatibility with assistive technologies

The eDiscovery Manager web client is compatible with the JAWS screen reader application. The web client has the properties that are required for JAWS to make on-screen information available to visually impaired users.

**Requirement:** You must start the JAWS screen reader by using the **java** command instead of the **javaw** command. If you start the screen reader with the **javaw** command, the screen reader does not work properly.

### Product documentation

Documentation for this product is available in accessible formats.

Documentation is available in an accessible Eclipse information center in HTML format. With the HTML format, you can view documentation according to the display preferences set in your browser. It also allows the use of screen readers and other assistive technologies.

Documentation is also available in PDF format.

---

## eDiscovery Manager architecture overview

IBM eDiscovery Manager can search unstructured content and retrieve documents or files that are stored in either IBM FileNet P8 or IBM Content Manager Enterprise Edition content servers.

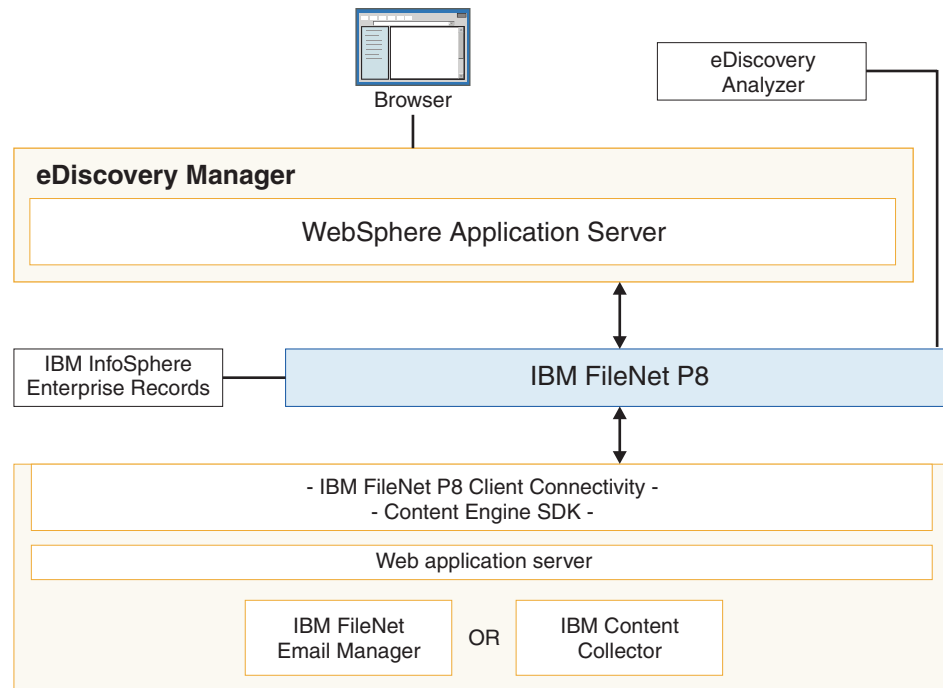
eDiscovery Manager is an enterprise application that runs on IBM WebSphere Application Server and retrieves documents and files from content management servers. Users can access eDiscovery Manager by using a web browser.

IBM eDiscovery Analyzer is an optional component in the IBM Archive and eDiscovery solution. Working together, eDiscovery Manager and eDiscovery Analyzer can help you to efficiently identify and deliver the precise set of data that is needed for the successful resolution of a legal matter. Take a guided tour through one common scenario and learn how easy it is to:

- Schedule a repeating search to gather relevant content during the discovery period
- Index the content in a case
- Flag content of interest
- Export content to an industry standard format (EDRM XML) for delivery to the opposing counsel

## IBM FileNet P8

The following graphic shows the typical architecture of eDiscovery Manager working with one or more FileNet P8 content servers. When you view this graphic in a web browser, you can click on some of the product names in the graphic to see more information about that product.

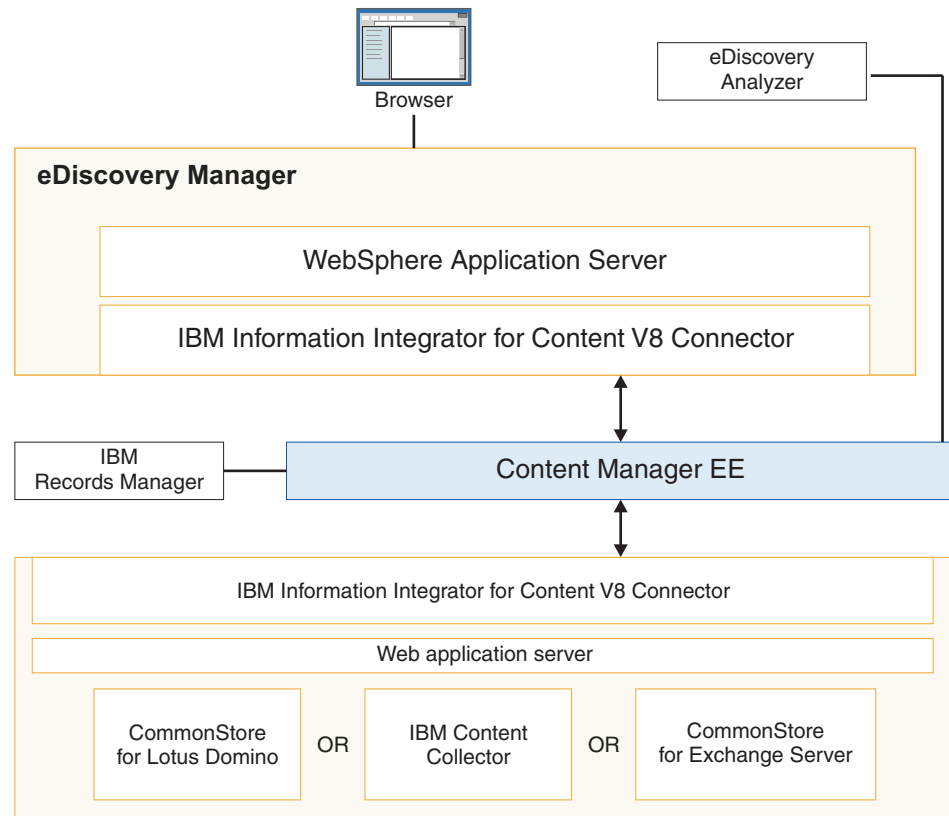


**Restriction:** If you are using IBM FileNet Email Manager with FileNet P8, you cannot search the body or attachments of email. You can search only the email metadata.

For FileNet P8, the connector component is installed by eDiscovery Manager.

## Content Manager EE

The following graphic shows the typical architecture of eDiscovery Manager working with one or more Content Manager EE content servers. When you view this graphic in a web browser, you can click on some of the product names in the graphic to see more information about that product.




For Content Manager EE, you must install the IBM Information Integrator for Content Version 8 connector.


#### Related tasks:

“Installing eDiscovery Manager to connect to Content Manager EE” on page 25  
Before installing IBM eDiscovery Manager, you must install all of the prerequisite software on the eDiscovery Manager system.

“Installing eDiscovery Manager to connect to FileNet P8” on page 43  
Before installing IBM eDiscovery Manager, you must install all of the prerequisite software on the eDiscovery Manager system.

#### Related reference:

 System requirements for IBM eDiscovery Manager  
See the product website for detailed system requirements.

 IBM eDiscovery Analyzer architecture overview  
IBM eDiscovery Analyzer searches email, attachments, and other documents that are collected into a case by using IBM eDiscovery Manager.

## End-to-end scenario: Electronic discovery of documents for legal cases

The business scenarios describe how a fictitious company called ExampleCo. Enterprises and its subsidiaries solve typical problems with business content management and electronic discovery for legal cases.

To manage data sources and prepare for electronic discovery, ExampleCo. Enterprises installs and configures IBM Content Collector to archive its business content. ExampleCo. Enterprises then uses IBM eDiscovery Manager to quickly

discover data that is potentially relevant to a legal matter and to place that data on legal hold to prevent deletion until the matter is resolved. Their legal staff then uses IBM eDiscovery Analyzer on this drastically reduced set of data to not only better understand its bearing on the legal matter, but to quickly distinguish between responsive, non-responsive, and privileged information.

## **Scenario: Prepare a system for the entire lifecycle of records for legal purposes**

ExampleCo. Enterprises, a fictitious company uses IBM Enterprise Records to manage all of their documents, email, and corporate announcements, and to track adherence to company safety standards, corporate guidelines, and employee training records to protect themselves from potential lawsuits.

The lawsuits result from the development practices that surround the products that they release in their appliance business. The company must track and store documents that must be declared as records. These records are associated with the following areas:

- Monitor safety standards and testing procedures to remain compliant with development practices. These procedures clearly contain proprietary knowledge that is owned by ExampleCo. Enterprises.
- Following company guidelines on time spent working on products and testing of components. These records show detailed time spent on specific ExampleCo. Enterprises products.
- Administering employee training that is received in both the manufacturing and the maintenance of their products. These documents and training programs account for ExampleCo. Enterprises-specific training details.

Chris, the head of the corporate litigation department, wants to set up a records management solution so that all types of records, both electronic and physical, can be created and maintained accurately, securely, and reliably, regardless of the storage media or format of the records. Chris and IT specialist Bob decide to use IBM Enterprise Records as their solution. This system allows ExampleCo. Enterprises employees to plan, control, and organize the creation, storage, usage, retrieval, and disposal of records. This solution helps to maintain records throughout their lifecycle of creation, active use, inactive storage, and disposition. IBM Enterprise Records eliminates the need to manually locate information through the product's use of disposition schedules and record sweep tools, and consequently makes it easier for ExampleCo. Enterprises to comply with record-keeping laws and regulations. This is important because compliance failures can lead to fines, penalties, and legal consequences.

ExampleCo. Enterprises already owns an IBM FileNet P8 system that Bob is familiar with. This system includes a Content Engine server and a Process Engine server and the site already has a Lotus Domino server for email. For the IBM Enterprise Records solution, Bob decides to add an application server with the following software:

- Workplace XT
- Lotus Domino client
- WebSphere Application Server

This solution enables Bob to set up a record object store on the Content Engine server, which he uses as a repository to contain all of their records. It also allows them to create a file plan object store on their Content Engine server that is used to hold the metadata for the records:

- format
- author
- subject
- location
- media type
- publication dates

The file plans define the organization of records. They create a file plan that reflects the business functions of the organization, for example, Payroll\_FPOS. They also associate a naming pattern with the file plan so that all the entities under the file plan follow the record-naming plan of prYYMMDD. This easily categorizes the records and organizes them so they are easily retrieved and dealt with as their file plan dictates. The file plan contains record categories, record folders, volumes, records, and record types.

IBM Enterprise Records lets them manage all their records independent of the storage media, so the records are easily accessible and easily disposed of when they are no longer useful or no longer required by legal, regulatory, or administrative directive. They use IBM Enterprise Records to create and maintain file plans for storing records and also to create retention and disposal schedules. For example, if ExampleCo. Enterprises has a particular customer that has a problem with one of their products a ExampleCo. Enterprises's records manager, Ranjun, can search for all records associated with that customer, and those records can be placed on hold. That way, none of these records can be destroyed until the legal department gives its approval and the hold is removed.

The reporting features delivered with IBM Enterprise Records help Ranjun see file plan information is organized based on configuration criteria such as user action, disposition actions and schedules, time of creation, viewed by user, and so on. Ranjun uses this information to help create reports for the legal department.

In addition to IBM Enterprise Records, Bob uses IBM Content Collector to automatically retain and archive significant email documents in the IBM FileNet P8 content management repository. Along with the records, the email documents can be archived for specific length of time and used in any legal issues that arise.

## **Scenario: Organize content with an IBM Enterprise Records and enterprise content management system solution**

ExampleCo. Enterprises, a fictitious company, uses IBM Enterprise Records to eliminate the need to manually locate information through the product's use of disposition schedules and record sweep tools, and consequently make it easier for the company to comply with record-keeping laws and regulations.

Compliance failures can lead to fines, penalties, and legal consequences. ExampleCo. Enterprises wants to set up a records management solution so that all types of records, both electronic and physical, can be created and maintained accurately, securely, and reliably, regardless of the storage media or format of the record. ExampleCo. Enterprises's IT specialist, Bob, selects IBM Enterprise Records as the solution. ExampleCo. Enterprises already has an IBM FileNet P8 system that Bob is familiar with. This system includes a Content Engine server and a Process Engine server, but there is no true records management system. The IBM Enterprise Records solution only requires that he add an application server with the IBM Enterprise Records product and their Workplace or Workplace XT version of choice.



This system allows ExampleCo. Enterprises employees to plan, control, and organize the creation, storage, usage, retrieval, and disposal of records. This solution encompasses all of the activities that need to be performed to maintain records throughout their life cycle of creation, active use, inactive storage and disposition.

This solution allows ExampleCo. Enterprises employees to set up a record object store on the Content Engine server, which can be used as a repository to contain all of their records. It also lets them create a file plan object store on their Content Engine server, which can be used to hold the metadata for the records:

- format
- author
- subject
- location
- media type
- publication dates

The file plans define the organization of records. For example, ExampleCo. Enterprises can create a file plan that reflects business functions of the organization, for example, Payroll\_FPOS. They also associate a naming pattern with the file plan so that all the entities under the file plan follow the record-naming plan of prYYMMDD. The file plan can contain record categories, record folders, volumes, records, and record types.

Bob and his team need to look at all of the documents they currently have stored in their repositories and decide the various object stores to create. They use IBM Enterprise Records to create and maintain a file plan for storing records and also to create retention and disposal schedules. For example, if ExampleCo. Enterprises has a particular customer that has a problem with one of their products a ExampleCo. Enterprises's records manager, Ranjun, can search for all records associated with that customer, and those records can be placed on hold. That way, none of these records can be destroyed until the legal department gives its approval and the hold is removed.

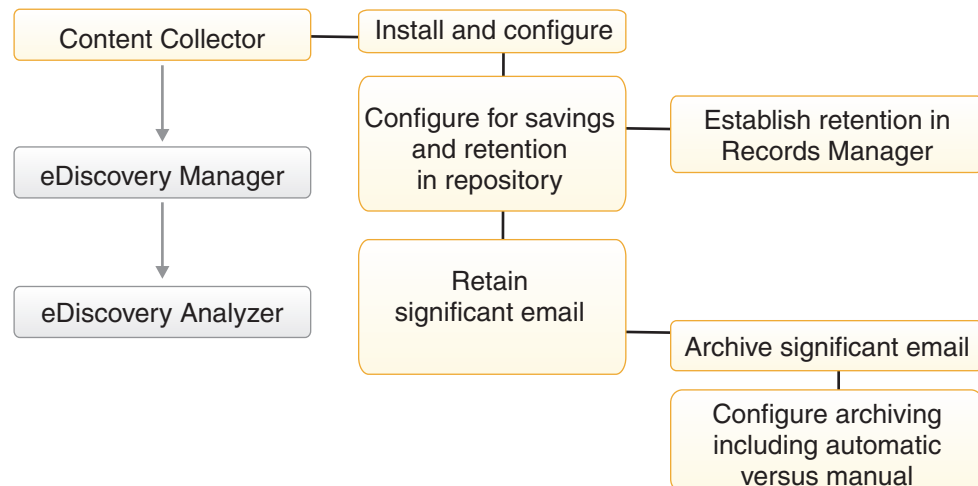
The reporting features delivered with IBM Enterprise Records help Ranjun see file plan information is organized based on configuration criteria such as user action, disposition actions and schedules, time of creation, viewed by user, and so on. Ranjun uses this information to help create reports.

To help Bob classify and organize the ExampleCo. Enterprises records, he also uses IBM Content Classification.

## **Scenario: Preparing the email repository for email analytics**

ExampleCo. Enterprises, a fictitious company that builds electronic appliances, must go to court to contest patent claims by other companies. Email, among other evidence, can prove that ExampleCo. Enterprises is the legal owner of their inventions. This scenario describes how employees in ExampleCo. Enterprises prepare their email archiving system to be able to find email that is relevant to a lawsuit.





Sometimes, competitors copy ExampleCo. Enterprises inventions illegally. When ExampleCo. Enterprises learns of such a case, it considers a lawsuit against the infringing party or demands compensation. The company needs to prove that it is the legal owner of these innovations. To do that, ExampleCo. Enterprises provides a law firm with blue prints, meeting minutes, product specifications, patents, patent applications, and email that date back to the time when a product was developed. The law firm analyzes the material and, based on the results, tries to negotiate a settlement with the accused party.

The email of the engineers at ExampleCo. Enterprises proves that ideas evolved at ExampleCo. Enterprises before they could have possibly been discussed by the competitor. Of special interest is email of engineers who left ExampleCo. Enterprises to work for the competition. Some of these documents contain hints that a technology was developed when the engineer still worked for ExampleCo. Enterprises and that therefore ExampleCo. Enterprises has the exclusive right to use this technology. In cases like this, the former managers and co-workers of the engineer must be identified so that they can testify if needed.

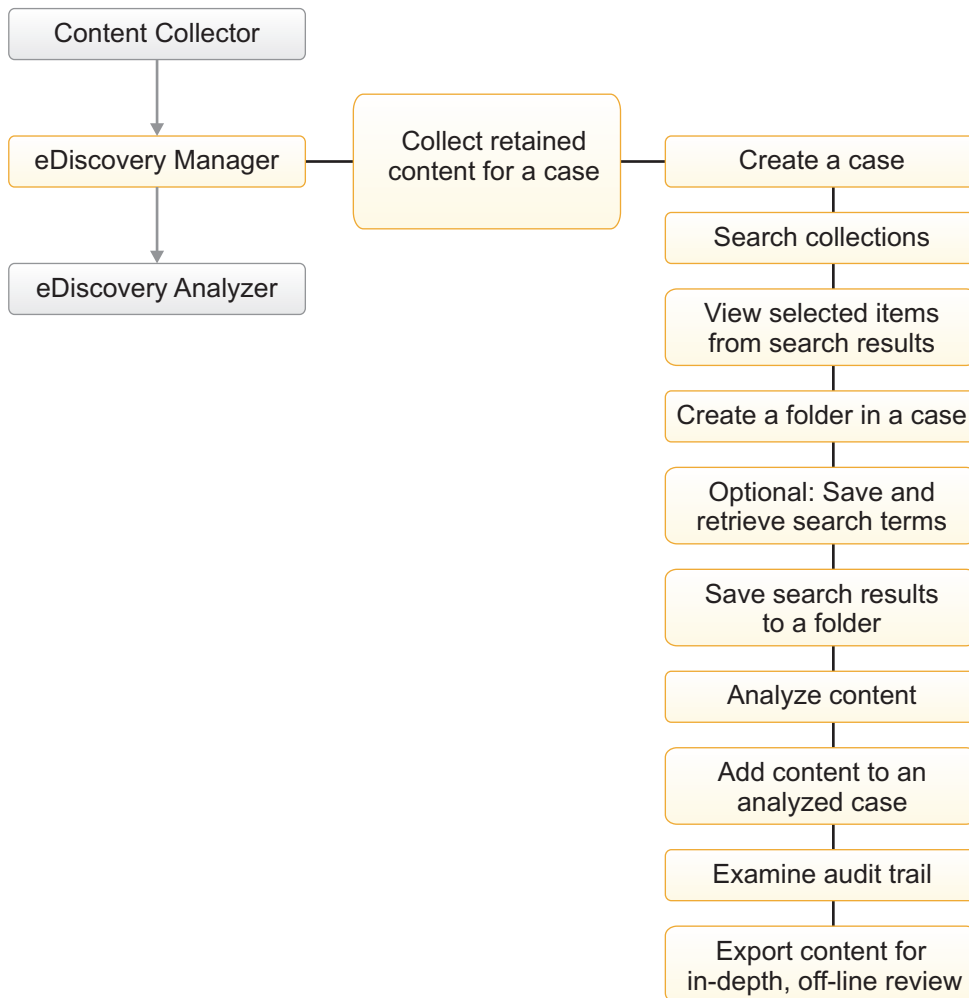
The information in the email can help the attorneys trace the departments that a person worked for and ensure that they find the right person. For that reason, Chris Marsh, the head of the corporate litigation department, and Alexandra Jackson, the legal case administrator, want to search for department numbers, for unique employee identifiers, and for the managers of employees and departments. To collect and preserve the email, they use a tool such as IBM eDiscovery Manager, and to analyze the email, they use email analytics tools like IBM eDiscovery Analyzer. To provide the appropriate search results, these tools require additional attributes to be set in the repository. Chris and Alexandra ask Judy Jameson, the IT administrator, to set up the repository appropriately.

Judy creates additional attributes in the content management system that is serving as the repository for the email documents. These attributes must contain department numbers, identifiers, and manager names. IBM Content Collector will store the information for each email that is archived in the repository. Because the information cannot be found in the email, it will be extracted from the company's Active Directory when the email is archived. Judy also adds the new attribute names to the configuration file for the text-search indexer that is provided by IBM Content Collector. This causes an extraction of the attribute values when the index is built, which adds this information to the text-search index. The information in the text-search index is used by IBM eDiscovery Manager.

## Scenario: Collecting electronic content for legal cases

This scenario describes how employees in ExampleCo. Enterprises, a fictitious company that has an extensive archive of email and other documents and files, and ExampleCo. LLC, a fictitious law firm that represents ExampleCo. Enterprises, address a recent lawsuit.

The following flowchart about collecting content is described in the text that follows.



Judy Jameson, an IT Administrator for ExampleCo. Enterprises, sets up IBM Content Manager Enterprise Edition as the content server so that IBM Content Collector can archive email and business documents or files into the Content Manager EE system. In addition, Judy installs and configures IBM eDiscovery Manager so that the email and business documents or files can be discovered, if needed. For better performance, she installs eDiscovery Manager on its own system.

After Judy gets the archive systems running, a lawsuit is filed against ExampleCo. Enterprises.

By using eDiscovery Manager, Alexandra Jackson, who is a Case Administrator for ExampleCo. LLC, creates a case and assigns Ben Williams, a paralegal with the eDiscovery Manager Case Builder role, to find content that might pertain to the lawsuit.

Alexandra provides the search terms that Ben will use to find the correct content. Ben logs in to the eDiscovery Manager web client and opens the case that Alexandra created. Before Ben performs the search, he saves the search terms so that he can load them, if needed, at a later time to modify them before rerunning the search. After the search is saved, Ben runs the search and it returns over 10,000 results. Ben searches on email addresses, date ranges, and specific search terms within the subject, body, and attachments of email to find content that is potentially relevant to the legal matter. In the business file collection, he also searches on author, creation date and specific search terms to identify more content that is potentially relevant.

Ben previews a few of the results to verify that the content is indeed what he is looking for. The results are appropriate for the current discovery order, and Ben adds the results to a folder within the case. By adding the results to a folder, Ben places a legal hold on the content. This content is automatically locked, ensuring that it cannot be deleted from the content server before the litigation process.

Ben receives new search terms from Alexandra. He searches on the additional terms, creates new folders, and adds the search results to the new folders. After searching for all of the new terms, Ben gathers relevant content into a single case folder by moving items from one folder to another. When Ben completes his work, he exports the content for further processing by an analytic tool and other legal reviewers. He is able to export the content because Ben's eDiscovery Manager user ID also includes the Exporter role.

Alexandra is also assigned the eDiscovery Manager Auditor role. She then generates an audit report from the eDiscovery Manager web client that shows the searches that were performed, the user who performed the searches, and a list of the content that was exported. She provides the report to both legal teams.

## **Scenario: Managing a case life cycle**

You use IBM eDiscovery Manager and IBM eDiscovery Analyzer together to create, manage, analyze, review, and export the documents in a case.

Alexandra Jackson has a background in information technology (IT), but she currently works closely with the general counsel for ExampleCo. LLC, a fictitious law firm. Alexandra's is responsible for understanding legal discovery requests and translating them into searches on archived documents Alexandra also works with email system administrators, email archive administrators, and other specialized IT administrators as required to search cases. Alexandra is responsible for creating cases in eDiscovery Manager, and for the basic configuration of eDiscovery Manager and eDiscovery Analyzer.

Ben Williams is a paralegal working on contract to ExampleCo. LLC, reviewing documents for a case before the documents are sent for outside review. Ben uses eDiscovery Analyzer to review case documents and flag the documents that are not relevant to the discovery order.

Alexandra created a case named Demo\_Case in eDiscovery Manager for a client of ExampleCo. LLC. Alexandra saved the search that determined which documents

are part of the case. Ben has completed some preliminary searches on Demo\_Case, and flagged a few documents. Ben transferred the results of his analysis to the content server, and the flags that Ben applied can be seen in Demo\_Case in eDiscovery Manager.

The attorneys on both sides of the case met and agreed to some changes in the search terms for documents that are relevant to the case. To apply the new terms to the existing case, Alexandra opens the saved search, changes the terms, saves the search again, and schedules the search to run each week, just in case the contents change again. When she runs the saved search, Alexandra selects the option to only show search results that are not already in the case.

A few weeks later, Alexandra logs in to eDiscovery Analyzer as an administrator and notices that the contents of Demo\_Case have indeed changed. The changes require that the case be updated. Alexandra updates the case, and notifies Ben to review the case again for any new documents. The documents that were previously flagged are still flagged, and previously flagged documents that are no longer in the case are gone. The new content is not flagged. Ben analyzes all of the documents that have not been flagged, and flags more documents that appear to be responsive.

When Ben finishes his analysis, he notifies Alexandra that she can transfer the case back to the content server. Alexandra transfers the case, and then exports the contents of the Responsive folder for review by an outside firm. Because she uses the EDRM format, flagging information is also included in the exported information.

## **Scenario: Analyzing collected documents for legal discovery**

Attorneys and paralegals at ExampleCo. LLC, a fictitious law firm, comply with the discovery order from a recent lawsuit brought against their client, ExampleCo. Enterprise, by analyzing documents that were previously collected and categorized by eDiscovery Manager.

Chris Marsh, a junior lawyer at ExampleCo. LLC, has been assigned to the lawsuit against ExampleCo. Enterprise. He logs on to eDiscovery Analyzer and in his list of cases he sees a new case for the ExampleCo. Enterprise lawsuit. The new case was created with eDiscovery Manager by Ben Williams, a paralegal in his firm, when he searched ExampleCo. Enterprise's large email archive for documents potentially relevant to the lawsuit's discovery order.

As an administrator in eDiscovery Analyzer, Chris indexes the new case so that its documents can be further analyzed. The case contains over 10,000 documents and email attachments.

After the case is fully indexed, Chris searches for a few general terms that would pertain to the lawsuit that appear in many of the documents. eDiscovery Analyzer lists aspects of the search results, such as phrases or email recipients, in order of their frequency. Chris reviews a few of the most frequently-occurring phrases to narrow his search to a smaller set of documents, and reviews a few of the documents in this smaller set to confirm their relevance.

Chris notices large blocks of recurring text in many emails that contain corporate disclaimers or contact information. Chris specifies this text as *ignore text*, and updates the index for the case so that the specified text is no longer included in future search results. Throughout his analysis, Chris realizes some important

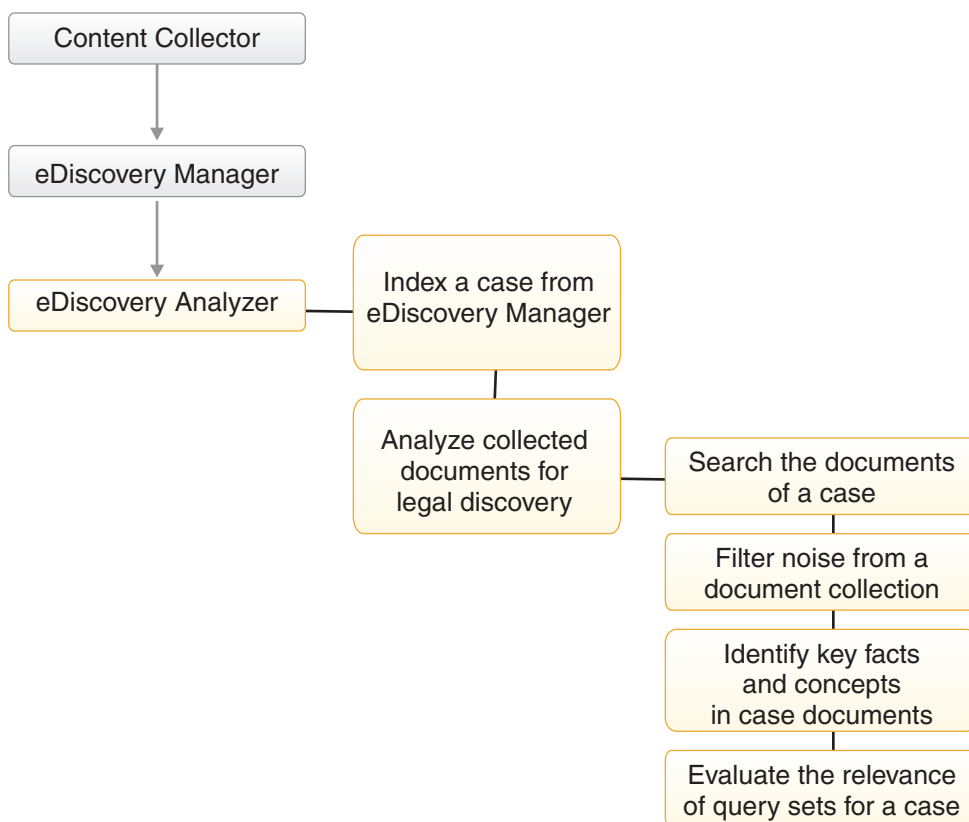
search terms (such as "confidential") return many irrelevant documents because the term is found in a standard email or document boilerplate text such as a footer or signature block. Chris marks these chunks of standard text as ignore text too to eliminate them from future searches.

Soon Chris notices entire documents that can be safely ignored, such as spam, automatically-generated email, or company announcements. He filters out this noise by searching for phrases or senders that frequently appear in these documents, and flags them as "Non-Responsive." He then excludes all documents flagged as "Non-Responsive" in his future searches.

Chris continues to analyze the case documents by successively viewing frequent phrases, email senders, and document authors. He uses the graphical timeline to further narrow the set of documents to a period of time when most of the emails were sent and documents were created. He follows several email threads to confirm his search criteria. By interacting with the case documents, successively narrowing and then broadening his searches, Chris identifies key facts and concepts within the documents. Chris also uses the graphical email diagram to identify key relationships and communications between email senders and recipients. He finds a few documents that might be extremely important in the lawsuit, and he marks these documents with a "Hot" flag as he finds them. Chris constructs several alternate search queries, based on his new understanding of the key facts underlying this case, and saves them as avenues of inquiry to pursue further.

After creating the best starting search query for the case, Chris flags these documents as "Relevant" to the lawsuit. Now finished with his analysis, Chris writes the case data back to the content server, with the flagged documents saved into folders in eDiscovery Manager. He can then export the case in a format suitable for later review by a senior lawyer at ExampleCo. LLC.

The following diagram illustrates a typical flow of documents being analyzed for legal discovery.



## Sample configurations

This section describes two sample system configurations based on two different content repositories: Content Manager EE and FileNet P8.

**Note:** All information in the sample system configurations is presented for your planning purpose. It is intended to show how you might design and plan an environment for your eDiscovery and Archive solution products. For specific hardware and software requirements for any product, see the documentation for that product.

### Planning IBM Content Collector, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with Content Manager EE

This topic describes a high level system configuration that might help you plan your adoption and implementation of IBM Content Collector, IBM eDiscovery Manager, and IBM eDiscovery Analyzer. This configuration assumes that you use Content Manager EE as content repository.

*Table 1. Planning IBM Content Collector, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with Content Manager EE*

Machine	User Role	Hardware Requirements	Software Requirements and Installation Order
Machine 1: Your content repository – Content Manager EE	Content Manager EE system administrator: Manages content storage, storage policy and other repository service.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008 R2</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 8 GB</li> <li>Disk Space: &gt; 500 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. DB2®</li> <li>2. DB2 Net Search Extender</li> <li>3. WebSphere Application Server</li> <li>4. Content Manager EE server</li> <li>5. IBM Content Collector indexer</li> </ol>
Machine 2: Your archival server – IBM Content Collector	Archival server administrator: Manages content archival and retention.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008 R2</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 8 GB</li> <li>Disk Space: &gt; 150 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. DB2</li> <li>2. Information Integrator for Content</li> <li>3. Outlook or Domino Server API</li> <li>4. IBM Content Collector</li> </ol>
Machine 3:eDiscovery Manager	eDiscovery administrator: Manages discovery of archived content.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 8 GB</li> <li>Disk Space: &gt; 500 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. Information Integrator for Content</li> <li>2. WebSphere Application Server</li> <li>3. Domino Server API</li> <li>4. eDiscovery Manager</li> </ol>
Machine 4: eDiscovery Analyzer	eDiscovery administrator: Manages discovery of archived content.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 4 GB</li> <li>Disk Space: &gt; 500 GB</li> </ul>	<p>eDiscovery Manager</p> <p>It is highly recommended that you install eDiscovery Analyzer on a different machine than the machine on which your eDiscovery Manager server is installed.</p>

## Planning IBM Content Collector, IBM Content Classification, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with Content Manager EE

This topic describes a high level system configuration that might help you plan your adoption and implementation of the entire Archive and eDiscovery solution suite. This configuration assumes that you use Content Manager EE as content repository.

*Table 2. Planning IBM Content Collector, IBM Content Classification, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with Content Manager EE*

Machine	User Role	Hardware Requirements	Software Requirements and Installation Order
Machine 1: Your content repository – Content Manager EE	Content Manager EE system administrator: Manages content storage, storage policy and other repository service.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008 R2</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 8 GB</li> <li>Disk Space: &gt; 500 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. DB2</li> <li>2. DB2 Net Search Extender</li> <li>3. WebSphere Application Server</li> <li>4. Content Manager EE server</li> <li>5. IBM Content Collector indexer</li> </ol>
Machine 2: Your archival server – IBM Content Collector	Archival server administrator: Manages content archival and retention.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008 R2</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 8 GB</li> <li>Disk Space: &gt; 150 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. DB2</li> <li>2. Information Integrator for Content</li> <li>3. Domino Server API or Outlook</li> <li>4. IBM Content Collector server</li> </ol>
Machine 3: IBM Content Classification	Archival server administrator: Manages content classification.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008</li> <li>CPU: 2.66 GHz</li> <li>Memory: 2 GB</li> <li>Disk Space: &gt; 100 GB</li> </ul>	
Machine 4: eDiscovery Manager	eDiscovery administrator: Manages discovery of archived content.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 8 GB</li> <li>Disk Space: &gt; 500 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. Information Integrator for Content</li> <li>2. WebSphere Application Server</li> <li>3. Domino Server API</li> <li>4. eDiscovery Manager</li> </ol>



*Table 2. Planning IBM Content Collector, IBM Content Classification, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with Content Manager EE (continued)*

Machine	User Role	Hardware Requirements	Software Requirements and Installation Order
Machine 5: eDiscovery Analyzer	eDiscovery administrator: Manages discovery of archived content.	Example specifications: <ul style="list-style-type: none"> <li>• Operating system: Windows Server 2008</li> <li>• CPU: 4-way, 4 x 2 GHz</li> <li>• Memory: 4 GB</li> <li>• Disk Space: &gt; 500 GB</li> </ul>	eDiscovery Manager  It is highly recommended that you install eDiscovery Analyzer on a different machine than the machine on which your eDiscovery Manager server is installed.

## Planning IBM Content Collector, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with FileNet P8

This topic describes a high level system configuration that might help you plan your adoption and implementation of IBM Content Collector, IBM eDiscovery Manager, and IBM eDiscovery Analyzer. This configuration assumes that you use FileNet P8 as content repository.

*Table 3. Planning IBM Content Collector, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with FileNet P8*

Machine	User Role	Hardware Requirements	Software Requirements and Installation Order
Machine 1: Your content repository – FileNet P8 Content Engine	FileNet P8 system administrator: Manages content storage, storage policy and other repository service.	Example specifications: <ul style="list-style-type: none"> <li>• Operating system: Windows Server 2008</li> <li>• CPU: 4-way, 4 x 2 GHz</li> <li>• Memory: 8 GB</li> <li>• Disk Space: &gt; 500 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. Active Directory</li> <li>2. DB2</li> <li>3. WebSphere Application Server</li> <li>4. Microsoft Web Services Enhancement</li> </ol>
Machine 2: Your archival server – IBM Content Collector	Archival server administrator: Manages content archival and retention.	Example specifications: <ul style="list-style-type: none"> <li>• Operating system: Windows Server 2008 R2</li> <li>• CPU: 4-way, 4 x 2 GHz</li> <li>• Memory: 8 GB</li> <li>• Disk Space: &gt; 150 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. DB2</li> <li>2. Microsoft WSE</li> <li>3. FileNet EM</li> <li>4. Content Engine Client</li> <li>5. Microsoft Outlook</li> </ol>

Table 3. Planning IBM Content Collector, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with FileNet P8 (continued)

Machine	User Role	Hardware Requirements	Software Requirements and Installation Order
Machine 3:eDiscovery Manager	eDiscovery administrator: Manages discovery of archived content.	Example specifications: <ul style="list-style-type: none"> <li>• Operating system: Windows Server 2008</li> <li>• CPU: 4-way, 4 x 2 GHz</li> <li>• Memory: 8 GB</li> <li>• Disk Space: &gt; 500 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. WebSphere Application Server</li> <li>2. Microsoft Outlook</li> <li>3. Content Engine</li> </ol>
Machine 4: eDiscovery Analyzer	eDiscovery administrator: Manages discovery of archived content.	Example specifications: <ul style="list-style-type: none"> <li>• Operating system: Windows Server 2008</li> <li>• CPU: 4-way, 4 x 2 GHz</li> <li>• Memory: 4 GB</li> <li>• Disk Space: &gt; 500 GB</li> </ul>	eDiscovery Manager <b>Note:</b> It is highly recommended that you install eDiscovery Analyzer on a different machine than the machine on which your eDiscovery Manager server is installed.

## Planning IBM Content Collector, IBM eDiscovery Manager, IBM eDiscovery Analyzer, and IBM Enterprise Records with FileNet P8

This topic describes a high level system configuration that might help you plan your adoption and implementation of IBM Content Collector, IBM eDiscovery Manager, IBM eDiscovery Analyzer, and IBM Enterprise Records. This configuration assumes that you use FileNet P8 as content repository.

Table 4. Planning IBM Content Collector, IBM eDiscovery Manager, IBM eDiscovery Analyzer, and IBM Enterprise Records with FileNet P8

Machine	User Role	Hardware Requirements	Software Requirements and Installation Order
Machine 1: Your content repository – FileNet P8 Content Engine	FileNet P8 system administrator: Manages content storage, storage policy and other repository service.	Example specifications: <ul style="list-style-type: none"> <li>• Operating system: Windows Server 2008</li> <li>• CPU: 4-way, 4 x 2 GHz</li> <li>• Memory: 8 GB</li> <li>• Disk Space: &gt; 500 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. Active Directory</li> <li>2. DB2</li> <li>3. WebSphere Application Server</li> <li>4. Microsoft Web Services Enhancement</li> </ol>

Table 4. Planning IBM Content Collector, IBM eDiscovery Manager, IBM eDiscovery Analyzer, and IBM Enterprise Records with FileNet P8 (continued)

Machine	User Role	Hardware Requirements	Software Requirements and Installation Order
Machine 2: Your archival server – IBM Content Collector	Archival server administrator: Manages content archival and retention.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008 R2</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 8 GB</li> <li>Disk Space: &gt; 150 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. DB2</li> <li>2. Microsoft WSE</li> <li>3. FileNet EM</li> <li>4. Content Engine Client</li> <li>5. Microsoft Outlook</li> </ol>
Machine 3: IBM Enterprise Records	Archival server administrator: Perform centralized policy management for file plans and maintain retention schedules	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008</li> <li>CPU: 2.66 GHz</li> <li>Memory: 2 GB</li> <li>Disk Space: &gt; 100 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. Workplace XT</li> <li>2. Content Engine Client</li> <li>3. Process Engine Client</li> <li>4. Content Engine</li> <li>5. Process Engine</li> </ol>
Machine 4:eDiscovery Manager	eDiscovery administrator: Manages discovery of archived content.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 8 GB</li> <li>Disk Space: &gt; 500 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. WebSphere Application Server</li> <li>2. Microsoft Outlook</li> <li>3. Content Engine</li> </ol>
Machine 5: eDiscovery Analyzer	eDiscovery administrator: Manages discovery of archived content.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 4 GB</li> <li>Disk Space: &gt; 500 GB</li> </ul>	eDiscovery Manager <b>Note:</b> It is highly recommended that you install eDiscovery Analyzer on a different machine than the machine on which your eDiscovery Manager server is installed.

## Planning IBM Content Collector, IBM Content Classification, IBM Enterprise Records, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with FileNet P8

This topic describes a high level system configuration that might help you plan your adoption and implementation of the entire Archive and eDiscovery solution suite. This configuration assumes that you use FileNet P8 as content repository.

*Table 5. Planning IBM Content Collector, IBM Content Classification, IBM Enterprise Records, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with FileNet P8*

Machine	User Role	Hardware Requirements	Software Requirements and Installation Order
Machine 1: Your content repository – FileNet P8 Content Engine	FileNet P8 system administrator: Manages content storage, storage policy and other repository service.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 8 GB</li> <li>Disk Space: &gt; 500 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. Active Directory</li> <li>2. DB2</li> <li>3. WebSphere Application Server</li> <li>4. Microsoft Web Services Enhancement</li> </ol>
Machine 2: Your archival server – IBM Content Collector	Archival server administrator: Manages content archival and retention.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008 R2</li> <li>CPU: 4-way, 4 x 2 GHz</li> <li>Memory: 8 GB</li> <li>Disk Space: &gt; 150 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. DB2</li> <li>2. Microsoft WSE</li> <li>3. FileNet EM</li> <li>4. Content Engine Client</li> <li>5. Microsoft Outlook</li> </ol>
Machine 3: IBM Content Classification	Archival server administrator: Manages content classification.	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008</li> <li>CPU: 2.66 GHz</li> <li>Memory: 2 GB</li> <li>Disk Space: &gt; 100 GB</li> </ul>	
Machine 4: IBM Enterprise Records	Archival server administrator: Perform centralized policy management for file plans and maintain retention schedules	Example specifications: <ul style="list-style-type: none"> <li>Operating system: Windows Server 2008</li> <li>CPU: 2.66 GHz</li> <li>Memory: 2 GB</li> <li>Disk Space: &gt; 100 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. Workplace XT</li> <li>2. Content Engine Client</li> <li>3. Process Engine Client</li> <li>4. Content Engine</li> <li>5. Process Engine</li> </ol>

Table 5. Planning IBM Content Collector, IBM Content Classification, IBM Enterprise Records, IBM eDiscovery Manager, and IBM eDiscovery Analyzer with FileNet P8 (continued)

Machine	User Role	Hardware Requirements	Software Requirements and Installation Order
Machine 5:eDiscovery Manager	eDiscovery administrator: Manages discovery of archived content.	Example specifications: <ul style="list-style-type: none"> <li>• Operating system: Windows Server 2008</li> <li>• CPU: 4-way, 4 x 2 GHz</li> <li>• Memory: 8 GB</li> <li>• Disk Space: &gt; 500 GB</li> </ul>	<ol style="list-style-type: none"> <li>1. WebSphere Application Server</li> <li>2. Microsoft Outlook</li> <li>3. Content Engine</li> </ol>
Machine 6: eDiscovery Analyzer	eDiscovery administrator: Manages discovery of archived content.	Example specifications: <ul style="list-style-type: none"> <li>• Operating system: Windows Server 2008</li> <li>• CPU: 4-way, 4 x 2 GHz</li> <li>• Memory: 4 GB</li> <li>• Disk Space: &gt; 500 GB</li> </ul>	eDiscovery Manager <b>Note:</b> It is highly recommended that you install eDiscovery Analyzer on a different machine than the machine on which your eDiscovery Manager server is installed.



---

## Chapter 2. Installing eDiscovery Manager

You can install IBM eDiscovery Manager on an AIX system or a Microsoft Windows system.


### Installing eDiscovery Manager on an AIX system

**Tips:**

- The default location of the installation directory is `/opt/IBM/eDM/`.
- If you decide to install eDiscovery Manager in a directory other than the default directory, ensure that:
  - The path to the eDiscovery Manager installation directory contains only characters that are defined in the active code page.
  - The path to the eDiscovery Manager installation directory does not contain any space characters.
- When installing eDiscovery Manager, you must be logged on to the system as the root user.
- Never install a lower version of eDiscovery Manager on a system that is already running a higher version of eDiscovery Manager. If you want to downgrade eDiscovery Manager, always uninstall the currently running version of eDiscovery Manager and reinstall the lower version.

### Installing eDiscovery Manager on a Windows system

**Tips:**

- The default location of the installation directory for 64-bit eDiscovery Manager installations is `C:\Program Files\IBM\eDM\`.
- If you decide to install eDiscovery Manager in a directory other than the default directory, ensure that:
  - The path to the eDiscovery Manager installation directory contains only characters that are defined in the active code page.
- When installing eDiscovery Manager, you must be logged on to the system as a member of the administrators group.
-  To avoid possible problems when installing eDiscovery Manager, ensure that the path names that are defined for the user environment variables TEMP and TMP do not contain any blank spaces.
- Never install a lower version of eDiscovery Manager on a system that is already running a higher version of eDiscovery Manager. If you want to downgrade eDiscovery Manager, always uninstall the currently running version of eDiscovery Manager and reinstall the lower version.

---

## Installing eDiscovery Manager to connect to Content Manager EE

Before installing IBM eDiscovery Manager, you must install all of the prerequisite software on the eDiscovery Manager system.

### About this task

**Prerequisites:**

- “Before installing eDiscovery Manager to connect to Content Manager EE” on page 27
- “Connecting eDiscovery Manager to Content Manager EE using single sign-on” on page 30

**Important:** If your system has existing <edmhome>\bin and <edmhome>\lib directories, those directories will be removed before they are installed by the installation program. If you have placed any files in those directories, copy them to another location.

Complete the following prerequisite tasks before you install eDiscovery Manager:

**Related tasks:**

“Before installing eDiscovery Manager to connect to Content Manager EE” on page 27


Before installing IBM eDiscovery Manager, ensure that the following prerequisites are met.

“Installation checklist (Content Manager EE)” on page 32

“Configuring single sign-on support” on page 131

Single sign-on (SSO) support enables users to log in only once and access both IBM eDiscovery Manager and the content servers. To enable SSO, you must first enable SSO code in the web.xml file for eDiscovery Manager.

**Related information:**

 System requirements for IBM eDiscovery Manager Version 2.2.2  
This document describes the hardware and software prerequisites for eDiscovery Manager.

## Before upgrading eDiscovery Manager

Before upgrading IBM eDiscovery Manager, complete the following tasks.

### Procedure

1. Back up the following systems:

- The eDiscovery Manager system
- The library server and resource manager databases
- The library server system
- The resource manager system




**Important:** The JVM arguments that are defined in the eDiscovery Manager profile are removed during the upgrade installation. If you added JVM arguments in the previous version, you will need to re-add them after the upgrade installation.

2. Check the product readme and related technotes for the most current information before upgrading.

3. Log in to the eDiscovery Manager web client as the administrator.

- Verify that all tasks on the Task Status pane of the Administration page are complete. Do not proceed to the next step unless all tasks are complete.
- Determine whether there are any cases in the inactive phase. Saved searches that belong to inactive cases cannot be upgraded. If you want the saved searches in an inactive case to be upgraded, move the case to the active phase before upgrading and then move the case back to the inactive phase after upgrading.



4. If you use email notifications, make a note of the EDMMail session settings in the WebSphere Application Server administrative console. After the upgrade is completed, the EDMMail session settings are removed, and you must reapply the settings. Navigate to **ResourcesMail SessionsEDMMailsession** to view your settings.
5. If you are upgrading or reinstalling eDiscovery Manager, stop the eDiscovery Manager application server.
  -  **AIX** Stop and restart the eDiscovery Manager application server as the root user. You must stop each eDiscovery Manager server in your environment.
  -  **Windows** Stop the eDiscovery Manager application server. You must stop each eDiscovery Manager server in your environment.See the WebSphere Application Server product information for details about stopping and starting an application server.
6. Verify that Lotus Notes®, Domino Administrator, and the Lotus Domino server are not running on the eDiscovery Manager system.
7.  **AIX** Update the additional process execution settings that are associated with the eDiscovery Manager profile by clearing the **Run as user** and **Run as group** fields. Use the WebSphere Administrative Console to access the additional process execution settings in **Application servers > server1 > Process definition > Process execution**.
8. Know that you cannot downgrade eDiscovery Manager.

Never install a lower version of eDiscovery Manager on a system that is already running a higher version of eDiscovery Manager. If you want to downgrade eDiscovery Manager, always uninstall the currently running version of eDiscovery Manager and reinstall the lower version.

## What to do next

After you complete all of these steps, you are ready to upgrade eDiscovery Manager. You can skip all of the prerequisite software installation topics and continue directly to “Installing or upgrading eDiscovery Manager in a Content Manager EE environment” on page 40.

### Related information:

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

## Before installing eDiscovery Manager to connect to Content Manager EE

Before installing IBM eDiscovery Manager, ensure that the following prerequisites are met.

### About this task

#### Procedure

1. Verify that your system meets the minimum hardware and software requirements listed at System requirements for eDiscovery Manager.

2. Ensure that you have a temporary directory with 700 MB of free space for installing eDiscovery Manager.

On AIX, the default temporary directory is /tmp. If you want to change the directory that the installation program uses, set the IATEMPDIR environment variable to specify a different directory.

On Microsoft Windows, the temporary directory is defined by the TMP environment variable. To specify a directory different from the current one, set the TMP system environment variable to point to the required location.

3. Ensure that you have a working IBM Content Manager Enterprise Edition system.

Global caching must be disabled on the Content Manager EE system. eDiscovery Manager does not support global caching. Disable global caching with the CPPGlobalCacheEnabled parameter in the cmbicmcache.ini file:

```
CPPGlobalCacheEnabled=FALSE
```

The default location for the cmbicmcache.ini file is in *IBMCMROOT\cmgmt\connectors\* on Microsoft Windows systems and in */home/ibmcmadm/cmgmt/connectors/* on AIX systems. For example: *C:\Program Files\IBM\db2cmv8\cmgmt\connectors* on a Microsoft Windows system.

4. Temporarily disable the deferred DDL execution feature of Content Manager EE before installing eDiscovery Manager. You can re-enable this feature after installing eDiscovery Manager.

If the deferred DDL execution feature is enabled on the Content Manager EE server that eDiscovery Manager connects to, the eDiscovery Manager installation will fail with a data model creation error (such as DGL5050A). The eDiscovery Manager installation program creates item types and relies on those item types being created immediately. Thus, the deferred DDL execution feature of Content Manager EE must be disabled.

5. Create a new Content Manager EE user account or choose an existing user account to serve as the eDiscovery administrator.

**Recommendation:** To make security configuration simpler, choose the account of a content server administrator to serve as the eDiscovery administrator.

The eDiscovery Manager installation program will prompt you for the user ID and password of the eDiscovery administrator on the Administrative Accounts pane. This information is saved in the *ral.properties* file and eDiscovery Manager recognizes this user as a Super User.

Complete the following steps:

- a. Assign the eDiscovery administrator to the DB2 users group (by default, DB2USERS), if the administrator is not already a member. The eDiscovery administrator must be an authorized DB2 user.
- b. On systems running DB2 Version 9.7 or later, if the DB2 system has operating system security enabled, grant database administration authority on the library server database to the eDiscovery administrator. To do this, run the following command in a DB2 command window on a single line:

```
GRANT DBADM WITH DATAACCESS WITH ACCESSCTRL ON DATABASE TO USER  
eDiscovery_administrator
```

For complete information, see the GRANT (database authorities) statement topic in the DB2 solution information center.

6.  Create a user ID for starting the eDiscovery Manager application server:

- a. Create an AIX non-root user ID. The eDiscovery Manager installation program will prompt you for this user ID on the Owner and Group pane.

- b. Create an AIX group and add the new AIX non-root user ID to it. The eDiscovery Manager installation program will prompt you for this group on the Owner and Group pane.

The `.profile` file for this user ID must exist in the `$HOME/AIX_non_root_user_ID` subdirectory.

- c. If the locale of the user ID is set to a multi-byte language, such as Japanese or Chinese, it is important that the locale supports Unicode (UTF-8). Otherwise, you might encounter problems while exporting email to Lotus Domino. For example, to enable Unicode support for Japanese, set export `LANG=jp_JP.UTF-8` in the `.profile` file for the user ID.

7. If your site uses resource manager replication, check with your Content Manager EE administrator to verify that the collection that is assigned to the eDiscovery administrator account is enabled for replication.

Because the audit report item type (EDMAuditRepts) and the search template item type (EDMSrchTempls) in Content Manager EE environments are resource item types, eDiscovery Manager requires a resource manager. eDiscovery Manager uses the default resource manager and default collection that are assigned to the eDiscovery administrator account for the eDiscovery Manager resource item types (EDMAuditRepts and EDMSrchTempls). If the default collection is not enabled for replication, eDiscovery Manager will be unable to access the replica resource manager during failover.

8. If your site uses resource manager migration, check with your Content Manager EE administrator to verify that if the default collection that is assigned to the eDiscovery administrator account is enabled for migration, it has no IBM Tivoli® Storage Manager archiving policy.

Because the search template item type (EDMSrchTempls) in Content Manager EE environments is a resource item type, eDiscovery Manager requires a resource manager. eDiscovery Manager uses the default resource manager and default collection that are assigned to the eDiscovery administrator account for the eDiscovery Manager resource item types (such as EDMSrchTempls). If the default collection has a Tivoli Storage Manager archiving policy, search templates that are migrated to Tivoli Storage Manager cannot be modified.

9. If your site uses Tivoli Storage Manager archiving, check with your Content Manager EE administrator to verify that eDiscovery Manager audit reports are assigned to a resource manager collection that has no Tivoli Storage Manager archiving policy.

Because the audit report item type in Content Manager EE environments is a resource item type, eDiscovery Manager requires a resource manager. eDiscovery Manager uses the default resource manager and default collection that are assigned to the eDiscovery administrator account for the eDiscovery Manager resource item types. However, archiving audit reports to a Tivoli Storage Manager storage device can significantly increase the time that is required to retrieve and display the reports in eDiscovery Manager.

10. **Lotus Domino and Lotus Notes environments only.** Complete the following steps:

- a. Create a Lotus Domino group called `EDISC_USERS` on the remote Lotus Domino server.

Locate the Name and Address book on the remote Lotus Domino server and follow the instructions in the Lotus Domino documentation for creating a group.



- b. Create a Lotus Notes user ID for eDiscovery Manager on the remote Lotus Domino server and add the new Lotus Notes user ID to the `EDISC_USERS` Lotus Domino group on that server.

An ID file is generated for the new user ID. eDiscovery Manager uses this ID file to connect to the remote Lotus Domino server, create databases, and export Lotus Domino email.

**Related concepts:**

“Configuring security in a Content Manager EE environment” on page 103  
During installation, IBM eDiscovery Manager creates a security group, privilege sets, privileges, and access control lists (ACLs) on the primary IBM Content Manager Enterprise Edition server.

**Related information:**

-  Installing and configuring Tivoli Storage Manager
-  Deferring DDL execution

## Connecting eDiscovery Manager to Content Manager EE using single sign-on

Before installing IBM eDiscovery Manager and its prerequisites, configure the connection between the eDiscovery Manager system and the IBM Content Manager Enterprise Edition content management system.

### About this task

These instructions are written for IBM WebSphere Application Server Version 8.0.

To configure the connection between the eDiscovery Manager system and the Content Manager EE server using single sign-on:

### Procedure

1. Start the WebSphere Application Server administrative console on the system where you will install eDiscovery Manager.
2. Click **Security > Global Security**.
3. Enable administration and application security:
  - a. Select the **Enable administrative security** option.
  - b. Clear the **Use Java 2 security to restrict application access to local resources** option.
  - c. Click the **Administrative user roles** link and add an administrative user. For more information, click the **More information about this page** link in the Help box on the right panel.
4. Enable single sign-on.
  - a. On the Global security panel, in the Application security area, select the **Enable application security** option.
  - b. Click **Web and SIP security**.
  - c. Click **Single sign-on (SSO)**.
  - d. Select **Enabled**.
  - e. Click **OK** to save your changes.
5. Configure the LDAP server:
  - a. From the Global security panel, select from the **Available realm definitions** list the type of LDAP configuration your content management system uses: **Standalone LDAP registry** or **Federated repositories**.
  - b. Click **Set as current**.

- c. Click **Configure** to configure settings for the standalone LDAP registry or the federated LDAP repositories.
  - d. From the Global security panel, click **OK** to save your changes.
6. Export the LTPA key for cross-cell single sign-on (SSO) from the Content Manager EE server and import it to the eDiscovery Manager application server:
  - a. Start the WebSphere Application Server administrative console on the Content Manager EE server.
  - b. Click **Security > Global security**.
  - c. Under Authentication, **Authentication mechanisms and expiration**, click LTPA.
  - d. Under Cross-cell single sign-on, enter the password that is used to encrypt the LTPA keys.
  - e. Enter a fully-qualified path and file name for the location where you want the exported LTPA keys to reside, for example: C:\LTPA\LTPA\_key\_name.
  - f. Click **Export keys**.
  - g. If you generated a new LTPA key, import the key file to the Content Manager EE server.
  - h. Import the key file to the eDiscovery Manager application server:
    - 1) Copy the key file from the Content Manager EE server to the eDiscovery Manager application server.
    - 2) If it is not already running, start the WebSphere Application Server administrative console on the eDiscovery Manager application server.
    - 3) Click **Security > Global security**.
    - 4) Under Authentication, **Authentication mechanisms and expiration**, click LTPA.
    - 5) Under Cross-cell single sign-on, enter the password that is used to encrypt the LTPA keys.  
This is the same password that you entered on the Content Manager EE server before exporting the key file.
    - 6) Enter the fully-qualified path and file name for the location of the key file that you copied to the eDiscovery Manager application server, for example: C:\LTPA\LTPA\_key\_name.
      - a) Click **Import Keys**.
      - b) Click **Apply** and then click **Save directly to the master configuration**.
7. Use the IBM Content Manager system administration client to update the privilege sets on the Content Manager EE server that are predefined for use by eDiscovery Manager. Enable the AllowTrustedLogon privilege for all eDiscovery Manager privilege sets.
8. Configure single sign-on (SSO) support by enabling SSO code in the web.xml file for eDiscovery Manager.

**Related tasks:**

“Configuring single sign-on support” on page 131

Single sign-on (SSO) support enables users to log in only once and access both IBM eDiscovery Manager and the content servers. To enable SSO, you must first enable SSO code in the web.xml file for eDiscovery Manager.

**Related information:**

 Update the privilege sets for use with single sign-on

## Installation checklist (Content Manager EE)

### About this task

Use the following checklist to gather the information that you will need to provide during installation. When you are prompted for information about your content management system, provide information for only one of the content servers in your environment. You can configure other content servers later.

*Table 6. Information checklist for an IBM eDiscovery Manager installation*

Information	Default or example value	Notes	Record your value here
Installation path for eDiscovery Manager	On AIX: /opt/IBM/eDM  On Windows: C:\Program Files\IBM\eDM	If the installation path contains non-ASCII characters, you must express the path in escaped Unicode. Use a tool such as the one that can be found in the Java™ JDK, such as native2ascii.  On AIX, the installation path cannot contain a space character.	
Path of the WebSphere Application Server instance to which to deploy eDiscovery Manager	On AIX: /opt/IBM/WebSphere/AppServer  On Windows: C:\Program Files\IBM\WebSphere\AppServer		
WebSphere Application Server profile to dedicate to eDiscovery Manager	AppSrv01		
WebSphere Application Server instance to dedicate to eDiscovery Manager	server1	Use the server1 instance to simplify the administration and monitoring of eDiscovery Manager from the WebSphere administration console.	
Whether WebSphere Application Server security is enabled	Yes		
WebSphere Application Server administrative user name		This information is relevant only if administrative security is enabled.	
WebSphere Application Server administrative password		This information is relevant only if administrative security is enabled.	

Table 6. Information checklist for an IBM eDiscovery Manager installation (continued)

Information	Default or example value	Notes	Record your value here
Installation path for the IBM Content Manager connector component of IBM Information Integrator for Content	On AIX: /opt/IBM/db2cmv8  On Windows: C:\Program Files\IBM\db2cmv8		
Content Manager EE library server database name	ICMNLSDB		
User name of a Content Manager EE administrator	ICMADMIN	This user must also be an authorized DB2 user.	
Password of the Content Manager EE administrator			
User name of the Content Manager EE account that will serve as the eDiscovery administrator		This user must also be an authorized DB2 user and a member of the DB2 administrative group.	
Password of the Content Manager EE account that will serve as the eDiscovery administrator			


## Installing WebSphere Application Server

Before you can install IBM eDiscovery Manager, you must install IBM WebSphere Application Server on the same system.

### About this task

You can install eDiscovery Manager to the following types of nodes:

- A WebSphere Application Server Network Deployment managed or unmanaged node
- A WebSphere Application Server Base managed or unmanaged node

**Remember:**  Set the **umask** value to 022 before you install WebSphere Application Server. See Preparing AIX systems for installation for more information about verifying and setting the umask value.

To install WebSphere Application Server in preparation for eDiscovery Manager:

### Procedure

1. Install the prerequisite software for WebSphere Application Server.

You can find a complete list of the WebSphere Application Server hardware and software requirements on the IBM Software Support site at <http://www.ibm.com/support/docview.wss?uid=swg27006921>.




2. Prepare the operating system for WebSphere Application Server.  
To find more information about preparing the operating system, see *Preparing the operating system for product installation*.
3. Install the appropriate version of WebSphere Application Server.  
For more information about installing WebSphere Application Server, see *Installing WebSphere Application Server*.
4. Create a new server profile for eDiscovery Manager.  
In WebSphere Application Server Base environments, when you create a server profile, WebSphere Application Server creates a default application server instance named `server1`. In WebSphere Application Server Network Deployment environments, an application server must be created before installation. Other alternatives in both environments include creating a new application server instance for eDiscovery Manager in an existing profile or installing eDiscovery Manager to an unused application server instance of an existing profile.

**Recommendation:** In WebSphere Application Server Base environments, use the `server1` instance to simplify the administration and monitoring of eDiscovery Manager. (The only application server instance that can be monitored by the WebSphere administration console is `server1`. If you use a server instance other than `server1` for eDiscovery Manager, you will not be able to start, stop, or monitor the status of eDiscovery Manager from within the WebSphere administration console because of this limitation.) You can find more information in *Creating an application server profile*.

**Requirement:** When you create a server profile, WebSphere Application Server places several applications in the server instance that is associated with the new profile. You can ignore these applications. Do not install other, non-WebSphere applications in the server instance that is associated with the eDiscovery Manager profile. For example, do not install IBM FileNet P8, the IBM Content Manager resource manager, or IBM Web Interface for Content Management in the eDiscovery Manager profile.

5. Verify that the WebSphere Application Server is prepared for the eDiscovery Manager installation.
  - If you are deploying eDiscovery Manager to an unmanaged node, start the server instance of the WebSphere Application Server to which you plan to install eDiscovery Manager.
  - If you are deploying eDiscovery Manager to a managed node:
    - a. Start the deployment manager.
    - b. Start the node agent.
    - c. Start the server instance for that node to which you plan to install eDiscovery Manager.

**Related information:**

 [System requirements for IBM eDiscovery Manager Version 2.2.2](#)  
This document describes the hardware and software prerequisites for eDiscovery Manager.

## Installing to a new WebSphere application server or a new WAS profile

You can perform an upgrade installation on the same 64-bit machine that a previous version of eDiscovery Manager was installed but to a different WAS home (64-bit WAS).



## Before you begin

Before you install eDiscovery Manager, make sure that your preferred WebSphere Application Server meets the prerequisites and is installed.

## About this task

You can choose a WAS home and/or WAS profile that is different from prior installations of eDiscovery Manager. However, if you choose to install to a different WAS home and/or WAS profile from the previous eDiscovery Manager installation, then you must perform these steps.

## Procedure

1. Install eDiscovery Manager and select your preferred WebSphere Application Server home and profile during the installation process.
2. If you installed eDiscovery Manager to a different WebSphere Application server or profile from your previous eDiscovery Manager installation, complete the following steps:
  - a. Delete the old WebSphere Application Server profile that was dedicated to eDiscovery Manager. To delete the old WebSphere Application Server profile that was dedicated to eDiscovery Manager, follow instructions in WebSphere Application Server documentation.
  - b. If you do not want to delete the old profile, manually remove the eDiscovery Manager applications by using the WebSphere Administrative console. To manually remove the eDiscovery Manager applications, open the WebSphere Administrative console, go to Applications > Application Types > WebSphere Enterprise Applications, select EDMClient and EDMWorkMgrServer, then click **Uninstall**.

## Installing an IBM Information Integrator for Content connector

IBM Information Integrator for Content is distributed with IBM Content Manager Enterprise Edition and it includes the IBM Content Manager connector. This connector allows you to quickly access information across all of your Content Manager EE servers.

## About this task

The IBM Content Manager connector is the only IBM Information Integrator for Content component that you need to install.


For complete information about IBM Information Integrator for Content, see the IBM DB2 Content Management Version 8.4 Information Center:

- Installing and configuring DB2 Information Integrator for Content

### Related tasks:

“Installation checklist (Content Manager EE)” on page 32

### Related information:

 System requirements for IBM eDiscovery Manager Version 2.2.2  
This document describes the hardware and software prerequisites for eDiscovery Manager.

## Installing the Lotus Domino server

To enable your users to export Lotus Notes content or to view content by using Lotus Notes, you must install the Lotus Domino server on the IBM eDiscovery Manager system. eDiscovery Manager requires only the Lotus Domino APIs, but these APIs are bundled with the Lotus Domino server; the APIs are not bundled separately. For this reason, you must install a Lotus Domino server on the eDiscovery Manager system or logical partition (LPAR), even though you do not start the server itself.

### About this task

In addition to the Lotus Domino server installed on the eDiscovery Manager system or LPAR, a remote Lotus Domino server must be installed on another system. The Lotus Domino server must then be configured to access this remote Lotus Domino server. The purpose of this remote Lotus Domino server is for viewing and exporting Lotus Notes content from your eDiscovery Manager system.

**Important:** On Windows, eDiscovery Manager requires a dedicated installation of the Lotus Domino V8.5 server, even though you do not start the Lotus Domino server. The following table shows the versions of the Lotus Domino server that might be installed on the eDiscovery Manager system. The remote Lotus Domino server can be any version 8 or above, and on any platform, for example, Windows or AIX.

Table 7. Versions of Lotus Domino that are supported on the local Lotus Domino server.



Server	eDiscovery Manager system on AIX	eDiscovery Manager system on Windows
<b>Local Lotus Domino server</b> (on eDiscovery Manager system)	Version 8 (64 bit) Version 8.5 (64-bit)	Version 8 (64 bit) Version 8.5 (64-bit)

To install a Lotus Domino server on the eDiscovery Manager system:

### Procedure

1. Install the Lotus Domino server on the eDiscovery Manager system. If you are installing Lotus Domino Version 8, you can find more information in the Guidepost for deploying Domino topic.

You do not need to configure this local Lotus Domino server if you are installing it only for the purpose of obtaining the Lotus Domino APIs, as recommended.

2.  Verify that the Lotus Domino installation directory was added to the PATH system environment variable, for example, C:\Program Files\IBM\Lotus\Domino.
3.  Log out and log back in to the eDiscovery Manager system as the root user to check the I/O completion port (IOCP):
  - a. Enter the following command to ensure that the IOCP module is installed on the eDiscovery Manager system:

```
$lslpp -l bos.iocp.rte
```

The output from the **lslpp** command should be similar to the following example:


Fileset	Level	State	Description
Path: /usr/lib/objrepos	5.2.0.10	COMMITTED	I/O Completion Ports API
bos.iocp.rte			
Path: /etc/objrepos	5.2.0.10	COMMITTED	I/O Completion Ports API
bos.iocp.rte			

- b. If the IOCP module (bos.iocp.rte) is not installed, install it from the AIX product CD, then enter the **lslpp -l bos.iocp.rte** command again to confirm that it is installed.
- c. Enter the following command to ensure that the status of the IOCP port is **Available**:  

```
$ lsdev -Cc iocp
```

The output from the **lsdev** command should be similar to the following example:

```
iocp0 Available I/O Completion Ports
```
- d. If the IOCP port status is **Defined**, change the status to **Available**:
  - 1) Enter the following command:  

```
# smit iocp
```
  - 2) Select **Change / Show Characteristics of I/O Completion Ports** and change **STATE to be configured at system restart** from **Defined** to **Available**.
  - 3) Reboot the eDiscovery Manager system and log in as the root user.
  - 4) Enter the **lsdev -Cc iocp** command again to confirm that the status of the IOCP port changed to **Available**.
4.  **AIX** Set up the environment for the AIX non-root user ID that starts the eDiscovery Manager application server. You created this user ID as a prerequisite.
  - a. Log out of the eDiscovery Manager system and log back in by using the user ID that starts the eDiscovery Manager application server.
  - b. In the \$HOME directory, create a notesdata subdirectory.
  - c. Copy the Lotus Notes user ID file for the user ID that starts the eDiscovery Manager application server from the remote Lotus Domino server to the \$HOME/notesdata subdirectory on the eDiscovery Manager system.  

You created this user ID as a prerequisite. eDiscovery Manager uses this ID file to connect to the remote Lotus Domino server, create databases, and export Lotus Notes content.
  - d. Create a notes.ini file in the \$HOME/notesdata subdirectory that contains the following lines, as well as a blank line at the end of the file:  

```
[Notes]
Directory=$HOME/notesdata
KeyFileName=Lotus_Notes_user_ID_for_eDM_appServer_starter.id
Ports=TCPIP
TCPIP=TCP,0,15,0
```

**Important:** If the Lotus Domino installation directory already contains a notes.ini file, then the notesConnect utility will always use it. This is true even if the notes.ini file that you created when installing the Lotus Domino server is first in the system path. For this reason, it is necessary to rename the notes.ini file in the Lotus Domino installation directory, if one exists.
  - e. Edit the .profile file for the user ID that starts the eDiscovery Manager application server.  

Remember that the .profile file for this user ID exists in the \$HOME/AIX\_non\_root\_user\_ID subdirectory.

Add the following lines to the .profile file:

```
# LIBPATH: Add the path to the ibmpow directory in the Lotus Domino
# installation directory:
LIBPATH=$LIBPATH:/opt/ibm/lotus64/lotus/notes/latest/ibmpow

# PATH: Add the paths to the notesdata directory,
# ibmpow and bin directories in the Lotus Domino installation directory,
# and resource subdirectory of the Lotus Domino installation directory.
# For example, in English locales, the path of the resource subdirectory is
# /opt/ibm/lotus/notes/latest/ibmpow/res/C
PATH=$PATH:$HOME/notesdata:/opt/ibm/lotus/notes/latest/ibmpow:
/opt/ibm/lotus/bin:/opt/ibm/lotus/notes/latest/ibmpow/res/C

Notes_ExecDirectory=/opt/ibm/lotus/notes/latest/ibmpow


LOTUS=/opt/ibm/lotus

NOTES_DATA_DIR=$HOME/notesdata

export LIBPATH PATH Notes_ExecDirectory LOTUS NOTES_DATA_DIR
```

- f. Copy the names.nsf file from the data directory (\$HOME/notesdata) of the Lotus Domino server (typically a remote server) to the \$HOME/notesdata directory on the eDiscovery Manager system.
- g. Log out of the eDiscovery Manager system and log back in by using the user ID that starts the eDiscovery Manager application server.

The changes that you made to the .profile file for this user ID are now in effect. You can run the **env** command to verify the changes.

5.  Set up the environment for the user ID that starts the eDiscovery Manager application server.
  - a. Create a notesdata directory in a convenient location of your choice, for example \your\_dir\notesdata.
  - b. Copy into the notesdata directory the names.nsf file from the Lotus Domino server that your eDiscovery Manager server will connect to for viewing and exporting Lotus Notes content, typically a remote Lotus Domino server.
  - c. Create a new user ID on the Lotus Domino server, for example, eDMNotesUser. Make sure that this user has read and write access to the eDMMail.nsf database, which is used for viewing Lotus Notes content. This database is created at the Lotus Domino Settings pane of the Administration page in the eDiscovery Manager web client. Also make sure that this user has the ability to create new databases on the Lotus Domino server.
  - d. An ID file is created for this new user ID. Copy this ID file (for example, eDMNotesUser.id) into the \your\_dir\notesdata directory that you just created.
  - e. In the \your\_dir\notesdata directory create a new file called notes.ini with the following contents:

```
[Notes]
Directory=\your_dir\notesdata
KeyFileName=Notes_user_ID_for_eDM.id
Ports=TCPIP
TCPIP=TCP,0,15,0
```

Substitute \your\_dir with the absolute path to your notesdata directory and Notes\_user\_ID\_for\_eDM.id with the new Lotus Notes user ID you created (for example, eDMNotesUser.id).

- f. Edit the system Path environment variable so that the `\your_dir\notesdata` directory is the first directory listed and that the `notes.ini` file is picked from this location.
6. Rename the `notes.ini` file in the Lotus Domino installation directory, if it exists.
7. Verify that the environment for the ID that starts the eDiscovery Manager application server is working by running the eDiscovery Manager `notesConnect` utility. Remember that on AIX systems this ID is a non-root user.  
The `notesConnect` utility connects to the remote Lotus Domino server and returns the title from the names database. Run the `notesConnect` utility on a single line from the `bin` subdirectory of the eDiscovery Manager installation directory. For example:

#### AIX

```
/opt/IBM/EDM/bin/notesConnect names.nsf [remote_Lotus_Domino_server]
```

#### Windows

```
C:\Program Files\IBM\EDM\bin\notesConnect names.nsf  
[remote_Lotus_Domino_server]
```

where `remote_Lotus_Domino_server` is the IP address or IP name of the remote Lotus Domino server.

The `notesConnect` utility uses the Lotus Notes user ID that is configured for the `KeyFileName` setting in the `$HOME/notesdata/notes.ini` file if on AIX or in the `\your_dir\notesdata\notes.ini` file if on Windows.

If the environment is configured properly, the title of the names database is returned. You might be prompted for a password.

#### Related tasks:

“Configuring Lotus Notes viewing” on page 115

If you have content in a collection that originally came from Lotus Domino before it was archived and you want your users to be able to open this content with Lotus Notes, you must configure Lotus Notes viewing. IBM eDiscovery Manager creates a viewing database and assigns read access to eDiscovery Manager users, but you must configure other aspects of the viewing environment.

“Configuring Lotus Notes export” on page 121

If you want your users to be able to export Lotus Notes content, you must configure Lotus Notes export. IBM eDiscovery Manager creates export databases and assigns read access to those eDiscovery Manager users that are assigned permission to export, but you must configure other aspects of the export environment.

## Reinstalling or upgrading the Lotus Domino server on the eDiscovery Manager system

After IBM eDiscovery Manager is installed, if you reinstall or upgrade the Lotus Domino server on the eDiscovery Manager system or logical partition (LPAR), be sure that the `Notes.jar` file is in the IBM WebSphere Application Server shared library class path.

### Procedure

To ensure that the `Notes.jar` file is in the WebSphere Application Server shared library class path:

1. Open the WebSphere Application Server administrative console by clicking **Start > Programs > IBM WebSphere > Application Server > Profiles > eDiscovery Manager application server profile > Administrative console**.
2. Expand **Environment**, **Shared Libraries**, and **EDMLibraries**.

3. Confirm that the **Classpath** field contains an entry for the fully qualified path to the Notes.jar file, for example, on a Windows system:  
C:\Program Files\Lotus\Domino\jvm\lib\ext\Notes.jar.
4. If there is no entry for the Notes.jar file, add one. Then stop and restart the eDiscovery Manager application server for your change to take effect.

**Related information:**

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

## Installing or upgrading eDiscovery Manager in a Content Manager EE environment



After you install and configure the prerequisite software, you can install IBM eDiscovery Manager as an IBM WebSphere Application Server instance and connect it to your IBM Content Manager Enterprise Edition system. Note that the process for upgrading eDiscovery Manager is identical to the process for installing eDiscovery Manager.

### Before you begin

**Prerequisite:** The Content Manager EE server must be started before you can install eDiscovery Manager. The resource manager that is associated with this Content Manager EE server also must be started.



### Procedure

To install or upgrade eDiscovery Manager:

1. Log on to the system by using an appropriate account.
  -  When installing eDiscovery Manager, you must be logged on to the system as the root user.
  -  When installing eDiscovery Manager, you must be logged on to the system as a member of the administrators group.
2. Modify the value of the JavaPool parameter in the cmbpool.ini file to be an empty string. (Do not comment out the JavaPool parameter; simply set its value to an empty string.)

JavaPool=

The cmbpool.ini file is used for IBM WebSphere Application Server connection pooling. The default location for the cmbpool.ini file is in *IBMCROOT\cmgmt\connectors\* on Microsoft Windows systems and in */home/ibmcmadm/cmgmt/connectors/* on AIX systems. For example: C:\Program Files\IBM\db2cmv8\cmgmt\connectors on a Microsoft Windows system.

3. If you are upgrading or reinstalling eDiscovery Manager, stop the eDiscovery Manager application server.
  -  Stop and restart the eDiscovery Manager application server as the root user. You must stop each eDiscovery Manager server in your environment.
  -  Stop the eDiscovery Manager application server. You must stop each eDiscovery Manager server in your environment.

See the WebSphere Application Server product information for details about stopping and starting an application server.

4. Start the installation program.
  - a. At a command prompt, change to the eDiscovery Manager CD or to the directory where you downloaded the product.
  - b. Start the installation program by entering the appropriate command for your operating system.

**AIX**     edM.bin

**Windows**

edM.exe

For performance reasons, consider changing the logging level of the eDMInstallConfig#.log file to INFO when you install eDiscovery Manager.

The default logging level of this file is FINE. To change the logging level, use the **-DLogLevel** parameter. For example, on a Microsoft Windows system, enter the following command to install eDiscovery Manager and change the logging level to be less verbose:

```
edM.exe -DLogLevel=INFO
```

Other optional parameters that you can use when installing eDiscovery Manager are:

**-DLogFileSize**

The default log file size is 10 MB.

**-DNumLogFiles**

The default number of log files is 10.

To change the logging level to be less verbose, to change the log file size to 30 MB, and to change the number of log files to 15, enter the following command to install eDiscovery Manager:

```
edM.exe -DLogLevel=INFO -DLogFileSize=30 -DNumLogFiles=15
```

5. Select your language and click **OK**.
6. Read and accept the software license terms.
7. Follow the on-screen prompts to complete the installation.

**Important tips:**

- If you decide to install eDiscovery Manager in a directory other than the default directory, ensure that:
  - The path to the eDiscovery Manager installation directory contains only characters that are defined in the active code page.
  - The path to the eDiscovery Manager installation directory does not contain any space characters.
- During the application server deployment phase, the installation program deploys the eDiscovery Manager web client and eDiscovery Manager work manager, and configures the application server instance to which they are deployed. This can take up to 20 minutes. Be patient and let the installation program complete on its own.



## Results

**Restriction:** During the eDiscovery Manager installation, the library server database name that is associated with the primary content server is written to the `ral.properties` file. This is the same library server database name that is specified in the Content Manager EE `cmbicmsrvs.ini` file. After eDiscovery Manager is installed, you cannot change the library server database name in either file. The value must be the same in both files and it must remain the same value that it was when eDiscovery Manager was installed.

**Errors:** If an error occurs during the silent installation process, the error will be printed in the eDiscovery Manager debug log file `eDMInstall*.log` files. The log files can be found in the *user.home* during the installation. After installation, they can be found in `edmhome\logs`.

## What to do next

### What to do next

If you upgraded eDiscovery Manager:

1. Start the eDiscovery Manager web client and confirm that the configuration settings on the Administration pages are correct.  
In particular, ensure that all paths are correct, including the absolute path of the export directory on the Export Settings pane and other settings in the Content Management Systems and Lotus Domino Settings panes.
2. Instruct all eDiscovery Manager web client users to close their browsers and then reopen them.  
Users might also want to clear their browser cache and delete temporary files. Doing so removes any cached JavaScript. Users that do not close and reopen their browsers after the upgrade might be unable to log in to the eDiscovery Manager web client.
3. After upgrading, you must configure your item type security.

### Related tasks:

“Configuring item type security” on page 105

Work with your IBM Content Manager Enterprise Edition administrator to use the IBM Content Manager system administration client to configure security for any item types that will belong to eDiscovery collections.

### Related information:

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

## Installation debug log files

To aid in troubleshooting, IBM eDiscovery Manager maintains installation debug log files.

**During the installation:** During the installation, the eDiscovery Manager installation program writes installation progress messages, error messages, and IBM WebSphere Application Server deployment information to installation debug log files. If the installation debug log file reaches 5 MB in size, eDiscovery Manager rolls it over and creates another log file. eDiscovery Manager creates up to four



installation log files (eDMInstallDebug00.log, eDMInstallDebug01.log, eDMInstallDebug02.log, and eDMInstallConfig3.log) before it begins overwriting the first log file.

**Before the installation completes:** Before the installation completes, the installation debug log files and the configuration debug log files exist in your home directory. On an AIX system, the home directory is defined by the HOME environment variable. On a Microsoft Windows system, the home directory is defined by the HOMEPATH environment variable. For example, on Microsoft Windows, your home directory might be C:\Users\yourUserName.

**After the installation completes:** After the installation completes, the installation debug log files and the configuration debug log files are copied to the logs subdirectory of the eDiscovery Manager installation directory. Also after installation, a single installation debug log file named eDMInstall.log is created in the same logs subdirectory.

## Database tuning to improve performance (Content Manager EE)

To improve the performance of IBM eDiscovery Manager in IBM Content Manager Enterprise Edition environments, see instructions at: <http://www.ibm.com/support/docview.wss?uid=swg21610751>

---

## Installing eDiscovery Manager to connect to FileNet P8

Before installing IBM eDiscovery Manager, you must install all of the prerequisite software on the eDiscovery Manager system.

### About this task

#### Prerequisites:

- “Before installing eDiscovery Manager to connect to FileNet P8” on page 46
- “Configuring the IIOP connection between the eDiscovery Manager system and the FileNet P8 server using single sign-on” on page 48

**Important:** If your system has existing <edmhome>\bin and <edmhome>\lib directories, those directories will be removed before they are installed by the installation program. If you have placed any files in those directories, copy them to another location.


Complete the following prerequisite tasks before you install eDiscovery Manager:

#### Related tasks:

“Before installing eDiscovery Manager to connect to FileNet P8” on page 46  
Before installing IBM eDiscovery Manager, ensure that the following prerequisites are met.

“Installation checklist (FileNet P8)” on page 51

#### Related information:

 System requirements for IBM eDiscovery Manager Version 2.2.2  
This document describes the hardware and software prerequisites for eDiscovery Manager.

## Before upgrading eDiscovery Manager

Before upgrading IBM eDiscovery Manager, complete the following tasks.

### About this task

#### Important:

#### FileNet P8 Search Behavior Change

Search behavior on FileNet P8 has been changed. Child classes are no longer included in the searching of parent object classes. In previous versions, a search targeting a specific object class returns:

- All items within that object class that match the search parameters, and
- All items in all child classes of the target class that match the search parameters

Starting with eDiscovery Manager Version 2.2.1, this behavior has been changed so that only the target object class is searched, and child classes of the target object class are not searched, unless specifically specified via a collection referenced within the search template in use.

#### Recommendation

This new behavior is the intended and recommended behavior of eDiscovery Manager searches going forward. IBM strongly recommends that all customers who upgrade from a prior version of eDiscovery Manager adopt the new search behavior immediately. This change has an impact on existing saved and scheduled searches. We recommend that you modify your search templates, collections, or both immediately after upgrade so that saved and scheduled searches target the same object classes as the previous behavior and the scopes of saved and scheduled searches are not altered as a result of the upgrade.

#### Example

Search template All Files contains only one collection ICC Files. The collection ICC Files has only one object class referenced in it: ICCFileInstance2. The ICCFileInstance2 object class has one child class ICCSharepointInstance2. In previous versions of eDiscovery Manager, a search using search template All Files results in a search of the object class ICCFileInstance2 and the object class ICCSharepointInstance2, because the target and child object classes are all searched. In eDiscovery Manager Version 2.2.1 and later, a search using search template All Files results in a search of only the target object class ICCFileInstance2 being searched, because child classes are no longer searched.

To preserve the behavior of existing saved and scheduled searches, searching using the search template All Files needs to search both the ICCFileInstance2 and the ICCSharepointInstance2 object classes. There are two ways to accomplish this:

- **If no current collection explicitly references ICCSharepointInstance2:** Add ICCSharepointInstance2 to the ICC Files collection. After that, both the target object classes in the ICC Files collection will be searched when the All Files search template is used.
- **If ICCSharepointInstance2 is referenced by an existing collection:** You cannot add it to another collection directly. In this case, add the collection that contains ICCSharepointInstance2 to the All Files search template. After that, a search

using the All Files search template will search the two contained collections, one for the ICCFileInstance2 object class and one for the ICCSharepointInstance2 object class.

### Previous Behavior



It is possible that you might want to continue having eDiscovery Manager Version 2.2.2 search FileNet P8 object classes and child classes in the same manner as prior versions. While IBM strongly discourages this approach, it can be achieved by adding the following line to the `ral.properties` configuration file, and then restarting the eDiscovery Manager server:


```
searchP8Subclasses=true
```

This facility to revert to the previous search behavior is a temporary mechanism and was deprecated with eDiscovery Manager Version 2.2.1. In any future release of eDiscovery Manager, IBM may remove this facility without further warning, and the new behavior will be the only way that FileNet P8 object classes are searched. There will be no way to search object classes and their child classes together, except via the approach described in the example above.

### Procedure

Follow these steps to prepare for your upgrade:

1. Back up the following systems:
  - The eDiscovery Manager system
  - The FileNet P8 database
  - The FileNet P8 system and object stores
2. Check the product readme and related technotes for the most current information before upgrading.
3. Log in to the eDiscovery Manager web client as the administrator.
  - Verify that all tasks on the Task Status pane of the Administration page are complete. Do not proceed to the next step unless all tasks are complete.
  - Determine whether there are any cases in the inactive phase. Saved searches that belong to inactive cases cannot be upgraded. If you want the saved searches in an inactive case to be upgraded, move the case to the active phase before upgrading and then move the case back to the inactive phase after upgrading.
4. If you are upgrading or reinstalling eDiscovery Manager, stop the eDiscovery Manager application server.
  -  **AIX** Stop and restart the eDiscovery Manager application server as the root user. You must stop each eDiscovery Manager server in your environment.
  -  **Windows** Stop the eDiscovery Manager application server. You must stop each eDiscovery Manager server in your environment.

See the WebSphere Application Server product information for details about stopping and starting an application server.
5. Verify that Lotus Notes, Domino Administrator, and the Lotus Domino server are not running on the eDiscovery Manager system.
6.  **AIX** Update the additional process execution settings that are associated with the eDiscovery Manager profile by clearing the **Run as user** and **Run as**

**group** fields. Use the WebSphere Administrative Console to access the additional process execution settings in **Application servers > server1 > Process definition > Process execution**.

7. Know that you cannot downgrade eDiscovery Manager.

Never install a lower version of eDiscovery Manager on a system that is already running a higher version of eDiscovery Manager. If you want to downgrade eDiscovery Manager, always uninstall the currently running version of eDiscovery Manager and reinstall the lower version.

If you decide to uninstall eDiscovery Manager and return to a prior release, you must reinstall that prior release against a different object store than the object store that you installed the current version of eDiscovery Manager against.

## What to do next

After you complete all of these steps, you are ready to upgrade eDiscovery Manager. You can skip all of the prerequisite software installation topics and continue directly to “Installing or upgrading eDiscovery Manager in a FileNet P8 environment” on page 60.

**Important:** Refer to “Exporting content that has an unsupported MIME type” on page 177 for information about backing up certain template and configuration files before installing eDiscovery Manager.

## Before installing eDiscovery Manager to connect to FileNet P8

Before installing IBM eDiscovery Manager, ensure that the following prerequisites are met.

### Procedure

1. Verify that your system meets the minimum hardware and software requirements listed at System requirements for eDiscovery Manager.
2. Ensure that you have a temporary directory with 700 MB of free space for installing eDiscovery Manager.

On AIX, the default temporary directory is /tmp. If you want to change the directory that the installation program uses, set the IATEMPDIR environment variable to specify a different directory.

On Microsoft Windows, the temporary directory is defined by the TMP environment variable. To specify a directory different from the current one, set the TMP system environment variable to point to the required location.
3. Ensure that you have a working IBM FileNet P8 system.
4. To improve the performance of the eDiscovery Manager installation program, create the following index. Enter the command on a single line in the directory that you defined:


```
CREATE INDEX IDX_OBJCLSID_OBJID ON GENERIC
(OBJECT_CLASS_ID ASC , OBJECT_ID ASC);
```

This is the same index that is recommended for login, case selection, date range searches, and adding secondary content servers.
5. Ensure that your system meets the following directory service requirements.
  - a. A directory service (such as Microsoft Active Directory, Tivoli Access Manager, and so on) must be configured in FileNet P8.
  - b. For all of the servers in the directory service farm that service eDiscovery Manager and eDiscovery Analyzer, complete the following steps:

- 1) Create a group for eDiscovery users, for example, EDISCOVERYUSERS. The group name must be 32 characters or fewer.
- 2) Create a new FileNet P8 user account or choose an existing user account to serve as the eDiscovery administrator.


**Recommendation:** To make security configuration simpler, choose the account of a content server administrator to serve as the eDiscovery administrator.

The eDiscovery Manager installation program will prompt you for the user ID and password of the eDiscovery administrator on the Administrative Accounts pane. This information is saved in the `ral.properties` file and eDiscovery Manager recognizes this user as a Super User.

- 3) Populate the eDiscovery group with users who you want to have access to eDiscovery Manager and IBM eDiscovery Analyzer. Be sure to add the eDiscovery administrator to this group.
- c. Create a group for eDiscovery users, for example, EDISCOVERYUSERS. The group name must be 32 characters or fewer.
6.  Create a user ID for starting the eDiscovery Manager application server:
  - a. Create an AIX non-root user ID. The eDiscovery Manager installation program will prompt you for this user ID on the Owner and Group pane.
  - b. Create an AIX group and add the new AIX non-root user ID to it. The eDiscovery Manager installation program will prompt you for this group on the Owner and Group pane.  
 The `.profile` file for this user ID must exist in the `$HOME/AIX_non_root_user_ID` subdirectory.
  - c. If the locale of the user ID is set to a multi-byte language, such as Japanese or Chinese, it is important that the locale supports Unicode (UTF-8). Otherwise, you might encounter problems while exporting email to Lotus Domino. For example, to enable Unicode support for Japanese, set `export LANG=jp_JP.UTF-8` in the `.profile` file for the user ID.
7. **Lotus Domino and Lotus Notes environments only.** Complete the following steps:
  - a. Create a Lotus Domino group called EDISC\_USERS on the remote Lotus Domino server.  
 Locate the Name and Address book on the remote Lotus Domino server and follow the instructions in the Lotus Domino documentation for creating a group.
  - b. Create a Lotus Notes user ID for eDiscovery Manager on the remote Lotus Domino server and add the new Lotus Notes user ID to the EDISC\_USERS Lotus Domino group on that server.  
 An ID file is generated for the new user ID. eDiscovery Manager uses this ID file to connect to the remote Lotus Domino server, create databases, and export Lotus Domino email.
8. Configure the connection between eDiscovery Manager and FileNet P8. See “Configuring the IIOP connection between the eDiscovery Manager system and the FileNet P8 server using single sign-on” on page 48 for details.
9. If the object store is configured to use date partitioning during content-based retrieval, temporarily disable date partitioning by using FileNet Enterprise Manager. You can re-enable this feature after installing eDiscovery Manager.

If date partitioning is enabled on the FileNet P8 server that eDiscovery Manager connects to, the eDiscovery Manager installation will fail with a data model creation error (such as DGL5050A). The eDiscovery Manager installation program creates object classes and relies on those object classes being created immediately. Thus, the date partitioning feature of FileNet P8 must be disabled.

**Related information:**

 [Creating a file plan](#)

## Configuring the IIOP connection between the eDiscovery Manager system and the FileNet P8 server using single sign-on

Before installing IBM eDiscovery Manager and its prerequisites, configure the IIOP connection between the eDiscovery Manager system and the IBM FileNet P8 server.

### About this task

If you plan to use the WSI transport method to connect eDiscovery Manager to FileNet P8, you do not need to configure the IIOP connection between these systems. See “Configuring eDiscovery Manager to connect to FileNet P8 by using the Web Services Interface (WSI) transport method” on page 127 for complete information. You can also use the Enterprise JavaBeans (EJB) protocol. See “Connection methods: EJB protocol, IIOP protocol, and the WSI transport method” on page 50.

These instructions are written for IBM WebSphere Application Server Version 8.0.

To configure the IIOP connection between the eDiscovery Manager system and the FileNet P8 server using single sign-on:

### Procedure

1. Start the WebSphere Application Server administrative console on the system where you will install eDiscovery Manager.
2. Click **Security > Global Security**.
3. Enable administration and application security:
  - a. Select the **Enable administrative security** option.
  - b. Clear the **Use Java 2 security to restrict application access to local resources** option.
  - c. Click the **Administrative user roles** link and add an administrative user. For more information, click the **More information about this page** link in the Help box on the right panel.
4. Enable single sign-on.
  - a. On the Global security panel, in the Application security area, select the **Enable application security** option.
  - b. Click **Web and SIP security**.
  - c. Click **Single sign-on (SSO)**.
  - d. Select **Enabled**.
  - e. Click **OK** to save your changes.
5. Configure the LDAP server:



- a. From the Global security panel, select from the **Available realm definitions** list the type of LDAP configuration your content management system uses: **Standalone LDAP registry** or **Federated repositories**.
  - b. Click **Set as current**.
  - c. Click **Configure** to configure settings for the standalone LDAP registry or the federated LDAP repositories.
  - d. From the Global security panel, click **OK** to save your changes.
6. Export the LTPA key for cross-cell single sign-on (SSO) from the FileNet P8 server and import it to the eDiscovery Manager application server:
  - a. Start the WebSphere Application Server administrative console on the FileNet P8 server.
  - b. Click **Security > Global security**.
  - c. Under Authentication, **Authentication mechanisms and expiration**, click LTPA.
  - d. Under Cross-cell single sign-on, enter the password that is used to encrypt the LTPA keys.
  - e. Enter a fully-qualified path and file name for the location where you want the exported LTPA keys to reside, for example: C:\LTPA\LTPA\_key\_name.
  - f. Click **Export keys**.
  - g. If you generated a new LTPA key, import the key file to the FileNet P8 server.
  - h. Import the key file to the eDiscovery Manager application server:
    - 1) Copy the key file from the FileNet P8 server to the eDiscovery Manager application server.
    - 2) If it is not already running, start the WebSphere Application Server administrative console on the eDiscovery Manager application server.
    - 3) Click **Security > Global security**.
    - 4) Under Authentication, **Authentication mechanisms and expiration**, click LTPA.
    - 5) Under Cross-cell single sign-on, enter the password that is used to encrypt the LTPA keys.  
This is the same password that you entered on the FileNet P8 server before exporting the key file.
    - 6) Enter the fully-qualified path and file name for the location of the key file that you copied to the eDiscovery Manager application server, for example: C:\LTPA\LTPA\_key\_name.
    - 7) Click **Import keys**.
    - 8) Click **Apply** and then click **Save directly to the master configuration**.
7. Set up the Java Authentication and Authorization Service (JAAS):
  - a. From the WebSphere Application Server administrative console on the eDiscovery Manager application server, click **Security > Global security**.
  - b. Under Authentication, **Authentication mechanisms and expiration**, click **Java Authentication and Authorization Service > Application logins**.
  - c. Click **New**.
  - d. In the **Alias** field, enter FileNetP8Engine.
  - e. Under **JAAS login modules**, click **New** and enter com.ibm.ws.security.common.auth.module.WSLoginModuleImpl in the **Module class name** field.
  - f. Select the **Use login module proxy** option.

- g. Choose **REQUIRED** from the **Authentication strategy** list.
  - h. Click **OK** and then **Save** to save your settings.
8. Set up RMI/IIOP connection security.
- a. From the WebSphere Application Server administrative console on the eDiscovery Manager application server, click **Security > Global security**.
  - b. Under Authentication, **Authentication mechanisms and expiration**, click **RMI/IIOP security**.
  - c. Click the **CSIV2 inbound communications** link, select **Never** for **CSIV2 Transport Layer** and **Client certificate authentication**, and select **TCP/IP** for **Transport** and **Centrally managed** for **SSL settings**.
  - d. Click the **CSIV2 outbound communications** link, select **Never** for **CSIV2 Transport Layer** and **Client certificate authentication**, and select **TCP/IP** for **Transport** and **Centrally managed** for **SSL settings**.
  - e. Save your settings.
9. Configure single sign-on (SSO) support by enabling SSO code in the `web.xml` file for eDiscovery Manager.

## What to do next

After installing, verify that the JVM `java.security.auth.login.config` is set as follows:





```
-Djava.security.auth.login.config=<edmhome>/config/jaas.conf.WebSphere
```

### Related tasks:

“Configuring single sign-on support” on page 131

Single sign-on (SSO) support enables users to log in only once and access both IBM eDiscovery Manager and the content servers. To enable SSO, you must first enable SSO code in the `web.xml` file for eDiscovery Manager.

### Related information:

-  Enabling security in WebSphere Application Server
-  Exporting Lightweight Third Party Authentication keys
-  Configuring stand-alone Lightweight Directory Access Protocol (LDAP)
-  Configuring Lightweight Directory Access Protocol (LDAP) for federated repositories

## Connection methods: EJB protocol, IIOP protocol, and the WSI transport method

When you install eDiscovery Manager, you provide the FileNet P8 Content Engine web address, which eDiscovery Manager uses to connect to the primary Content Engine content server. This connection can use either the Enterprise JavaBeans (EJB) protocol and Internet Inter-ORB Protocol (IIOP) or the Web Services Interface (WSI) transport method.

Table 1 shows the connection types (web addresses) that must be used with specific server environments.



*Table 8. eDiscovery Manager connection types for different server environments.*

Server environment	Connection type
Multiple FileNet P8 content servers in different domains.	<p>A web address that uses the WSI transport method.</p> <p>eDiscovery Manager does not support the use of EJB and IIOP to connect to multiple content servers that are hosted in different domains.</p>
Multiple FileNet P8 content servers in the same domain.	<p>A web address that uses the EJB/IIOP protocol or the WSI transport method.</p> <p>When you add connection information for secondary content servers on the Content Management System pane of the Administration page, specify web addresses that use the same connection type as the primary content server. Do not use the EJB/IIOP protocol for some content servers and the WSI transport method for other content servers.</p>

**Remember:** You can use single sign-on (SSO) in FileNet P8 environments only if you use EJB/IIOP to connect the eDiscovery Manager server to your FileNet P8 servers. You cannot use SSO if you use the WSI transport method to connect eDiscovery Manager to FileNet P8 servers. In environments with both eDiscovery Manager and eDiscovery Analyzer, only WSI connections are supported, so you cannot use SSO in these environments.

## Installation checklist (FileNet P8)

### About this task

Use the following checklist to gather the information that you will need to provide during installation. When you are prompted for information about your content management system, provide information for only one of the content servers in your environment. You can configure other content servers later.

*Table 9. Information checklist for an IBM eDiscovery Manager installation*

Information	Default or example value	Notes	Record your value here
Installation path for eDiscovery Manager	<p>On AIX: /opt/IBM/edm</p> <p>On Windows: C:\Program Files\ IBM\edm</p>	<p>If the installation path contains non-ASCII characters, you must express the path in escaped Unicode. Use a tool such as the one that can be found in the Java JDK, such as native2ascii.</p> <p>On AIX, the installation path cannot contain a space character.</p>	

Table 9. Information checklist for an IBM eDiscovery Manager installation (continued)

Information	Default or example value	Notes	Record your value here
Path of the WebSphere Application Server instance to which to deploy eDiscovery Manager	On AIX: /opt/IBM/WebSphere/AppServer  On Windows: C:\Program Files\IBM\WebSphere\AppServer		
WebSphere Application Server profile to dedicate to eDiscovery Manager	eDM		
WebSphere Application Server instance to dedicate to eDiscovery Manager	server1	WebSphere Application Server Base environments, use the server1 instance to simplify the administration and monitoring of eDiscovery Manager from the WebSphere administration console.	
Whether WebSphere Application Server security is enabled	Yes		
WebSphere Application Server administrative user name		This information is relevant only if administrative security is enabled.	
WebSphere Application Server administrative password		This information is relevant only if administrative security is enabled.	
IBM FileNet P8 domain name	p8domain		
IBM FileNet P8 object store name	FNCEOS		
IBM FileNet P8 Content Engine or Content Platform Engine URL	Example using the Hypertext Transfer Protocol (HTTP): http://server_IP:port/wsi/FNCEWS40MTOM/  Example using the Internet Inter-ORB Protocol (IIOP): iiop://server_IP:port/FileNet/Engine		

Table 9. Information checklist for an IBM eDiscovery Manager installation (continued)

Information	Default or example value	Notes	Record your value here
IBM FileNet P8 version number	<ul style="list-style-type: none"> <li>Version 4.5.1</li> <li>Version 5.0 or newer</li> </ul>	Oldest version of Content Engine or Content Platform Engine that will be used by eDiscovery Manager	
User name of an IBM FileNet P8 administrator		This user must also have the Modify Permissions access right, which allows the user to modify the ACL of the object store.	
Password of the IBM FileNet P8 administrator			
User name of the IBM FileNet P8 account that will serve as the eDiscovery administrator			
Password of the IBM FileNet P8 account that will serve as the eDiscovery administrator			


## Installing WebSphere Application Server

Before you can install IBM eDiscovery Manager, you must install IBM WebSphere Application Server on the same system.

### About this task

You can install eDiscovery Manager to the following types of nodes:

- A WebSphere Application Server Network Deployment managed or unmanaged node
- A WebSphere Application Server Base managed or unmanaged node

**Remember:**  Set the **umask** value to 022 before you install WebSphere Application Server. See Preparing AIX systems for installation for more information about verifying and setting the umask value.

To install WebSphere Application Server in preparation for eDiscovery Manager:

### Procedure

1. Install the prerequisite software for WebSphere Application Server.  
You can find a complete list of the WebSphere Application Server hardware and software requirements on the IBM Software Support site at <http://www.ibm.com/support/docview.wss?uid=swg27006921>.
2. Prepare the operating system for WebSphere Application Server.

To find more information about preparing the operating system, see Preparing the operating system for product installation.

3. Install the appropriate version of WebSphere Application Server.

For more information about installing WebSphere Application Server, see Installing WebSphere Application Server.

4. Create a new server profile for eDiscovery Manager.

In WebSphere Application Server Base environments, when you create a server profile, WebSphere Application Server creates a default application server instance named server1. In WebSphere Application Server Network Deployment environments, an application server must be created before installation. Other alternatives in both environments include creating a new application server instance for eDiscovery Manager in an existing profile or installing eDiscovery Manager to an unused application server instance of an existing profile.

**Recommendation:** In WebSphere Application Server Base environments, use the server1 instance to simplify the administration and monitoring of eDiscovery Manager. (The only application server instance that can be monitored by the WebSphere administration console is server1. If you use a server instance other than server1 for eDiscovery Manager, you will not be able to start, stop, or monitor the status of eDiscovery Manager from within the WebSphere administration console because of this limitation.) You can find more information in Creating an application server profile.

**Requirement:** When you create a server profile, WebSphere Application Server places several applications in the server instance that is associated with the new profile. You can ignore these applications. Do not install other, non-WebSphere applications in the server instance that is associated with the eDiscovery Manager profile. For example, do not install IBM FileNet P8, the IBM Content Manager resource manager, or IBM Web Interface for Content Management in the eDiscovery Manager profile.

5. Verify that the WebSphere Application Server is prepared for the eDiscovery Manager installation.
  - If you are deploying eDiscovery Manager to an unmanaged node, start the server instance of the WebSphere Application Server to which you plan to install eDiscovery Manager.
  - If you are deploying eDiscovery Manager to a managed node:
    - a. Start the deployment manager.
    - b. Start the node agent.
    - c. Start the server instance for that node to which you plan to install eDiscovery Manager.
6. Be sure to configure WebSphere Application Server as described in one of the following two information center topics, depending on which version of WebSphere Application Server you have installed:
  - WebSphere Application Server Version 7: See Configuring connection validation timeout
  - WebSphere Application Server Version 8: See Configuring connection validation timeout

If you do not configure WebSphere Application Server as described, your users can receive the following error when they attempt a task after the Content Engine database is stopped and restarted:

```
com.filenet.api.exception.EngineRuntimeException:  
DB_ERROR: An error occurred accessing the database.
```

#### **Related information:**



System requirements for IBM eDiscovery Manager Version 2.2.2

This document describes the hardware and software prerequisites for eDiscovery Manager.

### **Installing to a new WebSphere application server or a new WAS profile**

You can perform an upgrade installation on the same 64-bit machine that a previous version of eDiscovery Manager was installed but to a different WAS home (64-bit WAS).

#### **Before you begin**

Before you install eDiscovery Manager, make sure that your preferred WebSphere Application Server meets the prerequisites and is installed.

#### **About this task**

You can choose a WAS home and/or WAS profile that is different from prior installations of eDiscovery Manager. However, if you choose to install to a different WAS home and/or WAS profile from the previous eDiscovery Manager installation, then you must perform these steps.

#### **Procedure**

1. Install eDiscovery Manager and select your preferred WebSphere Application Server home and profile during the installation process.
2. If you installed eDiscovery Manager to a different WebSphere Application server or profile from your previous eDiscovery Manager installation, complete the following steps:
  - a. Delete the old WebSphere Application Server profile that was dedicated to eDiscovery Manager. To delete the old WebSphere Application Server profile that was dedicated to eDiscovery Manager, follow instructions in WebSphere Application Server documentation.
  - b. If you do not want to delete the old profile, manually remove the eDiscovery Manager applications by using the WebSphere Administrative console. To manually remove the eDiscovery Manager applications, open the WebSphere Administrative console, go to Applications > Application Types > WebSphere Enterprise Applications, select EDMClient and EDMWorkMgrServer, then click **Uninstall**.

### **Installing the Lotus Domino server**

To enable your users to export Lotus Notes content or to view content by using Lotus Notes, you must install the Lotus Domino server on the IBM eDiscovery Manager system. eDiscovery Manager requires only the Lotus Domino APIs, but these APIs are bundled with the Lotus Domino server; the APIs are not bundled separately. For this reason, you must install a Lotus Domino server on the eDiscovery Manager system or logical partition (LPAR), even though you do not start the server itself.

## About this task

In addition to the Lotus Domino server installed on the eDiscovery Manager system or LPAR, a remote Lotus Domino server must be installed on another system. The Lotus Domino server must then be configured to access this remote Lotus Domino server. The purpose of this remote Lotus Domino server is for viewing and exporting Lotus Notes content from your eDiscovery Manager system.

**Important:** On Windows, eDiscovery Manager requires a dedicated installation of the Lotus Domino V8.5 server, even though you do not start the Lotus Domino server. The following table shows the versions of the Lotus Domino server that might be installed on the eDiscovery Manager system. The remote Lotus Domino server can be any version 8 or above, and on any platform, for example, Windows or AIX.

Table 10. Versions of Lotus Domino that are supported on the local Lotus Domino server.


Server	eDiscovery Manager system on AIX	eDiscovery Manager system on Windows
Local Lotus Domino server (on eDiscovery Manager system)	Version 8 (64 bit) Version 8.5 (64-bit)	Version 8 (64 bit) Version 8.5 (64-bit)


To install a Lotus Domino server on the eDiscovery Manager system:

### Procedure

1. Install the Lotus Domino server on the eDiscovery Manager system. If you are installing Lotus Domino Version 8, you can find more information in the Guidepost for deploying Domino topic.

You do not need to configure this local Lotus Domino server if you are installing it only for the purpose of obtaining the Lotus Domino APIs, as recommended.

2.  Verify that the Lotus Domino installation directory was added to the PATH system environment variable, for example, C:\Program Files\IBM\Lotus\Domino.

3.  Log out and log back in to the eDiscovery Manager system as the root user to check the I/O completion port (IOCP):

- a. Enter the following command to ensure that the IOCP module is installed on the eDiscovery Manager system:

```
$lslpp -l bos.iocp.rte
```

The output from the **lslpp** command should be similar to the following example:

```
Fileset      Level    State    Description
-----
Path: /usr/lib/objrepos  5.2.0.10 COMMITTED I/O Completion Ports API
bos.iocp.rte
Path: /etc/objrepos    5.2.0.10 COMMITTED I/O Completion Ports API
bos.iocp.rte
```

- b. If the IOCP module (bos.iocp.rte) is not installed, install it from the AIX product CD, then enter the **lslpp -l bos.iocp.rte** command again to confirm that it is installed.

- c. Enter the following command to ensure that the status of the IOCP port is **Available**:

```
$ lsdev -Cc iocp
```

The output from the **lsdev** command should be similar to the following example:

```
iocp0 Available I/O Completion Ports
```

- d. If the IOCP port status is **Defined**, change the status to **Available**:


1) Enter the following command:

```
# smit iocp
```

2) Select **Change / Show Characteristics of I/O Completion Ports** and change **STATE to be configured at system restart** from **Defined** to **Available**.

3) Reboot the eDiscovery Manager system and log in as the root user.

4) Enter the **lsdev -Cc iocp** command again to confirm that the status of the IOCP port changed to **Available**.

4.  Set up the environment for the AIX non-root user ID that starts the eDiscovery Manager application server. You created this user ID as a prerequisite.

a. Log out of the eDiscovery Manager system and log back in by using the user ID that starts the eDiscovery Manager application server.

b. In the \$HOME directory, create a notesdata subdirectory.

c. Copy the Lotus Notes user ID file for the user ID that starts the eDiscovery Manager application server from the remote Lotus Domino server to the \$HOME/notesdata subdirectory on the eDiscovery Manager system.

You created this user ID as a prerequisite. eDiscovery Manager uses this ID file to connect to the remote Lotus Domino server, create databases, and export Lotus Notes content.

d. Create a notes.ini file in the \$HOME/notesdata subdirectory that contains the following lines, as well as a blank line at the end of the file:

```
[Notes]
Directory=$HOME/notesdata
KeyFileName=Lotus_Notes_user_ID_for_eDM_appServer_starter.id
Ports=TCPIP
TCPIP=TCP,0,15,0
```

**Important:** If the Lotus Domino installation directory already contains a notes.ini file, then the notesConnect utility will always use it. This is true even if the notes.ini file that you created when installing the Lotus Domino server is first in the system path. For this reason, it is necessary to rename the notes.ini file in the Lotus Domino installation directory, if one exists.

e. Edit the .profile file for the user ID that starts the eDiscovery Manager application server.

Remember that the .profile file for this user ID exists in the \$HOME/AIX\_non\_root\_user\_ID subdirectory.

Add the following lines to the .profile file:

```
# LIBPATH: Add the path to the ibmpow directory in the Lotus Domino
# installation directory:
LIBPATH=$LIBPATH:/opt/ibm/lotus64/lotus/notes/latest/ibmpow
```

```
# PATH: Add the paths to the notesdata directory,
# ibmpow and bin directories in the Lotus Domino installation directory,
# and resource subdirectory of the Lotus Domino installation directory.
# For example, in English locales, the path of the resource subdirectory is
# /opt/ibm/lotus/notes/latest/ibmpow/res/C
PATH=$PATH:$HOME/notesdata:/opt/ibm/lotus/notes/latest/ibmpow:
/opt/ibm/lotus/bin:/opt/ibm/lotus/notes/latest/ibmpow/res/C
```



```
Notes_ExecDirectory=/opt/ibm/lotus/notes/latest/ibmpow
```

```
LOTUS=/opt/ibm/lotus
```


```
NOTES_DATA_DIR=$HOME/notesdata
```

```
export LIBPATH PATH Notes_ExecDirectory LOTUS NOTES_DATA_DIR
```

- f. Copy the names.nsf file from the data directory (\$HOME/notesdata) of the Lotus Domino server (typically a remote server) to the \$HOME/notesdata directory on the eDiscovery Manager system.

- g. Log out of the eDiscovery Manager system and log back in by using the user ID that starts the eDiscovery Manager application server.

The changes that you made to the .profile file for this user ID are now in effect. You can run the **env** command to verify the changes.

5.  Set up the environment for the user ID that starts the eDiscovery Manager application server.

- a. Create a notesdata directory in a convenient location of your choice, for example \your\_dir\notesdata.

- b. Copy into the notesdata directory the names.nsf file from the Lotus Domino server that your eDiscovery Manager server will connect to for viewing and exporting Lotus Notes content, typically a remote Lotus Domino server.

- c. Create a new user ID on the Lotus Domino server, for example, eDMNotesUser. Make sure that this user has read and write access to the eDMMail.nsf database, which is used for viewing Lotus Notes content. This database is created at the Lotus Domino Settings pane of the Administration page in the eDiscovery Manager web client. Also make sure that this user has the ability to create new databases on the Lotus Domino server.


- d. An ID file is created for this new user ID. Copy this ID file (for example, eDMNotesUser.id) into the \your\_dir\notesdata directory that you just created.

- e. In the \your\_dir\notesdata directory create a new file called notes.ini with the following contents:

```
[Notes]
Directory=\your_dir\notesdata
KeyFileName=Notes_user_ID_for_eDM.id
Ports=TCPIP
TCPIP=TCP,0,15,0
```

Substitute \your\_dir with the absolute path to your notesdata directory and Notes\_user\_ID\_for\_eDM.id with the new Lotus Notes user ID you created (for example, eDMNotesUser.id).

- f. Edit the system Path environment variable so that the \your\_dir\notesdata directory is the first directory listed and that the notes.ini file is picked from this location.

6.  Rename the notes.ini file in the Lotus Domino installation directory, if it exists.

7. Verify that the environment for the ID that starts the eDiscovery Manager application server is working by running the eDiscovery Manager notesConnect utility. Remember that on AIX systems this ID is a non-root user.

The notesConnect utility connects to the remote Lotus Domino server and returns the title from the names database. Run the notesConnect utility on a single line from the bin subdirectory of the eDiscovery Manager installation directory. For example:



## AIX

```
/opt/IBM/eDM/bin/notesConnect names.nsf [remote_Lotus_Domino_server]
```

## Windows

```
C:\Program Files\IBM\eDM\bin\notesConnect names.nsf  
[remote_Lotus_Domino_server]
```

where *remote\_Lotus\_Domino\_server* is the IP address or IP name of the remote Lotus Domino server.

The notesConnect utility uses the Lotus Notes user ID that is configured for the KeyFileName setting in the \$HOME/notesdata/notes.ini file if on AIX or in the \your\_dir\notesdata\notes.ini file if on Windows.

If the environment is configured properly, the title of the names database is returned. You might be prompted for a password.

### Related tasks:

“Configuring Lotus Notes viewing” on page 115

If you have content in a collection that originally came from Lotus Domino before it was archived and you want your users to be able to open this content with Lotus Notes, you must configure Lotus Notes viewing. IBM eDiscovery Manager creates a viewing database and assigns read access to eDiscovery Manager users, but you must configure other aspects of the viewing environment.

“Configuring Lotus Notes export” on page 121

If you want your users to be able to export Lotus Notes content, you must configure Lotus Notes export. IBM eDiscovery Manager creates export databases and assigns read access to those eDiscovery Manager users that are assigned permission to export, but you must configure other aspects of the export environment.

## Reinstalling or upgrading the Lotus Domino server on the eDiscovery Manager system

After IBM eDiscovery Manager is installed, if you reinstall or upgrade the Lotus Domino server on the eDiscovery Manager system or logical partition (LPAR), be sure that the Notes.jar file is in the IBM WebSphere Application Server shared library class path.

### Procedure

To ensure that the Notes.jar file is in the WebSphere Application Server shared library class path:

1. Open the WebSphere Application Server administrative console by clicking **Start > Programs > IBM WebSphere > Application Server > Profiles > eDiscovery Manager application server profile > Administrative console**.
2. Expand **Environment, Shared Libraries**, and **EDMLibraries**.
3. Confirm that the **Classpath** field contains an entry for the fully qualified path to the Notes.jar file, for example, on a Windows system:  
C:\Program Files\Lotus\Domino\jvm\lib\ext\Notes.jar.
4. If there is no entry for the Notes.jar file, add one. Then stop and restart the eDiscovery Manager application server for your change to take effect.

### Related information:

 WebSphere Application Server Version 7.0 - Starting and stopping quick reference

 WebSphere Application Server Version 8.0 - Starting and stopping quick reference

## Installing or upgrading eDiscovery Manager in a FileNet P8 environment

After you install and configure the prerequisite software, you can install IBM eDiscovery Manager as an IBM WebSphere Application Server instance and connect it to your IBM FileNet P8 system. Note that the process for upgrading eDiscovery Manager is identical to the process for installing eDiscovery Manager.



### Before you begin

**Prerequisite:** The FileNet P8 server must be started before you can install eDiscovery Manager.

### About this task

To install or upgrade eDiscovery Manager:

### Procedure

1. Log on to the system by using an appropriate account.
  -  **AIX** When installing eDiscovery Manager, you must be logged on to the system as the root user.
  -  **Windows** When installing eDiscovery Manager, you must be logged on to the system as a member of the administrators group.
2. If you are upgrading or reinstalling eDiscovery Manager, stop the eDiscovery Manager application server.

See the WebSphere Application Server product information for details about stopping and starting an application server.

3. Start the installation program.
  - a. At a command prompt, change to the eDiscovery Manager CD or to the directory where you downloaded the product.
  - b. Start the installation program by entering the appropriate command for your operating system.

**AIX**     `edm.bin`

**Windows**  
          `edm.exe`

For performance reasons, consider changing the logging level of the `edmInstallConfig#.log` file to INFO when you install eDiscovery Manager.

The default logging level of this file is FINE. To change the logging level, use the **-DLogLevel** parameter. For example, on a Microsoft Windows system, enter the following command to install eDiscovery Manager and change the logging level to be less verbose:

```
edm.exe -DLogLevel=INFO
```

Other optional parameters that you can use when installing eDiscovery Manager are:

**-DLogFileSize**

The default log file size is 10 MB.

**-DNumLogFiles**

The default number of log files is 10.

To change the logging level to be less verbose, to change the log file size to 30 MB, and to change the number of log files to 15, enter the following command to install eDiscovery Manager:

```
edm.exe -DLogLevel=INFO -DLogFileSize=30 -DNumLogFiles=15
```

4. Select your language and click **OK**.
5. Read and accept the software license terms.
6. Follow the on-screen prompts to complete the installation.

#### Important tips:

- If you decide to install eDiscovery Manager in a directory other than the default directory, ensure that:
    - The path to the eDiscovery Manager installation directory contains only characters that are defined in the active code page.
    - The path to the eDiscovery Manager installation directory does not contain any space characters.
  - Install eDiscovery Manager on a different object store than the one on which IBM Enterprise Records is installed.
  - During the application server deployment phase, the installation program deploys the eDiscovery Manager web client and eDiscovery Manager work manager, and configures the application server instance to which they are deployed. This can take up to 20 minutes. Be patient and let the installation program complete on its own.
7. If eDiscovery Manager is installed on the same system as FileNet P8, set the JVM custom property for the Object Request Broker (ORB), `com.ibm.websphere.orb.uniqueServerName`, to `True`.
    - a. In the WebSphere Application Server administrative console, click **Servers > Application Servers > server\_name > Java and Process Management > Process Definition > Java Virtual Machine > Custom Properties > New**.
    - b. On the Custom Properties settings page, define the custom property by entering `com.ibm.websphere.orb.uniqueServerName` for the name and `TRUE` for the value.
    - c. Click **OK**, then click **Save** on the console task bar.

## Results

**Errors:** If an error occurs during the silent installation process, the error will be printed in the eDiscovery Manager debug log file `edmInstall*.log` files. The log files can be found in the *user.home* during the installation. After installation, they can be found in *edmhome\logs*.

## What to do next

### What to do next

If you upgraded eDiscovery Manager:

1. If the object store was enabled with date partitioning during content-based retrieval, re-enable the date partitioning by using FileNet Enterprise Manager.
2. Start the eDiscovery Manager web client and confirm that the configuration settings on the Administration pages are correct.

In particular, ensure that all paths are correct, including the absolute path of the export directory on the Export Settings pane and other settings in the Content Management Systems and Lotus Domino Settings panes.

3. Instruct all eDiscovery Manager web client users to close their browsers and then reopen them.

Users might also want to clear their browser cache and delete temporary files. Doing so removes any cached JavaScript. Users that do not close and reopen their browsers after the upgrade might be unable to log in to the eDiscovery Manager web client.

4. After upgrading, you must configure your object class security.

**Related tasks:**

“Configuring object class security” on page 108

Work with your IBM FileNet P8 administrator to use IBM FileNet Enterprise Manager to configure security for the object classes that will belong to eDiscovery collections.

“Installation checklist (FileNet P8)” on page 51

**Related information:**

 WebSphere Application Server Version 7.0 - Starting and stopping quick reference

 WebSphere Application Server Version 8.0 - Starting and stopping quick reference

## Installation debug log files

To aid in troubleshooting, IBM eDiscovery Manager maintains installation debug log files.

**During the installation:** During the installation, the eDiscovery Manager installation program writes installation progress messages, error messages, and IBM WebSphere Application Server deployment information to installation debug log files. If the installation debug log file reaches 5 MB in size, eDiscovery Manager rolls it over and creates another log file. eDiscovery Manager creates up to four installation log files (eDMInstallDebug00.log, eDMInstallDebug01.log, eDMInstallDebug02.log, and eDMInstallConfig3.log) before it begins overwriting the first log file.

**Before the installation completes:** Before the installation completes, the installation debug log files and the configuration debug log files exist in your home directory. On an AIX system, the home directory is defined by the HOME environment variable. On a Microsoft Windows system, the home directory is defined by the HOMEPATH environment variable. For example, on Microsoft Windows, your home directory might be C:\Users\yourUserName.

**After the installation completes:** After the installation completes, the installation debug log files and the configuration debug log files are copied to the logs subdirectory of the eDiscovery Manager installation directory. Also after installation, a single installation debug log file named eDMInstall.log is created in the same logs subdirectory.

## Database tuning to improve performance (FileNet P8)

To improve the performance of IBM eDiscovery Manager in IBM FileNet P8 environments, see instructions at: <http://www.ibm.com/support/docview.wss?uid=swg21610757>

**Related information:**

 IBM FileNet P8 Platform Performance Tuning Guide

Download the PDF from the FileNet P8 Platform Technical Notices table in this

---

## Validating the eDiscovery Manager installation

Before the IBM eDiscovery Manager installation completes, it attempts to start the eDiscovery Manager application server. You can validate the installation of eDiscovery Manager by starting the eDiscovery Manager web client, which connects to the eDiscovery Manager application server.

### About this task

To validate the eDiscovery Manager installation:

### Procedure

1. Start the eDiscovery Manager web client.

The syntax of the eDiscovery Manager web client URL is:

`http://server:port/EDMClient/`

where:

**server** Is the IP address or host name of IBM WebSphere Application Server.

**port** Is the port for the eDiscovery Manager application server.

To determine the port:

- a. Open the WebSphere Application Server administrative console by clicking **Start > Programs > IBM WebSphere > Application Server > Profiles > eDiscovery Manager application server profile > Administrative console**.
- b. Expand **Servers, Application servers, eDiscovery Manager application server profile**, and **Ports**.
- c. Find the WC default host row and check the value in the Port column.

#### EDMClient

Is case sensitive. Enter this portion of the eDiscovery Manager web client URL exactly as shown.

#### Examples:

`http://9.40.114.128:9080/EDMClient/`

`http://abc.example.com:9080/EDMClient/`

2. If the eDiscovery Manager web client does not start, verify that the eDiscovery Manager application server is running. If it is not already running, start it by following the instructions in "Starting and stopping the eDiscovery Manager server" on page 68. Then try starting the eDiscovery Manager web client again.

### What to do next

After validating the installation, configure eDiscovery Manager. Be sure to use the configuration checklists to prepare yourself for those configuration tasks that require the eDiscovery Manager web client.

**Related concepts:**

“Configuration checklists” on page 70

To configure IBM eDiscovery Manager, you need information about the products that eDiscovery Manager integrates with. Work with the administrators of these products to collect this information ahead of time and to make the configuration of eDiscovery Manager quick and efficient.

**Related tasks:**

Chapter 3, “Configuring eDiscovery Manager,” on page 69

Configuring IBM eDiscovery Manager consists of some tasks that you complete by using the eDiscovery Manager web client and some tasks that you complete outside of the web client. This section provides checklists to prepare you for the web client configuration tasks, which are described in the online help system. This section also provides detailed instructions for the configuration tasks that you complete outside of the web client.

---


## Silent installation

A silent installation can save you time and ensure consistency across systems. Perform silent installations if you want to install the same components on multiple systems or you want to clone a system.

During the normal (non-silent) installation process, a recording is made of the options that you selected in the graphical user interface of the installation program. The recording is contained in a simple text file, which is called a response file. You can use that response file in subsequent silent installations to quickly and easily re-create the same environment on multiple systems. Simply pass the response file to the installation program and wait for the installation to complete.

**Important:** Always perform an interactive (non-silent) installation of IBM eDiscovery Manager and use the response file that is generated by this installation for subsequent silent installations. Never use a response file from an older version of eDiscovery Manager when upgrading to a newer version. The parameters in the response file can change from version to version, so an older response file might not be appropriate for a newer installation program.

**Related information:**

 System requirements for IBM eDiscovery Manager Version 2.2.2  
This document describes the hardware and software prerequisites for eDiscovery Manager.

## Creating a response file

Each time that you run the eDiscovery Manager installation program, the information that you provide and the selections that you make are automatically saved in a response file. After editing the recorded values as needed, you can use this response file for subsequent silent installations.

### About this task

Always use a current response file when you install a new version or release of eDiscovery Manager. Do not use an old response file that was created for a previous version of eDiscovery Manager. Older response files might not contain the correct parameters needed for installing the current release.

### Procedure

To create a response file:

1. Follow the appropriate instructions for installing or upgrading eDiscovery Manager.

- **FileNet P8** “Installing or upgrading eDiscovery Manager in a FileNet P8 environment” on page 60
- **Content Mgr** “Installing or upgrading eDiscovery Manager in a Content Manager EE environment” on page 40

The eDiscovery Manager installer generates a response file automatically. The file named `installer.properties` is located in the `\logs` subdirectory of the eDiscovery Manager installation directory.

2. Edit the recorded values:
  - a. Open the response file with a text editor.
  - b. Modify the values of the parameters as needed. For example, passwords are not saved in the response file automatically. You must add them to the response file before you run the silent installation.  
Parameter descriptions and instructions are contained in the response file itself.

**Note:** When you define directories in the response file, specify any non-English characters in escape Unicode. For example:

Operating system	Example
AIX	USER_INSTALL_DIR=/opt/IBM/eDM/\u304B\u308F\u3048\u30AE\u30AC\u91D1\u66DC\u65E5
Windows	USER_INSTALL_DIR=C:\\Program Files\\IBM\\eDM\\u304B\u308F\u3048\u30AC\u91D1\u66DC\u65E5

- c. Save and close the response file.

## Running a silent installation

The `-f` flag tells the installation program to run in silent mode. No installation windows are displayed. The installation program progresses in the same manner as if you entered the response file values in the graphical user interface of the installation program.

### About this task

To run a silent installation:

### Procedure

- 1.

**Note:** For Content Manager EE only:

**Content Mgr** Modify the value of the `JavaPool` parameter in the `cmbpool.ini` file to be an empty string. (Do not comment out the `JavaPool` parameter; simply set its value to an empty string.)

`JavaPool=`

The `cmbpool.ini` file is used for IBM WebSphere Application Server connection pooling. The default location for the `cmbpool.ini` file is in `IBMCROOT\cmgmt\connectors\` on Microsoft Windows systems and in `/home/ibmcmadm/cmgmt/`



connectors/ on AIX systems. For example: C:\Program Files\IBM\db2cmv8\cmgmt\connectors on a Microsoft Windows system.

2. Stop and restart the IBM eDiscovery Manager application server.  
See the WebSphere Application Server product information for details about stopping and starting an application server.
3. Run the eDiscovery Manager installation program by entering one of the following commands at a command prompt:

Operating system	Command
AIX	edm.bin -f installer.properties
Windows	edm.exe -f installer.properties

**During the installation:** During the installation, the eDiscovery Manager installation program writes installation progress messages, error messages, and WebSphere Application Server deployment information to installation debug log files. When the installation completes, a message such as the following one is written to the end of the installation log file. The installation was successful if the exit code is 0 (zero).

```
Mon Dec 15 15:12:55.453 PST 2008 : STDERR : Exiting with exit code: 0
```

If the installation debug log file reaches 5 MB in size, eDiscovery Manager rolls it over and creates another log file. eDiscovery Manager creates up to four installation log files (eDMInstallDebug00.log, eDMInstallDebug01.log, eDMInstallDebug02.log, and eDMInstallConfig3.log) before it begins overwriting the first log file.

**Before the installation completes:** Before the installation completes, the installation debug log files and the configuration debug log files exist in your home directory. On an AIX system, the home directory is defined by the HOME environment variable. On a Microsoft Windows system, the home directory is defined by the HOMEPATH environment variable. For example, on Microsoft Windows, your home directory might be C:\Users\yourUserName.

**After the installation completes:** After the installation completes, the installation debug log files and the configuration debug log files are copied to the logs subdirectory of the eDiscovery Manager installation directory. Also after installation, a single installation debug log file named eDMInstall.log is created in the same logs subdirectory.

**Errors:** If an error occurs during the silent installation process, the error will be printed in the eDiscovery Manager debug log file eDMInstall\*.log files. The log files can be found in the *user.home* during the installation. After installation, they can be found in *edmhome\logs*.

4. Start the eDiscovery Manager application server if it is not already running. If the server is already running, stop it and then restart it.

#### Related information:


 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

“Silent installation fails to run and an error message is not displayed” on page 172  
After starting the eDiscovery Manager installation program, the program exits



without any indication of a problem.

 Silent install fails to run and error message is not displayed

---

## Post-installation changes to the configuration files

When you install eDiscovery Manager, Version 2.2.2, your existing configuration files are automatically backed up and new versions of the files are installed.

If you install eDiscovery Manager, Version 2.2.2 over an existing version of eDiscovery Manager, a backup copy of is automatically created of the following files:

- Appointment.xml
- docviewer.config
- emailnlskeys.properties
- emailtemplate.xml
- exchProperties.xml
- notesProperties.xml

These files were changed since eDiscovery Manager, Version 2.2. If you modified these files in a previous release and you want to keep your changes, use the backup file as a reference and apply your changes to the new versions of the files.

Both the backup files and the new versions of the files are in the/config subdirectory of the eDiscovery Manager installation directory. The backup files are named as follows:

- Appointment.xml.bkup0
- docviewer.config.bkup0
- emailnlskeys.properties.bkup0
- emailtemplate.xml.bkup0
- exchProperties.xml.bkup0
- notesProperties.xml.bkup0

You must apply your changes to the new configuration files because eDiscovery Manager uses the changed new files in the new installation.

### Note:

This information applies only to eDiscovery Manager upgrade installations. This information does not apply to new installations.

---

## Post-upgrade changes to the configuration files

If you had previously made changes to the eDiscovery Manager installation configuration files, you must make the same changes to the newly installed configuration files.

If you install eDiscovery Manager on a different machine or to a different directory than eDiscovery Manager was previously installed to, any changes you made to the previous install configuration files you must also make to the newly installed configuration files. Ensure that you update any configuration files that you changed after you upgrade eDiscovery Manager. In addition, you must copy all

files from the `EDM_HOME\properties\version` directory of the previous eDiscovery Manager installation to the `EDM_HOME\properties\version` directory of the new installation.

---

## Restoring email notifications after an upgrade

If you previously used email notifications, the EDMMail session settings in the WebSphere Application Server administrative console were removed during the upgrade. You must reapply the settings to enable email notifications after the upgrade.

### Procedure

To restore the EDMMail session settings:

1. From the WebSphere Application Server administrative console, navigate to **Resources > Mail Sessions > EDMMailsession**.
2. Enter the values for your system in the **Configuration** tab. See your pre-upgrade notes for the previous values.
3. Save your changes.

---

## Starting and stopping the eDiscovery Manager server

IBM eDiscovery Manager uses the application server instance in the IBM WebSphere Application Server that you specified during the eDiscovery Manager installation. From time to time, you need to stop and restart this application server instance.

The content server must be started before you can start eDiscovery Manager. In IBM Content Manager Enterprise Edition environments, the resource manager that is associated with the content server also must be started.

**Remember:**  Use the AIX non-root user ID that you created as a prerequisite to start and stop the eDiscovery Manager server.

Your preferred method for starting and stopping the eDiscovery Manager server depends on your specific WebSphere Application Server installation. It also depends on your preferred procedure for managing WebSphere Application Server applications, the platform that WebSphere Application Server is running on, and other configuration details.

See the WebSphere Application Server product information for complete details about starting and stopping an application server.

### Related information:

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

---

## Chapter 3. Configuring eDiscovery Manager

Configuring IBM eDiscovery Manager consists of some tasks that you complete by using the eDiscovery Manager web client and some tasks that you complete outside of the web client. This section provides checklists to prepare you for the web client configuration tasks, which are described in the online help system. This section also provides detailed instructions for the configuration tasks that you complete outside of the web client.

### About this task

Do the eDiscovery Manager configuration tasks in the following recommended order.

### Procedure

1. Depending on the type of content management system, configure different integration points between eDiscovery Manager and the content management system.

Option	Description
FileNet P8	<b>Optional:</b> Configure eDiscovery Manager to connect to FileNet P8 by using the WSI transport method.
Content Manager EE	Work with your Content Manager EE administrator to configure user security on the primary content server.


2. Gather site-specific information by using the appropriate configuration checklists, then complete the associated configuration tasks on the Administration page of the eDiscovery Manager web client. As you enter the configuration information, use your completed checklists and see the online help system for more detailed information, if necessary.

Option	Description
FileNet P8	"Configuration checklists (FileNet P8)" on page 70
Content Manager EE	"Configuration checklists (Content Manager EE)" on page 87

3. Tune the database in your content management system environment to improve eDiscovery Manager performance.

Option	Description
FileNet P8	"Database tuning to improve performance (FileNet P8)" on page 62
Content Manager EE	"Database tuning to improve performance (Content Manager EE)" on page 43

4. Configure features that you want to provide to your users. These features require configuration outside of the eDiscovery Manager web client.

If you want your users to be able to...	Do this...
Enter user directory information as search terms	Customize the user directory
 Preview many types of vector-based documents	Configure document preview
View an email by using IBM Lotus iNotes®	Configure IBM Lotus iNotes viewing
View an email by using Lotus Notes	Configure Lotus Notes viewing.
Export Lotus Notes email	Configure Lotus Notes export.
Receive email notifications when eDiscovery Manager tasks start and finish	Configure email notifications.
Log in only once and access both eDiscovery Manager and the content server	Configure single sign-on support.

5. If your site also purchased IBM eDiscovery Analyzer, configure eDiscovery Manager to work with eDiscovery Analyzer. See “Configuring eDiscovery Manager to work with eDiscovery Analyzer” on page 134 for complete information.
6. Familiarize yourself with configuration information and limitations in the content management systems and in the content archives that can impact the search experience of eDiscovery Manager users. Being aware of this information can help you provide better support to your users, set expectations, and improve their search experience. See “Searching and search results” on page 134 for complete information.

## Configuration checklists

To configure IBM eDiscovery Manager, you need information about the products that eDiscovery Manager integrates with. Work with the administrators of these products to collect this information ahead of time and to make the configuration of eDiscovery Manager quick and efficient.

The configuration checklists identify only the information that you will need for the eDiscovery Manager web client configuration tasks. Complete the checklist that is appropriate for your content management system, IBM FileNet P8 or IBM Content Manager Enterprise Edition.

### Configuration checklists (FileNet P8)

Print and complete the configuration checklists to collect the information that you will need for the IBM eDiscovery Manager web client configuration tasks.

**Tip:** To print the complete set of checklists, select the title of this topic in the table of contents, click the **Print topics** icon in the Contents toolbar, and select **Print selected topic and all subtopics**.

**Remember:** The eDiscovery Manager web client configuration tasks are described in the online help system.

### General settings

On the General Settings pane of the Administration page of the eDiscovery Manager web client, an IT Administrator specifies the type of content that your site archives.

Print this checklist and work with your content server administrator to determine the types of content that are archived and the type of software that is used to archive that content.

Table 11. Information for configuring the General Settings pane

Information	Notes	Record your values here
Content archive types	<p>One or more content archive types that your site uses. Valid values include:</p> <ul style="list-style-type: none"> <li>• Lotus Domino email (compound) – Content Collector</li> <li>• Lotus Domino email (Content Search Services compound) - Content Collector</li> <li>• Microsoft Exchange email (compound) – Content Collector</li> <li>• Microsoft Exchange email (Content Search Services compound) – Content Collector</li> <li>• Lotus Domino email (bundled) – Content Collector</li> <li>• Microsoft Exchange email (bundled) - Content Collector</li> <li>• Files – Content Collector</li> <li>• Microsoft SharePoint – Content Collector</li> <li>• IBM Connections - Content Collector</li> <li>• SMTP email</li> <li>• SMTP email (compound) - Content Collector</li> <li>• SMTP email (Content Search Services compound) - Content Collector</li> <li>• Lotus Domino email – FileNet Email Manager</li> <li>• Microsoft Exchange email – FileNet Email Manager</li> </ul>	

On the Administration page of the eDiscovery Manager web client, click **General Settings** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring general settings" in the online help system for complete information about content archive types.

#### User roles

On the User Roles pane of the Administration page of the eDiscovery Manager web client, you assign roles to each user.

Print this checklist and work with your content management system administrator to determine which role or roles are appropriate for each eDiscovery user.

Table 12. Information for configuring the User Roles pane.

Role and description	Record your values here
<b>Archive Searcher:</b> Search content archives and view any documents in those archives	

Table 12. Information for configuring the User Roles pane (continued).

Role and description	Record your values here
<b>Auditor:</b> Search for, and view, audit records. Create, view, and manage audit reports. Auditors cannot configure the tasks to be audited; this is the responsibility of the IT Administrator.	
<b>Case Administrator:</b> <ul style="list-style-type: none"> <li>• Create, update, and delete cases</li> <li>• Add documents to, and remove documents from, a case</li> <li>• Move documents between folders and copy documents from one folder to another folder</li> <li>• Search content archives</li> <li>• View documents in the client applications that created them</li> <li>• Export documents</li> <li>• Identify, add, delete, and edit ignore text</li> <li>• Analyze documents by using eDiscovery Analyzer</li> </ul>	
<b>Case Builder:</b> <ul style="list-style-type: none"> <li>• Add documents to, and remove documents from, a case</li> <li>• Move documents between folders and copy documents from one folder to another folder</li> <li>• Search content archives</li> </ul>	
<b>Case Reviewer:</b> Analyze documents by using eDiscovery Analyzer. Case Reviewers cannot download documents.	
<b>Case Searcher:</b> Search a case and view any documents in that case.	
<b>CSV File Creator:</b> Users with this role can search a case and view any content in that case. They can also save the data in all rows and columns in the search results or in a folder to a CSV file.	
<b>Exporter:</b> Export content.	
<b>IT Administrator:</b> Users with this role can configure all aspects of eDiscovery Manager except the assignment of roles to users. Role assignment is the responsibility of Super Users.	
<b>Native Viewer:</b> View documents in the client applications that created them. Users without this role can view documents only in HTML format.	
<b>Super User:</b> <ul style="list-style-type: none"> <li>• Configure all aspects of eDiscovery Manager including the assignment of roles to users.</li> <li>• Search on all fields, including administration-level fields.</li> <li>• See the Delete Case task and take action on it.</li> </ul>	

On the Administration page of the eDiscovery Manager web client, click **User Roles** in the Navigation pane to enter the values that you collected.

A user with the IT Administrator role can configure all aspects of eDiscovery Manager on the Administration page except for user roles and the content management system. Only users with the Super User role are allowed to configure user roles and the content management system. The corresponding panes on the Administration page are available only to Super Users.

#### Related information

- See "Configuring user roles" in the online help system for complete information about assigning roles to users.
- See "User roles" in the online help system for detailed information about the eDiscovery Manager tasks that are associated with each role.

### Content management system

When you installed IBM eDiscovery Manager, you provided connection information for a content server and eDiscovery Manager verified that it could connect to the server. If there is more than one content server in the content management system, you can specify connection information for additional servers on the Content Management System pane.

Print this checklist and work with your content management system administrator to gather the following information about the content servers that your site has.

*Table 13. Information for configuring the Content Management System pane*

Information	Notes	Record your value here
Content management type	The only valid value is FileNet P8.	<b>FileNet P8</b>
FileNet P8 Content Engine URL	Examples of valid formats: <ul style="list-style-type: none"> <li>• Hypertext Transfer Protocol (HTTP): http://server_IP:port/wsi/FNCEWS40MTOM/</li> <li>• Internet Inter-ORB Protocol (IIOP): iiop://server_IP:port/FileNet/Engine</li> </ul>	
User name of a FileNet P8 administrator		
Password of the FileNet P8 administrator		
FileNet P8 object store name	eDiscovery Manager must be installed on a different object store than the one on which IBM Enterprise Records is installed.	

On the Administration page of the eDiscovery Manager web client, click **Content Management System** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring the content management system" in the online help system for complete information about configuring connections to additional content management systems.

### Collections

Before you or your users can use IBM eDiscovery Manager to search for content, you must add at least one collection to eDiscovery Manager.

A collection is composed of one or more similar object classes. Users can perform searches across multiple object classes when the object classes are in the same collection.

Print this checklist and work with your IBM FileNet P8 administrator to gather the following information about the object classes and properties that you want eDiscovery Manager users to be able to search.

*Table 14. Information for configuring the Collections pane*

Information	Notes	Record your value here
Content archive type	Valid values are determined by the content archive types that you specified on the General Settings pane.  Example value: <b>Files – Content Collector</b>	
Content servers	The content servers that you want eDiscovery Manager users to be able to search.	
Object classes	The object classes that you want eDiscovery Manager users to be able to search.	
Content server properties	The object class properties that you want eDiscovery Manager users to be able to search.	

On the Administration page of the eDiscovery Manager web client, click **Collections** in the Navigation pane to enter the values that you collected.

**Important:** Use IBM FileNet Enterprise Manager to set the security for all object classes that belong to collections. Set the security level for the eDiscovery group to View properties and set the security level for the eDiscovery administrator to Modify properties.

#### **Related information**

- See "Adding and importing collections" in the online help system for complete information about creating new collections and importing existing collections.

#### **Clearing the index value for collections and date range partitioned object stores:**

When you define a collection that uses multiple object stores, do not use date partitioned object stores with object stores that are not date partitioned for that collection.

#### **About this task**

A collection can use date range-partitioned object stores, or it can use object stores that are not partitioned by date ranges. It cannot use both types of object stores. Searching a date range-partitioned object store returns no results if the search is performed against the index value of that object store. To avoid this potentially misleading result, clear the Text Index value for the date content server property when you map content server properties to collection fields. For example, email collections, by default, that are archived by Content Collector have an ICCMailDate content server property with a Text Index value of `icc_received_date`.



## Procedure

To clear the index value for the date content server property:

1. On the Collections pane of the Administration page, click the **Search Mapping** tab of the collection that contains the date range-partitioned object store.
2. Find the row that contains the ICCMailDate content server property.
3. In the **Text Index** column of that row, clear the `icc_received_date` value.

## What to do next

If you are not sure whether a specific object store is partitioned by a date range, contact your FileNet P8 administrator.

## Search templates

Before you or your users can use IBM eDiscovery Manager to search for content, you must add at least one search template to eDiscovery Manager. Search templates allow users to search one or more collections. When you create a search template, you specify the collections to be searched, the content server properties that can be searched, and the information to display in the search results.

Optionally, you can create combined fields for a search template. A combined field is a combination of two or more similar content server properties, typically from different collections, that are represented in the template as a single search field. For example, the **Sender** search field might map to the **From** properties in Lotus Domino and Microsoft Exchange email collections.

Print this checklist and work with your FileNet P8 administrator to identify which collections and object class properties will be searchable.

*Table 15. Information for configuring the Search Templates pane*

Information	Notes	Record your value here
Collections	The collections that you want eDiscovery Manager users to be able to search by using this search template.	
Collection fields on the Collections and Combined Fields pane	If you plan to create combined fields, which content server properties to combine into a single search field. For example, the <b>Recipients</b> search field might map to the <b>To</b> , <b>CC</b> , and <b>BCC</b> properties in Lotus Domino and Microsoft Exchange email collections.	
Search fields on the Search Fields pane	Which content server properties to make searchable.	
Search fields on the Search Results pane	Which content server properties to display in the search results.	

On the Administration page of the eDiscovery Manager web client, click **Search Templates** in the Navigation pane to enter the values that you collected.

## Related information

- See "Adding and importing search templates" in the online help system for complete information about creating new search templates and importing existing search templates.

## Export settings

Users must be able to export content for legal review. Before users can export content, you must configure export settings.

Print this checklist and work with your IT administrator to determine the best task and thread allocation for IBM eDiscovery Manager export operations.

Table 16. Information for configuring the Export Settings pane

Information	Notes	Record your value here
Export directory	The full path of the directory in which to place exported content. The path can be up to 40 characters, for example, C:\eDM\exportedDocs	
Maximum number of concurrent export tasks	The maximum number of simultaneous export tasks that you want eDiscovery Manager to support.  Range: 1 - 5  Default value: 1.	
Maximum threads for all exports	The maximum number of threads to allow for all exports.  Range: 1 - 99  Default value: 8.	

On the Administration page of the eDiscovery Manager web client, click **Export Settings** in the Navigation pane to enter the values that you collected.

### Related information

- See "Configuring export settings" in the online help system for complete information about export-related configuration settings.

#### Related reference:

"Export formats"

Users must export content for legal review. You might want to become familiar with the formats to which content is exported. If necessary, you can change any of the default export format settings.

"Lotus Domino settings" on page 82

Before your users can view emails with Lotus Notes or IBM Lotus iNotes, and before they can export Lotus Notes email to a Lotus Domino server, you must configure the connection to the IBM Lotus Domino server.

## Export formats

Users must export content for legal review. You might want to become familiar with the formats to which content is exported. If necessary, you can change any of the default export format settings.

IBM provides plug-ins for the following export formats:

- EDRM XML
- HTML
- Native
- PDF
- Custom export formats from a vendor or designed by you

You can configure export formats on the Administration page of the IBM eDiscovery Manager web client. Click **Export Formats** in the Navigation pane to modify values.

The following table describes export format fields to provide a better understanding of export format components. You should not modify any of these fields, except for the plug-in parameters (optional).

*Table 17. Information for configuring the Export Formats pane*

Export format field	Notes
Export formats	<p>The available formats to which content can be exported. When a user submits an export task, the user selects from one of the following export formats:</p> <ul style="list-style-type: none"> <li>• EDRM XML</li> <li>• HTML</li> <li>• Native</li> <li>• PDF</li> <li>• Custom export formats</li> </ul>
Plug-in name	<p>There are two plug-in points for each export format: Extract and BatchComplete. A name is given to each plug-in point. For example, for the EDRM XML export format, EDRMExtractPlugin and EDRMBatchCompletePlugin are the names given to the two plug-in points.</p>
Plug-in class name	<p>The Java class name that is called during export at the plug-in point. For example, the class name of the EDRM BatchComplete plug-in is com.ibm.icm.edc.plugin.defaultplugins.EDRMBatchCompletePlugin.</p>
Enabled	<p>Whether the plug-in is enabled for use.</p> <p>All export format plug-ins are enabled by default, except for the BatchComplete plug-ins for the PDF and HTML export formats. The BatchComplete plug-ins provide optional features that are not required for exporting, however, these features might be useful to your site. See the following table for more information about the individual plug-in parameters.</p>
Plug-in parameters	<p>Parameters and parameter values for each plug-in.</p> <p>See the tables that follow for brief information about the plug-in parameters for the IBM export formats. See the web client's online help system for complete information.</p> <p>If you have export format plug-ins from other vendors, see their product information.</p>

### Related information

- See "Configuring export formats" in the online help system for complete information about configuring export formats and their associated plug-ins.

The following tables describe default plug-in parameters, possible values (where applicable), and default values. Work with your users to understand their preferences for the format of exported content. If you have installed a custom format from a vendor, work with the vendor to understand the plug-in parameters and values.

## Plug-in parameters for the EDRM XML export format

Table 18. Plug-in parameters for the EDRM XML export format

Plug-in	Plug-in parameter	Notes	Default
Extract	Format.of.inline.content	The format of inline content. Valid values include: <ul style="list-style-type: none"> <li>• HTML</li> <li>• TEXT</li> </ul>	TEXT
Extract	Maximum.size.of.EDRM.XML.file	An output EDRM XML file is created that contains the files in each batch. This value specifies the maximum size in MB of this file that will be created per batch.	5
BatchComplete	Create.ZIP.file	Whether to create a ZIP file. Valid values include: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>	TRUE
BatchComplete	Maximum.size.of.ZIP.file	The maximum size in MB of the ZIP file. When the zip file reaches the specified threshold, eDiscovery Manager creates another one.	512

## Plug-in parameters for the HTML export format

Table 19. Plug-in parameters for the HTML export format

Plug-in	Plug-in parameter	Notes	Default
Extract	Email.XSLT.file.name	The name of an Extensible Stylesheet Language Transformation (XSLT) file to use for transforming content to HTML. This file must be in the EDM_Home/config directory.	HTMLExportTemplate.xsl
Extract	Retain.original.documents	Whether to retain copies of the content in its original format. Valid values include: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>	FALSE
Extract	Document.conversion.timeout.minutes	The duration in minutes that the export task waits for a piece of content to be converted to HTML before the task stops processing this item and starts processing the next piece of content in the batch.	3
BatchComplete	Maximum.size.of.ZIP.file	The maximum size in MB of the ZIP file. When the zip file reaches the specified threshold, eDiscovery Manager creates another one.	512

## Plug-in parameters for the Native export format

Table 20. Plug-in parameters for the Native export format

Plug-in	Plug-in parameter	Notes	Default
BatchComplete	Export.log.file.absolute.path	The full path of the export log file named dominoExport.log, for example, C:\eDM\logs\dominoExport.log.	The default is determined during installation.
BatchComplete	Logging.mode	<p>The logging level. Valid values include:</p> <ul style="list-style-type: none"> <li>• ERROR</li> <li>• DEBUG</li> </ul> <p><b>Recommendation:</b> After you determine that export is working successfully, set the value of this parameter to ERROR. Doing so prevents the export log file from becoming too large and consuming more disk space than needed.</p> <p><b>Important:</b> Check the size of the export log file regularly. If it becomes too large, delete it.</p>	DEBUG
BatchComplete	Lotus.Domino.server	The name of the Lotus Domino server, for example, D01MC084/01/M/ACME. If the value is not specified (recommended), the value is read from the LotusDominoserver field on the LotusDomino Settings panel.	A default value is intentionally not specified.
BatchComplete	Lotus.Domino.server.export.directory	A subdirectory under the Lotus Domino server's data directory into which the content is exported. If this directory does not already exist, it is created in the remote LotusDomino server's data directory.	exportedDocs
BatchComplete	Lotus.Mail.database.template	<p>The mail database template for creating export databases. If the value is not specified (recommended), the value is read from the Mail database template field on the Lotus Domino Settings panel.</p> <p><b>Restriction:</b> The file name of the mail database template can contain only English and system language characters. For example, if the system language is Japanese, the file name can contain only English and Japanese characters.</p>	A default value is intentionally not specified.

Table 20. Plug-in parameters for the Native export format (continued)

Plug-in	Plug-in parameter	Notes	Default
BatchComplete	Maximum.size.of.export.database	The maximum size, in MB, of an export file. When an export database file reaches the specified threshold, eDiscovery Manager creates another one.	512
BatchComplete	PST.package.Msg.File.To.PST	Whether (TRUE) or not (FALSE) to package all of the MSG files into a PST file. By default, MSG files are packaged into a PST file (TRUE). Valid values include: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>	TRUE
BatchComplete	PST.Maximum.filesize.in.megabytes	The maximum size, in MB, of a PST file that contains a batch of documents or a portion of a batch of documents.	512

### Plug-in parameters for the PDF export format

Table 21. Plug-in parameters for the PDF export format.

Plug-in	Plug-in parameter	Notes	Default
Extract	Email.XSLT.file.name	The name of an Extensible Stylesheet Language Transformation (XSLT) file to use for transforming content to PDF. This file must be in the EDM_Home/config directory.	PDFExportTemplate.xsl
Extract	Retain.original.documents	Whether to retain copies of the content in its original format. Valid values include: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>	FALSE
Extract	Document.conversion.timeout.minutes	The duration in minutes that the export task waits for a piece of content to be converted to PDF before the task stops processing this item and starts processing the next piece of content in the batch. See the following section for more information.	10
BatchComplete	Maximum.size.of.ZIP.file	The maximum size, in MB, of the ZIP file. When the zip file reaches the specified threshold, eDiscovery Manager creates another one.	512

## Document.conversion.timeout.minutes plug-in parameter

The **Document.conversion.timeout.minutes** plug-in parameter is part of the default Extract plug-ins for HTML and PDF export formats (HTMLExtractPlugin and PDFExtractPlugin). This parameter sets the number of minutes that the export task waits for an individual piece of content to be converted to the export format before the task stops processing that item and starts processing the next item in the export batch.

If you receive messages that your export tasks have stopped processing an item because the content conversion process is taking longer than expected, you can increase the value of the **Document.conversion.timeout.minutes** plug-in parameter for that export format. To change the value of this parameter, go to the Export Formats pane of the Administration page and click the export format (for example, PDF) that you want. In the Extract table, click **Edit this plug-in** for the default Extract plug-in (for example, PDFExtractPlugin). In the Plug-in Parameters table, click the current value for the **Document.conversion.timeout.minutes** plug-in parameter and enter a larger value.

### Related reference:

“Export settings” on page 76

Users must be able to export content for legal review. Before users can export content, you must configure export settings.

“Lotus Domino settings” on page 82

Before your users can view emails with Lotus Notes or IBM Lotus iNotes, and before they can export Lotus Notes email to a Lotus Domino server, you must configure the connection to the IBM Lotus Domino server.

### Attachment export:

Special characters in attachment names are replaced with underscores when attachments are exported.

Any of the following special characters, when used in attachment names, are replaced with an underscore ( \_ ) when the attachments are exported.

On Windows:

&	Ampersand
/	Forward slash
\	Back slash
	Pipe
>	Less than
<	Greater than
*	Asterisk
?	Question mark
:	Colon
"	Quotation mark
/t	Tab character

On AIX:

&        Ampersand  
/        Forward slash

## Audit configuration

IBM eDiscovery Manager audits some tasks by default. However, you can configure additional tasks to audit depending on the needs of your site.

Print this checklist and work with your legal department to determine which additional tasks to audit.

Table 22. Information for configuring the Audit Configuration pane

Information	Notes	Record your value here
Tasks to be audited	If you plan to audit additional tasks, which tasks to audit. Valid values include: <ul style="list-style-type: none"><li>• <b>Retrieve and view content</b></li><li>• <b>Remove content from folder</b></li><li>• <b>Move content between folders</b></li><li>• <b>Export content</b></li></ul>	
XSLT file name	If you plan to view audit reports in HTML, an XSLT file for your eDiscovery Manager audit reports, for example, auditReport.xslt.	

On the Administration page of the eDiscovery Manager web client, click **Audit Configuration** in the Navigation pane to enter the values that you collected.

### Related information

- See "Configuring tasks to be audited" in the online help system for complete information about configuring auditable tasks.

## Lotus Domino settings

Before your users can view emails with Lotus Notes or IBM Lotus iNotes, and before they can export Lotus Notes email to a Lotus Domino server, you must configure the connection to the IBM Lotus Domino server.

Print this checklist and work with your Lotus Domino administrator to gather the following information for connecting to the Lotus Domino server.

Table 23. Information for configuring the Lotus Domino pane

	Information	Notes	Record your value here
Viewing	Lotus Domino server	The name or IP address of the Lotus Domino server that the viewing database will reside on, for example, myServer/ibm or 9.30.123.434.	
	Mail database template	The mail database template for creating the viewing database, for example, mail8.ntf or myTemplates/mail8.ntf.	
	Viewing database path	A path and file name for the Lotus Notes viewing database, for example, myDirectory/EDMMail.nsf.	
	HTTP port	If you want to enable Lotus iNotes viewing, the HTTP port number of the Lotus Domino server.	



Table 23. Information for configuring the Lotus Domino pane (continued)

	Information	Notes	Record your value here
<b>Exporting</b>	Lotus Domino server	The name or IP address of the Lotus Domino server to which Lotus Notes email will be exported, for example, myMailServer/ibm or 9.30.123.435.	
	Mail database template	The mail database template for creating export databases, for example, mail6.ntf or myTemplates/mail6.ntf.	

On the Administration page of the IBM eDiscovery Manager web client, click **Lotus Domino Settings** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring Lotus Domino settings" in the online help system for complete information about configuring a connection to a Lotus Domino server.

#### Related reference:

"Export settings" on page 76

Users must be able to export content for legal review. Before users can export content, you must configure export settings.

"Export formats" on page 76

Users must export content for legal review. You might want to become familiar with the formats to which content is exported. If necessary, you can change any of the default export format settings.

### LDAP

If you want to make a user directory accessible to your users, you must configure the connection to a directory server that is accessed by the Lightweight Directory Access Protocol (LDAP). IBM eDiscovery Manager supports Lotus Domino, Microsoft Active Directory, and Tivoli Directory Server.

Print this checklist and work with your LDAP administrator to gather the following information about the LDAP server.

Table 24. Information for configuring the LDAP pane

Information	Notes	Record your value here
Server	The host name or IP address of the LDAP server.	
Port number	The port number of the LDAP server.  Default values: <ul style="list-style-type: none"> <li>• For most LDAP servers, including Tivoli Directory Server: 389</li> <li>• For Active Directory global catalog servers: 3268</li> </ul>	
Search base node	The search base node in the LDAP tree.	
Maximum number of results returned	The maximum number of results to return from the name address book lookup.  Default value: 100	
User name	If the LDAP server has basic security enabled, the user name of the LDAP server administrator.	

Table 24. Information for configuring the LDAP pane (continued)

Information	Notes	Record your value here
Password	If the LDAP server has basic security enabled, the password of the LDAP server administrator.	

On the Administration page of the eDiscovery Manager web client, click **LDAP Configuration** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring LDAP" in the online help system for complete information about configuring the connection to a directory server that is accessed by LDAP.

#### Logging

To facilitate troubleshooting, you can configure IBM eDiscovery Manager to capture messages for the web client and the work manager.

Print this checklist and work with your IT administrator to configure eDiscovery Manager logging.

Table 25. Information for configuring the Logging pane

	Information	Notes	Record your value here
Web client	Web client log file path	<p>The full path and a file name for the web client log file. The file extension of the log must be .log.</p> <p>Example values:</p> <ul style="list-style-type: none"> <li>• On AIX: /opt/IBM/edm/logs/edmWebClient.log</li> <li>• On Windows: C:\Program Files\IBM\edm\logs\edmWebClient.log</li> </ul>	
	Web client logging level	<p>The optimal logging level of the web client log file. Valid values include:</p> <ul style="list-style-type: none"> <li>• <b>Off</b></li> <li>• <b>Severe</b></li> <li>• <b>Warning</b></li> <li>• <b>Informational</b></li> <li>• <b>Fine</b></li> <li>• <b>Finer</b></li> <li>• <b>Finest</b></li> </ul> <p>Default value: <b>Severe</b></p>	
	Number of rotating web client log files	<p>The maximum number of web client log files to create.</p> <p>Consider this value in conjunction with the size limit of each log file, the amount of disk space that the eDiscovery Manager system has, and the amount of history that you want to keep.</p> <p><b>Tip:</b> Until your users establish average usage patterns, monitor the log files to ensure that the configured values are meeting your needs. Your site might also have policies and standards in place that dictate best practices.</p>	
	Size limit of each web client log file	<p>The maximum size in MB of each web client log file.</p> <p>Consider this value in conjunction with the number of rotating log files, the amount of disk space that the eDiscovery Manager system has, and the amount of history that you want to keep.</p> <p><b>Tip:</b> Until your users establish average usage patterns, monitor the log files to ensure that the configured values are meeting your needs. Your site might also have policies and standards in place that dictate best practices.</p>	

Table 25. Information for configuring the Logging pane (continued)

	Information	Notes	Record your value here
Work manager	Work manager log file path	<p>The full path and a file name for the work manager log file. The file extension of the log must be .log.</p> <p>Example values:</p> <ul style="list-style-type: none"> <li>On AIX: /opt/IBM/eDM/logs/edmWorkMgr.log</li> <li>On Windows: C:\Program Files\IBM\EDM\logs\edmWorkMgr.log</li> </ul>	
	Work manager logging level	<p>The optimal logging level of the work manager log file. Valid values include:</p> <ul style="list-style-type: none"> <li>Off</li> <li>Severe</li> <li>Warning</li> <li>Informational</li> <li>Fine</li> <li>Finer</li> <li>Finest</li> </ul> <p>Default value: <b>Severe</b></p>	
	Number of rotating work manager log files	<p>The maximum number of work manager log files to create.</p> <p>Consider this value in conjunction with the size limit of each log file, the amount of disk space that the eDiscovery Manager system has, and the amount of history that you want to keep.</p> <p><b>Tip:</b> Until your users establish average usage patterns, monitor the log files to ensure that the configured values are meeting your needs. Your site might also have policies and standards in place that dictate best practices.</p>	
	Number of rotating work manager log files	<p>The maximum size in MB of each work manager log file.</p> <p>Consider this value in conjunction with the number of rotating log files, the amount of disk space that the eDiscovery Manager system has, and the amount of history that you want to keep.</p> <p><b>Tip:</b> Until your users establish average usage patterns, monitor the log files to ensure that the configured values are meeting your needs. Your site might also have policies and standards in place that dictate best practices.</p>	

On the Administration page of the eDiscovery Manager web client, click **Logging Configuration** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring logging" in the online help system for complete information about the logging levels and for recommendations about the number and size of log files to define.

## Configuration checklists (Content Manager EE)

Print and complete the configuration checklists to collect the information that you will need for the IBM eDiscovery Manager web client configuration tasks.

**Tip:** To print the complete set of checklists, select the title of this topic in the table of contents, click the **Print topics** icon in the Contents toolbar, and select **Print selected topic and all subtopics**.

**Remember:** The eDiscovery Manager web client configuration tasks are described in the online help system.

### General settings

On the General Settings pane of the Administration page of the eDiscovery Manager web client, an IT Administrator specifies the type of content that your site archives.

Print this checklist and work with your content server administrator to determine the types of content that are archived and the type of software that is used to archive that content.

Table 26. Information for configuring the General Settings pane

Information	Notes	Record your values here
Content archive types	<p>One or more content archive types that your site uses. Valid values include:</p> <ul style="list-style-type: none"> <li>• <b>Lotus Domino email (compound) – Content Collector</b></li> <li>• <b>Microsoft Exchange email (compound) – Content Collector</b></li> <li>• <b>Lotus Domino email (bundled) – Content Collector</b></li> <li>• <b>Microsoft Exchange email (bundled) - Content Collector</b></li> <li>• <b>Files – Content Collector</b></li> <li>• <b>Microsoft SharePoint – Content Collector</b></li> <li>• <b>IBM Connections - Content Collector</b></li> <li>• <b>SMTP email</b></li> <li>• <b>SMTP email (compound) - Content Collector</b></li> <li>• <b>Lotus Domino email – CommonStore</b></li> <li>• <b>Microsoft Exchange email – CommonStore</b></li> </ul>	

On the Administration page of the eDiscovery Manager web client, click **General Settings** in the Navigation pane to enter the values that you collected.

### Related information

- See "Configuring general settings" in the online help system for complete information about content archive types.

## User roles

On the User Roles pane of the Administration page of the eDiscovery Manager web client, you assign roles to each user.

Print this checklist and work with your content management system administrator to determine which role or roles are appropriate for each eDiscovery user.

Table 27. Information for configuring the User Roles pane.

Role and description	Record your values here
<b>Archive Searcher:</b> Search content archives and view any documents in those archives	
<b>Auditor:</b> Search for, and view, audit records. Create, view, and manage audit reports. Auditors cannot configure the tasks to be audited; this is the responsibility of the IT Administrator.	
<b>Case Administrator:</b> <ul style="list-style-type: none"><li>• Create, update, and delete cases</li><li>• Add documents to, and remove documents from, a case</li><li>• Move documents between folders and copy documents from one folder to another folder</li><li>• Search content archives</li><li>• View documents in the client applications that created them</li><li>• Export documents</li><li>• Identify, add, delete, and edit ignore text</li><li>• Analyze documents by using eDiscovery Analyzer</li></ul>	
<b>Case Builder:</b> <ul style="list-style-type: none"><li>• Add documents to, and remove documents from, a case</li><li>• Move documents between folders and copy documents from one folder to another folder</li><li>• Search content archives</li></ul>	
<b>Case Reviewer:</b> Analyze documents by using eDiscovery Analyzer. Case Reviewers cannot download documents.	
<b>Case Searcher:</b> Search a case and view any documents in that case.	
<b>CSV File Creator:</b> Users with this role can search a case and view any content in that case. They can also save the data in all rows and columns in the search results or in a folder to a CSV file.	
<b>Exporter:</b> Export content.	
<b>IT Administrator:</b> Users with this role can configure all aspects of eDiscovery Manager except the assignment of roles to users. Role assignment is the responsibility of Super Users.	
<b>Native Viewer:</b> View documents in the client applications that created them. Users without this role can view documents only in HTML format.	

Table 27. Information for configuring the User Roles pane (continued).

Role and description	Record your values here
<b>Super User:</b> <ul style="list-style-type: none"> <li>• Configure all aspects of eDiscovery Manager including the assignment of roles to users.</li> <li>• Search on all fields, including administration-level fields.</li> <li>• See the Delete Case task and take action on it.</li> </ul>	

On the Administration page of the eDiscovery Manager web client, click **User Roles** in the Navigation pane to enter the values that you collected.

A user with the IT Administrator role can configure all aspects of eDiscovery Manager on the Administration page except for user roles and the content management system. Only users with the Super User role are allowed to configure user roles and the content management system. The corresponding panes on the Administration page are available only to Super Users.

#### Related information

- See "Configuring user roles" in the online help system for complete information about assigning roles to users.
- See "User roles" in the online help system for detailed information about the eDiscovery Manager tasks that are associated with each role.

#### Content management system

When you installed IBM eDiscovery Manager, you provided connection information for a content server and eDiscovery Manager verified that it could connect to the server. If there is more than one content server in the content management system, you can specify connection information for additional servers on the Content Management System pane.

Print this checklist and work with your content management system administrator to gather the following information about the content servers that your site has.

Table 28. Information for configuring the Content Management System pane

Information	Notes	Record your value here
Content management type	The only valid value is Content Manager EE.	<b>Content Manager EE</b>
Library server database name		
User name of a Content Manager EE administrator	Default value: ICMADMIN.	
Password of the Content Manager EE administrator		
DB2 Net Search Extender expansion limit	<p>The expansion limit is the maximum number of terms to which a wildcard term can be expanded when searching.</p> <p>Default value: 20000.</p>	

On the Administration page of the eDiscovery Manager web client, click **Content Management System** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring the content management system" in the online help system for complete information about configuring connections to additional content management systems.

### Collections

Before you or your users can use IBM eDiscovery Manager to search for content, you must add at least one collection to eDiscovery Manager.

A collection is composed of one or more similar item types. Users can perform searches across multiple item types when the item types are in the same collection.

Print this checklist and work with your Content Manager EE administrator to gather the following information about the IBM Content Manager item types and attributes that you want eDiscovery Manager users to be able to search.

*Table 29. Information for configuring the Collections pane*

Information	Notes	Record your value here
Content archive type	Valid values are determined by the content archive types that you specified on the General Settings pane.  Example value: <b>Files – Content Collector</b>	
Content servers	The content repository servers that you want eDiscovery Manager users to be able to search.	
Item types	The item types that you want eDiscovery Manager users to be able to search.	
Content server properties	The item type attributes that you want eDiscovery Manager users to be able to search.	

**Important:** Use the IBM Content Manager system administration client to update the access control lists (ACLs) of all item types that will belong to an eDiscovery collection. See "Configuring item type security" on page 105 for complete information.

On the Administration page of the eDiscovery Manager web client, click **Collections** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Adding and importing collections" in the online help system for complete information about creating new collections and importing existing collections.

### Search templates

Before you or your users can use IBM eDiscovery Manager to search for content, you must add at least one search template to eDiscovery Manager. Search templates allow users to search one or more collections. When you create a search template, you specify the collections to be searched, the content server properties that can be searched, and the information to display in the search results.

Optionally, you can create combined fields for a search template. A combined field is a combination of two or more similar content server properties, typically from



different collections, that are represented in the template as a single search field. For example, the **Sender** search field might map to the **From** properties in Lotus Domino and Microsoft Exchange email collections.

Print this checklist and work with your IBM Content Manager Enterprise Edition administrator to identify which collections and item type attributes will be searchable.

*Table 30. Information for configuring the Search Templates pane*

Information	Notes	Record your value here
Collections	The collections that you want eDiscovery Manager users to be able to search by using this search template.	
Collection fields on the Collections and Combined Fields pane	If you plan to create combined fields, which content server properties to combine into a single search field. For example, the <b>Recipients</b> search field might map to the <b>To</b> , <b>CC</b> , and <b>BCC</b> properties in Lotus Domino and Microsoft Exchange email collections.	
Search fields on the Search Fields pane	Which content server properties to make searchable.	
Search fields on the Search Results pane	Which content server properties to display in the search results.	

On the Administration page of the eDiscovery Manager web client, click **Search Templates** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Adding and importing search templates" in the online help system for complete information about creating new search templates and importing existing search templates.

#### Export settings

Users must be able to export content for legal review. Before users can export content, you must configure export settings.

Print this checklist and work with your IT administrator to determine the best task and thread allocation for IBM eDiscovery Manager export operations.

*Table 31. Information for configuring the Export Settings pane*

Information	Notes	Record your value here
Export directory	The full path of the directory in which to place exported content. The path can be up to 40 characters, for example, C:\eDM\exportedDocs	
Maximum number of concurrent export tasks	The maximum number of simultaneous export tasks that you want eDiscovery Manager to support.  Range: 1 - 5  Default value: 1.	
Maximum threads for all exports	The maximum number of threads to allow for all exports.  Range: 1 - 99  Default value: 8.	

On the Administration page of the eDiscovery Manager web client, click **Export Settings** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring export settings" in the online help system for complete information about export-related configuration settings.

#### Related reference:

"Export formats"

Users must export content for legal review. You might want to become familiar with the formats to which content is exported. If necessary, you can change any of the default export format settings.

"Lotus Domino settings" on page 97

Before your users can view emails with Lotus Notes or IBM Lotus iNotes, and before they can export Lotus Notes email to a Lotus Domino server, you must configure the connection to the IBM Lotus Domino server.

### Export formats

Users must export content for legal review. You might want to become familiar with the formats to which content is exported. If necessary, you can change any of the default export format settings.

IBM provides plug-ins for the following export formats:

- EDRM XML
- HTML
- Native
- PDF
- Custom export formats from a vendor or designed by you

You can configure export formats on the Administration page of the IBM eDiscovery Manager web client. Click **Export Formats** in the Navigation pane to modify values.

The following table describes export format fields to provide a better understanding of export format components. You should not modify any of these fields, except for the plug-in parameters (optional).

*Table 32. Information for configuring the Export Formats pane.*

Export format field	Notes
Export format name	The available formats to which content can be exported. When a user submits an export task, the user selects from one of the following export formats: <ul style="list-style-type: none"><li>• EDRM XML</li><li>• HTML</li><li>• Native</li><li>• PDF</li><li>• Custom export formats</li></ul>
Plug-in name	There are two plug-in points for each export format: Extract and BatchComplete. A name is given to each plug-in point. For example, for the EDRM XML export format, EDRMExtractPlugin and EDRMBatchCompletePlugin are the names given to the two plug-in points.

Table 32. Information for configuring the Export Formats pane (continued).

Export format field	Notes
Plug-in class name	The Java class name that is called during export at the plug-in point. For example, the class name of the EDRM BatchComplete plug-in is com.ibm.icm.edc.plugin.defaultplugins.EDRMBatchCompletePlugin.
Enabled	Whether the plug-in is enabled for use.  All export format plug-ins are enabled by default, except for the BatchComplete plug-ins for the PDF and HTML export formats. The BatchComplete plug-ins provide optional features that are not required for exporting, however, these features might be useful to your site. See the following table for more information about the individual plug-in parameters.
Plug-in parameters	Parameters and parameter values for each plug-in.  See the tables that follow for brief information about the plug-in parameters for the IBM export formats. See the web client's online help system for complete information.  If you have export format plug-ins from other vendors, see their product information.

### Related information

- See "Configuring export formats" in the online help system for complete information about configuring export formats and their associated plug-ins.

The following tables describe default plug-in parameters, possible values (where applicable), and default values. Work with your users to understand their preferences for the format of exported content. If you have installed a custom format from a vendor, work with the vendor to understand the plug-in parameters and values.

### Plug-in parameters for the EDRM XML export format

Table 33. Plug-in parameters for the EDRM XML export format.

Plug-in	Plug-in parameter	Notes	Default
Extract	Format.of.inline.content	The format of inline content. Valid values include: <ul style="list-style-type: none"> <li>• HTML</li> <li>• TEXT</li> </ul>	TEXT
Extract	Maximum.size.of.EDRM.XML.file	An output EDRM XML file is created that contains the files in each batch. This value specifies the maximum size in MB of this file that will be created per batch.	5
BatchComplete	Create.ZIP.file	Whether to create a ZIP file. Valid values include: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>	TRUE
BatchComplete	Maximum.size.of.ZIP.file	The maximum size in MB of the ZIP file. When the zip file reaches the specified threshold, eDiscovery Manager creates another one.	512

## Plug-in parameters for the HTML export format

Table 34. Plug-in parameters for the HTML export format.

Plug-in	Plug-in parameter	Notes	Default
Extract	Email.XSLT.file.name	The name of an Extensible Stylesheet Language Transformation (XSLT) file to use for transforming content to HTML. This file must be in the EDM_Home/config directory.	HTMLExportTemplate.xsl
Extract	Retain.original.documents	Whether to retain copies of the content in its original format. Valid values include: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>	FALSE
Extract	Document.conversion.timeout.minutes	The duration in minutes that the export task waits for a piece of content to be converted to HTML before the task stops processing this item and starts processing the next piece of content in the batch.	3
BatchComplete	Maximum.size.of.ZIP.file	The maximum size in MB of the ZIP file. When the zip file reaches the specified threshold, eDiscovery Manager creates another one.	512

## Plug-in parameters for the Native export format

Table 35. Plug-in parameters for the Native export format.

Plug-in	Plug-in parameter	Notes	Default
BatchComplete	Export.log.file.absolute.path	The full path of the export log file named dominoExport.log, for example, C:\eDM\logs\dominoExport.log.	The default is determined during installation.
BatchComplete	Logging.mode	The logging level. Valid values include: <ul style="list-style-type: none"> <li>• ERROR</li> <li>• DEBUG</li> </ul> <p><b>Recommendation:</b> After you determine that export is working successfully, set the value of this parameter to ERROR. Doing so prevents the export log file from becoming too large and consuming more disk space than needed.</p> <p><b>Important:</b> Check the size of the export log file regularly. If it becomes too large, delete it.</p>	DEBUG

Table 35. Plug-in parameters for the Native export format (continued).

Plug-in	Plug-in parameter	Notes	Default
BatchComplete	Lotus.Domino.server	The name of the Lotus Domino server, for example, D01MC084/01/M/ACME. If the value is not specified (recommended), the value is read from the LotusDominoServer field on the LotusDomino Settings panel.	A default value is intentionally not specified.
BatchComplete	Lotus.Domino.server.export.directory	A subdirectory under the Lotus Domino server's data directory into which the content is exported. If this directory does not already exist, it is created in the remote LotusDomino server's data directory.	exportedDocs
BatchComplete	Lotus.Mail.database.template	The mail database template for creating export databases. If the value is not specified (recommended), the value is read from the Mail database template field on the Lotus Domino Settings panel. <b>Restriction:</b> The file name of the mail database template can contain only English and system language characters. For example, if the system language is Japanese, the file name can contain only English and Japanese characters.	A default value is intentionally not specified.
BatchComplete	Maximum.size.of.export.database	The maximum size, in MB, of an export file. When an export database file reaches the specified threshold, eDiscovery Manager creates another one.	512
BatchComplete	PST.package.Msg.File.To.PST	Whether (TRUE) or not (FALSE) to package all of the MSG files into a PST file. By default, MSG files are packaged into a PST file (TRUE). Valid values include: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>	TRUE
BatchComplete	PST.Maximum.filesize.in.megabytes	The maximum size, in MB, of a PST file that contains a batch of documents or a portion of a batch of documents.	512

## Plug-in parameters for the PDF export format

Table 36. Plug-in parameters for the PDF export format.

Plug-in	Plug-in parameter	Notes	Default
Extract	Email.XSLT.file.name	The name of an Extensible Stylesheet Language Transformation (XSLT) file to use for transforming content to PDF. This file must be in the EDM_Home/config directory.	PDFExportTemplate.xsl
Extract	Retain.original.documents	Whether to retain copies of the content in its original format. Valid values include: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul>	FALSE
Extract	Document.conversion.timeout.minutes	The duration in minutes that the export task waits for a piece of content to be converted to PDF before the task stops processing this item and starts processing the next piece of content in the batch. See the following section for more information.	10
BatchComplete	Maximum.size.of.ZIP.file	The maximum size, in MB, of the ZIP file. When the zip file reaches the specified threshold, eDiscovery Manager creates another one.	512

### Document.conversion.timeout.minutes plug-in parameter

The **Document.conversion.timeout.minutes** plug-in parameter is part of the default Extract plug-ins for HTML and PDF export formats (HTMLExtractPlugin and PDFExtractPlugin). This parameter sets the number of minutes that the export task waits for an individual piece of content to be converted to the export format before the task stops processing that item and starts processing the next item in the export batch.

If you receive messages that your export tasks have stopped processing an item because the content conversion process is taking longer than expected, you can increase the value of the **Document.conversion.timeout.minutes** plug-in parameter for that export format. To change the value of this parameter, go to the Export Formats pane of the Administration page and click the export format (for example, PDF) that you want. In the Extract table, click **Edit this plug-in** for the default Extract plug-in (for example, PDFExtractPlugin). In the Plug-in Parameters table, click the current value for the **Document.conversion.timeout.minutes** plug-in parameter and enter a larger value.

#### Related reference:

“Export settings” on page 91

Users must be able to export content for legal review. Before users can export content, you must configure export settings.

“Lotus Domino settings”

Before your users can view emails with Lotus Notes or IBM Lotus iNotes, and before they can export Lotus Notes email to a Lotus Domino server, you must configure the connection to the IBM Lotus Domino server.

### Audit configuration

IBM eDiscovery Manager audits some tasks by default. However, you can configure additional tasks to audit depending on the needs of your site.

Print this checklist and work with your legal department to determine which additional tasks to audit.

*Table 37. Information for configuring the Audit Configuration pane*

Information	Notes	Record your value here
Tasks to be audited	If you plan to audit additional tasks, which tasks to audit. Valid values include: <ul style="list-style-type: none"><li>• <b>Retrieve and view content</b></li><li>• <b>Remove content from folder</b></li><li>• <b>Move content between folders</b></li><li>• <b>Export content</b></li></ul>	
XSLT file name	If you plan to view audit reports in HTML, an XSLT file for your eDiscovery Manager audit reports, for example, <code>auditReport.xslt</code> .	

On the Administration page of the eDiscovery Manager web client, click **Audit Configuration** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring tasks to be audited" in the online help system for complete information about configuring auditable tasks.

### Lotus Domino settings

Before your users can view emails with Lotus Notes or IBM Lotus iNotes, and before they can export Lotus Notes email to a Lotus Domino server, you must configure the connection to the IBM Lotus Domino server.

Print this checklist and work with your Lotus Domino administrator to gather the following information for connecting to the Lotus Domino server.

Table 38. Information for configuring the Lotus Domino pane

	Information	Notes	Record your value here
Viewing	Lotus Domino server	The name or IP address of the Lotus Domino server that the viewing database will reside on, for example, myServer/ibm or 9.30.123.434.	
	Mail database template	The mail database template for creating the viewing database, for example, mail8.ntf or myTemplates/mail8.ntf.	
	Viewing database path	A path and file name for the Lotus Notes viewing database, for example, myDirectory/EDMail.nsf.	
	HTTP port	If you want to enable Lotus iNotes viewing, the HTTP port number of the Lotus Domino server.	
Exporting	Lotus Domino server	The name or IP address of the Lotus Domino server to which Lotus Notes email will be exported, for example, myMailServer/ibm or 9.30.123.435.	
	Mail database template	The mail database template for creating export databases, for example, mail6.ntf or myTemplates/mail6.ntf.	

On the Administration page of the IBM eDiscovery Manager web client, click **Lotus Domino Settings** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring Lotus Domino settings" in the online help system for complete information about configuring a connection to a Lotus Domino server.

#### Related reference:

"Export settings" on page 91

Users must be able to export content for legal review. Before users can export content, you must configure export settings.

"Export formats" on page 92

Users must export content for legal review. You might want to become familiar with the formats to which content is exported. If necessary, you can change any of the default export format settings.

### LDAP

If you want to make a user directory accessible to your users, you must configure the connection to a directory server that is accessed by the Lightweight Directory Access Protocol (LDAP). IBM eDiscovery Manager supports Lotus Domino, Microsoft Active Directory, and Tivoli Directory Server.

Print this checklist and work with your LDAP administrator to gather the following information about the LDAP server.

Table 39. Information for configuring the LDAP pane

Information	Notes	Record your value here
Server	The host name or IP address of the LDAP server.	



Table 39. Information for configuring the LDAP pane (continued)

Information	Notes	Record your value here
Port number	<p>The port number of the LDAP server.</p> <p>Default values:</p> <ul style="list-style-type: none"> <li>• For most LDAP servers, including Tivoli Directory Server: 389</li> <li>• For Active Directory global catalog servers: 3268</li> </ul>	
Search base node	The search base node in the LDAP tree.	
Maximum number of results returned	<p>The maximum number of results to return from the name address book lookup.</p> <p>Default value: 100</p>	
User name	If the LDAP server has basic security enabled, the user name of the LDAP server administrator.	
Password	If the LDAP server has basic security enabled, the password of the LDAP server administrator.	

On the Administration page of the eDiscovery Manager web client, click **LDAP Configuration** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring LDAP" in the online help system for complete information about configuring the connection to a directory server that is accessed by LDAP.

#### Logging

To facilitate troubleshooting, you can configure IBM eDiscovery Manager to capture messages for the web client and the work manager.

Print this checklist and work with your IT administrator to configure eDiscovery Manager logging.

Table 40. Information for configuring the Logging pane

	Information	Notes	Record your value here
Web client	Web client log file path	<p>The full path and a file name for the web client log file. The file extension of the log must be .log.</p> <p>Example values:</p> <ul style="list-style-type: none"> <li>• On AIX: /opt/IBM/eDM/logs/edmWebClient.log</li> <li>• On Windows: C:\Program Files\IBM\edm\logs\edmWebClient.log</li> </ul>	
	Web client logging level	<p>The optimal logging level of the web client log file. Valid values include:</p> <ul style="list-style-type: none"> <li>• <b>Off</b></li> <li>• <b>Severe</b></li> <li>• <b>Warning</b></li> <li>• <b>Informational</b></li> <li>• <b>Fine</b></li> <li>• <b>Finer</b></li> <li>• <b>Finest</b></li> </ul> <p>Default value: <b>Severe</b></p>	
	Number of rotating web client log files	<p>The maximum number of web client log files to create.</p> <p>Consider this value in conjunction with the size limit of each log file, the amount of disk space that the eDiscovery Manager system has, and the amount of history that you want to keep.</p> <p><b>Tip:</b> Until your users establish average usage patterns, monitor the log files to ensure that the configured values are meeting your needs. Your site might also have policies and standards in place that dictate best practices.</p>	
	Size limit of each web client log file	<p>The maximum size in MB of each web client log file.</p> <p>Consider this value in conjunction with the number of rotating log files, the amount of disk space that the eDiscovery Manager system has, and the amount of history that you want to keep.</p> <p><b>Tip:</b> Until your users establish average usage patterns, monitor the log files to ensure that the configured values are meeting your needs. Your site might also have policies and standards in place that dictate best practices.</p>	

Table 40. Information for configuring the Logging pane (continued)

	Information	Notes	Record your value here
Work manager	Work manager log file path	<p>The full path and a file name for the work manager log file. The file extension of the log must be .log.</p> <p>Example values:</p> <ul style="list-style-type: none"> <li>• On AIX: /opt/IBM/eDM/logs/edmWorkMgr.log</li> <li>• On Windows: C:\Program Files\IBM\edm\logs\edmWorkMgr.log</li> </ul>	
	Work manager logging level	<p>The optimal logging level of the work manager log file. Valid values include:</p> <ul style="list-style-type: none"> <li>• <b>Off</b></li> <li>• <b>Severe</b></li> <li>• <b>Warning</b></li> <li>• <b>Informational</b></li> <li>• <b>Fine</b></li> <li>• <b>Finer</b></li> <li>• <b>Finest</b></li> </ul> <p>Default value: <b>Severe</b></p>	
	Number of rotating work manager log files	<p>The maximum number of work manager log files to create.</p> <p>Consider this value in conjunction with the size limit of each log file, the amount of disk space that the eDiscovery Manager system has, and the amount of history that you want to keep.</p> <p><b>Tip:</b> Until your users establish average usage patterns, monitor the log files to ensure that the configured values are meeting your needs. Your site might also have policies and standards in place that dictate best practices.</p>	
	Size limit of each work manager log file	<p>The maximum size in MB of each work manager log file.</p> <p>Consider this value in conjunction with the number of rotating log files, the amount of disk space that the eDiscovery Manager system has, and the amount of history that you want to keep.</p> <p><b>Tip:</b> Until your users establish average usage patterns, monitor the log files to ensure that the configured values are meeting your needs. Your site might also have policies and standards in place that dictate best practices.</p>	

On the Administration page of the eDiscovery Manager web client, click **Logging Configuration** in the Navigation pane to enter the values that you collected.

#### Related information

- See "Configuring logging" in the online help system for complete information about the logging levels and for recommendations about the number and size of log files to define.

---

## Configuring security

When you and your users log on to the IBM eDiscovery Manager web client, you connect to a content server. The type of content management system (IBM FileNet P8 or IBM Content Manager Enterprise Edition) determines how you configure security, create user IDs, and assign access rights and privileges.

### User IDs

**FileNet P8** In FileNet P8 environments, the user IDs that users enter when they log on to the eDiscovery Manager web client are created by an LDAP administrator.

**Content Mgr** In Content Manager EE environments, the user IDs that users enter when they log on to the eDiscovery Manager web client can be created by a Content Manager EE administrator or by an LDAP administrator. LDAP user IDs are recommended because they can be imported into Content Manager EE and they are then synchronized across content servers.

### Logging in to the eDiscovery Manager web client

**Content Mgr** When users log into eDiscovery Manager, they log into the primary content server. The same user IDs and passwords are then used across all content servers that the users access. For this reason, user IDs and passwords must be synchronized across content servers. If they are not synchronized, users will be unable to access secondary content servers and to search the content on those servers. Use the **Synchronize Users** button on the User Roles pane of the Administration page to create an eDiscovery group on each secondary content server and to ensure that all eDiscovery users are added to that group.

**Exception:** **Content Mgr** The user ID and password of the eDiscovery administrator on the primary content server does not need to be synchronized across content servers. This exception exists because the user ID and password of the content server administrator is used when the eDiscovery administrator accesses a secondary content server. For this reason, it is recommended that you designate the content server administrator on each secondary content server to serve as the eDiscovery administrator for that system.

### Roles

eDiscovery Manager supports a set of predefined roles that are enforced by content server security models. Together, eDiscovery Manager roles and content server security control what users can do and what objects they can access. The role or roles that an eDiscovery Manager Super User assigns to a user determine the tasks which that user can perform. For example, IT Administrators can configure eDiscovery Manager. Archive Searchers can search content archives and view their content. Case Builders can not only search content archives and view their content, but they can add content to a case, remove content from a case, and move and copy content between folders.

See the "User roles" online help topic for complete information about user roles and see the "Configuring user roles" online help topic for information about assigning roles to users.

**Related information:**

Managing Content Manager EE users with LDAP

## Configuring security in a Content Manager EE environment

During installation, IBM eDiscovery Manager creates a security group, privilege sets, privileges, and access control lists (ACLs) on the primary IBM Content Manager Enterprise Edition server.

### Configuring user security on the primary content server

When you install IBM eDiscovery Manager, you identify the primary content server in your content management system. After installing eDiscovery Manager, work with the IBM Content Manager Enterprise Edition administrator on the primary content server to configure the initial security for eDiscovery group members.

#### About this task

To configure the initial security for eDiscovery group members by using the IBM Content Manager system administration client:

#### Procedure

1. On the Define Users tab of the User Properties window, assign each eDiscovery Manager user and each eDiscovery Analyzer user an initial maximum privilege set of ClientUserReadOnly.

**Exception:** During the eDiscovery Manager installation, the eDiscovery administrator was assigned a maximum privilege set that is appropriate for the Super User role. Do not change the maximum privilege set of the eDiscovery administrator.

**Important:** Never assign a maximum privilege set of AllPrivs to any user except the eDiscovery administrator on a secondary content server. Doing so overrides any roles that are assigned to the user and allows that user to perform any eDiscovery task that the eDiscovery administrator can perform. eDiscovery Manager does not perform security checks on users with full administration privileges.

2. On the Assign to Groups tab of the User Properties window, assign each eDiscovery Manager user and each eDiscovery Analyzer user to the eDiscovery group.
3. If the eDiscovery Manager server is running while the Content Manager EE administrator configures user security, stop and restart the eDiscovery Manager server when the Content Manager EE administrator is done.

**Related information:**

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

## Configuring user security on secondary content servers

After installing IBM eDiscovery Manager, you can identify secondary content servers in your content management system. Work with the IBM Content Manager Enterprise Edition administrator on the secondary content servers to configure the initial security for eDiscovery group members.

### About this task

To configure the initial security for eDiscovery group members:

### Procedure

1. For DB2 users:

Complete the following steps:

- a. Assign the eDiscovery administrator to the DB2 users group (by default, DB2USERS), if the administrator is not already a member. The eDiscovery administrator must be an authorized DB2 user.
- b. On systems running DB2 Version 9.7 or later, if the DB2 system has operating system security enabled, grant database administration authority on the library server database to the eDiscovery administrator. To do this, run the following command in a DB2 command window on a single line:

```
GRANT DBADM WITH DATAACCESS WITH ACCESSCTRL ON DATABASE TO USER  
eDiscovery_administrator
```

For complete information, see the GRANT (database authorities) statement topic in the DB2 solution information center.

2. Work with the Content Manager EE administrator to use the IBM Content Manager system administration client to create the following elements.
  - a. Create a new Content Manager EE user account or choose an existing user account to serve as the eDiscovery administrator.

**Recommendation:** To make security configuration simpler, choose the account of a content server administrator to serve as the eDiscovery administrator.

Be sure to select the **Use system password** option.

On the Define Users tab of the User Properties window, assign the eDiscovery administrator a maximum privilege set of AllPrivs.

On the Assign to Groups tab of the User Properties window, assign the eDiscovery administrator to the eDiscovery group.

On the Set Defaults tab of the User Properties window, set the default item access control list for the eDiscovery administrator to PublicReadACL.

- b. Create new user accounts for all other eDiscovery Manager users and eDiscovery Analyzer users.

For each user, use the same user ID and password that you used on the primary content server.

On the Define Users tab of the User Properties window, assign each eDiscovery Manager user and each eDiscovery Analyzer user an initial maximum privilege set of ClientUserReadOnly.

3. If the eDiscovery Manager server is running while the Content Manager EE administrator configures user security, stop and restart the eDiscovery Manager server when the Content Manager EE administrator is done.

## Results

You do not need to create an eDiscovery group on each of the secondary content servers. eDiscovery Manager creates this group on each server when you configure secondary content servers on the Content Management System pane of the Administration page. eDiscovery Manager adds all eDiscovery users to this group when you synchronize users across all content servers from the User Roles pane of the Administration page.

### Secondary content servers at sites that have IBM eDiscovery Analyzer installed:

On a site that has eDiscovery Analyzer and eDiscovery Manager installed, when you use the Content Management System pane of the Administration page of the eDiscovery Manager web client to add secondary content servers, you identify those content servers only to eDiscovery Manager. This information is not shared with eDiscovery Analyzer.

## Configuring item type security

Work with your IBM Content Manager Enterprise Edition administrator to use the IBM Content Manager system administration client to configure security for any item types that will belong to eDiscovery collections.

### About this task

To configure security for item types that will belong to eDiscovery collections, update the access control lists (ACLs) that are assigned to those item types to ensure that eDiscovery users can access the content.

### Procedure

1. Verify that the eDiscovery administrator has write access to the item types. Write access ensures that the item types can be added to collections.  
The default privilege set (EDMSUPERUSER) of the eDiscovery administrator on the primary content server provides write access. Similarly, the default privilege set (AllPrivs) of eDiscovery administrators on secondary content servers provides write access.
2. Give all other eDiscovery users read access to the item types. Read access ensures that the item types can be searched.  
The easiest way to give read access to eDiscovery users is to add the eDiscovery group to the ACLs of the item types and specify a privilege set of ClientUserReadOnly.

**Reminder:** In addition to updating the ACLs for email item types, remember to update the ACLs for email attachment item types too.

3. If the eDiscovery Manager server is running while the Content Manager EE administrator configures item type security, stop and restart the eDiscovery Manager server when the Content Manager EE administrator is done.

### Related information:

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

## Roles and privilege sets

IBM eDiscovery Manager creates its own roles and privilege sets. Each role has its own eDiscovery privileges, which are combined with IBM Content Manager privileges, to grant the appropriate authority on content server objects. When the eDiscovery administrator assigns roles to a user, the user's maximum privilege set is automatically updated from ClientUserReadOnly to an eDiscovery privilege set.

*Table 41. Roles and their associated privilege sets*

Role	eDiscovery Privilege Set
Archive Searcher	EDMARCHIVESearcher
Auditor	EDMAUDITOR
Case Administrator	EDMCASEADMIN
Case Builder	EDMCASEANALYST
Case Reviewer	EDMCASEREVIEWER
Case Searcher	EDMCASESEARCHER
Exporter	EDMEXPORTER
IT Administrator	EDMITADMIN
Native Viewer	EDMNATIVEVIEWER
Super User	EDMSUPERUSER

**Important:** To view multipart documents, IBM Content Manager requires that users have access to all of the document part types that are defined in the item type. Ensure that the Access Control List that is assigned to each part grants the EDISCOVERYUSERS group read access, at a minimum. Otherwise, eDiscovery Manager users will be unable to view multipart documents.

**Restriction:** eDiscovery Manager automatically updates a user's maximum privilege set each time that the eDiscovery administrator assigns roles to that user. However, eDiscovery Manager does not automatically update the user's privileges on cases to which the user is already assigned. You must manually update the user's privileges on these cases.

- After assigning a non-Super User role to a user, the Case Administrator or eDiscovery administrator must remove the user from each case access list and then add the user back to each case access list. Doing so refreshes the user's privileges on that case based on the user's current role assignments.
- After assigning the Super User role to a user, the Content Manager EE administrator must use the IBM Content Manager system administration client to remove the user's entry from each case ACL. With an eDiscovery privilege set of EDMSUPERUSER, the user now has the appropriate authority on all cases; the user does not need individual entries on case ACLs.

## Synchronizing the user membership of the eDiscovery Manager group

This topic describes how to synchronize the user membership of the eDiscovery Manager group.

### Procedure

To synchronize the user membership of the eDiscovery Manager group:

1. Define the same eDiscovery user on each content server.



2. Add the eDiscovery user to the eDiscovery group on the primary content server.
3. Assign roles to the eDiscovery users on the User Roles pane of the Administration page of the eDiscovery Manager web client.
4. Click **Synchronize Users** to add all eDiscovery users to the eDiscovery groups on the secondary content servers. Clicking **Synchronize Users** also logs details about eDiscovery users and groups on all content servers. For example, you can see the following information:
  - Which users were added to the eDiscovery group on each content server.
  - Which users were removed from the eDiscovery group on each secondary content server because the users were not members of the eDiscovery group on the primary content server.
  - Which users eDiscovery Manager tried to add but could not add to the eDiscovery group on each content server.

By default, logs are stored in the logs subdirectory of the eDiscovery Manager installation directory, and the default web client log file is edmapp#.log.

## Access Control Lists

A user's access to item types is based on the roles that are assigned to that user. Access is controlled by access control lists (ACLs), which combine users and groups with privilege sets. If a user is assigned multiple roles, IBM eDiscovery Manager creates a customized privilege set that combines the privilege sets of all of the user's roles.

**Important:** eDiscovery Manager ACLs are for the sole use of eDiscovery Manager. Do not assign eDiscovery Manager ACLs to non-eDiscovery Manager item types and do not change the definitions of eDiscovery Manager ACLs.

## Changing your Content Manager EE password

You and your users can change your IBM Content Manager Enterprise Edition passwords on the IBM eDiscovery Manager Login window. (This feature is available only in single content server environments. If you have multiple content servers defined to eDiscovery Manager, this feature is not available.)

### About this task

**Microsoft Windows restriction:** eDiscovery Manager cannot change the password of any user whose Content Manager EE account is also a Windows operating system account.

### Procedure

To change your Content Manager EE password:

1. Enter your user name and password in the Log In window. Then click **Change Password**.
2. Enter your new password and confirm it by entering it again. Your new password and the confirmation password must match.
3. Click **OK**.

## Configuring security in a FileNet P8 environment

During installation, IBM eDiscovery Manager creates object classes and security adapters on the IBM FileNet P8 server.

**Restriction:** IBM eDiscovery Manager automatically updates a user's maximum privilege set each time that the IBM eDiscovery Manager administrator assigns roles to that user. However, IBM eDiscovery Manager does not automatically update the user's privileges on cases to which the user is already assigned.

To update a user's privileges after assigning him a non-Super User role, the Case Administrator or IBM eDiscovery Manager administrator must remove the user from each case and then add the user back to each case. Doing so refreshes the user's privileges on that case based on the user's current role assignments.

## **Configuring user security**

In IBM FileNet P8 environments, most of the work of configuring user security occurs before you install IBM eDiscovery Manager. The directory service administrator creates a group for eDiscovery users and populates that group with users who will need access to eDiscovery Manager and eDiscovery Analyzer. The eDiscovery administrator is an important member of this group. During the installation of eDiscovery Manager, the existence of the eDiscovery group is verified.

### **About this task**

After eDiscovery Manager is installed, ensure that the eDiscovery administrators on secondary content servers have sufficient privileges to create and install AddOns. eDiscovery administrators must have write privileges on the object store.

If you need to configure user security on secondary content servers, in the Add Connection Information for a Content Server window, you must specify FileNet P8 Content Engine web addresses that use the WSI transport method. Because eDiscovery Analyzer supports only WSI connections, eDiscovery Manager must also use WSI connections. Do not specify FileNet P8 Content Engine web addresses that use IIOP connections.

## **Configuring object class security**

Work with your IBM FileNet P8 administrator to use IBM FileNet Enterprise Manager to configure security for the object classes that will belong to eDiscovery collections.

### **About this task**

To configure security for object classes that will belong to eDiscovery collections:

#### **Procedure**

1. For each object class, set the security level for the eDiscovery administrator to Full Control.  
The eDiscovery administrator must have write access to the object classes. Write access ensures that the object classes can be added to collections.
2. For each object class, set the security level for the eDiscovery group to Custom and grant the group View all properties and View content rights.  
eDiscovery users must have read access to the object classes. Read access ensures that the object classes can be searched.

## Results

**Default reservation type:** eDiscovery Manager defines the default reservation behavior at the object store level by setting the `DefaultReservationType` property to 16 (COLLABORATIVE).

### Related tasks:

“Before installing eDiscovery Manager to connect to FileNet P8” on page 46  
Before installing IBM eDiscovery Manager, ensure that the following prerequisites are met.

### Related information:

Versioning Concepts

See the Reservation Object section of this topic for complete information about the `DefaultReservationType` property.

## Security adapters

A user's access to object classes is based on the roles that are assigned to that user. Access is controlled by security adapters.

## Changing the eDiscovery administrator password

If the password of the eDiscovery administrator account on the primary content server changes, you must reconfigure IBM eDiscovery Manager immediately. Similarly, if the password of the eDiscovery administrator account on a secondary content server changes and the administrator of that content server is also the eDiscovery administrator you must reconfigure eDiscovery Manager immediately.

### About this task

eDiscovery Manager tasks depend on the ability of the eDiscovery administrator account to access content servers. If the credentials of the eDiscovery administrator are not kept up-to-date, eDiscovery Manager tasks will fail.

### Procedure

1. If the password of the eDiscovery administrator on the primary content server changes, tell eDiscovery Manager.

- a. Use a text editor to change the value of the `adminPassword` parameter (which is encoded) in the `ral.properties` file.

The default file location of the `ral.properties` file is:

**AIX**    `/opt/IBM/eDM/config/ral.properties`

#### Windows

`C:\Program Files\IBM\eDM\config\ral.properties`

- b. After saving your change and closing the `ral.properties` file, stop and restart the eDiscovery Manager application server for your change to take effect.

When the server restarts, it overwrites the new password that you specified with an encoded version of that password.

2. If the password of the eDiscovery administrator on a secondary content server changes and the eDiscovery administrator is also the content server administrator, reconfigure eDiscovery Manager.

- a. On the Administration page of the eDiscovery Manager web client, click **Content Management System** in the Navigation pane.
- b. Click the **Modify the connection information for this content server** icon.

- c. Change the administrator password, then click **Test Connection**.
- d. Click **Apply**.

---

## Customizing the user directory

An IBM eDiscovery Manager IT Administrator can work with the site's LDAP administrator to customize the user directory function in eDiscovery Manager for users.

### Procedure

To change the default user directory function that is available to users on the Search page of the eDiscovery Manager web client:

1. Open the `ldapAttributes.xml` file with a text editor.

*Table 42. Default location of the LDAP attributes XML file*

Operating system	Default file location
AIX	/opt/IBM/eDiscovery/config/ldapAttributes.xml
Windows	C:\Program Files\IBM\eDiscovery\config\ldapAttributes.xml

2. Define the attributes to search by using `<search-attribute>` entries.

For example, if you want your users to be able to search by name and email address, and your LDAP server uses `cn` for names and `mail` for email addresses, define the following search attributes:

```
<search-attribute>cn</search-attribute>
<search-attribute>mail</search-attribute>
```

3. Define the attributes that are returned by using `<display-attribute>` entries.

For example, if you want users to see common names in the search results and your LDAP server uses `name` for common names, define the following display attribute:

```
<display-attribute>name</display-attribute>
```

4. Define the attributes that display in the ToolTip when a user hovers over a row in the search results by using `<tooltip-attribute>` entries.

For example, if you want users to see department names and locations in the search results and your LDAP server uses `department` for departments and `l` (lowercase L) for locations, define the following hover help attributes:

```
<tooltip-attribute index="1" nls-key="jsp.searchrequest.
addressbook.tooltip.department">department
</tooltip-attribute>
<tooltip-attribute index="2" nls-key="jsp.searchrequest.
addressbook.tooltip.l">l</tooltip-attribute>
```

**Tip:** You can define your own labels for ToolTip attributes by creating entries in the `custom_label.properties` file, which resides in the same directory as `ldapAttributes.xml`. For example, if you defined the following ToolTip attributes in `ldapAttributes.xml`:

```
<tooltip-attribute nls-key="mytooltip.country">co
</tooltip-attribute>
<tooltip-attribute nls-key="mytooltip.lastname">sn
</tooltip-attribute>
```

You could define the following labels in `custom_label.properties`:

```
mytooltip.country Your country of origin
mytooltip.lastname Your surname (family name)
```

Detailed instructions are provided in the `custom_label.properties` file.

5. Define the attributes to append to the search terms by using the `<append-attribute>` entries.

For example, if you want to append the email address to the search terms and your LDAP server uses `mail` for email addresses, define the following append attribute:

```
<append-attribute>mail</append-attribute>
```

6. Define the required attribute that uniquely identifies an LDAP record by using the `<uid-attribute>` entry.

For example, if your LDAP schema uses an attribute called `uid` for unique identifiers, define the following unique identifier attribute:

```
<uid-attribute>uid</uid-attribute>
```

7. Restart the eDiscovery Manager application server for your changes to take effect.

## User directory file (Lotus Domino)

The `ldapAttributes.xml` file defines the user directory function on the Search page of the IBM eDiscovery Manager client application.

This sample is for a site that runs IBM Lotus Domino.

- 1 Attribute that you want to search.
- 2 Attribute that you want to search.
- 3 Attribute that you want returned.
- 4 Attribute that displays in the ToolTip when a user hovers over a row in the search results.
- 5 Attribute that displays in the ToolTip when a user hovers over a row in the search results.
- 6 Attribute to append to the search terms.
- 7 Attribute that uniquely identifies an LDAP record.

```
<ldap-attribute-config>
  <!-- These attributes are queried during LDAP search. -->
  <!-- The filter is (|(attr1=xxx)(attr2=xxx)(attr3=xxx)...) -->
  1 <search-attribute>cn</search-attribute>
  2 <search-attribute>mail</search-attribute>
  <!-- This attribute is displayed in the returned list. -->
  3 <display-attribute>cn</display-attribute>
  <!-- These attributes are displayed in the ToolTip when the -->
  <!-- user hovers over a row in the returned list. -->
  4 <tooltip-attribute nls-key="jsp.searchrequest.addressbook.
tooltip.div">div</tooltip-attribute>
  5 <tooltip-attribute nls-key="jsp.searchrequest.addressbook.
tooltip.email">emailaddress</tooltip-attribute>
  <!-- These attributes are appended to the search terms -->
  <!-- (possibly via a translator first). -->
  6 <append-attribute>mail</append-attribute>
  <!-- The attribute containing a unique LDAP record ID -->
  <!-- must be a single value -->
  7 <uid-attribute>uid</uid-attribute>
</ldap-attribute-config>
```

## User directory file (Microsoft Active Directory)

The `ldapAttributes.xml` file defines the user directory function on the Search page of the IBM eDiscovery Manager client application.

Without customization, no users will be visible in the user directory on the Search page of the eDiscovery Manager web client.

This sample is for a site that runs Microsoft Active Directory.

- 1** Attribute that you want to search.
- 2** Attribute that you want to search.
- 3** Attribute that you want returned.
- 4** Attribute that displays in the ToolTip when a user hovers over a row in the search results.
- 5** Attribute that displays in the ToolTip when a user hovers over a row in the search results.
- 6** Attribute to append to the search terms.
- 7** Attribute that uniquely identifies an LDAP record.

The value of this attribute must be sAMAccountName for sites with Microsoft Active Directory.

```
<ldap-attribute-config>
<!-- These attributes are queried during LDAP search. -->
<!-- The filter is (|(attr1=xxx)(attr2=xxx)(attr3=xxx)...) -->
1 <search-attribute>cn</search-attribute>
2 <search-attribute>mail</search-attribute>
<!-- This attribute (only one!) is displayed in the search result list. -->
3 <display-attribute>cn</display-attribute>
<!-- These attributes are displayed in the ToolTip when the -->
<!-- user hovers over a row in the returned list. The index attribute -->
<!-- defined the order. -->
4 <tooltip-attribute index = "1" nls-key="jsp.searchrequest.addressbook.
tooltip.name">displayName</tooltip-attribute>
<tooltip-attribute index = "2" nls-key="jsp.searchrequest.addressbook.
tooltip.email">mail</tooltip-attribute>
5 <tooltip-attribute index = "3" nls-key="jsp.searchrequest.addressbook.
tooltip.address">streetAddress</tooltip-attribute>
<tooltip-attribute index = "4" nls-key="jsp.searchrequest.addressbook.
tooltip.city">l</tooltip-attribute>
<tooltip-attribute index = "5" nls-key="jsp.searchrequest.addressbook.
tooltip.state">st</tooltip-attribute>
<tooltip-attribute index = "6" nls-key="jsp.searchrequest.addressbook.
tooltip.zip">postalCode</tooltip-attribute>
<tooltip-attribute index = "7" nls-key="jsp.searchrequest.addressbook.
tooltip.country">c</tooltip-attribute>
<!-- These attributes are appended to the search terms -->
<!-- (possibly via a translator first). -->
6 <append-attribute>cn</append-attribute>
<!-- The attribute containing a unique LDAP record ID -->
<!-- must be a single value -->
7 <uid-attribute>sAMAccountName</uid-attribute>
</ldap-attribute-config>
```

---

## Configuring document preview (AIX)

To preview many types of vector-based documents, IBM eDiscovery Manager servers that run on AIX systems must be configured with an X Window System server.

### About this task

An eDiscovery Manager server that runs on an AIX system uses an X Window System server with Motif to properly preview several kinds of vector-based documents, such as Portable Document Format (PDF), PowerPoint (PPT), and many Computer-Aided Design (CAD) files. An X Window System server is not needed for eDiscovery Manager servers that run on Windows systems.

The X Window System server must use a Motif-based window manager.

## Procedure

To install and set up an X Window System on a server:

1. Start the X Window System server.
2. Run the following command on the system where the eDiscovery Manager application server is running:  

```
export DISPLAY=X_Server:display_num.screen_num
```

where
  - *X\_Server* is the IP address or host name of the system running the X Window System server.
  - *display\_num* is the display number.
  - *screen\_num* is the screen number for the specified display.

The values for *display\_num* and *screen\_num* are typically 0 (zero), indicating the first display and the first screen on that display. In some cases, the DISPLAY environment variable might be set already. For example, if you log on to an AIX system from many X Window System server implementations, the DISPLAY environment variable is automatically set to the proper value for that session. If you start the eDiscovery Manager application server from that session, you do not need to set the DISPLAY value.

For example:

```
export DISPLAY=svr1.myhost.com:0.0
```

3. Start the eDiscovery Manager application server.

---

## Configuring viewing

IBM eDiscovery Manager users who are assigned the proper role can view the contents of a document or file that is displayed on the Search Results page of the eDiscovery Manager web client in one of several ways.

### Previewing

By clicking the document or file, the user can see a partial preview of the its content at the bottom of the Search Results pane. By double-clicking the document or file, the user can see a full-screen preview of the its content in a new browser window. No configuration is required to enable previewing.

### IBM Lotus iNotes viewing (HTTP)

The document or file is displayed in a new browser page by Lotus iNotes. Enable Lotus iNotes viewing on the Lotus Domino Settings pane of the Administration page of the eDiscovery Manager web client.

### Lotus Notes viewing

The document or file is displayed in the Lotus Notes client. Enable Lotus Notes viewing on the Lotus Domino Settings pane of the Administration page of the eDiscovery Manager web client and by configuring the Lotus Notes password manager.

### Microsoft Outlook viewing

The document or file is displayed in Microsoft Outlook with the content streamed directly to the browser on the user's system. If Microsoft Outlook is installed on the user's system, Microsoft Internet Explorer will start it automatically to view the document or file. No configuration is required to enable Microsoft Outlook viewing.



**Limitation:** Because of a limitation in Microsoft Internet Explorer, text attachments in languages that are read right to left, such as Hebrew and Arabic, are displayed from left to right.

**Plain text character limitation:** Before eDiscovery Manager can preview content other than email, it uses a set of libraries that were acquired from another vendor to convert the content to UTF-8 encoding in HTML format. Because plain text does not contain any encoding information, eDiscovery Manager is unable to determine the original encoding of plain text and is unable to correctly convert plain text that was not originally in UTF-8 encoding. If the plain text content was originally in UTF-8 encoding, then both ASCII and non-ASCII characters are displayed correctly. Otherwise, only ASCII characters are displayed correctly; non-ASCII characters cannot be displayed correctly.

## Configuring Lotus iNotes viewing

If you have documents in a collection that were Lotus Domino email before they were archived and you want your users to be able to open these documents with IBM Lotus iNotes, you must configure Lotus iNotes viewing.

### About this task

To configure Lotus iNotes viewing:

### Procedure

1. Verify that a Lotus Domino server is installed on the IBM eDiscovery Manager system.
2. Configure the Lotus Notes password manager to supply the password for the Lotus Notes user ID that eDiscovery Manager uses to the remote Lotus Domino server. (See the link to the instructions.)

If the Lotus Notes user ID for eDiscovery Manager does not have a password, you do not need to configure the password manager.

3. Enable the remote Lotus Domino server that hosts the viewing database for HTTP access.
4. Configure Lotus iNotes viewing on the Lotus Domino Settings pane of the Administration page of the eDiscovery Manager web client.

Be sure to enter an HTTP port number for the Lotus Domino server. Refer to the eDiscovery Manager web client's help system for complete information.

### Related tasks:

“Installing the Lotus Domino server” on page 36

To enable your users to export Lotus Notes content or to view content by using Lotus Notes, you must install the Lotus Domino server on the IBM eDiscovery Manager system. eDiscovery Manager requires only the Lotus Domino APIs, but these APIs are bundled with the Lotus Domino server; the APIs are not bundled separately. For this reason, you must install a Lotus Domino server on the eDiscovery Manager system or logical partition (LPAR), even though you do not start the server itself.



“Configuring the password manager for Lotus iNotes and Lotus Notes viewing” on page 116

When the Lotus Domino server that stores the Lotus Notes viewing database is accessed, IBM eDiscovery Manager must authenticate with the Lotus Domino environment. It does so by using a Lotus Notes ID file and having the Lotus Notes password manager programmatically supply the password for the eDiscovery Manager user ID. Configuring the eDiscovery Manager system to bypass the Lotus Domino password prompt is a prerequisite to your users successfully viewing email with IBM Lotus iNotes or Lotus Notes.

## Configuring Lotus Notes viewing

If you have content in a collection that originally came from Lotus Domino before it was archived and you want your users to be able to open this content with Lotus Notes, you must configure Lotus Notes viewing. IBM eDiscovery Manager creates a viewing database and assigns read access to eDiscovery Manager users, but you must configure other aspects of the viewing environment.

### Before you begin

To view content in the native application that created the content, a user must be assigned the Native Viewer role.

### Procedure

To configure Lotus Notes viewing:

1. Configure the Lotus Notes password manager to supply the password for the Lotus Notes user ID that eDiscovery Manager uses to the remote Lotus Domino server. (See the link to the instructions.)

If the Lotus Notes user ID for eDiscovery Manager does not have a password, you do not need to configure the password manager.

2. Configure Lotus Notes viewing on the Lotus Domino Settings pane of the Administration page of the eDiscovery Manager web client. Refer to the eDiscovery Manager web client's help system for complete information.
3. Ask your users to verify that their Lotus Notes environments are set up to access the eDiscovery Manager viewing database by having them open the database from their Lotus Notes clients. (This is the viewing database that you configured on the Lotus Domino Settings pane of the Administration page of the eDiscovery Manager web client.)

The database will not contain any email yet, but your users should be able to open the database for viewing.

### Related tasks:

“Installing the Lotus Domino server” on page 36

To enable your users to export Lotus Notes content or to view content by using Lotus Notes, you must install the Lotus Domino server on the IBM eDiscovery Manager system. eDiscovery Manager requires only the Lotus Domino APIs, but these APIs are bundled with the Lotus Domino server; the APIs are not bundled separately. For this reason, you must install a Lotus Domino server on the eDiscovery Manager system or logical partition (LPAR), even though you do not start the server itself.

“Configuring the password manager for Lotus iNotes and Lotus Notes viewing”  
When the Lotus Domino server that stores the Lotus Notes viewing database is accessed, IBM eDiscovery Manager must authenticate with the Lotus Domino environment. It does so by using a Lotus Notes ID file and having the Lotus Notes password manager programmatically supply the password for the eDiscovery Manager user ID. Configuring the eDiscovery Manager system to bypass the Lotus Domino password prompt is a prerequisite to your users successfully viewing email with IBM Lotus iNotes or Lotus Notes.

## Configuring the password manager for Lotus iNotes and Lotus Notes viewing

When the Lotus Domino server that stores the Lotus Notes viewing database is accessed, IBM eDiscovery Manager must authenticate with the Lotus Domino environment. It does so by using a Lotus Notes ID file and having the Lotus Notes password manager programmatically supply the password for the eDiscovery Manager user ID. Configuring the eDiscovery Manager system to bypass the Lotus Domino password prompt is a prerequisite to your users successfully viewing email with IBM Lotus iNotes or Lotus Notes.

### About this task

If you configure your Lotus Domino environment with a server ID file or a Lotus Notes user ID file that does not have a password set, then you do not need to configure the Lotus Notes password manager. If you already configured the password manager while you configured export, you do not need to configure it again. These instructions are the same as the instructions for configuring the password manager for export.

**Important:** Configure password manager on the eDiscovery Manager system, not on the Lotus Domino server.

To configure the Lotus Notes password manager on the eDiscovery Manager system:

### Procedure

1. Ensure that the following file is in the `lib` subdirectory of the eDiscovery Manager installation directory.

Operating system	File
AIX	<code>liblotuspwmgr.a</code>
Windows	<code>LotusPWMgr.dll</code>

2. Verify that the eDiscovery Manager system environment is properly configured for Lotus Domino:

**AIX** Verify that the AIX steps are completed in Installing the Lotus Domino server.

#### Windows

Verify that the PATH system variable contains the settings:

- The PATH system variable must contain the path to the Lotus Domino executable directory. For example, add: `C:\Program Files\Lotus\Domino`.

- The PATH system variable must contain the path to the notesdata directory that contains the notes.ini file. You created this notesdata directory when you installed the Lotus Domino server.
3. If you made any of changes in the previous step, stop and restart the eDiscovery Manager application server for your changes to take effect.
  4. Update the notes.ini file for the Lotus Domino server on the eDiscovery Manager system.
    - a. Add the following lines to the notes.ini file that you created when you installed the Lotus Domino server.

#### AIX

```
EXTMGR_ADDINS=liblotuspwmgr.a
EDMLotusPWMgrPasswordFile=/opt/IBM/eDM/resources/LotusPWMgr.ini
EDMLotusPWMgrLogFile=/opt/IBM/eDM/logs/LotusPWMgr.log
```

**Important:** Modify the paths if you did not install eDiscovery Manager in the default location.

#### Windows

```
EXTMGR_ADDINS=LotusPWMgr.dll
EDMLotusPWMgrPasswordFile=C:\Program Files\IBM\eDM\resources\
  LotusPWMgr.ini
EDMLotusPWMgrLogFile=C:\Program Files\IBM\eDM\logs\LotusPWMgr.log
```

**Important:** Modify the paths if you did not install eDiscovery Manager in the default location.

- b. Specify the Lotus Notes user ID file for the Lotus Notes user that is used to connect to the remote Domino server:

#### user notes.ini file

Set the KeyFileName parameter to equal the user ID file.

#### server notes.ini file

Set both the KeyFileName and the ServerKeyFileName parameters to equal the user ID file.

5. Set the password of the Lotus Notes user ID for eDiscovery Manager on the eDiscovery Manager system.
  - a. Open the LotusPWMgr.ini file in a text editor.
 

This file is in the resources subdirectory of the eDiscovery Manager installation directory.
  - b. Enter the password that is used to access the remote Lotus Domino server.
 

This password corresponds to the Lotus Notes user ID for eDiscovery Manager, which you specified for the KeyFileName parameter in the notes.ini file.
  - c. Save and close the file.

The password can be stored in clear text because the first time that the password manager initializes, it encrypts the password in the file.

6. Test the password manager on the eDiscovery Manager system in one of the following ways.
  - Run the eDiscovery Manager utility notesConnect.
    - a. Go to the bin subdirectory of the eDiscovery Manager installation directory. For example:

#### AIX

```
cd /opt/IBM/eDM/bin/
```

## Windows

```
cd C:\Program Files\IBM\eDM\bin
```

- b. Enter the following command, which uses the notesConnect utility to connect to the remote Lotus Domino server, and return the title from the specified database. The utility uses the Lotus Notes user ID that is configured for the KeyFileName setting in the notes.ini file.

```
notesConnect database_name [Lotus_Domino_server]
```

where:

- *database\_name* is the name of the database whose title to return, for example, names.nsf.
- *Lotus\_Domino\_server* is the IP address or IP name of the remote Lotus Domino server.

If the password prompt does not open and the database title is successfully returned, the password manager is configured correctly.

Also, check the LotusPwMgr.log file on your system for the message Successfully retrieved password.

- On AIX, the default location of the LotusPwMgr.log file is /opt/IBM/eDM/logs/.
- On Windows, the default location of the LotusPwMgr.log file is C:\Program Files\IBM\eDM\logs\.

- Start the eDiscovery Manager web client, perform a search to return Lotus Notes content, and click the **View this content with Lotus Notes** icon.

If the password prompt does not open and you can successfully view the content, the password manager is configured correctly. You can also check the LotusPwMgr.log file for the message Successfully retrieved password.

## Results

**Important:** The notes.ini file that password manager reads is the one that is listed first in the system's PATH environment variable. Make sure that the notes.ini file that you created when you installed Lotus Domino is the first notes.ini file in the PATH.

### Related tasks:

“Installing the Lotus Domino server” on page 36

To enable your users to export Lotus Notes content or to view content by using Lotus Notes, you must install the Lotus Domino server on the IBM eDiscovery Manager system. eDiscovery Manager requires only the Lotus Domino APIs, but these APIs are bundled with the Lotus Domino server; the APIs are not bundled separately. For this reason, you must install a Lotus Domino server on the eDiscovery Manager system or logical partition (LPAR), even though you do not start the server itself.

“Installing the Lotus Domino server” on page 55

To enable your users to export Lotus Notes content or to view content by using Lotus Notes, you must install the Lotus Domino server on the IBM eDiscovery Manager system. eDiscovery Manager requires only the Lotus Domino APIs, but these APIs are bundled with the Lotus Domino server; the APIs are not bundled separately. For this reason, you must install a Lotus Domino server on the eDiscovery Manager system or logical partition (LPAR), even though you do not start the server itself.

### Related information:

 WebSphere Application Server Version 7.0 - Starting and stopping quick reference

## Configuring export

Configure export to allow IBM eDiscovery Manager users to export selected content for external review or storage.

### eDiscovery Manager web client configuration

The eDiscovery Manager web client is your primary export configuration tool. Before your users can export content, you must configure exports on the following panes of the Administration page of the eDiscovery Manager web client.

- User Roles

An eDiscovery Manager Super User must assign the Exporter user role to users to permit them to export content.

- Export Settings

Export settings include the absolute path or, in some circumstances, Universal Naming Convention (UNC) path of the export directory, the maximum number of simultaneous export tasks that you want eDiscovery Manager to support, and the maximum number of threads to allocate for all export tasks.

**Important:** WebSphere Application Server might not be able to locate mapped network drives in Microsoft Windows under certain circumstances. Because of how permissions are assigned to mapped network drives, not all users are able to access these drives through the drive letters. Only the services owned by the Local System Account can map network drives that can be seen by all other accounts. In this case, you must configure the path of the directory that will contain all exported content as a UNC path.

- Export Formats

You can configure the content export formats that eDiscovery Manager provides, or you can create and configure new content export formats. Be sure to configure the plug-in properties of the Extract and BatchComplete plug-in points for all formats to which your users will want to export.

### Syntax for the export file name

When you export Content Collector files or when you export multipart documents in custom collections, the names of the export files depend on whether the collection definition includes a FILE\_NAME collection field.

If a FILE\_NAME collection field is included in the collection, content in that collection is exported to files that have names with the following syntax where *originalFileName* is the original name of the archived file:

*originalFileName\_itemID\_or\_GUID.extension*

If a FILE\_NAME collection field is not included in the collection, content in that collection is exported to files that have names with the following syntax:

*itemID\_or\_GUID.extension*


To verify whether a FILE\_NAME collection field is included in a collection of custom or Content Collector file types, check the **Search Mapping** tab on the Collections pane of the Administration page. For these types of collections,

mapping the relevant content server property or attribute to a collection field that is named FILE\_NAME can be useful.

## Configuring PDF export

To enable users to successfully export content to PDF, you must configure some PDF font settings.

### AIX true type font directory

 If you want your users to be able to export content to PDF, you must set the TRUETYPEFONTDIR environment variable to a directory that contains true type fonts.

### Font substitution

Ensure that the same fonts that are used on the computer where the content was created are present in the eDiscovery Manager server font directory. If the eDiscovery Manager server does not contain the fonts that are used in the input file, another font is substituted in the PDF. Font substitution can cause text to overlap.

### Arial Unicode MS font required for non-Latin-1 characters

To ensure that characters from the non-Latin-1 character set are properly converted when they are exported to PDF, ensure that the Arial Unicode MS font is installed on the IBM eDiscovery Manager server. Also ensure that the MS Mincho font is not installed.

### PDF rendering results

The export to PDF does not always produce results that are identical to the original documents and is designed to produce a readable version of the output. If you require the exact formatting from the original documents, export the documents in their native format and view them in the original application instead of exporting to PDF.

**Important:** When a document is exported to a nonnative format it does not retain the format in the original document that was stored on the server. This may cause a document to look different when it is viewed.

## PST export configuration of Exchange emails

By default, Exchange emails are exported to PST format.

In previous releases of eDiscovery Manager, Exchange emails were exported to individual .msg files. New to this release, Exchange emails are exported to .pst files, with each pst file containing all of the Exchange emails for one batch.

For example, if you export several thousand Exchange emails and specify the output file prefix 'myExchangeEmails', the emails will be exported to myExchangeEmails\_batch0.pst, myExchangeEmails\_batch1.pst, and so forth. If you want to change this new default behavior and export to .msg files (as in previous eDiscovery Manager releases), modify the 'Native' export format in the eDiscovery

Manager Administration panel. In the NativeBatchCompletePlugin plugin parameters, change the value of parameter PST.Package.Msg.Files.To.PST from 'true' to 'false'.

When exporting Exchange emails, Microsoft Outlook is not required on the eDiscovery Manager system; however you will need Microsoft Outlook to view the exported PST files. The exported PST files can be viewed only with Microsoft Outlook 2007.

## Configuring Lotus Notes export

If you want your users to be able to export Lotus Notes content, you must configure Lotus Notes export. IBM eDiscovery Manager creates export databases and assigns read access to those eDiscovery Manager users that are assigned permission to export, but you must configure other aspects of the export environment.

### Procedure

To configure Lotus Notes export:

1. Configure the Lotus Notes password manager to supply the password for the Lotus Notes user ID that eDiscovery Manager uses to the remote Lotus Domino server. (See the link to the instructions.)

If the Lotus Notes user ID for eDiscovery Manager does not have a password, you do not need to configure the password manager.

2. On the User Roles pane of the Administration page, make sure the proper users are assigned an eDiscovery Manager user role that permits them to export content.
3. Configure the Native content export format on the Export Formats pane of the Administration page of the eDiscovery Manager web client.

Configure the Native content export format so that your users can export Lotus Notes email to Lotus Domino databases (NSF files). At a minimum, you must add the Lotus Domino server name and database template name on the Lotus Domino Settings pane of the Administration page. You can optionally configure other aspects of Lotus Notes exports with the plug-in parameters of the BatchComplete point for the Native export format. Refer to the help system in the eDiscovery Manager web client for complete information.

4. Verify that Lotus Notes export is configured properly by exporting content from the eDiscovery Manager web client and then validating that the export task is successful from the Tasks pane of the Case Information page.

**Tip:** To aid in troubleshooting, set the value of the Logging.mode plug-in parameter of the Native content export format to DEBUG before exporting any content. For information about the export task, check the dominoExport.log file, which is in the logs subdirectory of the eDiscovery Manager installation directory, by default. After you verify that your content is successfully being exported to your Lotus Domino server, change the value from DEBUG to ERROR for production usage to prevent the dominoExport.log file from growing.

When the locale of the user ID for the eDiscovery Manager application server is set to a multi-byte language, such as Japanese or Chinese, it is important that the locale supports Unicode (UTF-8). Otherwise, you might encounter problems when exporting email to Lotus Domino. For example, to enable Unicode support for Japanese on AIX, set export LANG=jp\_JP.UTF-8 in the .profile file for the user ID.



## What to do next

**Attention:** Be aware that Lotus Notes limits the maximum size of a database. If you configure eDiscovery Manager with no limit on the size of the export database and the database subsequently exceeds the Lotus Notes limitation during an export, the export task completes with errors. Large email attachments can also cause Lotus Domino export databases to exceed the limit set by the **Maximum.size.of.export.database plug-in** parameter. You can resolve this problem by specifying a value up to 4096 for the **Maximum.size.of.export.database** plug-in parameter and then restarting the export task. To limit the size of the export database, specify a value no larger than 4096. To let the export database grow without limit, specify a value no smaller than 4300.

## Configuring the password manager for Lotus Notes export

When accessing the Lotus Domino server that stores the Lotus Notes export databases, IBM eDiscovery Manager must authenticate with the Lotus Domino environment. It does so by using a Lotus Notes ID file and having the Lotus Notes password manager programmatically supply the password for the eDiscovery Manager user ID. Configuring the eDiscovery Manager system to bypass the Lotus Domino password prompt is a prerequisite to your users successfully exporting content to Lotus Notes databases.

### About this task

If you configure your IBM Lotus Domino environment with a server ID file or with a Lotus Notes user ID for eDiscovery Manager that does not have a password, you do not need to configure the Lotus Notes password manager. If you already configured the password manager in the process of configuring viewing, you do not need to configure it again. These instructions are the same as those for configuring password manager for viewing.

**Important:** Configure password manager on the eDiscovery Manager system, not on the Lotus Domino server.

To configure the Lotus Notes password manager on the eDiscovery Manager system:

### Procedure

1. Ensure that the following file is in the `lib` subdirectory of the eDiscovery Manager installation directory.

Operating system	File
AIX	<code>liblotuspwmgr.a</code>
Windows	<code>LotusPWMgr.dll</code>

2. Verify that the eDiscovery Manager system environment is properly configured for Lotus Domino:

**AIX** Verify that the AIX steps are completed in Installing the Lotus Domino server.

#### Windows

Verify that the PATH system variable contains the settings:



- The PATH system variable must contain the path to the Lotus Domino executable directory. For example, add: C:\Program Files\Lotus\Domino.
  - The PATH system variable must contain the path to the notesdata directory that contains the notes.ini file. You created this notesdata directory when you installed the Lotus Domino server.
3. If you made any of changes in the previous step, stop and restart the eDiscovery Manager application server for your changes to take effect.
  4. Update the notes.ini file for the Lotus Domino server on the eDiscovery Manager system.
    - a. Add the following lines to the notes.ini file that you created when you installed the Lotus Domino server.

#### AIX

```
EXTMGR_ADDINS=liblotuspwmgr.a
EDMLotusPWMgrPasswordFile=/opt/IBM/eDM/resources/LotusPWMgr.ini
EDMLotusPWMgrLogFile=/opt/IBM/eDM/logs/LotusPWMgr.log
```

**Important:** Modify the paths if you did not install eDiscovery Manager in the default location.

#### Windows

```
EXTMGR_ADDINS=LotusPWMgr.dll
EDMLotusPWMgrPasswordFile=C:\Program Files\IBM\eDM\resources\
  LotusPWMgr.ini
EDMLotusPWMgrLogFile=C:\Program Files\IBM\eDM\logs\LotusPWMgr.log
```

**Important:** Modify the paths if you did not install eDiscovery Manager in the default location.

- b. Specify the Lotus Notes user ID file for the Lotus Notes user that is used to connect to the remote Domino server:

#### user notes.ini file

Set the KeyFilename parameter to equal the user ID file.

#### server notes.ini file

Set both the KeyFileName and the ServerKeyFileName parameters to equal the user ID file.

5. Set the password of the Lotus Notes user ID for eDiscovery Manager on the eDiscovery Manager system.
  - a. Open the LotusPWMgr.ini file in a text editor.  
This file is in the resources subdirectory of the eDiscovery Manager installation directory.
  - b. Enter the password that is used to access the remote Lotus Domino server.  
This password corresponds to the Lotus Notes user ID for eDiscovery Manager, which you specified for the KeyFileName parameter in the notes.ini file.
  - c. Save and close the file.

The password can be stored in clear text because the first time that the password manager initializes, it encrypts the password in the file.

6. Test the password manager on the eDiscovery Manager system in one of the following ways.
  - Run the eDiscovery Manager utility notesConnect.
    - a. Go to the bin subdirectory of the eDiscovery Manager installation directory. For example:

## AIX

```
cd /opt/IBM/eDM/bin/
```

## Windows

```
cd C:\Program Files\IBM\eDM\bin
```

- b. Enter the following command, which uses the notesConnect utility to connect to the remote Lotus Domino server, and return the title from the specified database. The utility uses the Lotus Notes user ID that is configured for the KeyFileName setting in the notes.ini file.

```
notesConnect database_name [Lotus_Domino_server]
```

where:

- *database\_name* is the name of the database whose title to return, for example, names.nsf.
- *Lotus\_Domino\_server* is the IP address or IP name of the remote Lotus Domino server.

If the password prompt does not open and the database title is successfully returned, the password manager is configured correctly.

Also, check the LotusPWMgr.log file on your system for the message Successfully retrieved password.

- On AIX, the default location of the LotusPWMgr.log file is /opt/IBM/eDM/logs/.
  - On Windows, the default location of the LotusPWMgr.log file is C:\Program Files\IBM\eDM\logs\.
- Start the eDiscovery Manager web client, perform a search to return Lotus Notes content, and click the **View this content with Lotus Notes** icon.

If the password prompt does not open and you can successfully view the content, the password manager is configured correctly. You can also check the LotusPWMgr.log file for the message Successfully retrieved password.

## Results

**Important:** The notes.ini file that password manager reads is the one that is listed first in the system's PATH environment variable. Make sure that the notes.ini file that you created when you installed Lotus Domino is the first notes.ini file in the PATH.

### Related tasks:

“Installing the Lotus Domino server” on page 36

To enable your users to export Lotus Notes content or to view content by using Lotus Notes, you must install the Lotus Domino server on the IBM eDiscovery Manager system. eDiscovery Manager requires only the Lotus Domino APIs, but these APIs are bundled with the Lotus Domino server; the APIs are not bundled separately. For this reason, you must install a Lotus Domino server on the eDiscovery Manager system or logical partition (LPAR), even though you do not start the server itself.

“Installing the Lotus Domino server” on page 55

To enable your users to export Lotus Notes content or to view content by using Lotus Notes, you must install the Lotus Domino server on the IBM eDiscovery Manager system. eDiscovery Manager requires only the Lotus Domino APIs, but these APIs are bundled with the Lotus Domino server; the APIs are not bundled separately. For this reason, you must install a Lotus Domino server on the eDiscovery Manager system or logical partition (LPAR), even though you do not start the server itself.

## Disabling the ability to specify a fully qualified export directory

You can prevent users from entering a fully qualified path for exporting documents or saving a CSV file. When the fully qualified path is disabled, users must enter a directory name that is relative to the export directory that the administrator configured. By default, users can enter a fully qualified path or a relative path.

### About this task

### Procedure

To disable the ability to specify a fully qualified path:

1. Use a text editor to open the `ral.properties` file.

Option	Description
AIX	/opt/IBM/eDM/config/ral.properties
Windows	C:\Program Files\IBM\eDM\config\ral.properties

2. Add the following line to the file:  
`AllowFullyQualifiedExportDirectory=false`
3. Save your changes and close the file.
4. Stop and restart the server.

### What to do next

If you later decide to allow fully qualified paths, then open the file again and change the value for **AllowFullyQualifiedExportDirectory** to true, or delete the entire line from the file. You must restart the server for the change to take effect.

## Using short names for directories and files

On Microsoft Windows systems, the maximum length of a file path is limited to 254 characters and for IBM Lotus Domino export databases, the maximum length of a file path is limited to 109 bytes. Avoid problems with these limitations by configuring a short name for the export directory. Also advise your users to specify short names for their export file name prefixes and export subdirectories. These limitations also apply to the directories and file names for saving content to a CSV file.

### Windows

### About this task

When IBM eDiscovery Manager exports email attachments temporarily to the export directory, the path of each attachment consists of the following components:  
*export\_directory\_path/BatchN/Attachments/GUID\_or\_itemID/attachment\_file\_name*

If the absolute path of an exported email attachment exceeds the Windows limit of 254 characters, the file name of the attachment might be truncated. If the file path for the Lotus Domino export database exceeds 109 bytes, the export of the file will fail with an error message that states the path must be shortened. If truncating the

attachment file name does not reduce the path of the exported email attachment, then the attachment might not be exported successfully and the **Errors** count on the export task is increased by 1.

**Recommendation for IT Administrators:**

- On the Export Settings pane of the Administration page, enter as short a path as possible for the export directory. (The path can be up to 120 characters in length.)
- On the Export Formats pane of the Administration page, select the Native export format. Under the list of BatchComplete plug-ins, edit the NativeBatchCompletePlugin. At the Modify Plug-in panel, select the Lotus.Domino.server.export.directory plug-in parameter and reduce the length of its value.

**Recommendations for users who can export content:**

- In the Export Content window, reduce the length of the **Export directory** field value, the **Export file name prefix** field value, or both. (The prefix can be up to 120 characters in length.)

**Recommendations for users who can save search and folder content:**

- In the Save the Data in All Rows and Columns to a CSV File window, reduce the length of the **Directory name for saved CSV file** field value, the **File name prefix** field value, or both. (The prefix can be up to 120 characters in length.)

## EDRM XML plug-in and output compression limitations

IBM eDiscovery Manager provides a plug-in that enables selected users to export documents to EDRM (Electronic Discovery Reference Model) XML files. This plug-in compresses all of the extracted files into a ZIP file if an IT Administrator sets the value of the Create.ZIP.file plug-in parameter for the BatchComplete point of the plug-in to TRUE. The default value is FALSE. The following compression utility limitations exist when the Create.ZIP.file plug-in parameter value is TRUE.

### Long file names

Not all compression utilities can correctly handle long file names (for example, over 100 characters). The EDRM export generated ZIP file might include a file that has a long name. When you open the compressed file, you might see errors like the following message:

```
Compressed (zipped) Folders Error
The Compressed (zipped) Folder is invalid or corrupted.
```

If you have documents with long file names, be sure that you have a ZIP file decompression utility that can correctly handle long file names.

**Recommendation:** In our testing, 7-Zip provided the best support for opening and decompressing ZIP files that contain files with long file names.

### Accented characters

Not all compression utilities can correctly handle file names that include accented characters. The EDRM export generated ZIP file might include a file whose name contains accented characters. When you open the compressed file, the file name might be garbled or corrupted, depending on the utility that you use for decompression.

This can be a problem for users that export documents because the users can specify a prefix for export files. And when exporting Lotus Domino documents, users **must** specify a prefix for export files.

**Recommendation:** If you want your users to be able to use accented characters in export file prefixes, set the value of the Create.ZIP.file plug-in parameter to FALSE. Otherwise, advise your users not to use accented characters when they enter export file prefixes.

### File name encoding

If the names of any compressed files or attachments are not UTF encoded, the ZIP file that is created by the EDRM XML plug-in must be opened on a system that has the same encoding as the eDiscovery Manager system where the ZIP file was created. If the systems do not have the same encoding, the names of the files or attachments that were not UTF encoded are not displayed correctly.

---

## Configuring email notifications

Configure email notifications if you want to be able to alert your users when IBM eDiscovery Manager tasks start and finish. Work with your mail server administrator to configure the mail session settings by using the IBM WebSphere Application Server administrative console.

### About this task

When eDiscovery Manager is installed, a WebSphere mail session called EDMMailSession is automatically created. Provide values for the fields in the **Outgoing Mail Properties** section only if you want to enable email notifications. (Use the WebSphere Administrative Console to access the outgoing mail properties settings in **Resources > Mail > Mail Sessions > EDMMailSession > Outgoing Mail Properties**. The exact property names are dependent upon your WebSphere Application Server version and might be different from the settings in this example.) Then, restart WebSphere Application Server.

**Important:** Ensure that you specify a return email address for each email notification. If a return email address is not specified, the email notification will not work.

**Tip:** Set the value of the return email address field to the email address of the eDiscovery Manager administrator in case an eDiscovery Manager user responds to an email notification.

### Related information:

 Mail session configuration settings on the WebSphere Application Server Version 8.0 administrative console

 Mail session configuration settings on the WebSphere Application Server Version 7.0 administrative console

---

## Configuring eDiscovery Manager to connect to FileNet P8 by using the Web Services Interface (WSI) transport method

Sites that deploy IBM FileNet P8 in environments that are not based on WebSphere technology typically need to be connected by using WSI.

## About this task

To configure IBM eDiscovery Manager to connect to FileNet P8 by using the WSI transport method:

### Procedure

1. Confirm that the Java Virtual Machine (JVM) properties for the eDiscovery Manager application server are set to:  
`-Djava.security.auth.login.config=eDM_install_directory/config/jaas.conf.WSI`
2. Confirm that the `ral.properties` file contains the following parameter values. The `ral.properties` configuration file is installed in the `config` subdirectory of the eDiscovery Manager installation directory.  
`p8Uri=http://server_host_address:port/wsi/FNCEWS40MTOM/`  
`p8Protocol=FileNetP8WSI`  
  
**Note:** Depending on whether you installed eDiscovery Manager by using the HTTP or HTTP Secure (HTTPS) protocol, the `P8Uri` value can start with `"http://"` or `"https://"`.
3. If eDiscovery Manager is installed on the same system as FileNet P8, set the JVM custom property for the Object Request Broker (ORB), `com.ibm.websphere.orb.uniqueServerName`, to `True`.
  - a. In the WebSphere Application Server administrative console, click **Servers > Application Servers > server\_name > Java and Process Management > Process Definition > Java Virtual Machine > Custom Properties > New**.
  - b. On the Custom Properties settings page, define the custom property by entering `com.ibm.websphere.orb.uniqueServerName` for the name and `TRUE` for the value.
  - c. Click **OK**, then click **Save** on the console task bar.
4. Stop and restart the WebSphere Application Server.

### Related information:

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

---

## Configuring eDiscovery Manager to use SSL to connect to FileNet P8

Enabling Secure Sockets Layer (SSL) provides secure communication between eDiscovery Manager and FileNet P8.

### Before you begin

Ensure that FileNet P8 Content Engine or Content Platform Engine is configured to use SSL.

### Procedure

To configure SSL to connect to FileNet P8:

1. Create a client self-signed certificate, keystore, and SSL configuration in the `ssl.client.props` file for eDiscovery Manager:

- a. On the eDiscovery Manager server, open a command prompt and change to the `/WAS_Home/AppServer/profiles/AppSrv_name/bin` directory.
- b. Run the following command:

```
retrieveSigners.bat remoteKeyStoreName localKeyStoreName -host host_name
                    -port port_number -username admin_user -password admin_password
```

**remoteKeyStoreName**

The name of a truststore that is in the Content Engine or Content Platform Engine server from which to retrieve the signers. This parameter is typically the `CellDefaultTrustStore` file for a managed environment or the `NodeDefaultTrustStore` file for an unmanaged environment.

**localKeyStoreName**

The name of the truststore that is in the `ssl.client.props` file for the eDiscovery Manager profile. This parameter is typically the `ClientDefaultTrustStore` file for either a managed or unmanaged environment.

**host\_name**

The host name of the Content Engine or Content Platform Engine server from which the signers are retrieved.

**port\_number**

The Content Engine or Content Platform Engine server SOAP port.

**admin\_user**

The FileNet P8 administrative user.

**admin\_password**

The FileNet P8 administrative user password.

**Example output:**

```
CWPKI0308I: Adding signer alias "default_1" to local keystore
"AnotherTrustStore" with the following SHA digest:
B0:7A:23:DF:8D:B8:EC:BE:23:EA:00:6A:26:A2:D4:47:00:E4:52:F2
```

2. Copy the local truststore file, usually named `trust.p12`, from the `/WAS_Home/AppServer/profiles/profile_name/etc` directory to the `/WAS_Home/AppServer/profiles/profile_name/config/cells/cell_name/nodes/node_name` directory.
3. Use the WebSphere Application Server administration tool to enable SSL and point to the `localKeyStoreName` keystore.
4. Stop and restart the application server.

**Related tasks:**

“Enabling secure cookies” on page 130

You can enhance the security of an IBM eDiscovery Manager system that already uses HTTPS by also enabling secure cookies for it.

**Related information:**

 [WebSphere Application Server Version 7.0 - Creating a Secure Sockets Layer configuration](#)

 [WebSphere Application Server Version 8.0 - Creating a Secure Sockets Layer configuration](#)



---

## Enabling secure cookies

You can enhance the security of an IBM eDiscovery Manager system that already uses HTTPS by also enabling secure cookies for it.

### About this task

If your eDiscovery Manager system has enabled HTTPS for secure communications, you can further increase system security by also enabling secure cookies in the IBM WebSphere Application Server that hosts your eDiscovery Manager instance.

### Procedure

1. Open the WebSphere Application Server administrative console by clicking **Start > Programs > IBM WebSphere > Application Server > Profiles > eDiscovery Manager application server profile > Administrative console**.
2. Expand **Applications, Enterprise Applications, EDMClient** and **Session management**.
3. Click **Enable Cookies**.
4. Select **Restrict cookies to HTTPS sessions**.
5. After saving these settings, stop and restart the eDiscovery Manager application server instance in WebSphere Application Server.

#### Related tasks:

“Configuring eDiscovery Manager to use SSL to connect to FileNet P8” on page 128

Enabling Secure Sockets Layer (SSL) provides secure communication between eDiscovery Manager and FileNet P8.

#### Related reference:

“Starting and stopping the eDiscovery Manager server” on page 68

IBM eDiscovery Manager uses the application server instance in the IBM WebSphere Application Server that you specified during the eDiscovery Manager installation. From time to time, you need to stop and restart this application server instance.

#### Related information:

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

---

## Configuring IBM eDiscovery Manager to open and save compressed attachments

Open and save compressed attachments in their native format.

### About this task

By default, when you click a link in eDiscovery Manager to open an attachment, the attachment is displayed in HTML. If you want to open and save attachments in their native format, you must edit the defaultAttachConversionFormat property in the <EDM\_HOME>\config directory\docviewer.config file.

To edit the docviewer.config file:



## Procedure

1. Open the <EDM\_HOME>\config directory\docviewer.config file.
2. Search for defaultAttachConversionFormat=0
3. Change defaultAttachConversionFormat=0 to defaultAttachConversionFormat=1, then save the file.
4. Restart the eDiscovery Manager application server. Document attachments can now be viewed and saved in their native format.

---

## Adding FileNet P8 version 4.5.1 servers

You can add one or more FileNet P8 Version 4.5.1 servers to your eDiscovery Manager system after you specified version 5.0. or later during the initial installation.

## Procedure

To add FileNet P8 version 4.5.1 servers:

1. Use a text editor to open the *EDM\_HOME/scriptsWAS/appdeploy.properties* file.
2. Change the entry *p8EnableV451=FALSE* to *p8EnableV451=TRUE*.
3. Save your changes and close the file.
4. Copy all files in the *EDM\_HOME/P8\_V451/lib* directory to the *EDM\_HOME/lib* directory.
5. Copy all files in the *EDM\_HOME/P8\_V451/config* directory to the *EDM\_HOME/config* directory.
6. Copy all files in the *EDM\_HOME/P8\_V451/lib* directory to the *WAS\_HOME/profiles/profile\_name/installedApps/node\_cell/EDMClient.ear/EDCConsole.war/WEB-INF/lib* directory.
7. Copy all files in the *EDM\_HOME/P8\_V451/lib* directory to the *WAS\_HOME/profiles/profile\_name/installedApps/node\_cell/EDMWorkMgrServer.ear/EDMWorkMgrServer.war/WEB-INF/lib* directory.

---

## Configuring single sign-on support

Single sign-on (SSO) support enables users to log in only once and access both IBM eDiscovery Manager and the content servers. To enable SSO, you must first enable SSO code in the *web.xml* file for eDiscovery Manager.

## Before you begin

**FileNet P8** You can use SSO in IBM FileNet P8 environments only if you use Internet Inter-ORB Protocol (IIOP) to connect the eDiscovery Manager server to your FileNet P8 servers. You cannot use SSO if you use the Web Services Interface (WSI) transport method to connect eDiscovery Manager to FileNet P8 servers.

## About this task

To set up single sign-on:

## Procedure

1. Create a temporary directory and copy the *EDM\_Home\dist\EDCConsole.ear* file to the temporary directory.

2. Edit the WEB-INF/web.xml file that is contained in the EDCCConsole.ear file in the temporary directory.
  - a. Extract the EDCCConsole.war file from the EDCCConsole.ear file by running the following command:
 

```
WAS_HOME\java\bin\jar -xvf EDCCConsole.ear EDCCConsole.war
```
  - b. Extract the web.xml file from the EDCCConsole.war file by running the following command:
 

```
WAS_HOME\java\bin\jar -xvf EDCCConsole.war WEB-INF/web.xml
```
  - c. In the web.xml file, remove the comments around the portion of code labeled Enable SSO:
 

```
<!-- Enable SSO
<context-param>
  <description></description>
  <param-name>isSSOEnabled</param-name>
  <param-value>true</param-value>
</context-param>

...

<security-role>
  <description></description>
  <role-name>AllAuthenticated</role-name>
</security-role>

-->
```
  - d. Add the revised web.xml file to the EDCCConsole.war file by running the following command:
 

```
WAS_HOME\java\bin\jar -uvf EDCCConsole.war WEB-INF/web.xml
```
  - e. Add the EDCCConsole.war file to the EDCCConsole.ear file by running the following command:
 

```
WAS_HOME\java\bin\jar -uvf EDCCConsole.ear EDCCConsole.war
```
3. Manually redeploy the EDMConsole.ear file by running eDiscovery Manager WebSphere Application Server scripts. The scripts are provided in the EDM\_Home\scriptsWAS directory.
  - a. Create a backup of the EDM\_Home\dist\EDCCConsole.ear file.
  - b. Copy the EDCCConsole.ear file that was revised in step 2 from the temporary directory to the EDM\_Home\dist directory, overwriting the existing EDCCConsole.ear file.
  - c. On Windows systems only: Edit the EDM\_Home\scriptsWAS\edMAppConfig.bat file as follows. These changes keep the command window open when you redeploy so that you can monitor the deployment process.
    - Change exit 0 to rem exit 0
    - Change exit %rc% to echo %rc%
  - d. Deploy eDiscovery Manager from the command line. To capture console log messages, redirect the output of the deployment command to a log file. For example, to deploy eDiscovery Manager to a secure WebSphere Application Server, run the following commands:
    - On AIX: edMAppConfig.sh install WAS\_admin\_username WAS\_admin\_password >> output.log
    - On Windows: edMAppConfig.bat install WAS\_admin\_username WAS\_admin\_password >> output.log
4. Map the security role and enable the security service for the work manager in the eDiscovery Manager profile.

- a. Open the WebSphere Application Server administrative console by clicking **Start > Programs > IBM WebSphere > Application Server > Profiles > eDiscovery Manager application server profile > Administrative console**.
  - b. Click **Application > Enterprise Application > EDMConsole**.
  - c. Under Detail properties, click **Security role to user/group mapping**.
  - d. Select the AllAuthenticated role and enable **All authenticated**.
  - e. Apply and save this change.
  - f. Click **Resources > Asynchronous beans > Work managers**.
  - g. Select **EDMClientWorkManager**.
  - h. In the Service names section of General Properties, select **Security**.
  - i. Apply and save this change.
5. Stop and restart the WebSphere Application Server application server instance for eDiscovery Manager.

## What to do next

Configure the connections between eDiscovery Manager and the content servers in the content management system.

- Configuring the connection between the eDiscovery Manager system and the FileNet P8 system
- Configuring the connection between the eDiscovery Manager system and the Content Manager EE system

---

## Configuring IBM eDiscovery Manager to access documents in different IBM Content Manager item types

This topic outlines the steps that you can follow to configure IBM eDiscovery Manager to access documents that were archived into different IBM Content Manager item types based on the document date.

### Before you begin

Ensure that you created the new item types and appropriately configured IBM Content Collector. See related links for reference in IBM Content Collector documentation.

### About this task

Archiving documents into different item types can improve performance and help to reduce the risk of the index becoming corrupted.

### Procedure

1. Log in to IBM eDiscovery Manager and go to **Administration**.
2. Select **Collections**.
3. Expand your selected collection.
4. Click **Item Types**.
5. Click on **Add an Item Type** and specify the new item type that was created in IBM Content Collector.
6. Save the settings.

#### Related tasks:

Installing Content Collector

#### Related information:



IBM FileNet P8 Platform Performance Tuning Guide

Download the PDF from the FileNet P8 Platform Technical Notices table in this FileNet P8 Product Documentation page.

Configuring Content Collector

---

## Configuring eDiscovery Manager to work with eDiscovery Analyzer

Ensure that the same values for the IBM Information Integrator for Content ICMSEVER parameters are used on the IBM eDiscovery Manager system and on every IBM eDiscovery Analyzer system. The ICMSEVER parameters are set in the cmbicmsrvs.ini file.

---

## Searching and search results

Searching and search results are dependent on the content management systems that IBM eDiscovery Manager users access and on the content archives under those content management systems. This section covers configuration information and limitations in the content management systems and content archives that can impact the search experience of your users.

**Search result count:** **Content Mgr** After running a search using eDiscovery Manager, you can find out how many results the search yielded by clicking **Get Result Count**. The current count is displayed and the progress bar is at 0%. If there is only one item type being queried, the progress bar does not advance as the count is determined; it moves from 0% to 100% when IBM Content Manager returns the count. If there are multiple item types being queried, the progress bar advances incrementally, taking one step for each item type. The difference in progress bar behavior for the number of item types is due to a limitation in IBM Content Manager.

## Date range searches

IBM eDiscovery Manager handles dates as time stamps and all dates are normalized to UTC (Coordinated Universal Time) for searching and display.

**Content Mgr** In IBM Content Manager Enterprise Edition, date attributes can be configured as date types or time stamp types. This means that if date attributes are configured as date types, eDiscovery Manager might return search results that include content whose dates are either one day before or one day after the specified date range. For example, a search for content in the range 11/03/2008 to 11/03/2008 (November 3, 2008) can return content that is dated 11/02/2008 or 11/04/2008 as well as content that is dated 11/03/2008.

**Note:** When you select the Sort option for a search across a broad date range, the search response time slows down significantly. For optimal performance of searches across a broad range of dates when the Sort option is selected, set the FullTextRowDefault property of the IBM FileNet P8 object store.

**Recommendation:** **Content Mgr** Use only time stamp attributes for date range searching and store dates in UTC for accurate date handling.

## Searching the Subject or content field of email with non-English language search terms

When using IBM eDiscovery Manager in a non-English language locale with an IBM FileNet P8 content management system, searching the **Subject or content** field with non-English language search terms might not return any results, depending on which email archive is also being used.

- **Email Mgr** When a FileNet P8 content management system stores an IBM FileNet Email Manager email archive, searching the **Subject or content** field with non-English language search terms does not return any results. This behavior occurs because of the Verity K2 style set, which is the only style set available for the full-text indexing with FileNet Email Manager.
- **ICC** When a FileNet P8 content management system stores an IBM Content Collector email archive, searching the **Subject or content** field with non-English language search terms returns proper results when you use the Content Collector style set instead of the Verity K2 style set.

## Configuring the style.lex file for nonalphanumeric, special, and wildcard character searches

To search some kinds of special characters in an IBM FileNet P8 collections, an IBM eDiscovery Manager IT Administrator must configure the style.lex file.

If you want your eDiscovery Manager users to be able to search for nonalphanumeric characters, special characters as literals, and wildcard characters as literals, you must configure the style.lex file for the collections to be searched. See the *Verity Query Language and Topic Guide* for more information about configuring the style.lex file for these types of searches.

**Recommendation:** If your users question the search results that are returned by eDiscovery Manager, verify the results by using IBM FileNet Enterprise Manager and Verity K2 Dashboard with the same search terms that your users provided to eDiscovery Manager.

**Related information:**



Verity Query Language and Topic Guide

## Searching files not encoded in ASCII or UTF-8

Plain text files that are not encoded in ASCII or UTF-8 cannot be indexed by IBM Content Collector or IBM CommonStore, and therefore cannot be searched in IBM eDiscovery Manager.

## Saving search results to a folder

When IBM eDiscovery Manager saves search results to a folder, it does not move the content or create a copy of the content.

eDiscovery Manager saves content by reference; it creates pointers to the content on the content server. Doing so allows eDiscovery Manager to link the content with a case without incurring the additional overhead of moving or copying the content.

## Limitation in successful item count

After saving search results to a folder, the successful item count that is reported by the search task might be higher than the number of documents or files that are saved to the folder.

**Note:** Your ability to search or save content depends on the user roles you have been assigned.

The discrepancy between the item count and document count occurs because some queries related to IBM Legacy Content Search Engine return result sets with duplicate items. The number of items that are found and processed by the IBM eDiscovery Manager work manager comprise the result set, which can include duplicate items. When the search results are saved to a folder, eDiscovery Manager removes any duplicate items. Therefore, the number of documents or files in the folder can be less than the number of items in the search results. However, duplicate items are not removed when saving results from a search that includes multiple content servers. Duplicate items are removed only when saving results that originate from the same content server.

For information about full-text queries, see the SQL Syntax Reference in the IBM FileNet P8 information center.

In short, full-text queries can return matches on more than one content element of a document, or on the document and CBR-enabled string properties of a document. In this case, duplicate rows for that document can be returned in the query results. At most, one row is returned for each content element and one row is returned for all CBR-enabled string properties.

**Related information:**

 [IBM FileNet P8 SQL Syntax Reference](#)

## IBM Legacy Content Search Engine related functionality that affects searching in eDiscovery Manager

Searching and search results are dependent on the content management systems that IBM eDiscovery Manager users access and on the content archives under those content management systems. Several administrative-level, IBM Legacy Content Search Engine related searching details and search configuration issues can affect the search experience for users.

### CBR-enabled document class properties

**Note:** The ability to search content depends on the roles a user has been assigned.

If Content Based Retrieval (CBR) is enabled for one or more document class properties, those properties are considered to be part of the content. When the content of a document is searched, its CBR-enabled properties are also searched. The content and the properties are searched separately so that the document is returned if the search criteria is met by either the document itself or by the CBR-enabled properties of that document. For example:

- If a user searches for the existence of a term, even if the term is not contained in a document, the document is returned as part of the search results if the term is contained in at least one of the CBR-enabled class properties of that document.

- If a user searches for the nonexistence of a term (by using the logical operator NOT), even if the term is contained in a document, the document is returned as part of the search results if the term is not contained in any of the CBR-enabled class properties of that document.

If you do not want document class properties to be searched by eDiscovery Manager, do not enable them for content based retrieval.

For complete information, see the "Full-Text Queries" section in the SQL Syntax Reference of the IBM FileNet P8 documentation.

**Recommendation:** If your users question the search results that are returned by eDiscovery Manager, verify the results by using IBM FileNet Enterprise Manager and IBM Legacy Content Search Engine K2 Dashboard with the same search terms that your users provided to eDiscovery Manager.

## Document format support

IBM Legacy Content Search Engine provides indexing support for certain document formats, but not for all documents that you might have archived. See the Supported Document Formats appendix of the IBM Legacy Content Search Engine Collection Reference (collectionreference.pdf) in the IBM Legacy Content Search Engine installation directory (.\verity\k2\_61\data\docs\) for complete information about which formats are supported.

### Related information:

 [IBM FileNet P8 SQL Syntax Reference](#)

---

## Using IBM eDiscovery Manager with multi-part SharePoint documents archived by IBM Content Collector

You can use IBM eDiscovery Manager to search Microsoft SharePoint items that are archived by IBM Content Collector, Version 3.0 or later. This topic briefly explains the supported scenarios, configuration steps, and available content search options.

You can find more information about how SharePoint items and attachments archived by IBM Content Collector V3.0 are represented in IBM Content Manager, Version 8 or IBM FileNet P8 in the documentation for IBM Content Collector. See the *IBM Content Collector Indexing Guide*, which has detailed information on indexing and field sections.

With IBM Content Collector, you can archive all content of a SharePoint list item, including attachments.

## Viewing SharePoint documents

Files from SharePoint libraries are archived in their own format and viewable if the MIME type is supported by the eDiscovery Manager viewer. SharePoint items from other list types are rendered and archived as HTML in a way that is very similar to the way the item looked in the original SharePoint context. The HTML rendering mirrors the styling in Windows SharePoint Server 3.0 with the following exceptions:

- Images in a page will not display if their source was external and is not available.
- Dates are displayed in the ISO-8601 format.



- Users are displayed as both Display name and login name, for example, Joe Smith (DOMAIN\jsmith).
- Attachment file names are listed but not hyperlinked. To retrieve the attachments, use the export feature or a target repository client that can access the content elements or parts, for example, Workplace XT for FileNet P8.

## Exporting SharePoint documents

eDiscovery Manager supports exporting SharePoint files and rendered items with attachments in their native format.

## Searching SharePoint documents

See the related topics for descriptions of search configuration options for IBM FileNet P8 and IBM Content Manager.

### Limitations

- FileNet P8 with Verity-based search (Legacy Search Service) is not supported for use with SharePoint content that has attachments.
- Dates that are indexed are truncated to a per hour resolution. This means that searches on a subhour resolution are not supported.
- Highlighting is not supported.

## Searching SharePoint documents (FileNet P8)

When you use IBM eDiscovery Manager to search Microsoft SharePoint items that are archived by IBM Content Collector, Version 3.0 or later, refer to these search configuration options for IBM FileNet P8.

IBM Content Collector creates a default document class with the following name and properties.

Document class symbolic name:

- ICCSharepointInstance2

Document properties:

- DocumentTitle
- ICCCreatedBy
- ICCCreatedDate
- ICCExpirationDate
- ICCFileName
- ICCFilePath
- ICCFolderPath
- ICCExpirationDate
- ICCLastModifiedDate
- ICCLibrary
- ICCModifiedBy
- ICCSharePointGUID
- ICCSharePointVersion
- ICCSite



To use multi-part content archived from SharePoint by IBM Content Collector 3.0 or above in an IBM FileNet P8 repository with IBM eDiscovery Manager, create a new eDiscovery Manager collection using the collection type "Microsoft SharePoint - Content Collector". This collection type provides a good starting point which can be modified and extended to create a richer field definition. Initially, the field definitions have the following fields:

*Table 43. Collection fields for the new eDiscovery Manager collection using the collection type "Microsoft SharePoint - Content Collector"*

Collection field	Content server property	Type	Text index
EXTERNAL_ID	Id	String	
CREATED_DATE	ICCCreatedDate	Date	
MODIFIED_DATE	ICCLastModifiedDate	Date	
EXPIRATION_DATE	ICCEExpirationDate	String	
LIBRARY	ICCLibrary	String	
SITE	ICCSite	String	
SHAREPOINT_VERSION	ICCSharePointVersion	String	
FOLDER_PATH	ICCFolderPath	String	
FILE_NAME	ICCFileName	String	

Delete the definition for CONTENT and then add the following definitions to get to the full, new field definitions:

*Table 44. Definitions that need to be added to get to the full, new field definitions*

Collection field	Type	Text index	Description
CONTENT	String	//icc_content	Matches all of the content, including attachments of a SharePoint item.
RAW_CONTENT	String	\$FULL_TEXT\$	Matches all of the content and XML tags.
DOCUMENT	String	//icc_main	Matches primary file content only, whether file or HTML rendering.
PRIMARY_FILE_NAME	String	//icc_main @name	Matches primary file, file name only.
ATTACHMENT	String	//icc_attachment	Matches attachment content only.
ATTACHMENT_NAME	String	/icc_attachment @name	Matches attachment file name only.

## XPath syntax supported in field mappings

The subset of XPath that is supported is defined by CSS XML search engines XPath support. It differs from standard XPath in the following ways:

- It does not support iteration and ranges in path expressions.
- It eliminates filter expressions: that is, it allows filtering only in the predicate expression, not in the path expression.
- It does not allow absolute path names in predicate expressions.
- It implements only one axis (tag) and allows propagation only in the forward direction.

The following characters are unsupported in the XML search syntax:

- /\*
- /\*\*
- /@
- /\*\*@

## Disregarding of XML namespaces

Namespace prefixes are not retained in the indexing of XML tag and attribute names. You can search XML documents by using namespaces, but namespace prefixes are discarded during indexing and removed from XML search queries.

## Numeric values

Predicates that compare attribute values to numbers are supported.

## Complete match

The operator = (equal sign) with a string argument in a predicate means that a complete match of all tokens in the string with all tokens in the identified text span is required. The order of the tokens is important.

For more details on the XML search syntax, see the FileNet P8 topic "SQL Syntax Reference" and go to the "XML Search" section.

### Related information:

 [FileNet P8 SQL Syntax Reference \(see "XML Search" section\)](#)

## Searching SharePoint documents (IBM Content Manager)

When you use IBM eDiscovery Manager to search Microsoft SharePoint items that are archived by IBM Content Collector, Version 3.0 or later, refer to these search configuration options for IBM Content Manager.

IBM Content Manager will create a default item type with the following name and properties.

Item type name:

- ICCSharePointDM

Attributes:

- ICCCreatedBy
- ICCCreatedDate
- ICCFileName
- ICCFolderPath
- ICCLastModifiedDate
- ICCLibrary
- ICCModifiedBy
- ICCSharePointGUID
- ICCSharePointVersion
- ICCSite
- ICMDDeleteHold

To use multi-part content archived from SharePoint by IBM Content Collector 3.0 or above in an IBM Content Manager repository with IBM eDiscovery Manager, create a new eDiscovery Manager collection using the collection type "Microsoft SharePoint - Content Collector". This collection type provides a good starting point which can be modified and extended to create a richer field definition. Initially, the field definitions have the following fields:

*Table 45. Collection fields for the new collection type "Microsoft SharePoint - Content Collector"*

Collection field	Content server property	Type	Text index
EXTERNAL_ID	Id	String	
CREATED_DATE	ICCCreatedDate	Date	
MODIFIED_DATE	ICCLastModifiedDate	Date	
LIBRARY	ICCLibrary	String	
SITE	ICCSite	String	
SHAREPOINT_VERSION	ICCSharePointVersion	String	
FOLDER_PATH	ICCFolderPath	String	
FILE_NAME	ICCFileName	String	

Delete the definition for CONTENT and then add the following definitions to get to the full, new field definitions:

*Table 46. Definitions that need to be added to get to the full, new field definitions.*

Collection field	Type	Text index	Description
CONTENT	String	document	Matches all of the content, including attachments of a SharePoint item.
RAW_CONTENT	String	\$FULL_TEXT\$	Matches all of the content and XML tags.
DOCUMENT	String	generic_content	Matches primary file content only, whether file or HTML rendering.
PRIMARY_FILE_NAME	String	generic_content_name	Matches primary file, file name only.
ATTACHMENT	String	generic_attachment	Matches attachment content only.
ATTACHMENT_NAME	String	generic_attachment_name	Matches attachment file name only.

## Using IBM eDiscovery Manager with IBM Connections documents archived by IBM Content Collector

You can use IBM eDiscovery Manager to search IBM Connections documents that are archived by IBM Content Collector, Version 3.0 or later. This topic briefly explains the supported scenarios, configuration steps, and available content search options.

You can find more information about how IBM Connections documents that are archived by IBM Content Collector V3.0 are represented in IBM Content Manager, Version 8 or IBM FileNet P8 in the documentation for IBM Content Collector. See the *IBM Content Collector Indexing Guide*, which has detailed information on indexing and field sections.

With IBM Content Collector, you can archive all the content of an IBM Connections application. Indirectly related content will not be archived. An example of indirect content is a profile graphic that is shown in a blog comment of a blog post. The profile graphic is owned by the Profiles application and is archived when you archive the profiles. When you archive a blog post, the profile graphic is not archived because it is indirectly related content. Also, any custom widgets and content in IBM Connections pages are not archived.

## Viewing IBM Connections documents

IBM Connections content will be rendered by the eDiscovery Manager viewer similarly to how page looked in the original IBM Connections context. However, because this is done only in the eDiscovery Manager viewer and IBM Connections is not required, there are some differences. The rendering mirrors the styling that you see IBM Connections, V3.0.1 with the following exceptions:

- IBM Connections content that contains links to external locations will be highlighted with an icon in the eDiscovery Manager preview. Clicking a link will open a new window that navigates to the page.
- Graphics in a page might not be displayed if the graphics source was external or is not yet archived.
- Search terms will be highlighted in the IBM Connections document preview.
- Dates are displayed as UTC with a UTC suffix.
- If information cannot be retrieved for the archive, "Unavailable" is displayed. For example, the **Background** tab information of a Profile is not archived, therefore, "Background (Unavailable)" is displayed on that tab.

## Exporting IBM Connections documents

eDiscovery Manager supports exporting IBM Connections documents in native XML format or HTML format. The native XML format that is stored is based on open standards such as the ATOM feed protocol with specific IBM Connections extensions.

The HTML export is similar to the HTML that is generated for viewing except that no highlighting will be performed. The PDF export format is not supported for IBM Connections content.

## Searching IBM Connections documents

See the related topics for descriptions of search configuration options for IBM FileNet P8 and IBM Content Manager.

## Limitations

- FileNet P8 with Verity-based search (Legacy Search Service) is not supported for use with IBM Connections content.
- The PDF export format is not supported for IBM Connections content.
- Dates that are indexed are truncated to a per hour resolution. This means that searches on a subhour resolution are not supported.
- Highlighting will only work for search terms entered for the content field.
- IBM Connections cannot provide all Information available in a browser through the application API. Specifically, IBM Content Collector will not archive the following information because the API does not provide the following information:

- Name of a wiki that contains a specific wiki page
- Name, number, or size of child pages of a wiki page
- Background tab of the profiles application

## Searching IBM Connections documents (FileNet P8)

When you use IBM eDiscovery Manager to search IBM Connections documents that are archived by IBM Content Collector, Version 3.0 or later, refer to these search configuration options for IBM FileNet P8.

IBM Content Collector will create a default document class with the following name and properties.

Document class symbolic name:

- ICCConnectionsInstance

Document properties:

- DocumentTitle
- ICCCreatedDate
- ICCExpirationDate
- ICCLastModifiedDate
- ICCModifiedBy
- ICCApplicationName
- ICCCreatedBy

From eDiscovery Manager, to view and search IBM Connections content that is archived by IBM Content Collector and is stored in a Content Engine object store, create a new eDiscovery Manager custom collection type and use the following field mapping:

*Table 47. Collection fields for the new eDiscovery Manager custom collection type*

Collection field	Content server property	Type	Text index	Description
CONTENT		String	//icc_content	Matches all of the content, including attachments of an IBM Connections document.
DOCUMENT		String	//icc_part	Matches all of the content of an IBM Connections document except the attachment plain text extract.
ATTACHMENT		String	//icc_attachment	Matches the plain text extract of an attachment.
ATTACHMENT_NAME		String	//icc_attachment@name	Matches the display name of a attachment, as shown in IBM Connections.
TITLE	Document Title	String	//title	Matches the title or name of an IBM Connections application content, for example, a wiki page title, blog post title, or profile title.
SUB_TITLE		String	//subtitle	Matches, if available, the activity goal of an IBM Connections activity.
ENTRY_ID		String	//entry/id	Matches the GUID set by IBM Connections to identify a specific portion of content, for example, a wiki page or blog post.

Table 47. Collection fields for the new eDiscovery Manager custom collection type (continued)

Collection field	Content server property	Type	Text index	Description
AUTHOR		String	//author/name	Matches the names of persons who created an IBM Connections application content or subcontent.
CONTRIBUTOR		String	//contributor/name	Matches the names of persons who change an IBM Connections application content or subcontent.
MODIFIER		String	//modifier/name	Matches names of persons who changed an IBM Connections wiki page. This is used instead of contributor by IBM Connections wiki page application.
CUSTOM_FIELD		String	//field	Matches values of custom fields for the IBM Connections applications that support custom fields (activities).
PUBLISHED		Date	//published/@icc_date	Matches the published date of any content or subcontent, for example, published date of a blog post or a specific comment to a blog post. <b>Remember:</b> <ul style="list-style-type: none"> <li>An IBM Connections profile does not have a published date and thus it is not searchable by an index; however, the ICCCreatedDate value will be set to the updated date of the profile.</li> <li>An IBM Connections activity that does not contain any subactivity does not have a published date and thus it is not searchable by an index; however, the ICCCreatedDate value will be set to the updated date of the activity.</li> </ul>
UPDATED	ICCLastModifiedDate	Date	//updated/@icc_date	Matches the updated date of any content or subcontent (see PUBLISHED). This field is available for all IBM Connections content.
TAG		String	//category/@term	Matches the tags given to any content or subcontent of IBM Connections content.
APPLICATION_NAME	ICC Application Name	String	//icc_application_name	Matches the IBM Connections application name. The valid values are: <ul style="list-style-type: none"> <li>FILES</li> <li>PROFILES</li> <li>WIKIS</li> <li>BLOGS</li> <li>BOOKMARKS</li> <li>FORUMS</li> <li>ACTIVITIES</li> </ul>
RAW_CONTENT		String	\$FULL_TEXT\$	Matches the complete content indexed for an IBM Connections document. Use this only for debugging purposes.
AUTHOR_PRIMARY_ATTRIBUTE	ICC CreatedBy	String		Names of persons who created an IBM Connections application content, for example, a blog post author, but not comment author. This is one of the several authors available under AUTHOR. This field is useful as a result list column. This field is necessary for IBM Connections Files because metadata is not part of content.

Table 47. Collection fields for the new eDiscovery Manager custom collection type (continued)

Collection field	Content server property	Type	Text index	Description
PUBLISHED_PRIMARY_ATTRIBUTE	ICC CreateDate	String		Matches the published date of any content, for example, the published date of a blog post). This is one of the several dates available under PUBLISHED. This field is useful as a result list column. This field is necessary for IBM Connections because metadata is not part of content.

IBM Connections Files content differs from other IBM Connections applications content because for Files, only the actual file content is text-indexed and can be text-searched. Therefore, most of the collection fields listed previously are not applicable to IBM Connections Files. Because of this difference, it is recommended that you create two eDiscovery Manager search templates based on the custom collection definition above: One for IBM Connections Files that adds only search fields for the AUTHOR\_PRIMARY\_ATTRIBUTE, PUBLISHED\_PRIMARY\_ATTRIBUTE, APPLICATION\_NAME and CONTENT fields, and one search template for the other IBM Connections applications content, which has all the other fields and does not use the AUTHOR\_PRIMARY\_ATTRIBUTE and PUBLISHED\_PRIMARY\_ATTRIBUTE fields or only uses them as a result list column where needed.

For applications other than Files, the complete XML content of an IBM Connections document is indexed. Therefore, more complex Xpath statements can be built to address specific subelements in the content.

An example for such a complex query would be to search just in the content of comments that are created specifically for IBM Connections content.

To configure a search field for such a use case, which is not covered with the default mapping provided above, perform the following steps:

1. Look at a sample IBM Connections document in FileNet P8 by using IBM FileNet Enterprise Manager.
2. Identify the relevant content element (MIME type application/icc-comment-atom+xml for comments).
3. Look at the content to identify the relevant XML structure (/feed/entry/content for comments).
4. Derive the following expression from that build:  
//icc\_part[@mimetype="application/icc-comment-atom+xml"]/feed/entry/content.
5. See the table of MIME types that are defined by IBM Content Collector for IBM Connections context.
6. Create a new eDiscovery Manager Collection field that uses this index expression.

You can now search explicitly on IBM Connections comments.

## XPath syntax supported in field mappings

The subset of XPath that is supported is defined by CSS XML search engines XPath support. It differs from standard XPath in the following ways:

- It does not support iteration and ranges in path expressions.

- It eliminates filter expressions: that is, it allows filtering only in the predicate expression, not in the path expression.
- It does not allow absolute path names in predicate expressions.
- It implements only one axis (tag) and allows propagation only in the forward direction.

The following characters are unsupported in the XML search syntax:

- /\*
- /\*\*
- /@\*
- /\*\*@\*

## Disregarding of XML namespaces

Namespace prefixes are not retained in the indexing of XML tag and attribute names. You can search XML documents by using namespaces, but namespace prefixes are discarded during indexing and removed from XML search queries.

## Numeric values

Predicates that compare attribute values to numbers are supported.

## Complete match

The operator = (equal sign) with a string argument in a predicate means that a complete match of all tokens in the string with all tokens in the identified text span is required. The order of the tokens is important.

For more details on the XML search syntax, see the FileNet P8 topic "SQL Syntax Reference" and go to the "XML Search" section.

## List of MIME types used by IBM Content Collector for archiving IBM Connections content

IBM Content Collector uses a specific set of MIME types to identify different types of content in an IBM Connections system. If you are working with IBM FileNet P8 and a CSS, the MIME types table will help you build advanced queries.

*Table 48. MIME types used by IBM Content Collector to identify different types of IBM Connections content*

Extension	MIME type	Description
.afu_acl_xml	Application/icc-acl-atom+xml	Member information of an IBM Connections document
.afu_activity_trash_xml	Application/icc-activity-trash-atom+xml	IBM Connections Activities trash document
.afu_activity_xml	Application/icc-activity-atom+xml	IBM Connections Activities document
.afu_attachment_xml	Application/icc-attachment-atom+xml	Attachment metadata of an IBM Connections document
.afu_blog_xml	Application/icc-blog-atom+xml	IBM Connections blog post document
.afu_board_xml	Application/icc-board-atom+xml	IBM Connections profile board document
.afu_bookmark_xml	Application/icc-bookmark-atom+xml	IBM Connections bookmark document
.afu_comment_xml	Application/icc-comment-atom+xml	Comments of an IBM Connections document
.afu_forum_reply_xml	Application/icc-forum-reply-atom+xml	Forum replies for an IBM Connections Forum topic
.afu_forum_topic_xml	Application/icc-forum-topic-atom+xml	IBM Connections forum topic



Table 48. MIME types used by IBM Content Collector to identify different types of IBM Connections content (continued)

Extension	MIME type	Description
.afu_forum_xml	Application/icc-forum-atom+xml	IBM Connections forum metadata
.afu_link_xml	Application/icc-link-atom+xml	Links document of an IBM Connections profile
.afu_media_xml	Application/icc-media-atom+xml	Content of an IBM Connections wiki page
.afu_network_xml	Application/icc-network-atom+xml	Network document of an IBM Connections Profile
.afu_profile_xml	Application/icc-profile-atom+xml	IBM Connections Profile document
.afu_recommend_xml	Application/icc-recommend-atom+xml	Recommendation document of an IBM Connections document
.afu_reporting_xml	Application/icc-reportingChain-atom+xml	Reporting chain document of an IBM Connections Profile
.afu_status_xml	Application/icc-status-atom+xml	Status document of an IBM Connections Profile
.afu_tag_xml	Application/icc-tag-atom+xml	Tags given to an IBM Connections document
.afu_version_xml	Application/icc-version-atom+xml	Version metadata of an IBM Connections wiki page
.afu_wiki_xml	Application/icc-wiki-atom+xml	IBM Connections wiki page

#### Related information:

 FileNet P8 SQL Syntax Reference (see "XML Search" section)

## Searching IBM Connections documents (IBM Content Manager)

When you use IBM eDiscovery Manager to search IBM Connections documents that are archived by IBM Content Collector, Version 3.0 or later, refer to these search configuration options for IBM Content Manager.

IBM Content Collector creates a default item type named ICCConnections with the following table.

Table 49. Field mapping used by the new eDiscovery Manager collection of collection type "IBM Connections - Content Collector".

Collection field	Content server property	Type	Text index	Description
CONTENT		String	document	Matches all of the content, including attachments of an IBM Connections application document.
DOCUMENT		String	content	Matches all of the content of an IBM Connections document except the attachment plain text extract.
ATTACHMENT		String	attachment	Matches the plain text extract of an attachment.
ATTACHMENT_NAME		String	attachment_name	Matches the display name of a attachment, as shown in IBM Connections.
TITLE	ICCTitle	String	icc_title	Matches the title or name of an IBM Connections application content, for example, a wiki page title, blog post title, or profile title.
ENTRY_ID		String	icc_entry_id	Matches the GUID set by IBM Connections to identify a specific portion of content, for example, a wiki page or blog post.
AUTHOR		String	icc_displayName_author_primary	Matches the names of persons who created an IBM Connections application content, for example, a blog post author (but not comment author).*

Table 49. Field mapping used by the new eDiscovery Manager collection of collection type "IBM Connections - Content Collector" (continued).

Collection field	Content server property	Type	Text index	Description
AUTHOR_SUBCONTENT		String	icc_displayName_author	Matches the names of persons who created an IBM Connections application content, for example, a comment author.*
CONTRIBUTOR		String	icc_displayName_contributor_primary	Matches the names of persons who modified an IBM Connections application subcontent, for example, a blog post.*
CONTRIBUTOR_SUBCONTENT		String	icc_displayName_contributor	Matches the names of persons who modified an IBM Connections application subcontent, for example, a blog post.*
CUSTOM_FIELD		String	icc_custom TextValue	Matches values of custom fields for the IBM Connections applications that support custom fields (activities).
PUBLISHED		Date	icc_published_primary	Matches the published date of any content, for example, published date of a blog post. <b>Remember:</b> <ul style="list-style-type: none"> <li>An IBM Connections profile does not have a published date and thus it is not searchable by an index; however, the ICCCreatedDate value will be set to the updated date of the profile.</li> <li>An IBM Connections activity that does not contain any subactivity does not have a published date and thus it is not searchable by an index; however, the ICCCreatedDate value will be set to the updated date of the activity.*</li> </ul>
PUBLISHED_SUBCONTENT		Date	icc_published	Matches the published date of subcontent, for example, the published date of a comment.
UPDATED	ICC Modified Date	Date	icc_updated_primary	Matches the updated date of any content. (See PUBLISHED.) This field is available for all IBM Connections content.*
UPDATED_SUBCONTENT		Date	icc_updated	Matches the updated date of any subcontent. (See PUBLISHED.) This field is available for all IBM Connections content.*
TAG		String	icc_tags	Matches the tags given to any content or subcontent of IBM Connections content.
APPLICATION_NAME	ICC Application Name	String	icc_application_name	Matches the IBM Connections application name. The valid values are: <ul style="list-style-type: none"> <li>FILES</li> <li>PROFILES</li> <li>WIKIS</li> <li>BLOGS</li> <li>BOOKMARKS</li> <li>FORUMS</li> <li>ACTIVITIES</li> </ul>
RAW_CONTENT		String	\$FULL_TEXT\$	Matches the complete content indexed for an IBM Connections document. Use this only for debugging purposes.

Table 49. Field mapping used by the new eDiscovery Manager collection of collection type "IBM Connections - Content Collector" (continued).

Collection field	Content server property	Type	Text index	Description
AUTHOR_PRIMARY_ATTRIBUTE	ICC Created By	String		This field is useful as a result list column. This field is necessary for IBM Connections Files because metadata is not part of content.
PUBLISHED_PRIMARY_ATTRIBUTE	ICC Created Date	String		This field is useful as a result list column. This field is necessary for IBM Connections because metadata is not part of content.

\* For all index fields that are suffixed with "primary," there is a secondary field definition for subcontent. These fields can be used to created combined or grouped fields in an eDiscovery Manager search template to search for all authors, contributors, published, and modified entries.

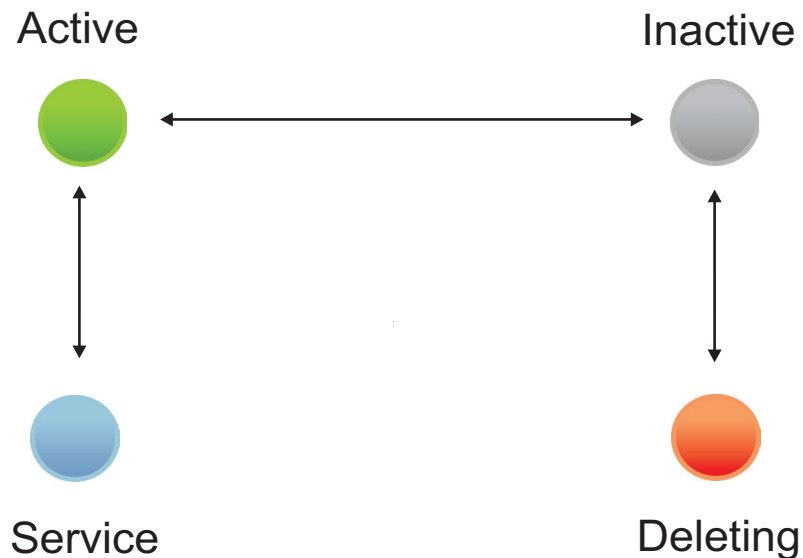
IBM Connections Files content differs from other IBM Connections applications content because for Files, only the actual file content is text-indexed and can be text-searched. Therefore, most of the collection fields listed previously are not applicable to IBM Connections Files. Because of this difference, it is recommended that you create two eDiscovery Manager search templates based on the custom collection definition above: One for IBM Connections Files that adds only search fields for the AUTHOR\_PRIMARY\_ATTRIBUTE, PUBLISHED\_PRIMARY\_ATTRIBUTE, APPLICATION\_NAME and CONTENT fields, and one search template for the other IBM Connections applications content, which has all the other fields and does not use the AUTHOR\_PRIMARY\_ATTRIBUTE and PUBLISHED\_PRIMARY\_ATTRIBUTE fields or only uses them as a result list column where needed.



---

## Chapter 4. Managing cases in eDiscovery Manager

Manage cases from the Case Information page of the IBM eDiscovery Manager web client.



A case can be in one of several phases:

- **Active**

When a case is created, it is put into the active phase.

- **Service**

When a resource in a case is locked because a user starts a long-running task (such as copying or moving content between folders, exporting content, and so on), eDiscovery Manager automatically moves the case from the active phase to the service phase. Users can still perform tasks on the case, but they cannot perform tasks on the locked resource. For example, one user cannot copy a folder while another user is adding content to that folder. After all resources are unlocked, eDiscovery Manager automatically moves the case back into the active phase.

- **Inactive**

When a case is no longer needed, a Case Administrator can move the case into the inactive phase. Users can still search the case, but they cannot perform folder or case tasks.

- **Deleting**

When the case is no longer useful, a Case Administrator can move the case from the inactive phase to the deleting phase. At this time, all folders, tasks, audit records, legal holds, and so on for the case are deleted from eDiscovery Manager. However, all content that was related to the case continues to exist in the content archive. eDiscovery Manager writes a single audit record to record the deletion of the case.

**Important:** After a case is deleted, it cannot be restored.

---

## Allowed tasks during phases of a case

Throughout the life of a case, tasks are allowed or disallowed depending on the current phase of the case.

The following table shows which tasks are allowed (Yes) or disallowed (No) during the different life cycle phases of a case. No tasks are allowed while a case is being deleted or after the case is deleted.

**Note:** The ability to perform specific tasks in a case also depends on the roles assigned to the user.

*Table 50. Allowed and disallowed tasks during life cycle phases of a case.*

Task	Active	Service	Inactive
Search	Yes	Yes	Yes
Add content to a folder	Yes	Yes	No
View a piece of content or entire folder contents	Yes	Yes	Yes
Move a piece of content or entire folder contents	Yes	Yes <sup>2</sup>	No
Copy content or entire folder contents	Yes	Yes <sup>2</sup>	No
Rename a folder	Yes <sup>3</sup>	Yes <sup>2, 3</sup>	No
Export content	Yes	Yes	No
Remove items from folders	Yes	Yes <sup>2</sup>	No
Delete folders	Yes	Yes <sup>2</sup>	No
Edit case information, such as the case name, description, and user access	Yes	Yes	No
Change a case to the active phase	No	Yes <sup>1</sup>	Yes
Change a case to the deleting phase	No	No	Yes
Change a case to the service phase	Yes <sup>1</sup>	No	No
Change a case to the inactive phase	Yes	No	No

<sup>1</sup> This is an automatic transition.

<sup>2</sup> This task cannot be performed if it involves any locked folders.

<sup>3</sup> A folder cannot be renamed if it contains any content.

---

## Legal holds in eDiscovery Manager

IBM eDiscovery Manager provides a basic legal hold mechanism for case content. Whenever a user saves a piece of content to a folder in eDiscovery Manager, an implicit legal hold is placed on the content to prevent it from being deleted from the content server.

Placing a legal hold on content ensures that potentially relevant content is preserved in the content server for future litigation. As long as a piece of content exists in an eDiscovery Manager folder, the content cannot be deleted from the content server. Even other applications that might have access to the content on the content server cannot delete that piece of content.

eDiscovery Manager releases its hold on a piece of content when the content is removed from all folders that contain it, when all the folders that contain the

content are deleted, or when all the cases that contain the content are deleted.





---

## Chapter 5. Monitoring eDiscovery Manager system status

The IBM eDiscovery Manager web client is supported by a server, which is called the eDiscovery Manager work manager. The work manager is a servlet that schedules and handles all of the asynchronous tasks that are created by users of the eDiscovery Manager web client. These tasks include saving search results to folders, copying and moving content between folders, exporting content, and so on.

You can check the status of the eDiscovery Manager system to ensure that it is running properly by using your browser to access the Work Manager status page with one of the following URLs:

`http://server IP address:port/EDMWorkMgrServer/Status?User=user_name&Password=password`

or:

`http://server host address:port/EDMWorkMgrServer/Status?User=user_name&Password=password`

### Examples:

`http://9.40.114.128:9080/EDMWorkMgrServer/Status?User=ediscadmin&Password=mypasswd`

`http://abc.example.com:9080/EDMWorkMgrServer/Status?User=ediscadmin&Password=mypasswd`

The Work Manager status page shows whether:

- The work manager can establish connections to content servers.
- The work manager thread pool was properly initialized.
- The task finder is currently active. The task finder polls every 30 seconds to find new tasks for the work manager.
- The email notification session is accessible.

The Work Manager status page also includes information about the tasks that are currently in the work manager memory. This includes tasks that the work manager is currently processing and tasks that the work manager recently completed. (If the eDiscovery Manager application server is restarted, any tasks that were in the work manager memory and that have completed are removed.)

**Tip:** If the task list is too long, click **Clear** to delete all of the completed tasks from the list.

The work manager is multithreaded, so it can handle multiple tasks simultaneously and it can process multiple batches of the same task in parallel.

---

## How the eDiscovery Manager work manager schedules tasks

The IBM eDiscovery Manager work manager is a servlet that schedules and handles all of the asynchronous tasks that are created by eDiscovery Manager users. The work manager processes tasks on a First In, First Out (FIFO) basis.

As soon as a task is set up, the task is placed on the work manager queue, and can be processed. Tasks are not processed by creation date but rather by their

availability for processing. This means that a task that is created earlier but takes a long time to set up might be processed after a task that is created later but takes a short time to set up.

If you have time-sensitive tasks, such as large document export tasks, consider scheduling the tasks so that you can control the order in which the tasks are processed. Also, consider increasing the **Maximum concurrent exports** option from its default of 1 to indicate that you want eDiscovery Manager to process multiple export tasks simultaneously.

---

## Chapter 6. Troubleshooting eDiscovery Manager

When you experience problems, you might need to perform troubleshooting tasks to determine the corrective action to take.

---

### eDiscovery Manager messages

All IBM eDiscovery Manager messages have the same format.

The first three characters of all eDiscovery Manager messages are DYR. The fourth character identifies the component in which the error occurred:

C	eDiscovery Manager web client
E	Email convertor
L	LDAP server
S	eDiscovery Manager application server

The next four characters are a unique, numeric identifier. All eDiscovery Manager messages end in E.

With the exception of DYRC9999E, the sections that follow describe eDiscovery Manager messages that do not yet have message text. Message text will be assigned to these messages in a future release.

#### DYRC9999E

eDiscovery Manager displays message DYRC9999E when it receives an error from an underlying product. Thus, this message can be generated by a variety of causes. The format of the message is:

An error was received from {*messageSource*}. Error received: {*error*}.  
To obtain detailed information about the error, ask your administrator to search the log file for the keyword "SEVERE" and provide the information to IBM Support.

where:

*messageSource*

identifies one of the following products as the source of the problem:

- IBM Content Manager Enterprise Edition
- IBM FileNet P8
- LDAP Server

*error* is the error message that eDiscovery Manager received from the product.

**Example:** One possible cause of this message is that global caching is enabled in Content Manager EE.

#### Administrator response

Global caching must be disabled on the Content Manager EE system. eDiscovery Manager does not support global caching. Disable global caching with the CPPGlobalCacheEnabled parameter in the cmbicmcache.ini file:

```
CPPGlobalCacheEnabled=FALSE
```

The default location for the `cmbicmcache.ini` file is in `IBMCMROOT\cmgmt\connectors\` on Microsoft Windows systems and in `/home/ibmcadm/cmgmt/connectors/` on AIX systems. For example: `C:\Program Files\IBM\db2cmv8\cmgmt\connectors` on a Microsoft Windows system.

---

## Troubleshooting installation and uninstallation problems

Solve common problems that might occur when you install or remove the product.

### WASX7017E and WASX7116E exceptions when deploying eDiscovery Manager

During installation or upgrade, when deploying IBM eDiscovery Manager to the IBM WebSphere Application Server, an error occurs.

#### Symptoms

You find messages like the following message in the `eDMInstallDebug*.log` file:

```
WASX7017E: Exception received while running file "/tmp/wsant19741jac1";  
exception information: com.ibm.ws.scripting.ScriptingException:  
WASX7116E: Cannot copy file "/opt/IBM/eDM/dist/EDCConsole.ear" to  
file "/tmp/app2761.ear"
```

#### Causes

Possible causes of WASX7017E and WASX7116E exceptions:

- The temporary directory does not have enough free space for installing eDiscovery Manager. If this is the cause, you also might see a message like this:  
Unpacking the JRE...  
tar: jre/jre/bin/libj9prt23.so: Cannot write extracted data:  
No space left on device
- You are upgrading from one version of eDiscovery Manager to another version and there is a problem with permissions and ownership of profile directories. After you installed eDiscovery Manager the last time, the permissions and ownership of several files and directories were changed from the root user to a non-root user. This prevents the eDiscovery Manager installation program, which is running as the root user, from updating the eDiscovery Manager profile directories.

#### Resolving the problem

Resolve this problem depending on which situation is causing it.

- If the temporary directory contains insufficient space, increase the amount of disk space that is allocated to it, and run the deployment scripts in the `scriptsWAS` subdirectory of the eDiscovery Manager installation directory. 450 MB of disk space is required to install eDiscovery Manager.  
The default temporary directory that the eDiscovery Manager installation program uses is `/tmp`. If you want to change the directory that the installation program uses, set the `IATEMPDIR` environment variable to specify a different directory.
- If you are upgrading from one version of eDiscovery Manager to another, complete the following steps before you attempt to reinstall eDiscovery Manager:
  1. Update the additional process execution settings that are associated with the eDiscovery Manager profile by clearing the **Run as user** and **Run as group** fields.
  2. Stop the WebSphere Application Server and restart it as the root user.

## DGL0394A: Cannot instantiate class when installing or uninstalling

When installing or uninstalling IBM eDiscovery Manager, a DGL0394A error results.

### Symptoms

```
Tue Jun 03 09:31:36.159 PDT 2008 :
INFO : com.ibm.mm.sdk.common.DKDatastoreAccessError:
DGL0394A: Error in ::DriverManager.getConnection;
Cannot instantiate class: com.ibm.websphere.naming.WsnInitialContextFactory;
[SERVER = LSCMI27, USERID = icmadmin]
at com.ibm.mm.sdk.server.DKDatastoreICM.connect(DKDatastoreICM.java:1961)
at com.ibm.icm.edc.ral.bootstrap.cm.impl.DataModelCM.connect(DataModelCM.java:1611)
at com.ibm.icm.edc.ral.bootstrap.cm.impl.DataModelCM.main(DataModelCM.java:627)
Exception in thread "main" com.ibm.mm.sdk.common.DKDatastoreAccessError:
DGL0394A: Error in ::DriverManager.getConnection;
Cannot instantiate class: com.ibm.websphere.naming.WsnInitialContextFactory;
[SERVER = LSCMI27, USERID = icmadmin]
at com.ibm.mm.sdk.server.DKDatastoreICM.connect(DKDatastoreICM.java:1961)
at com.ibm.icm.edc.ral.bootstrap.cm.impl.DataModelCM.connect(DataModelCM.java:1611)
at com.ibm.icm.edc.ral.bootstrap.cm.impl.DataModelCM.main(DataModelCM.java:627)
```

### Causes

eDiscovery Manager does not use the connection pooling feature of IBM WebSphere Application Server.

### Resolving the problem

Modify the value of the JavaPool parameter in the cmbpool.ini file to be an empty string. (Do not comment out the JavaPool parameter; simply set its value to an empty string.)

JavaPool=

The cmbpool.ini file is used for IBM WebSphere Application Server connection pooling. The default location for the cmbpool.ini file is in *IBMCMROOT\cmgmt\connectors\* on Microsoft Windows systems and in */home/ibmcmadm/cmgmt/connectors/* on AIX systems. For example: *C:\Program Files\IBM\db2cmv8\cmgmt\connectors* on a Microsoft Windows system.

## Installation program not progressing


The IBM eDiscovery Manager installation program does not seem to be making progress.

### Symptoms

When installing eDiscovery Manager, the installation program seems to be stuck for a long time during the application server deployment.

### Causes

During the application server deployment phase, the installation program deploys the eDiscovery Manager web client and eDiscovery Manager work manager, and configures the application server instance to which they are deployed. This process can take from several minutes to 20 minutes.

 After deployment is complete on AIX systems, a post-installation script is run which can take up to 30 minutes.

### Resolving the problem

To resolve the problem:

1. Do not cancel the installation. Let the installation program complete on its own. If you are installing on an AIX system, the application server deployment phase is complete. The post-installation script is running if you see the following message:

Configuration tasks in progress... This step can take up to 5 or 10 minutes.

If you are not installing on AIX, or if the AIX post-installation script has not started yet, and it looks like the application server deployment is not progressing, wait at least 45 minutes for deployment. After 45 minutes, check the status of the application server by running the IBM WebSphere Application Server command **serverStatus**. Enter the following command on a single line.

Operating system	Command
AIX	<code>/usr/IBM/WebSphere/AppServer/profiles/ eDMProfileName/bin/serverStatus.sh serverName</code>
Windows	<code>drive_letter:\Program Files\IBM\WebSphere AppServer\bin\serverStatus serverName</code>

The deployment is running if you see the following message:

Application server deployment in progress...  
This step can take up to 15 or 20 minutes.

If the server status shows that there is a problem with the application server, you can cancel the installation process and then manually deploy eDiscovery Manager. If you are installing on an AIX system, you must also manually run the post-installation script after deployment.

2. If you already canceled the installation, verify in the log files that there were no installation failures by checking log files in the following locations:
  - Your home directory, which on an AIX system is defined by the HOME environment variable and on a Microsoft Windows system is defined by the HOMEPATH environment variable
  - The eDiscovery Manager installation directory
  - The logs subdirectory of the eDiscovery Manager installation directory
  - The `WAS_HOME/profiles/eDM_profile/logs/eDM_app_server_instance` directory
3. If there were no installation failures, manually deploy the eDiscovery Manager web client and work manager. If you are installing on an AIX system, manually run the post-installation script too:
  - a. Remove the eDiscovery Manager objects from the WebSphere Application Server by using the WebSphere Administrative Console:

#### Servers

In Application servers > *server\_name* > Process definition > Environment Entries:

- LIBPATH (C:\IBM\EDM\lib)
- PATH (C:\IBM\EDM\lib)

#### Class loaders

In Application servers > *server\_name* > Java and Process Management > Class loader, remove all class loaders that are associated with the EDMLibraries application.

**Note:** If you dedicated the server profile to eDiscovery Manager, as required, you can delete all of the class loaders. If you did not dedicate the server profile to eDiscovery Manager, some of the class loaders might belong to the other applications that share the server profile. In the latter case, complete the following steps:

- 1) Determine which class loaders are associated with eDiscovery Manager by selecting each class loader ID and then selecting **Shared Library reference** from the right-click menu.
- 2) If the associated application is EDMLibraries, remove the class loader.

#### Applications

- EDMClient
- EDMWorkMgrServer

#### Async beans work managers

- EDMClientWorkManager
- EDMServerWorkManager
- EDMWorkItemManager


#### Mail, Mail Session

EDMMailSession

#### Shared libraries

- EDMLibraries
- EDMWorkMgrLibrary
- EDMClientLibrary

#### JVM Properties

- heap size=254, max heap size=1 GB
- classpath, for example on Windows C:\IBM\EDM\config\resources;C:\IBM\EDM\config;C:\Program Files\IBM\db2cmv8\cmgmt
- In the Generic JVM arguments:  
-DedmBinDir=C:\IBM\EDM\bin\
-  An additional parameter in the Generic JVM argument:  
-Djava.security.auth.login.config=EDM\_HOME\config\jaas.conf.WebSphere

- b. Deploy the eDiscovery Manager web client and work manager.

 For AIX:

- 1) Go to the scriptsWAS subdirectory of the eDiscovery Manager installation directory. For example:  
`cd /opt/IBM/EDM/scriptsWAS`
- 2) Deploy eDiscovery Manager from the command line by using the following command:  
`./EDMAppConfig.sh install WAS_userid WAS_password > deploy.log`


 For Microsoft Windows:

- 1) Go to the scriptsWAS subdirectory of the eDiscovery Manager installation directory. For example:  
`c:\program files\IBM\EDM\scriptsWAS`
- 2) Open the file EDMAppConfig.bat and remove the following two exits from the end of the file:

```
exit 0
exit %rc%
```

3) Run the deployment with the following command:

```
eDMAppConfig.bat install WAS_userid WAS_password > deploy.log
```


- c.  Run the `postinstalledm.sh` shell script to perform some necessary post-installation tasks.

The eDiscovery Manager scripts are in the `scripts` subdirectory of the eDiscovery Manager installation directory. For example, enter the following command to run the script on a WebSphere Application Server that has security enabled:

```
/opt/IBM/eDM/scripts/postinstalledm.sh TRUE WAS_admin_username \
WAS_admin_password
```

If security is not enabled on the WebSphere Application Server, run the `postinstalledm.sh` shell script with only the `FALSE` parameter. For example:

```
/opt/IBM/eDM/scripts/postinstalledm.sh FALSE
```

- d.  Start the eDiscovery Manager server. See the WebSphere Application Server product information for details about stopping and starting an application server.

4. If there was an installation failure:

- a. Identify the cause of the failure and correct it.

Causes of installation failures include:

- An incorrect application server instance was identified. The default value is eDM, but that might not be the appropriate value for your site.
- An incorrect WebSphere Application Server user name or password was specified and security is enabled.

- b. Manually deploy the eDiscovery Manager web client and work manager:

- 1) Remove the eDiscovery Manager objects from the WebSphere Application Server by using the WebSphere Administrative Console:

#### Servers

In Application servers > *server\_name* > Process definition > Environment Entries:

- LIBPATH (C:\IBM\eDM\lib)
- PATH (C:\IBM\eDM\lib)

#### Class loaders

In Application servers > *server\_name* > Java and Process Management > Class loader, remove all class loaders that are associated with the EDMLibraries application.

**Note:** If you dedicated the server profile to eDiscovery Manager, as required, you can delete all of the class loaders. If you did not dedicate the server profile to eDiscovery Manager, some of the class loaders might belong to the other applications that share the server profile. In the latter case, complete the following steps:

- a) Determine which class loaders are associated with eDiscovery Manager by selecting each class loader ID and then selecting **Shared Library reference** from the right-click menu.
- b) If the associated application is EDMLibraries, remove the class loader.



## Applications

- EDMClient
- EDMWorkMgrServer

## Async beans work managers

- EDMClientWorkManager
- EDMServerWorkManager
- EDMWorkItemManager


## Mail, Mail Session

EDMMailSession

## Shared libraries

- EDMLibraries
- EDMWorkMgrLibrary
- EDMClientLibrary

## JVM Properties

- heap size=254, max heap size=1 GB
- classpath, for example on Windows C:\IBM\EDM\config\resources;C:\IBM\EDM\config;C:\Program Files\IBM\db2cmv8\cmgmt
- In the Generic JVM arguments:  
-DedmBinDir=C:\IBM\EDM\bin\
-  An additional parameter in the Generic JVM argument:  
-Djava.security.auth.login.config=EDM\_HOME\config\jaas.conf.WebSphere


## 2) Deploy the eDiscovery Manager web client and work manager.

 For AIX:

- a) Go to the scriptsWAS subdirectory of the eDiscovery Manager installation directory. For example:  
`cd /opt/IBM/EDM/scriptsWAS`
- b) Deploy eDiscovery Manager from the command line by using the following command:  
`./EDMAppConfig.sh install WAS_userid WAS_password > deploy.log`

 For Microsoft Windows:

- a) Go to the scriptsWAS subdirectory of the eDiscovery Manager installation directory. For example:  
`c:\program files\IBM\EDM\scriptsWAS`
- b) Open the file EDMAppConfig.bat and remove the following two exits from the end of the file:  
`exit 0`  
`exit %rc%`
- c) Run the deployment with the following command:  
`EDMAppConfig.bat install WAS_userid WAS_password > deploy.log`


- c.  Run the postinstalledm.sh shell script to perform some necessary post-installation tasks.

The eDiscovery Manager scripts are in the scripts subdirectory of the eDiscovery Manager installation directory. For example, enter the following command to run the script on a WebSphere Application Server that has security enabled:

```
/opt/IBM/eDM/scripts/postinstalledm.sh TRUE WAS_admin_username \  
WAS_admin_password
```

If security is not enabled on the WebSphere Application Server, run the postinstalledm.sh shell script with only the FALSE parameter. For example:

```
/opt/IBM/eDM/scripts/postinstalledm.sh FALSE
```

- d.  Start the eDiscovery Manager server. See the WebSphere Application Server product information for details about stopping and starting an application server.

#### Related information

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

## Installation program not progressing during application server deployment in a FileNet P8 environment

When you install IBM eDiscovery Manager in an IBM FileNet P8 environment, the installation program seems to be frozen during the application server deployment.

### Symptoms

The eDiscovery Manager installation program seems to be frozen and it displays the following message for more than 20 minutes:

```
Application server deployment in progress  
This step can take up to 5 or 10 minutes.
```

### Causes

This problem might be caused by one of the following situations:

- The IBM WebSphere Application Server SSL certificate might be expired.
- For performance reasons, your system might require more time to complete the installation.

### Resolving the problem

To resolve the problem:

1. Do not cancel the installation. Wait for about 45 minutes for the installation to complete.
2. After you wait for about 45 minutes, check the status of the eDiscovery Manager server by running the WebSphere Application Server **serverStatus** command:

Operating system	Command
AIX	<pre>/usr/IBM/WebSphere/AppServer/profiles /eDMProfileName/bin/serverStatus.sh serverName</pre>
Windows	<pre>drive_letter:\Program Files\IBM\WebSphere \AppServer\bin\serverStatus serverName</pre>

3. If a WebSphere Application Server message prompts you for more information, enter the appropriate response. This information might resolve the problem.

4. If the server status shows that there are problems with the server, complete the following steps:
  - a. Cancel the installation.
  - b. Fix the server problems.
  - c. Ensure that you can stop and start the server.
  - d. Reinstall eDiscovery Manager.
5. If the server status shows that there are no problems with the eDiscovery Manager server, check the status of the FileNet P8 server by running the **serverStatus** WebSphere Application Server command:

Operating system	Command
AIX	<code>/usr/IBM/WebSphere/AppServer/profiles/ /eDMProfileName/bin/serverStatus.sh serverName</code>
Windows	<code>drive_letter:\Program Files\IBM\WebSphere \AppServer\bin\serverStatus serverName</code>

6. If the server status shows that there are problems with the server, complete the following steps:
  - a. Cancel the installation.
  - b. Fix the server problems.
  - c. Ensure that you can stop and start the server.
  - d. Reinstall eDiscovery Manager.
7. If the server status shows that there are no problems with the server, complete the following steps:
  - a. Cancel the installation.
  - b. Check the installation log files at `user.home/eDMInstallDebug*.log`.
  - c. Ensure that you can stop and start the eDiscovery Manager and FileNet P8 servers.
  - d. Reinstall eDiscovery Manager.

## ERROR: Setup for Microsoft Visual C++ Redistributable Package was not successful.

While installing IBM eDiscovery Manager, you receive an error that the Microsoft Visual C++ Redistributable Package was not installed successfully.

### Symptoms

ERROR: Setup for the Microsoft Visual C++ Redistributable Package was not successful.

### Causes

The C runtime environment was not installed properly.

### Resolving the problem

Depending on your operating system and the error message that you received, successfully install an appropriate version of the Microsoft Visual C++ Redistributable Package after installing IBM eDiscovery Manager.

Operating system	Error message	Post-installation action
64-bit	Setup for the Microsoft Visual C++ 2008 Redistributable Package (x64) was not successful.	Run the <i>EDM_HOME</i> \bin\vcredist2008\vcredist_x64.exe file.
64-bit	Setup for the Microsoft Visual C++ 2010 Redistributable Package (x64) was not successful.	Run the <i>EDM_HOME</i> \bin\vcredist2010\vcredist_x64.exe file.

## Installation completes with errors

If you receive errors when installing IBM eDiscovery Manager, check the eDiscovery Manager installation log and, in some cases, manually deploy the IBM WebSphere Application Server.

### Symptoms

The Installation Complete window of the eDiscovery Manager installation program reports that the installation completed with errors, for example (on a Windows system):

The installation completed with errors.

To get more detailed information, see the eDiscovery Manager installation log files.

eDiscovery Manager installation log files:  
C:\Program Files\IBM\EDM\logs\EDMInstallDebug\*.log

### Causes

Possible causes for the installation errors are:

- Specifying a directory that is not writable or does not exist.
- Failing a prerequisite check.
- Selecting the wrong WebSphere Application Server profile or selecting a WebSphere Application Server profile for which security was enabled, but not providing an administrative user name and password.
- Errors occurred when the eDiscovery Manager application server was being deployed to the WebSphere Application Server.

### Resolving the problem

To resolve the problem:

1. Check the eDiscovery Manager installation log files to see more detailed information. Search for errors at the end of the log file or files.


**During the installation:** During the installation, the eDiscovery Manager installation program writes installation progress messages, error messages, and IBM WebSphere Application Server deployment information to installation debug log files. If the installation debug log file reaches 5 MB in size, eDiscovery Manager rolls it over and creates another log file. eDiscovery Manager creates up to four installation log files (eDMInstallDebug00.log, eDMInstallDebug01.log, eDMInstallDebug02.log, and eDMInstallConfig3.log) before it begins overwriting the first log file.

**Before the installation completes:** Before the installation completes, the installation debug log files and the configuration debug log files exist in your home directory. On an AIX system, the home directory is defined by the HOME environment variable. On a Microsoft Windows system, the home directory is

defined by the HOMEPATH environment variable. For example, on Microsoft Windows, your home directory might be C:\Users\yourUserName.

2. If necessary, use WebSphere Application Server scripts to manually deploy the eDiscovery Manager application server:

The eDiscovery Manager deployment scripts are in the scriptsWAS subdirectory of the eDiscovery Manager installation directory.

- a.  Find and change the following lines in the eDMSAppConfig.bat file to keep the window open so that you can watch the deployment process:

```
Change: exit 0
to: rem exit 0
Change: exit %rc%
to: echo %rc%
```

- b. Based on the log file errors that you found, change the values of the appropriate variables in the setenv file and the appdeploy.properties file.

For example, if you selected the wrong WebSphere Application Server profile, change the value of the profile name parameter:

#### Windows (setenv.bat)

```
set PROFILE_NAME=eDMServer
set PROFILE_PATH=/usr/IBM/WebSphere/AppServer/profiles/eDMServer
```

**Tip:** You might also need to change the cellName and nodeName parameter values too. For example:

```
set PROFILE_NAME=eDMServer
set PROFILE_PATH=C:\Program Files\IBM\WebSphere\AppServer\profiles\
eDMServer
set cellName=mmr1aNode02Cell
set nodeName=mmr1aNode02
```

#### Windows (appdeploy.properties)

```
profileName=eDMServer
WASProfilePath=C:/Program Files/IBM/WebSphere/AppServer/profiles/
eDMServer
```

#### AIX (setenv.sh)

```
export PROFILE_NAME=eDMServer
export PROFILE_PATH=/usr/IBM/WebSphere/AppServer/profiles/eDMServer
```

**Tip:** You might also need to change the cellName and nodeName parameter values too. For example:

```
export PROFILE_NAME=eDMServer
export PROFILE_PATH=/usr/IBM/WebSphere/AppServer/profiles/
eDMServer
export cellName=mmr1aNode02Cell
export nodeName=mmr1aNode02
```

#### AIX (appdeploy.properties)

```
profileName=eDMServer
WASProfilePath=/usr/IBM/WebSphere/AppServer/profiles/eDMServer
```

- c. Deploy eDiscovery Manager from the command line. To capture console log messages, redirect the output of the deployment command to a log file.

For example, to deploy eDiscovery Manager to a secure WebSphere Application Server, enter:

#### AIX When installing:

```
eDMSAppConfig.sh install WAS_admin_username WAS_admin_password \
>> output.log
```

When upgrading:

```
eDAppConfig.sh update-all WAS_admin_username WAS_admin_password \  
>> output.log
```


### Windows

When installing:

```
eDAppConfig.bat install WAS_admin_username WAS_admin_password \  
>> output.log
```

When upgrading:

```
eDAppConfig.bat update-all WAS_admin_username WAS_admin_password \  
>> output.log
```

- d.  Run the `postinstalledm.sh` shell script to perform some necessary post-installation tasks.

The eDiscovery Manager scripts are in the `scripts` subdirectory of the eDiscovery Manager installation directory. For example, enter the following command to run the script on a WebSphere Application Server that has security enabled:

```
/opt/IBM/eDM/scripts/postinstalledm.sh TRUE WAS_admin_username \  
WAS_admin_password
```

If security is not enabled on the WebSphere Application Server, run the `postinstalledm.sh` shell script with only the `FALSE` parameter. For example:

```
/opt/IBM/eDM/scripts/postinstalledm.sh FALSE
```

## Where is the installation log file?

### Symptoms

You want to check the IBM eDiscovery Manager installation log files for errors, but you cannot find them.

### Causes

The eDiscovery Manager installation log files are in one directory during installation, and they are copied into another directory after the installation completes.

### Resolving the problem

**Before the installation completes:** Before the installation completes, the installation debug log files and the configuration debug log files exist in your home directory. On an AIX system, the home directory is defined by the `HOME` environment variable. On a Microsoft Windows system, the home directory is defined by the `HOMEPATH` environment variable. For example, on Microsoft Windows, your home directory might be `C:\Users\yourUserName`.

**After the installation completes:** After the installation completes, the installation debug log files and the configuration debug log files are copied to the `logs` subdirectory of the eDiscovery Manager installation directory. Also after installation, a single installation debug log file named `eDMInstall.log` is created in the same `logs` subdirectory.

## Uninstallation program not progressing

The IBM eDiscovery Manager uninstallation program appears to be frozen.

### Symptoms

When removing eDiscovery Manager, the uninstallation program appears to be stuck for a long time.

## Causes

The IBM WebSphere Application Server is frozen.

## Resolving the problem

To resolve the problem:

1. To check the status of the uninstallation process, go to the *WAS\_HOME/bin* directory and run the `serverStatus` WebSphere Application Server command for the WebSphere Application Server profile used by eDiscovery Manager, for example:  

```
> cd c:\Program Files\IBM\WebSphere\AppServer\bin
> serverStatus server1 -profilename AppSrv01 -username wasuserid
    -password waspassword
```

The `serverStatus` command might report a message from the server prompting you for user input, which could explain a delay in the uninstallation.
2. If the `serverStatus` command does not work, try to stop the WebSphere Application Server.
3. If you cannot stop the WebSphere Application Server, stop or kill the operating system process that the server is associated with.  
For example, on Windows, open the Windows Task Manager, select the `java.exe` process, and click **End Process**.

This should restore the WebSphere Application Server to a processing state, and the eDiscovery Manager uninstallation program should be able to finish.

If the uninstallation program is still unable to remove eDiscovery Manager, try the following manual uninstallation procedure:

1. Starting at the end of the file, check the eDiscovery Manager uninstallation log file (*user.home\EDMUninstallDebug\*.log*) for errors.
2. If errors occurred because the eDiscovery Manager data could not be deleted from the server, remove the data from the server manually.
3. If errors occurred because objects were removed from the WebSphere Application Server before the uninstallation program was run, you can ignore these errors.
4. If errors occurred when the eDiscovery Manager application server was being removed from, or upgraded to, the WebSphere Application Server, use the WebSphere Administrative Console to manually remove any eDiscovery Manager objects that were not removed by the eDiscovery Manager uninstallation program.

### Servers

In Application servers > *server\_name* > Process definition > Environment Entries:

- LIBPATH (C:\IBM\edm\lib)
- PATH (C:\IBM\edm\lib)

### Class loaders

In Application servers > *server\_name* > Java and Process Management > Class loader, remove all class loaders that are associated with the EDMLibraries application.

**Note:** If you dedicated the server profile to eDiscovery Manager, as required, you can delete all of the class loaders. If you did not dedicate the server profile to eDiscovery Manager, some of the class loaders might belong to the other applications that share the server profile. In the latter case, complete the following steps:

- a. Determine which class loaders are associated with eDiscovery Manager by selecting each class loader ID and then selecting **Shared Library reference** from the right-click menu.
- b. If the associated application is EDMLibraries, remove the class loader.

#### Applications

- EDMClient
- EDMWorkMgrServer

#### Async beans work managers

- EDMClientWorkManager
- EDMServerWorkManager
- EDMWorkItemManager


#### Mail, Mail Session

EDMMailSession

#### Shared libraries

- EDMLibraries
- EDMWorkMgrLibrary
- EDMClientLibrary

#### JVM Properties

- heap size=254, max heap size=1 GB
- classpath, for example on Windows C:\IBM\eDM\config\resources;C:\IBM\eDM\config;C:\Program Files\IBM\db2cmv8\cmgmt
- In the Generic JVM arguments:
  - DedmBinDir=C:\IBM\eDM\bin\
-  An additional parameter in the Generic JVM argument:
  - Djava.security.auth.login.config=eDM\_HOME\config\jaas.conf.WebSphere

5. If necessary, remove eDiscovery Manager from the WebSphere Application Server by entering one of the following commands:

#### AIX

```
eDmAppConfig.sh uninstall WAS_admin_username  
WAS_admin_password > deploy.log
```

#### Windows

```
eDmAppConfig.bat uninstall WAS_admin_username  
WAS_admin_password > deploy.log
```

6. If the eDiscovery Manager installation directory was not removed by the previous step:
  - a. Delete the eDiscovery Manager installation directory and all of its subdirectories.
  - b. Use a text editor to ensure that the .com.zerog.registry.xml file does not contain any eDiscovery Manager entries.
    - On AIX, this file resides in the /var directory.




- On Windows, this file resides in the C:\Program Files\Zero G Registry directory.


For example, remove the eDiscovery Manager <product> section and the related <component> sections from this excerpt of the file:

```
<products>
  <product
    name="IBM eDiscovery Manager"
    id="774ec792-1ee7-11b2-b690-81c32a44cc0a"
    version="2.1.0.0"
    copyright="2008"
    info_url="w3.ibm.com"
    support_url="w3.ibm.com"
    location="C:\IBM\EDM"
    last_modified="2008-05-06 12:59:31">
    <![CDATA[$PRODUCT_ID_DESCRIPTION$]]>
  <vendor
    name="IBM"
    id="72938779-1ee7-11b2-b3ce-81c32a44cc0a"
    home_page="w3.ibm.com"
    email="w3.ibm.com"/>
  <feature
    name="FCL"
    last_modified="2008-05-06 12:59:43">
    <![CDATA[]]>
    <component
      ref_id="72938789-1ee7-11b2-b3d4-81c32a44cc0a"
      version="1.0.0.0"
      location="C:\IBM\EDM\Uninstall_eDM\Uninstall_eDM.exe"/>
    <component
      ref_id="72938789-1ee7-11b2-b3d9-81c32a44cc0a"
      version="1.0.0.0"
      location="C:\IBM\EDM\jre"/>
    <component
      ref_id="72938788-1ee7-11b2-b3d7-81c32a44cc0a"
      version="1.0.0.0"
      location=""/>
    </feature>
  </product>
</products>
<components>
  <component
    id="72938788-1ee7-11b2-b3d7-81c32a44cc0a"
    version="1.0.0.0"
    name="InstallAnywhere Uninstall Component"
    location=""
    vendor="IBM"/>
  <component
    id="72938789-1ee7-11b2-b3d9-81c32a44cc0a"
    version="1.0.0.0"
    name="InstallAnywhere VM Component"
    location="C:\IBM\EDM\jre"
    vendor="IBM"/>
  <component
    id="72938789-1ee7-11b2-b3d4-81c32a44cc0a"
    version="1.0.0.0"
    name="Common"
    location="C:\IBM\EDM\Uninstall_eDM\Uninstall_eDM.exe"
    vendor="IBM"/>
</components>
```

- Remove c:\ibm\edm\lib\edcutil.jar from the CLASSPATH system environment variable.
- Remove c:\ibm\edm\lib from the PATH system environment variable.

#### Related information

 WebSphere Application Server Version 7.0 Information Center  
Welcome to the IBM WebSphere Application Server information center where you can find the documentation for various editions of the application server.

 WebSphere Application Server Version 8.0 Information Center  
Welcome to the IBM WebSphere Application Server information center where you can find the documentation for various editions of the application server.

## Uninstallation stops due to a DGL3704A error from DB2

The IBM eDiscovery Manager uninstallation program stops due to a DGL3704A error from DB2.

### Symptoms

[ERROR] DGL3704A: Error found in component type attribute; ICM7015:  
During an SQL operation in the library server, an unexpected error occurred. For details on the error, refer to the database document.  
(STATE) : [LS RC = 7015, SQL RC = -911]

### Causes

The eDiscovery Manager application server was not stopped and restarted before the uninstallation program was run.

### Resolving the problem

Stop and restart the eDiscovery Manager application server, then run the uninstallation program again. See the WebSphere Application Server product information for details about stopping and starting an application server.

If running the uninstallation program a second time produces the same error, try restarting DB2 to release any locks that were held.

### Related information

 WebSphere Application Server Version 7.0 - Starting and stopping quick reference

 WebSphere Application Server Version 8.0 - Starting and stopping quick reference

## Silent installation fails to run and an error message is not displayed

After starting the eDiscovery Manager installation program, the program exits without any indication of a problem.

### Symptoms

The installation program fails to run and no log is created.

### Causes

There is not enough disk space to run the installation program.

### Diagnosing the problem

After five minutes, if no *user home\EDMInstallDebug00.logfile* is created and no *EDM.exe* process is running, check that there is enough disk space.

### Resolving the problem

**User response:** Verify that your system meets the minimum hardware and software requirements. See eDiscovery Manager, V2.2.2 system requirements.

## eDiscovery Manager component could not be removed

When removing or upgrading IBM eDiscovery Manager, you receive a message that one of the eDiscovery Manager components could not be uninstalled.

### Symptoms

Uninstallation errors are recorded in the eDiscovery Manager uninstallation log file (*user.home\EDMUninstallDebug\*.log*).

### Causes

Possible causes for the uninstallation errors are:

- The eDiscovery Manager data could not be deleted from the server.
- Some or all the eDiscovery Manager objects were manually removed from the IBM WebSphere Application Server before you tried to remove or upgrade eDiscovery Manager.
- Errors occurred while the eDiscovery Manager application server was being removed from the WebSphere Application Server.

### Resolving the problem

To resolve the problem:

1. Starting at the end of the file, check the eDiscovery Manager uninstallation log file (*user.home\EDMUninstallDebug\*.log*) for errors.
2. If errors occurred because the eDiscovery Manager data could not be deleted from the server, remove the data from the server manually.
3. If errors occurred because objects were removed from the WebSphere Application Server before the uninstallation program was run, you can ignore these errors.
4. If errors occurred when the eDiscovery Manager application server was being removed from, or upgraded to, the WebSphere Application Server, use the WebSphere Administrative Console to manually remove any eDiscovery Manager objects that were not removed by the eDiscovery Manager uninstallation program.

### Servers

In Application servers > *server\_name* > Process definition > Environment Entries:

- LIBPATH (C:\IBM\EDM\lib)
- PATH (C:\IBM\EDM\lib)

### Class loaders

In Application servers > *server\_name* > Java and Process Management > Class loader, remove all class loaders that are associated with the EDMLibraries application.

**Note:** If you dedicated the server profile to eDiscovery Manager, as required, you can delete all of the class loaders. If you did not dedicate the server profile to eDiscovery Manager, some of the class loaders might belong to the other applications that share the server profile. In the latter case, complete the following steps:

- a. Determine which class loaders are associated with eDiscovery Manager by selecting each class loader ID and then selecting **Shared Library reference** from the right-click menu.
- b. If the associated application is EDMLibraries, remove the class loader.

### Applications

- EDMClient
- EDMWorkMgrServer

### Async beans work managers

- EDMClientWorkManager
- EDMServerWorkManager
- EDMWorkItemManager

### Mail, Mail Session

EDMMailSession

### Shared libraries

- EDMLibraries
- EDMWorkMgrLibrary
- EDMClientLibrary

### JVM Properties

- heap size=254, max heap size=1 GB
- classpath, for example on Windows C:\IBM\EDM\config\resources;C:\IBM\EDM\config;C:\Program Files\IBM\db2cmv8\cmgmt
- In the Generic JVM arguments:  
-DedmBinDir=C:\IBM\EDM\bin\
- **FileNet P8** An additional parameter in the Generic JVM argument:  
-Djava.security.auth.login.config=eDM\_HOME\config\jaas.conf.WebSphere

5. If necessary, remove eDiscovery Manager from the WebSphere Application Server by entering one of the following commands:

### AIX

```
eDmAppConfig.sh uninstall WAS_admin_username  
WAS_admin_password > deploy.log
```

### Windows

```
eDmAppConfig.bat uninstall WAS_admin_username  
WAS_admin_password > deploy.log
```

6. If the eDiscovery Manager installation directory was not removed by the previous step:
  - a. Delete the eDiscovery Manager installation directory and all of its subdirectories.
  - b. Use a text editor to ensure that the .com.zerog.registry.xml file does not contain any eDiscovery Manager entries.
    - On AIX, this file resides in the /var directory.
    - On Windows, this file resides in the C:\Program Files\Zero G Registry directory.

For example, remove the eDiscovery Manager <product> section and the related <component> sections from this excerpt of the file:

```
<products>  
  <product  
    name="IBM eDiscovery Manager"  
    id="774ec792-1ee7-11b2-b690-81c32a44cc0a"  
    version="2.1.0.0"  
    copyright="2008"  
    info_url="w3.ibm.cm"
```

```

        support_url="w3.ibm.com"
        location="C:\IBM\edm"
        last_modified="2008-05-06 12:59:31">
<![CDATA[$PRODUCT_ID_DESCRIPTION$]]>
<vendor
  name="IBM"
  id="72938779-1ee7-11b2-b3ce-81c32a44cc0a"
  home_page="w3.ibm.com"
  email="w3.ibm.com"/>
<feature
  name="FCL"
  last_modified="2008-05-06 12:59:43">
<![CDATA[]]>
<component
  ref_id="72938789-1ee7-11b2-b3d4-81c32a44cc0a"
  version="1.0.0.0"
  location="C:\IBM\edm\Uninstall_edm\Uninstall_edm.exe"/>
<component
  ref_id="72938789-1ee7-11b2-b3d9-81c32a44cc0a"
  version="1.0.0.0"
  location="C:\IBM\edm\jre"/>
<component
  ref_id="72938788-1ee7-11b2-b3d7-81c32a44cc0a"
  version="1.0.0.0"
  location=""/>
</feature>
</product>
</products>
<components>
<component
  id="72938788-1ee7-11b2-b3d7-81c32a44cc0a"
  version="1.0.0.0"
  name="InstallAnywhere Uninstall Component"
  location=""
  vendor="IBM"/>
<component
  id="72938789-1ee7-11b2-b3d9-81c32a44cc0a"
  version="1.0.0.0"
  name="InstallAnywhere VM Component"
  location="C:\IBM\edm\jre"
  vendor="IBM"/>
<component
  id="72938789-1ee7-11b2-b3d4-81c32a44cc0a"
  version="1.0.0.0"
  name="Common"
  location="C:\IBM\edm\Uninstall_edm\Uninstall_edm.exe"
  vendor="IBM"/>
</components>

```

- c. Remove c:\ibm\edm\lib\edcutil.jar from the CLASSPATH system environment variable.
- d. Remove c:\ibm\edm\lib from the PATH system environment variable.

## ACL data and privilege set exceptions when deleting eDiscovery Manager data

ACL data and privilege set exceptions (for example, DGL3757A DGL3795A) can occur when you try to remove IBM eDiscovery Manager and its data.

### Symptoms

If you choose to delete the eDiscovery Manager data when uninstalling, DGL3757A and DGL3795A errors can occur, which prevent the uninstallation program from deleting some data.

### Causes

These errors indicate that the specified access control list (ACL) or privilege set cannot be removed. This situation typically occurs when one or more user definitions have the specified ACL as their default item ACL or have the specified privilege set as their maximum privilege set. It can also occur when one or more ACL definitions reference the specified privilege sets.

## Resolving the problem

To resolve the problem:

1. Work with the IBM Content Manager Enterprise Edition administrator to use the IBM Content Manager system administration client to find the user or users that are referencing the ACL or privilege set, and remove those references.
2. Try to remove eDiscovery Manager again:
  - If you are performing a non-silent uninstallation, when prompted by the uninstallation program to delete the data, click **Yes**.
  - If you are performing a silent uninstallation, enter this command:  
`Uninstall_eDM.exe -DDELETE_DATA=YES`

Alternatively, if you want to resolve the data deletion issue later and let the uninstallation program continue without deleting the rest of the data:

- If you are performing a non-silent uninstallation, when prompted by the uninstallation program to try deleting the data again, click **No**.
- If you are performing a silent uninstallation, enter this command:  
`Uninstall_eDM.exe -DDELETE_DATA=NO`

## Some eDiscovery Manager files might not be removed during uninstallation

If the IBM eDiscovery Manager uninstallation program is unable to remove all of its files during the uninstallation process, some unused files are left on the system.

### Symptoms

None.

### Causes

This situation can occur if a process is using any of the eDiscovery Manager files when you uninstall the product. Also, the uninstallation program does not remove any file that has been changed after being originally installed.

## Resolving the problem

To determine that all the eDiscovery Manager files were removed, look for the following directories. If these directories remain after uninstallation, check their contents for any data that you want to keep. Otherwise, you can safely delete them.

- The eDiscovery Manager installation directory and its contents. For example:  
`C:\Program Files\IBM\EDM\`
- The two following subdirectories under `WAS_home\profiles\EDMServer_profile\installedApps\cell_name\`
  - `EDMClient.ear`
  - `EDMWorkMgrServer.ear`

For example:

`C:\WebSphere\AppServer\profiles\AppSrv2\installedApps\c1Node2Cell\EDMClient.ear\`

**Important:** If the EDMClient.ear and EDMWorkMgrServer.ear directories exist after uninstallation, you can safely delete them and their contents, but do not delete their parent directory *WAS\_home\profiles\edMServer\_profile\installedApps\cell\_name\*. This parent directory is managed by IBM WebSphere Application Server, not by eDiscovery Manager.

## Installation fails because a supported version of IBM Information Integrator for Content was not found

The IBM eDiscovery Manager installation program cannot find IBM Information Integrator for Content even when a correct installation directory for it is provided.

### Symptoms

You receive an error on the Configuration panel of the eDiscovery Manager installation program that states a supported version of IBM Information Integrator for Content was not found even though one was correctly specified. Also, the installation debug log file might contain a line stating Errors occurred, after which a path name for the user installing eDiscovery Manager appears to be truncated, for example:

```
Errors occurred: 1
(from com.ibm.icm.edc.installer.util.FindCMClientLevel2.cmClientLevel)
Wed Jul 21 16:39:13.984 PDT 2010 : INFO : ICM_CLIENT_VERSION_STDERR=The java
class is not found: Settings\Temp\1\edmtmp;C:\DOCUME~1\user_name\Local
```

### Causes

You have a TEMP or TMP user environment variable that contains a space in its path name when you install eDiscovery Manager.

### Resolving the problem

Before installing eDiscovery Manager, change the values for the TEMP and TMP user environment variables so that neither value contains any spaces. Make a note of the current values for these variables if you want to restore them after you install eDiscovery Manager.

To change the values of the TEMP and TMP variables:

1. On the Desktop, right-click **My Computer**, then select **Properties**.
2. Click the **Advanced** tab.
3. Click **Environment Variables**.
4. In the **User variables** list, repeat the following steps for both the TEMP and TMP variables:
  - a. Select the TEMP variable and then click **Edit**.
  - b. In the **Variable value** field, change the value to a path that contains no spaces. For example, change it to C:\TEMP.
5. Click **OK** until you exit the **Properties** dialog.

## Exporting content that has an unsupported MIME type

When content is exported to HTML and PDF formats, you might get an output export file that states a MIME type is not supported.

### Symptoms

When you export content to HTML and PDF formats, it is possible to get an export file that contains only this single sentence:

This document has a MIME type that is unsupported by this export plug-in.

An export file such as this one does not represent an error.

### **Diagnosing the problem**

The underlying, vendor-acquired component of eDiscovery Manager that converts items from one format to another format is working as designed. These export files are created when the conversion of an item to HTML or PDF format is not possible. For example, MP3 files cannot be converted to HTML or PDF format. Exporting content to its native format does not produce these export files because native exports do not convert items from one format to another format.

---

## **Troubleshooting configuration problems**

Solve common configuration problems.

### **Cannot access eDiscovery Manager (Content Manager EE)**

Your eDiscovery users cannot log in to the IBM eDiscovery Manager web client.

#### **Symptoms**

When a user tries to log in to the eDiscovery Manager web client, the user receives the following error:

The configuration information could not be retrieved from the content server.

Ensure that the server is running and try the operation again.

If the problem persists, see more detailed information by starting at the end of the web client log file and searching backwards for the keyword "SEVERE" near the time that this error occurred. By default, log files are stored in the logs subdirectory of the eDiscovery Manager installation directory.

#### **Causes**

The user was not added to the eDiscovery group or the user was not assigned a privilege set.

#### **Resolving the problem**

Work with the IBM Content Manager Enterprise Edition system administrator to use the IBM Content Manager system administration client to verify the following things:

- On the Define Users tab, each user is assigned a maximum privilege set of ClientUserReadOnly or one of the EDM\* privilege sets.
- On the Assign to Groups tab, each user is assigned to the eDiscovery group.
- On the Set Defaults tab, the default item ACL for each user is set to EDMModelItemACL.

### **Cannot access eDiscovery Manager (FileNet P8)**

Your eDiscovery users cannot log in to the IBM eDiscovery Manager web client.

#### **Symptoms**

When a user tries to log in to the eDiscovery Manager web client, the user receives the following error:

The configuration information could not be retrieved from the content server.

Ensure that the server is running and try the operation again.

If the problem persists, see more detailed information by starting at the end of the web client log file and searching backwards for the keyword "SEVERE" near the time that this error occurred. By default, log files are stored in the logs subdirectory of the eDiscovery Manager installation directory.

#### **Causes**



The user was not added to the eDiscovery group.

### Resolving the problem

Work with the directory service administrator to verify that all users who want access to eDiscovery Manager are members of the eDiscovery group.

## Users and administrators prompted for Lotus Notes password

The Lotus Notes password manager is not configured correctly to supply IBM eDiscovery Manager with the password for accessing the Lotus Domino server.

### Symptoms

Users are prompted for their passwords when they click the **View this content in Lotus Notes** icon in the Native View column of the Search Results pane of the eDiscovery Manager web client. Administrators are prompted for their passwords when they run the eDiscovery Manager utility notesConnect.

### Causes

One or more environment variables on the eDiscovery Manager system are not set correctly.

### Resolving the problem

To resolve the problem, verify that the PATH system variable includes:

- The path to the ibmpow subdirectory of the Lotus Domino installation directory, for example, /opt/IBM/Lotus/Notes/latest/ibmpow
- The path to the C subdirectory of the Lotus Domino installation directory, for example, /opt/IBM/Lotus/Notes/latest/ibmpow/res/C
- The path to the Lotus Domino data directory, for example, /opt/notesdata
- The path to the bin subdirectory of the Lotus Domino server, for example, /opt/IBM/Lotus/bin

#### Related tasks

“Configuring the password manager for Lotus iNotes and Lotus Notes viewing” on page 116

When the Lotus Domino server that stores the Lotus Notes viewing database is accessed, IBM eDiscovery Manager must authenticate with the Lotus Domino environment. It does so by using a Lotus Notes ID file and having the Lotus Notes password manager programmatically supply the password for the eDiscovery Manager user ID. Configuring the eDiscovery Manager system to bypass the Lotus Domino password prompt is a prerequisite to your users successfully viewing email with IBM Lotus iNotes or Lotus Notes.

## [Servlet Error]-[action]: java.lang.NoClassDefFoundError: lotus.domino.NotesException

After clicking **Apply** on one of the configuration panes of the Administration page, an error occurs.

### Symptoms

[Servlet Error]-[action]: java.lang.NoClassDefFoundError:  
lotus.domino.NotesException

### Causes

The Notes.jar file was not in the IBM WebSphere Application Server shared library classpath.

## Resolving the problem

Verify that the Notes.jar file is in the WebSphere Application Server shared library classpath:

1. Open the WebSphere Application Server administrative console by clicking **Start > Programs > IBM WebSphere > Application Server > Profiles > eDiscovery Manager application server profile > Administrative console**.
2. Expand **Environment, Shared Libraries, and EDMLibraries**.
3. Confirm that the **Classpath** field contains an entry for the fully-qualified path to the Notes.jar file, for example: C:/Program Files/Lotus/Domino/jvm/lib/ext/Notes.jar.
4. If there is no entry for the Notes.jar file, add one.
5. Stop and restart the IBM eDiscovery Manager application server for your change to take effect.

### Related information

 WebSphere Application Server Version 7.0 - Starting and stopping quick reference

 WebSphere Application Server Version 8.0 - Starting and stopping quick reference

## Configuring the TCP/IP timeout value for Lotus Domino servers

If exports of Lotus Domino content fail randomly and you see a DYRS5033E error on the Work Manager status page when the exports fail, try increasing the TCP/IP timeout value.

### Symptoms

DYRS5033E: Unable to find path to server <hostname>

### Causes

By default, the TCP/IP timeout value on Lotus Domino servers is five seconds, which might be too short when exporting Lotus Domino content.

## Resolving the problem

To avoid time-outs during content exports, you can set the TCP/IP timeout value to a higher value such as 30 seconds or 60 seconds. To set the TCP/IP timeout value:

1. Edit the notes.ini file on both the primary and secondary Lotus Domino servers and set the default timeout value to 30 seconds by changing the value of the TCPIP\_TcpConnectTimeout parameter to 0,30. For example:  
TCPIP\_TcpConnectTimeout=0,30
2. Stop both the primary Lotus Domino server and the IBM eDiscovery Manager application server.
3. Run the following command on the primary Lotus Domino server and the eDiscovery Manager application server. Run this command from the Lotus Notes data directory as the Lotus Notes user.  
nsd -kill
4. Restart the primary Lotus Domino server and the eDiscovery Manager application server.
5. If exports of Lotus Domino content continue to fail, increase the TCP/IP timeout value on the primary and secondary Lotus Domino servers to a higher value, depending on your network speed. For example:

TCPIP\_TcpConnectTimeout=0,60

## Error while searching for senders or recipients by using LDAP from the IBM eDiscovery Manager web client

You received an error while trying to search for senders or recipients using LDAP from the eDM web client.

### Symptoms

The edmapp0.log file shows an error like the following:

```
[2011-03-31 11:33:26.455] [20927 ] [SEVERE ] [24 ] [METHOD ] [com.ibm.icm.chl.console.exception.Message] [init ] Unprocessed Continuation Reference(s)
```

```
com.ibm.icm.edc.emailconv.ldap.LdapLookupServiceException: Unprocessed Continuation Reference(s)
```

### Causes

You might encounter this problem if not all of your users are located in your domain root.

### Resolving the problem

When you use the Active Directory as your LDAP server, use port 3268 (the Global Catalog port) rather than the default port 389 in the eDiscovery Manager LDAP Configuration panel.

## Enabling eDiscovery Manager logging

Users that are assigned the IT Administrator role can enable logging for the IBM eDiscovery Manager web client and the eDiscovery Manager work manager on the Administration page of the eDiscovery Manager web client. Information about logging configuration options is available in the online help system.

By default, when logging is enabled, eDiscovery Manager maintains four rotating log files with a maximum size of 2 MB each.

For performance and disk space reasons, it is a good idea to configure multiple log files that are smaller rather than a single large log file. When the last log file reaches the maximum size, eDiscovery Manager begins writing to the first log file again, and the previous entries in that file are overwritten. For example, if two files are configured with a maximum size of 1 MB, when the first log file is full, eDiscovery Manager begins writing to the second log file. When the second log file is full, eDiscovery Manager begins writing to the first log file again.

Specifying a value of 0 (zero) for either of the **Size limit of each log file (MB)** fields on the Logging pane of the Administration page has two implications:

- The log file size is unlimited. The log file will continue to grow with no restrictions on its size.
- Regardless of the value that you provide for the **Number of rotating log files** field, only one log file will be created. With no limit on the log file size, there is no need to roll over the first log file and create another one.

**Recommendation:** Never set the value of a **Size limit of each log file (MB)** field to 0 (zero).

Log files contain messages about system operation that can help with troubleshooting. When you configure logging, you can choose which level of

messages will be logged. The logging levels are standard Java logging categories. To maximize performance, do not configure a more detailed logging level than you need.

Log files are stored in the logs subdirectory of the eDiscovery Manager installation directory.

---

## Troubleshooting problems during search or use

Solve errors that occur during search or product usage.

### Opening multiple browser windows or tabs causes unexpected behavior

Browsers that support multiple open tabs or multiple open windows can confuse users.

#### Symptoms

After a user logs in to the IBM eDiscovery Manager web client, the user can open another tab or window in the same browser and paste the URL from the first session into the address field of the new tab or windows. Doing this appears to bypass the eDiscovery Manager login page and open a new session with the user automatically logged in to the second session.

#### Causes

This behavior is typical of web browsers, but it can cause confusion if users are not aware of it.

#### Resolving the problem

This behavior does not bypass the eDiscovery Manager login page and therefore does not pose a security risk. Users must understand the typical behavior of their browsers:

- Internet Explorer—Multiple tabs in the same browser instance use the same session. Multiple browser instances use different sessions.
- Mozilla Firefox—Multiple tabs in the same browser instance use the same session. Multiple browser instances also use the same session.

**Recommendation:** Users should access eDiscovery Manager in only one tab in their web browser. In addition, users should log out of the eDiscovery Manager web client or close all browser windows when they are done using the web client.

### DYRC2004E when accessing a folder

A user tried to access a folder after an eDiscovery administrator changed a collection name or removed a collection.

#### Symptoms

DYRC2004E: The folder contains content from a collection (*collectionName*) that was renamed. Administrator response: Change the name of the collection back to its original name on the Collections pane of the Administration page.

#### Causes

Because the collection name was associated with the case (and thus, the folder), attempts to access the folder failed when the collection was not found.

## Resolving the problem

In general, after a collection is defined, its name should not be changed and the collection should not be removed because cases, folders, and saved searches have dependencies on collection names.

**Administrator responses:** Resolve the problem in one of three ways from the Collections pane of the Administration page.

- If a collection name was modified, change it back to its original name.
- If a collection was inadvertently removed, add it back.
- If a collection was purposely removed:
  1. Temporarily add the collection back.
  2. If the case in which the folder resides is not already inactive, make the case inactive.
  3. Delete the case.
  4. Inactivate, then delete any case that references the collection name. A collection is not completely removed until all cases that reference it are deleted.

**Attention:** Content from multiple collections can exist in the same case, so be sure that you really want to delete a case before doing so. When you delete a case, you remove all folders, content references, saved searches, and audit records that are associated with the case. Content is not deleted from the content archive.

5. Delete the collection.

## DYRC1028E when viewing folder contents

A user tried to select a folder to view its contents after an eDiscovery administrator changed a collection name or removed a collection.

### Symptoms

DYRC1028E: The folder contains content from one or more collections (*collectionName*) that no longer exist. Administrator response: From the Collections pane of the Administration page, take one of two actions: If a collection name was modified, change the collection name back to its original name. If a collection was removed, add the collection back.

### Causes

Because the collection name was associated with the case (and thus, the folder), attempts to access the folder failed when the collection was not found.

## Resolving the problem

In general, after a collection is defined, its name should not be changed and the collection should not be removed because cases, folders, and saved searches have dependencies on collection names.

**Administrator responses:** Resolve the problem in one of three ways from the Collections pane of the Administration page.

- If a collection name was modified, change it back to its original name.
- If a collection was inadvertently removed, add it back.
- If a collection was purposely removed:
  1. Temporarily add the collection back.
  2. If the case in which the folder resides is not already inactive, make the case inactive.

3. Delete the case.
4. Inactivate, then delete any case that references the collection name. A collection is not completely removed until all cases that reference it are deleted.

**Attention:** Content from multiple collections can exist in the same case, so be sure that you really want to delete a case before doing so. When you delete a case, you remove all folders, content references, saved searches, and audit records that are associated with the case. Content is not deleted from the content archive.

5. Delete the collection.

## Export to NSF file not progressing

An export task is in the Running state but it is not making progress.

### Symptoms

An export task is in the Running state but the process appears to be frozen.

### Causes

This typically indicates a configuration problem.

### Resolving the problem

To resolve the problem:

1. Verify whether the dominoExport.exe process is lingering in the task list. If it is, end the task.
2. Test that the Lotus Notes password manager is properly configured by running the IBM eDiscovery Manager utility notesConnect.
  - a. Run notesConnect without specifying parameters to get usage information.  
The notesConnect utility is in the bin subdirectory of the eDiscovery Manager installation directory.
  - b. Run notesConnect again with the Lotus Domino server parameter to connect to the Lotus Domino server and return the title from the database name that is supplied. If the password prompt does not appear, the password manager is configured correctly.
  - c. Check the LotusPwMgr.log file on your system for the message Successfully retrieved password.

### Related tasks

“Configuring the password manager for Lotus iNotes and Lotus Notes viewing” on page 116

When the Lotus Domino server that stores the Lotus Notes viewing database is accessed, IBM eDiscovery Manager must authenticate with the Lotus Domino environment. It does so by using a Lotus Notes ID file and having the Lotus Notes password manager programmatically supply the password for the eDiscovery Manager user ID. Configuring the eDiscovery Manager system to bypass the Lotus Domino password prompt is a prerequisite to your users successfully viewing email with IBM Lotus iNotes or Lotus Notes.

## Export not progressing or Lotus Notes viewing causes eDiscovery Manager application server to crash

An export task appears to be frozen or, when users try to view content in their Lotus Notes clients, HTTP errors occur that cause the IBM eDiscovery Manager application server to crash.

## Symptoms

When exporting content, the export appears to be stuck for a long time. The export does not appear to be progressing.

Users that attempt to view content in their Lotus Notes client receive HTTP errors. These errors cause the eDiscovery Manager application server to crash.

## Causes

The WebSphere JVM crashes when eDiscovery Manager tries to load the Lotus Notes password manager on the AIX system where the Lotus Domino server is running.

## Resolving the problem

To resolve the problem:

1. Set the LDR\_CNTRL environment variable in the .profile file of the Lotus Notes user ID on that system by entering the following command:  

```
export LDR_CNTRL=MAXDATA=0XC0000000@DSA
```
2. Restart the Lotus Domino server.
3. Restart the eDiscovery Manager application server.

## Invalid password causes Lotus Domino export failure

If an invalid password is stored in the LotusPWMgr.ini file on the IBM eDiscovery Manager system, exports of Lotus Domino content can fail without notification.

## Symptoms

A task that exports Lotus Domino content remains in the Running state indefinitely.

## Causes

The LotusPWMgr.ini file on the eDiscovery Manager system contains an invalid Lotus Domino password.

## Diagnosing the problem

To verify the cause of the task failure, examine the LotusPWMgr.log file or run the eDiscovery Manager utility notesConnect.

## Resolving the problem

Enter a valid password in the LotusPWMgr.ini file. See step 5 of “Configuring the password manager for Lotus Notes export” on page 122

## Internal Server Error during export of Lotus Domino Lotus Domino content

While exporting Lotus Domino content, you receive an HTTP Internal Server Error. A related Windows runtime error can occur when you manually run dominoExport.exe.

## Symptoms

The system cannot connect to the server. The server might be down or there might be a network problem. HTTP error code: 500, error text: Internal Server Error.

## Causes

The C runtime environment was not running during the export.



## Resolving the problem

Manually run the Microsoft Visual C++ 2008 Redistributable Package and the Microsoft Visual C++ 2010 Redistributable Package (vcredist\_64.exe for 64-bit installations) before attempting to export content again.

**On 64-bit installations, run these files:**

- *EDM\_HOME\bin\vcredist2008\vcredist\_x64.exe*
- *EDM\_HOME\bin\vcredist2010\vcredist\_x64.exe*

## Lotus Domino Server Not Found error during export

During a high-volume export of Lotus Domino content, you receive a Domino Server Not Found error.

### Symptoms

A Lotus Domino Server Not Found error occurs during a high-volume export of Lotus Domino content in an IBM FileNet P8 environment.

### Causes

The IBM WebSphere Application Server Maximum Java Heap value is too high for FileNet P8 on the AIX platform.

### Environment

AIX

## Resolving the problem

Set the WebSphere Application Server Maximum Java Heap to the correct value for your environment. To determine the correct value, download the FileNet P8 Performance Tuning Guide.

## File name issues with the collection definition export

When you export a collection definition and that collection has a name that includes special characters, the resulting XML file might not have the name that you expect.

### Symptoms

Depending on your browser type, file names such as [1].xml can result from exporting a collection definition if the collection name includes certain characters.

## Resolving the problem

The following characters are the special characters that can result in unexpected file name output:

'	Apostrophe
/	Forward slash
?	Question mark
*	Asterisk
#	Hash symbol
]	Right bracket
@	At sign
[	Left bracket
}	Right curly bracket



	\	Back slash
	{	Left curly bracket
	)	Right parenthesis
	^	Caret
	(	Left parenthesis
	;	Semicolon
	:	Colon
	%	Percent symbol
	~	Tilde
	,	Comma
	.	Period
	_	Underscore
	\$	Dollar sign
		Pipe
	!	Exclamation point
	+	Plus sign

## NSFDbOpenExtended: This database cannot be opened because a consistency check of it is needed

During a high volume export of Lotus Domino content, the export task stopped and could not be restarted.

### Symptoms

The dominoExport.log file contains the following error message:

```
Tue Dec 09 15:25:40 2008 PID 992 - Error checking existence of database \
9.30.152.129!!exportedDocs\1209\TC1_20081208T22200036_72...retrying 1 of 1.
NSFDbOpenExtended: This database cannot be opened because a consistency \
check of it is needed.
Tue Dec 09 15:25:40 2008 PID 332 - Verify that Password Manager and the Domino \
server name are configured correctly.
Tue Dec 09 15:25:40 2008 PID 332 - RESULT -6
Tue Dec 09 15:25:40 2008 PID 332 - ERROR Creating or opening \
exportedDocs\1209\TC1_20081208T22200036_72: NOTES ERROR in method \
NSFDbOpenExtended: This database cannot be opened because a consistency check \
of it is needed. Exiting.
```

### Causes

A Lotus Notes database (NSF file) was corrupted during its creation.

### Resolving the problem

Contact IBM Software Support to request a Lotus Domino fix for this problem.

- If you have Lotus Domino Version 8.5 Fix Pack 1, request SPR #DROO7NSSCB.
- If you have a version of Lotus Domino other than Version 8.5 Fix Pack 1, request that the SPR for Version 8.5.1 be used as the basis for fixing your version.

**Workaround:** If you choose not to apply the Lotus Domino fix, delete all of the Lotus Notes databases (NSF files) that were created by the failed export task, then create and run a new export task. Do not try to restart or resume the failed export task.

## Attempt to create duplicate template rejected

When an export task creates a temporary Lotus Notes database, a harmless message is written to the Lotus Domino server.

### Symptoms

```
07/25/2008 12:47:44 Attempt by CN=cma61/0=svlibm to create duplicate template
StdR8Mail in database /opt/notesdata/exportedDocs/51091/eDM01_20080725T15360047.
nsf - rejected.
07/25/2008 12:48:14 Closed session for cma61/svlibm Databases accessed:      2
Documents read:      0 Documents written: 999
07/25/2008 12:48:24 Closed session for cma61/svlibm Databases accessed:      2
Documents read:      0 Documents written: 1000
07/25/2008 12:48:30 Closed session for cma61/svlibm Databases accessed:      2
Documents read:      0 Documents written: 1000
07/25/2008 12:48:45 Closed session for cma61/svlibm Databases accessed:      2
Documents read:      0 Documents written: 1000
07/25/2008 12:49:30 Attempt by CN=cma61/0=svlibm to create duplicate template
StdR8Mail in database /opt/notesdata/exportedDocs/51091/eDM01_20080725T15360047.
nsf - rejected.
07/25/2008 12:49:30 Attempt by CN=cma61/0=svlibm to create duplicate template
StdR8Mail in database /opt/notesdata/exportedDocs/51091/eDM01_20080725T15360047.
nsf - rejected.
07/25/2008 12:49:34 Closed session for cma61/svlibm Databases accessed:      2
Documents read:      0 Documents written: 1000
```

### Causes

The mail database template that is used to create the temporary Lotus Notes database is configured to be a master template.

### Resolving the problem

To resolve the problem:

1. Use Domino Designer to open the mail database template.
2. On the Design tab of the Database Properties window, clear the **Database file is a master template** option.
3. Close the mail database template.

## Problems occur when EDRM exported files are uncompressed

When you uncompress EDRM exported files, you might encounter problems if there are names that contain non-system encoded characters.

### Symptoms

When the EDRM XML export format is configured to compress the exported files into a .zip file, you might encounter problems when uncompressing source file names or attachment names that contain characters that are not part of your system's default encoding.

The uncompressed file or attachment names might contain unexpected characters such as questions marks (??) or underscores (\_\_\_), or, in some cases, an entire file name might be unreadable or a file missing from the .zip file.

### Resolving the problem

To avoid this issue, configure the EDRM XML export format to not compress exported files into .zip files. Make this change on the Export Formats pane of the Administration page by editing the EDRMBatchCompletePlugin for the EDRM XML export format and changing the value of the Create.ZIP.file plug-in parameter value from TRUE to FALSE. You can also try using other utilities to uncompress the .zip files.

## DYRC1029E when exporting documents

A user tried to export the contents of a folder after an eDiscovery administrator changed a collection name or removed a collection.

### Symptoms

DYRC1029E: You tried to export the contents of a folder that contains documents from a collection (*collectionName*) that no longer exists. Ask your administrator to do one of two things on the Search Mapping pane of the Administration page before you attempt to export the contents of the folder again. If a collection name was modified, change the collection name back to its original name. If a collection was removed, add the collection back into the system.

### Causes

Because the collection name was associated with the case (and thus, the folder), attempts to access the folder failed when the collection was not found.

### Resolving the problem

In general, after a collection is defined, its name should not be changed and the collection should not be removed because cases, folders, and saved searches have dependencies on collection names.

**Administrator responses:** Resolve the problem in one of three ways from the Collections pane of the Administration page.

- If a collection name was modified, change it back to its original name.
- If a collection was inadvertently removed, add it back.
- If a collection was purposely removed:
  1. Temporarily add the collection back.
  2. If the case in which the folder resides is not already inactive, make the case inactive.
  3. Delete the case.
  4. Inactivate, then delete any case that references the collection name. A collection is not completely removed until all cases that reference it are deleted.

**Attention:** Content from multiple collections can exist in the same case, so be sure that you really want to delete a case before doing so. When you delete a case, you remove all folders, content references, saved searches, and audit records that are associated with the case. Content is not deleted from the content archive.

5. Delete the collection.

## Internal server error when viewing or exporting content

Users receive internal server errors when they try to export Lotus Domino content or view content by either displaying a full-screen preview or using the Lotus Notes client.

### Symptoms

The system cannot connect to the server. The server might be down or there might be a network problem. HTTP error code: 500, error text: Internal Server Error

or

Application failed to initialize.

The WebSphere Application Server log file (SystemOut.log) for the IBM eDiscovery Manager server can show either of the following error messages:

```
java.lang.UnsatisfiedLinkError: DominoImport (This application has
failed to start because the application configuration is incorrect. Reinstalling
the application may fix this problem.)
```

or

```
java.lang.UnsatisfiedLinkError: ICUInterface40d (Not found in java.library.path)
```

### Causes

Viewing and exporting content both require the Microsoft Visual C++ 2008 Redistributable Package and the Microsoft Visual C++ 2010 Redistributable Package. The error messages indicate that eDiscovery Manager does not have the necessary libraries to connect to the Lotus Domino server. The libraries are defined by running `vcredist_x86.exe` on 32-bit eDiscovery Manager installations, or `vcredist_64.exe` on 64-bit eDiscovery Manager installations.

### Resolving the problem

Successfully reinstall the Microsoft Visual C++ 2008 Redistributable Package and the Microsoft Visual C++ 2010 Redistributable Package. Both packages reside in the `bin` subdirectory of the eDiscovery Manager installation directory.

**On 64-bit installations, run these files:**

- `EDM_HOME\bin\vcredist2008\vcredist_x64.exe`
- `EDM_HOME\bin\vcredist2010\vcredist_x64.exe`

## Exporting content that has an unsupported MIME type

When content is exported to HTML and PDF formats, you might get an output export file that states a MIME type is not supported.

### Symptoms

When you export content to HTML and PDF formats, it is possible to get an export file that contains only this single sentence:

This document has a MIME type that is unsupported by this export plug-in.

An export file such as this one does not represent an error.

### Diagnosing the problem

The underlying, vendor-acquired component of eDiscovery Manager that converts items from one format to another format is working as designed. These export files are created when the conversion of an item to HTML or PDF format is not possible. For example, MP3 files cannot be converted to HTML or PDF format. Exporting content to its native format does not produce these export files because native exports do not convert items from one format to another format.

## What are CSN\_ERROR files?

There are `*.csn_error` files in the temporary directory. Why?

### Symptoms

There are `*.csn_error` files in the temporary directory. What are these files?

### Causes

When an export task fails, the CSN files in the temporary directory are renamed to have the extension `.csn_error`. This is working as designed.

## Resolving the problem

Do not remove the \*.csn\_error files from the temporary directory.

## NO\_PERMISSION exception when connecting to a FileNet P8 server

When starting the IBM WebSphere Application Server on the IBM eDiscovery Manager server, the connection to a IBM FileNet P8 server failed.

### Symptoms

The eDiscovery Manager web client fails to start, which prevents browsers from loading the eDiscovery Manager login page. The following messages appear on the WebSphere Application Server console and log file:

```
[2/23/09 17:39:18:648 PST] 00000017 SystemErr R javax.naming.NoPermissionException: \
NO_PERMISSION exception caught [Root exception is org.omg.CORBA.NO_PERMISSION:
>> SERVER (id=4506ec2f, host=p8ce400vm101.p8rm40.filenet.com) TRACE START:
>> org.omg.CORBA.NO_PERMISSION: Subject is null. Authentication Failed. vmcid: \
0x49424000 minor code: 300 completed: No
```

### Causes

eDiscovery Manager was unable to connect to an IBM FileNet P8 server because the cross-cell authentication is not current.

## Resolving the problem

Export the LTPA key for cross-cell single sign-on (SSO) from the FileNet P8 server and import it to the eDiscovery Manager application server:

### Administrator response:

1. Start the WebSphere Application Server administrative console on the FileNet P8 server.
2. Click **Security > Global security**.
3. Under Authentication, **Authentication mechanisms and expiration**, click LTPA.
4. Under Cross-cell single sign-on, enter the password that is used to encrypt the LTPA keys.
5. Enter a fully-qualified path and file name for the location where you want the exported LPTA keys to reside, for example: C:\LTPA\LTPA\_key\_name.
6. Click **Export keys**.
7. If you generated a new LTPA key, import the key file to the FileNet P8 server.
8. Import the key file to the eDiscovery Manager application server:
  - a. Copy the key file from the FileNet P8 server to the eDiscovery Manager application server.
  - b. If it is not already running, start the WebSphere Application Server administrative console on the eDiscovery Manager application server.
  - c. Click **Security > Global security**.
  - d. Under Authentication, **Authentication mechanisms and expiration**, click LTPA.
  - e. Under Cross-cell single sign-on, enter the password that is used to encrypt the LTPA keys.

This is the same password that you entered on the FileNet P8 server before exporting the key file.
  - f. Enter the fully-qualified path and file name for the location of the key file that you copied to the eDiscovery Manager application server, for example: C:\LTPA\LTPA\_key\_name.

- g. Click **Import keys**.
- h. Click **Apply** and then click **Save directly to the master configuration**.

#### Related tasks

“Configuring the IIOP connection between the eDiscovery Manager system and the FileNet P8 server using single sign-on” on page 48

Before installing IBM eDiscovery Manager and its prerequisites, configure the IIOP connection between the eDiscovery Manager system and the IBM FileNet P8 server.

## Export fails with NOTES ERROR message in the dominoExport.log file

An attempt to export Lotus Domino content fails with NOTES ERROR messages written to the dominoExport.log file.

### Symptoms

After an export of Lotus Domino content fails, the Lotus Domino export log file contains any of the following error messages:

```
RC = 16649: NOTES ERROR in method NSFDbOpenExtended: File truncated - file may \
have been damaged
NOTES ERROR in method NSFNoteUpdate: Database is corrupt -- Cannot allocate space
NOTES ERROR in method NSFNoteUpdate: This database cannot be read due to an \
invalid on disk structure
```

By default, the Lotus Domino export log file is named dominoExport.log and it is located in the logs subdirectory of the IBM eDiscovery Manager installation directory, for example, at C:\Program Files\IBM\EDM\logs\dominoExport.log on Windows systems and at /opt/IBM/EDM/dominoExport.log on AIX systems.

### Causes

This error might occur when multiple export tasks attempt to access the same Lotus Domino database.

### Resolving the problem

To work around this issue, reduce the number of export threads that are running simultaneously:

1. From the Export Settings pane of the Administration page of the eDiscovery Manager web client, reduce the value currently shown in the **Maximum threads for all exports** field by one.
2. Have your users close their current eDiscovery Manager web client sessions and start new ones.
3. Try the export again.
4. If the error persists, repeat steps 1 to 3, reducing the maximum threads value by one more.
5. Keep reducing the maximum threads value and then trying the export again in a new eDiscovery Manager web client session until the export succeeds with no errors.

## Lotus export fails with NSFDbCreateAndCopy error 16643 and a File does not exist message

Users might be unable to export Lotus Notes content if the total length of the export file name prefix and the export task name is too long.

### Symptoms

When a user exports Lotus Notes content, the export fails with an error code of 16643 from the Lotus Notes API NSFDbCreateAndCopy. The error message File does not exist is also written to the export log file, dominoExport.log.

### Causes

The total length of the export file name prefix and the export task name is too long.

The path that is used by IBM eDiscovery Manager for the Lotus Domino export database is limited to 100 bytes. This path is a combination of the following values:

- The export directory
- The export file name prefix
- The export task name

### Resolving the problem

To avoid this problem, request that users complete the following tasks in the Export Content window:

- Reduce the lengths of the names that they enter for the **Export file name prefix** field.
- Reduce the default name that is set for the **Export task name** field.

Additionally, as an eDiscovery Manager IT Administrator, you can complete the following task:

- Reduce the length of the export directory, as defined by the Lotus.Domino.server.export.directory plug-in parameter of the Native export format. You specify this value on the Export Formats pane of the Administration page as one of the parameters for the BatchComplete plug-in point of the Native export format.

## Web client sessions time out after 30 minutes

By default, IBM eDiscovery Manager is configured to disconnect the web client (or *time out*) after 30 minutes, regardless whether the user was inactive or not. You can disable this behavior at the IBM WebSphere Application Server administrative console.

### Symptoms

When an eDiscovery Manager session expires, the user receives a timeout message and the user is then prompted to log in again to reactivate the session.

### Resolving the problem

To prevent eDiscovery Manager web client sessions from timing out after 30 minutes:

1. Open the WebSphere Application Server administrative console by clicking **Start > Programs > IBM WebSphere > Application Server > Profiles > eDiscovery Manager application server profile > Administrative console**.
2. Expand **Applications, Enterprise Applications, EDMClient and Session management**.
3. In the General Properties section, select the **Override session management** option and clear the **Enable URL rewriting** option.
4. Under the Session Timeout section, click **Set timeout** and specify your preferred timeout duration (in minutes). Alternatively, to completely stop sessions from expiring due to user inactivity, click **No timeout**.
5. Click **OK** to save your changes.



6. Stop and restart your eDiscovery Manager server.

#### About the timing of session timeout messages

The timeout message that a user receives is typically displayed after eDiscovery Manager responds to a user action. For example, if a session expires and then the user clicks the **Change case** link, eDiscovery Manager first displays the Select Case window and then displays the timeout message. This behavior is expected in AJAX applications such as eDiscovery Manager because the timeout condition is detectable only after the client makes a request of the server.

#### Related information

 WebSphere Application Server Version 7.0 - Starting and stopping quick reference

 WebSphere Application Server Version 8.0 - Starting and stopping quick reference

## Web client session is closed when accessing multiple eDiscovery Manager servers

A user is unable to run multiple web clients to access different IBM eDiscovery Manager application servers.

### Symptoms

If a user runs multiple instances of the eDiscovery Manager web client on the same system to access multiple eDiscovery Manager application servers, a single client session is shared among those web client instances. As a result, using one of the web client instances causes the other instances to be logged out.

### Resolving the problem

To prevent the web client instances from being logged out:

1. Open the IBM WebSphere Application Server administrative console by clicking **Start > Programs > IBM WebSphere > Application Server > Profiles > eDiscovery Manager application server profile > Administrative console**.
2. Click **Servers > Application servers > eDiscovery Manager application server > Web container settings > Session management > Enable cookies**.
3. On the Configuration page, change the name of the session management cookie from JSESSIONID to JSESSIONID2 (or change the name of the cookie to any other unique name), then apply and save your change.
4. Navigate to **Servers > Application servers > eDiscovery Manager application server > Installed applications > EDCConsoleEAR > Session management**.
5. Confirm that the value of the **Override session management** option is set to False.
6. Restart the eDiscovery Manager application server.
7. Repeat steps 1 to 6 for all but one eDiscovery Manager application server to ensure that all servers have unique session management cookies. Doing so prevents one web client instance from overwriting the session IDs of other instances and prevents instances from sharing session IDs and session data.

#### Related information

 WebSphere Application Server Version 7.0 - Starting and stopping quick reference

 WebSphere Application Server Version 8.0 - Starting and stopping quick reference



## DYRC9999E error when searching and the log file contains DGL5052A: Operand type mismatch in a query string

When searching, a user receives a DYRC9999E error that indicates that IBM Content Manager Enterprise Edition returned an error.

### Symptoms

The component of subsystem "DB2 Content Manager" received the following error: "Debug Message: State errcode 7015 Id 4 Event IDStr".

After searching the eDiscovery Manager web client log file for the DYRC9999E error, you locate a preceding log file entry like this one:

```
Caused by: com.ibm.mm.sdk.common.DKUsageError: DGL5052A: Operand type mismatch in a query string. An operation was attempted between two operands of incompatible types. XQPE query: //ICCEmailLD1Q[(((@ICCMailDate BETWEEN "1001-01-01-08.00.00.000000" AND "2009-11-04-07:59:59:000000"))) AND (@TIEFLAG = "18"))]. Return code: 7015. Reason code: 0. Extended return code: -401. Ext Reason Code: 0. (SERVER RC): 7015
```

### Causes

An incorrect data type is specified for one of the content server properties on the **Search Mapping** tab of the Collections pane.

### Resolving the problem

To resolve the problem:

1. Determine which search template the user was using.
2. Determine which collections are associated with the search template and then determine which of those collections has the content server property or properties that the user was searching.
3. Work with your content server administrator to verify that for each content server property on the **Search Mapping** tab of the Collections pane of the appropriate collection, the selected data type is correct.

In the example in this scenario, the data type for the TIEFLAG property was mistakenly set to String. However, the correct data type for the TIEFLAG property is Integer.

## Two views of the same Lotus Notes email have different timestamps

The timestamps of Lotus Notes email in the Search Results pane might be different from the timestamps of the same email when viewed in the Preview pane.

### Symptoms

**CommonStore** **Content Mgr** The timestamp difference is typically the same for all of the email, and it is in hourly increments. For example, all email in the Search Results pane might have timestamps that are exactly 5 hours later than the corresponding timestamps shown in the Preview pane.

### Causes

This problem occurs when email is archived by IBM CommonStore for Lotus Domino without the Coordinated Universal Time (UTC) timestamp. If you use or intend to use eDiscovery Manager to search email that is archived by CommonStore, the email must be archived with a UTC timestamp.

## Resolving the problem

Enable UTC timestamps by setting the parameter `CSLDTimestampInUTC` to 1 in the `notes.ini` file that is used by CommonStore for Lotus Domino before archiving email that will be searched by eDiscovery Manager.

If you previously used CommonStore to archive email without enabling UTC timestamps and you now want to use UTC timestamps, you must archive the email to a new collection. The email that was archived without UTC timestamps cannot be changed to have UTC timestamps.

### Related information



IBM CommonStore for Lotus Domino Administrator's and Programmer's Guide

## Error 404: No target servlet configured for uri: /edmcclient or HTTP 404 - File not found

When logging on to the IBM eDiscovery Manager web client, a user receives an Error 404 or HTTP 404 message instead of the eDiscovery Manager logon page.

### Symptoms

In a Mozilla Firefox web browser, a message like the following text appears instead of the eDiscovery Manager web client logon page: Error 404: No target servlet configured for uri: /edmcclient.

In an Internet Explorer web browser, a similar 404 message appears: HTTP 404 - File not found.

### Causes

The user entered a misspelled portion of the web client URL, in this example, entering `edmcclient` instead of `EDMClient`. The `EDMClient` portion of the URL is case sensitive.

## Resolving the problem

Re-enter the URL for the eDiscovery Manager web client with `EDMClient` and any other portions of the URL spelled with the correct mix of uppercase and lowercase letters.

## Some Microsoft Outlook email attachments cannot be previewed

Some Microsoft Outlook email attachments that are encoded in MacBinary format cannot be previewed because the file extension might not indicate that the file is in MacBinary format.

### Symptoms

A user can successfully search and find some Microsoft Outlook email attachments by name, but the attachments cannot be previewed. When a user attempts to preview the attachment within the IBM eDiscovery Manager web client, no error messages are shown, but the link to the attachment does not open or it shows garbled content.

### Causes

When you archive attachments, IBM Content Collector stores attachment data together with the file name and extension. However, the file extension might not reflect the correct encoding of the data. Attachments that were created from MIME

email that was sent from Mac OS computers might be encoded in MacBinary format, but the file extensions might not reflect this encoding. In such situations, the wrong application is used to display the archived attachment. For example, if the attachment is a JPG file named test.jpg and it is encoded in MacBinary format, previewing the attachment shows garbled content, because the content is not really JPG. Starting with version 2.1.1 fix pack 2, Content Collector appends a .bin suffix to the attachment's file name to be able to identify MacBinary encoded files after they were archived.

For example, Content Collector archives the file test.jpg with file name test.jpg.bin. However, because only few applications can handle MacBinary encoded files, previewing the attachment still shows garbled content.

### Resolving the problem

If the user is assigned the Native Viewer role, the user can view the email and its attachments by opening the email with the native Microsoft Outlook client. Under the Native View column, click the **View this content with Microsoft Outlook** icon next to the email that you want.

## Tasks fail due to insufficient privileges

All of the tasks in the system hang with an INSUFFICIENT\_PRIVILEGES exception.

### Symptoms

The following exception occurs for all tasks:

```
com.ibm.icm.edc.ral.security.SecurityServiceException:INSUFFICIENT_PRIVILEGES:
  User does not have the authority to retrieve tasks to run.
at com.ibm.icm.edc.ral.taskmgmt.impl.TaskServiceImpl.getTasksToRun
(TaskServiceImpl.java:979)
at com.ibm.icm.edc.workmgr.work.WorkInitializer.run(WorkInitializer.java:167)
```

### Causes

The eDiscovery administrator is not in the EDMSUPERUSER group.

### Resolving the problem

To resolve the problem:

1. The IBM Content Manager Enterprise Edition administrator must add the eDiscovery administrator to the EDMSUPERUSER group.
2. Restart the IBM eDiscovery Manager application server.

## Export task fails with an REPOSITORY\_UNAVAILABLE error

Sometimes an export task fails to complete, which is typically caused because the connection was lost to the repository.

### Symptoms

An error message similar to the following message is displayed:

```
[2013-09-13 03:15:28.330] [43196403] [SEVERE    ] [3351      ] [METHOD          ]
[com.ibm.icm.edc.workmgr.work.ExportWork] [runBatches          ]
"Export_EX_Native_20130913T00490048      - EDiscovery connection no longer
available. Reconnecting and reattempting the operation.
com.ibm.icm.edc.ral.query.EDiscQueryServiceException:
com.ibm.ecm.rs.query.QueryException:
REPOSITORY_UNAVAILABLE: Failed to get next result
at com.ibm.icm.edc.ral.query.impl.EDiscResultsIteratorImpl.
getNextResult(EDiscResultsIteratorImpl.java:101)
at com.ibm.icm.edc.workmgr.work.ExportWork.runBatches
```

```
|      (ExportWork.java:881)
|      at com.ibm.icm.edc.workmgr.work.ExportWork.run(ExportWork.java
|      :226)
|      at com.ibm.ws.asyncbeans.J2EEContext.run(J2EEContext.java:809)
|      at com.ibm.ws.asyncbeans.WorkWithExecutionContextImpl.go
|      (WorkWithExecutionContextImpl.java:222)
```

## **Causes**

The connection to the repository was lost.

## **Resolving the problem**

To resolve the problem:

1. Ensure that the repository server is running.
2. Restart the export task in IBM eDiscovery Manager.

---

## Chapter 7. Removing and reinstalling eDiscovery Manager

The proper procedure for removing and reinstalling IBM eDiscovery Manager depends on which content server you use and the type of installation you want.

---

### Removing and reinstalling eDiscovery Manager (Content Manager EE)


The proper procedure for removing and reinstalling IBM eDiscovery Manager in an IBM Content Manager Enterprise Edition environment depends on whether you intend to reinstall the current version or reinstall a previous version.

#### Removing eDiscovery Manager with the intent to reinstall this version (Content Manager EE)

Follow the procedure in this topic if you are removing IBM eDiscovery Manager and you plan to reinstall the same version.

##### Procedure

1. Remove eDiscovery Manager, but do not choose to delete the eDiscovery Manager data.

 After uninstalling eDiscovery Manager, verify that the following directory was deleted: C:\Documents and Settings\your\_user\_ID\Start Menu\Programs\IBM eDiscovery Manager. If it still exists, delete it.

2. Reinstall eDiscovery Manager.

If you are reinstalling a fix pack version, you must first install the "base" version for the fix pack. For example, if you removed version 2.2.1 fix pack 1, then install 2.2.1 by using one of the following commands:

Operating System	Command
AIX	eDM.bin
Windows	eDM.exe

3. Optional: If you are reinstalling a fix pack version of eDiscovery Manager, install the fix pack after reinstalling the "base" version. For example, install version 2.2.1 fix pack 1 on top of the version 2.2.1 you reinstalled previously by using one of the following commands:

Operating System	Command
AIX	eDM.bin
Windows	eDM.exe

##### Related tasks:

"Installing or upgrading eDiscovery Manager in a Content Manager EE environment" on page 40

After you install and configure the prerequisite software, you can install IBM eDiscovery Manager as an IBM WebSphere Application Server instance and connect it to your IBM Content Manager Enterprise Edition system. Note that the process for upgrading eDiscovery Manager is identical to the process for installing eDiscovery Manager.

Chapter 8, “Removing eDiscovery Manager,” on page 203

You can remove IBM eDiscovery Manager from an AIX or Microsoft Windows system.

“Before upgrading eDiscovery Manager” on page 26

Before upgrading IBM eDiscovery Manager, complete the following tasks.

## Removing eDiscovery Manager with the intent to reinstall a previous version (Content Manager EE)

Follow this procedure if you are removing IBM eDiscovery Manager and you plan to reinstall a previous version.

### Procedure

1. Remove eDiscovery Manager and choose to delete the eDiscovery Manager data.

**Windows** After uninstalling eDiscovery Manager, verify that the following directory was deleted: C:\Documents and Settings\*your\_user\_ID*\Start Menu\Programs\IBM eDiscovery Manager. If it still exists, delete it.

2. Install the previous version of eDiscovery Manager that you want. For example, if the current version you removed was 2.2, then you can install version 2.1.1 or 2.1 by using one of the following commands:

Operating System	Command
AIX	eDM.bin
Windows	eDM.exe

3. Optional: If a fix pack is available for the version of eDiscovery Manager that you installed in the previous step, upgrade to the fix pack by using one of the following commands:

Operating System	Command
AIX	eDM.bin
Windows	eDM.exe

### Results

**Remember:** Never install a lower version of eDiscovery Manager on a system that is running a higher version of eDiscovery Manager. If you want to revert to an earlier version of eDiscovery Manager, always remove the currently running version of eDiscovery Manager and reinstall the version that you want.

#### Related tasks:

“Installing or upgrading eDiscovery Manager in a Content Manager EE environment” on page 40

After you install and configure the prerequisite software, you can install IBM eDiscovery Manager as an IBM WebSphere Application Server instance and connect it to your IBM Content Manager Enterprise Edition system. Note that the process for upgrading eDiscovery Manager is identical to the process for installing eDiscovery Manager.

Chapter 8, “Removing eDiscovery Manager,” on page 203

You can remove IBM eDiscovery Manager from an AIX or Microsoft Windows system.

“Before upgrading eDiscovery Manager” on page 26  
Before upgrading IBM eDiscovery Manager, complete the following tasks.

## Removing and reinstalling eDiscovery Manager (FileNet P8)

The proper procedure for removing and reinstalling IBM eDiscovery Manager in an IBM FileNet P8 environment depends on whether you intend to reinstall the current version or reinstall a previous version.

### Removing eDiscovery Manager with the intent to reinstall this version (FileNet P8)

Follow the procedure in this topic if you are removing IBM eDiscovery Manager and you plan to reinstall the same version.

#### Procedure

1. Remove eDiscovery Manager.

**Windows** After uninstalling eDiscovery Manager, verify that the following directory was deleted: C:\Documents and Settings\*your\_user\_ID*\Start Menu\Programs\IBM eDiscovery Manager. If it still exists, delete it.

2. Reinstall eDiscovery Manager.

If you are reinstalling a fix pack version, you must first install the "base" version for the fix pack. For example, if you removed version 2.2.1 fix pack 1, then install 2.2.1 by using one of the following commands:

Operating System	Command
AIX	EDM.bin -Dno_create_dm=TRUE
Windows	EDM.exe -Dno_create_dm=TRUE

The -Dno\_create\_dm flag directs the eDiscovery Manager installation program not to re-create the eDiscovery Manager objects in the object store.

3. Optional: If you are reinstalling a fix pack version of eDiscovery Manager, install the fix pack after reinstalling the "base" version.

Operating System	Command
AIX	EDM.bin
Windows	EDM.exe

#### Related tasks:

“Installing or upgrading eDiscovery Manager in a FileNet P8 environment” on page 60

After you install and configure the prerequisite software, you can install IBM eDiscovery Manager as an IBM WebSphere Application Server instance and connect it to your IBM FileNet P8 system. Note that the process for upgrading eDiscovery Manager is identical to the process for installing eDiscovery Manager.

Chapter 8, “Removing eDiscovery Manager,” on page 203

You can remove IBM eDiscovery Manager from an AIX or Microsoft Windows system.

“Before upgrading eDiscovery Manager” on page 26


Before upgrading IBM eDiscovery Manager, complete the following tasks.

## Removing eDiscovery Manager with the intent to reinstall a previous version (FileNet P8)

Follow this procedure if you are removing IBM eDiscovery Manager and you plan to reinstall a previous version.

### Procedure

1. Remove eDiscovery Manager.

 After uninstalling eDiscovery Manager, verify that the following directory was deleted: C:\Documents and Settings\*your\_user\_ID*\Start Menu\Programs\IBM eDiscovery Manager. If it still exists, delete it.

2. Install the previous version of eDiscovery Manager that you want, but install against a different object store than the object store that you used previously for eDiscovery Manager. For example, if the current version you removed was 2.2, then you can install version 2.1.1 or 2.1 by using one of the following commands:

Operating System	Command
AIX	edm.bin
Windows	edm.exe

3. Optional: If a fix pack is available for the version of eDiscovery Manager that you installed in the previous step, upgrade to the fix pack by using one of the following commands:

Operating System	Command
AIX	edm.bin
Windows	edm.exe

### Results

**Remember:** Never install a lower version of eDiscovery Manager on a system that is running a higher version of eDiscovery Manager. If you want to revert to an earlier version of eDiscovery Manager, always remove the currently running version of eDiscovery Manager and reinstall the version that you want.

#### Related tasks:

“Installing or upgrading eDiscovery Manager in a FileNet P8 environment” on page 60

After you install and configure the prerequisite software, you can install IBM eDiscovery Manager as an IBM WebSphere Application Server instance and connect it to your IBM FileNet P8 system. Note that the process for upgrading eDiscovery Manager is identical to the process for installing eDiscovery Manager.

Chapter 8, “Removing eDiscovery Manager,” on page 203

You can remove IBM eDiscovery Manager from an AIX or Microsoft Windows system.

“Before upgrading eDiscovery Manager” on page 26

Before upgrading IBM eDiscovery Manager, complete the following tasks.





---

## Chapter 8. Removing eDiscovery Manager

You can remove IBM eDiscovery Manager from an AIX or Microsoft Windows system.

### About this task

-  On AIX, the default location of the installation directory is /opt/IBM/EDM/.
-  On Microsoft Windows 64-bit operating systems, the default location of the installation directory is C:\Program Files\IBM\EDM\.


---

### Before removing eDiscovery Manager

Before uninstalling IBM eDiscovery Manager, remove users from the eDiscovery group, remove eDiscovery Manager privilege sets from users, and remove eDiscovery Manager ACLs from items.

### About this task

You must remove all users from the eDiscovery group. (Work with your IBM Content Manager Enterprise Edition administrator to use the IBM Content Manager system administration client to make these changes on the **Assign to Groups** tab of the User Properties window.) If you upgraded to eDiscovery Manager Version 2.2.2 from a previous version, remove users from the following groups, if they still exist.


- Remove former eDiscovery Manager administrators from the EDISC\_ADMIN\_GROUP group.
- Remove former eDiscovery Manager users from the EDISC\_MANAGER\_GROUP group.
- Remove former IBM eDiscovery Analyzer users from the EDISC\_ANALYSIS\_GROUP group.
- 

**Important:** If you override any of the default eDiscovery Manager group names by setting the adminGroup, managerGroup, or analysisGroup parameters in the ral.properties file, remove the users from those groups. The default location of the ral.properties file depends on the operating system:

**AIX** /opt/IBM/EDM/config/ral.properties

#### Windows

C:\Program Files\IBM\EDM\config\ral.properties

-  Remove all eDiscovery (EDM\*) maximum privilege sets from eDiscovery users. (Work with your Content Manager EE administrator to use the IBM Content Manager system administration client to make these changes on the **Define Users** tab of the User Properties window.)

If you upgraded to eDiscovery Manager from a previous version, remove the following privilege sets, if they still exist.

- Remove the EDMPrivSetUpdateAdmin privilege set from former eDiscovery Manager administrators.

- Remove the EDMPrivSetUpdate privilege set from former eDiscovery Manager users.

**Tip:** If you do not remove the references between eDiscovery Manager users and privilege sets, the uninstallation program is unable to delete the eDiscovery Manager data. In this case, a return code of 100 (RC=100) is written to the uninstallation log file (*edMHome\logs\EDMUninstall\*.log*).

- **Content Mgr** Remove all eDiscovery (EDM\*) default item access control lists from eDiscovery users. (Work with your Content Manager EE administrator to use the IBM Content Manager system administration client to make these changes on the **Set Defaults** tab of the User Properties window.)

If you upgraded to eDiscovery Manager from a previous version, remove the following ACLs, if they still exist.

- Remove the EDMModelItemACL ACL from all eDiscovery Manager item types.

**Tip:** If you do not remove the references between eDiscovery Manager users and ACLs, the uninstallation program is unable to delete the eDiscovery Manager data. In this case, a return code of 100 (RC=100) is written to the uninstallation log file (*edMHome\logs\EDMUninstall\*.log*).

### Configuring the uninstallation program not to run in silent mode

If you silently installed eDiscovery Manager, then by default, the uninstallation program runs in silent mode too. If you do not want run the uninstallation program in silent mode, modify the *Uninstall\_eDM.lax* file.

### Procedure

To configure the uninstallation program not to run in silent mode:

1. Open the *Uninstall\_eDM.lax* file in a text editor.
2. Change the following line:  
`lax.command.line.args=$CMD_LINE_ARGUMENTS$ -u`  
to:  
`lax.command.line.args -i gui $CMD_LINE_ARGUMENTS$`
3. Save and close the file.

---

## Removing eDiscovery Manager

How to remove eDiscovery Manager.

### About this task

When you uninstall IBM eDiscovery Manager, the installation program removes the following files and directories:

- All the directories that were installed by the IBM eDiscovery Manager installation program except the *edMhome\plugins* and *edMhome\logs* directories
- All the files that are in those directories, including any files that you copied into those directories after the installation

The following directories and files are preserved during the uninstallation process:

- The *edMhome\plugins* and *edMhome\logs* directories

- Any directories that you created after the installation, for example, *edmhome\tmp* and *edmhome\exportedDocs*

To remove eDiscovery Manager:

## Procedure

1. **Content Mgr** Modify the value of the JavaPool parameter in the *cmbpool.ini* file to be an empty string. (Do not comment out the JavaPool parameter; simply set its value to an empty string.)

JavaPool=

The *cmbpool.ini* file is used for IBM WebSphere Application Server connection pooling. The default location for the *cmbpool.ini* file is in *IBMCMROOT\cmgmt\connectors\* on Microsoft Windows systems and in */home/ibmcmadm/cmgmt/connectors/* on AIX systems. For example: *C:\Program Files\IBM\db2cmv8\cmgmt\connectors* on a Microsoft Windows system.

2. Stop and restart the application server instance that is associated with the eDiscovery Manager profile. See the WebSphere Application Server product information for details about stopping and starting an application server.
3. Browse to the *Uninstall\_eDM* subdirectory of the eDiscovery Manager installation directory.
4. Run the uninstallation program:

Operating system	Command
AIX	<i>Uninstall_eDM.bin</i>
Windows	<i>Uninstall_eDM.exe</i> or select the <b>Uninstall</b> option for eDiscovery Manager from the Windows <b>Start</b> menu

5. **Content Mgr** Decide whether to delete the eDiscovery Manager data from the server.

If you plan to reinstall eDiscovery Manager later, do not delete the data. If you do not delete the eDiscovery Manager data now, you can delete it any time by running the eDiscovery Manager installation program and then running the eDiscovery Manager uninstallation program.

If you delete the eDiscovery Manager data, it is deleted from the primary content server and all of the secondary content servers. In addition, if you delete the eDiscovery Manager data on a IBM Content Manager Enterprise Edition server, all of the eDiscovery Manager roles, privilege sets, and privileges are deleted. There is no equivalent action for IBM FileNet P8.

## Results

eDiscovery Manager writes uninstallation progress messages and error messages to uninstallation log files. If an error occurs, check the *EDM\_HOME\logs\EDMUninstall\*.log* file.

If a log file reaches 5 MB in size, eDiscovery Manager rolls it over and creates another log file. eDiscovery Manager creates up to three uninstallation log files (*EDMUninstallDebug00.log*, *EDMUninstallDebug01.log*, and *EDMUninstallDebug02.log*) before it begins overwriting the first log file.

**FileNet P8 Object store:** When you remove eDiscovery Manager, the eDiscovery Manager objects in the object store are not deleted. Because AddOn resources do

not support the concept of uninstallation, if you want to delete eDiscovery Manager objects from the object store, you must delete them manually.

**Related information:**

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

---


## Running a silent uninstallation

When the uninstallation program runs in silent mode, no uninstallation windows are displayed. The uninstallation program progresses in the same manner as if you entered the response file values in the graphical user interface of the uninstallation program.

### About this task

To run a silent uninstallation:


### Procedure

1.  **Content Mgr** Modify the value of the JavaPool parameter in the `cmbpool.ini` file to be an empty string. (Do not comment out the JavaPool parameter; simply set its value to an empty string.)

JavaPool=

The `cmbpool.ini` file is used for IBM WebSphere Application Server connection pooling. The default location for the `cmbpool.ini` file is in `IBMCMROOT\cmgmt\connectors\` on Microsoft Windows systems and in `/home/ibmcmadm/cmgmt/connectors/` on AIX systems. For example: `C:\Program Files\IBM\db2cmv8\cmgmt\connectors` on a Microsoft Windows system.

2. Stop and restart the application server instance that is associated with the IBM eDiscovery Manager profile. See the WebSphere Application Server product information for details about stopping and starting an application server.

3.  **Content Mgr** Decide whether to delete the eDiscovery Manager data from the server.

If you plan to reinstall eDiscovery Manager later, do not delete the data. If you do not delete the eDiscovery Manager data now, you can delete it any time by running the eDiscovery Manager installation program and then running the eDiscovery Manager uninstallation program.

If you delete the eDiscovery Manager data, it is deleted from the primary content server and all of the secondary content servers. In addition, if you delete the eDiscovery Manager data on a IBM Content Manager Enterprise Edition server, all of the eDiscovery Manager roles, privilege sets, and privileges are deleted. There is no equivalent action for IBM FileNet P8.

4. Navigate to the `Uninstall_eDM` subdirectory of the eDiscovery Manager installation directory.
5. At a command prompt, enter:

Operating system	Command
AIX	<p>To remove eDiscovery Manager without deleting the data, enter: <code>Uninstall_eDM.bin -DDELETE_DATA=NO</code></p> <p>To remove eDiscovery Manager and delete the data, enter: <code>Uninstall_eDM.bin -DDELETE_DATA=YES</code></p>
Windows	<p>To remove eDiscovery Manager without deleting the data, enter: <code>Uninstall_eDM.exe -DDELETE_DATA=NO</code></p> <p>To remove eDiscovery Manager and delete the data, enter: <code>Uninstall_eDM.exe -DDELETE_DATA=YES</code></p>

If the user name and password of the IBM WebSphere Application Server administrator changed since you installed the product, use the `WAS_SECURITY_USER_NAME` and `WAS_SECURITY_PW` parameters to specify the new values. For example, on a Microsoft Windows system, enter:

```
Uninstall_eDM.exe
-DDELETE_DATA=NO
-DWAS_SECURITY_USER_NAME=was_admin_userName
-DWAS_SECURITY_PW=was_admin_password
```

**Content Mgr** If the user name and password of the IBM Content Manager Enterprise Edition administrator changed since you installed the product, use the `ICM_ADMIN_USER_NAME` and `ICM_ADMIN_USER_PW` parameters to specify the new values. For example, on a Microsoft Windows system, enter:

```
Uninstall_eDM.exe
-DDELETE_DATA=NO
-DICM_ADMIN_USER_NAME=icm_admin_userName
-DICM_ADMIN_USER_PW=icm_admin_password
```

## Results

eDiscovery Manager writes uninstallation progress messages and error messages to uninstallation log files. If a log file reaches 3 MB in size, eDiscovery Manager rolls it over and creates another log file. eDiscovery Manager creates up to three uninstallation log files (`eDMUninstallDebug00.log`, `eDMUninstallDebug01.log`, and `eDMUninstallDebug02.log`) before it begins overwriting the first log file.

**Errors:** If an error occurs during the uninstallation, a message is written to the uninstallation log files in your home directory. Search this file for the keyword `ERRSI` to find messages that are related to the error. On an AIX system, the home directory is defined by the `HOME` environment variable. On a Microsoft Windows system, the home directory is defined by the `HOMEPATH` environment variable. For example, on Microsoft Windows 2008, your home directory might be `C:\Users\YourUserName\`.

**FileNet P8 Object store:** The object store is not deleted during the removal process. If you want to delete the object store, you must delete it manually.

### Related information:

 [WebSphere Application Server Version 7.0 - Starting and stopping quick reference](#)

 [WebSphere Application Server Version 8.0 - Starting and stopping quick reference](#)

---

## 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 grant 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 106-0032, 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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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  
J46A/G4  
555 Bailey Avenue  
San Jose, CA 95141-1003  
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, the 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.



Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. Copyright IBM Corp. 2004, 2006.

Portions of this product are:

- Copyright Outside In Viewer Technology 1992-2005 Stellent Chicago, Inc. All rights reserved.

## **Trademarks**

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: <http://www.ibm.com/legal/copytrade.shtml>

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Other company, product, and service names may be trademarks or service marks of others.



---

## Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at <http://www.ibm.com/privacy> and IBM’s Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at <http://www.ibm.com/software/info/product-privacy>.



---

# Index

## Numerics

404 errors 196

## A

access control lists (ACLs) 107  
accessibility ix, 3  
active phase 151  
AIX  
    installation path 25, 203  
AllPrivs maximum privilege set 103  
Arabic  
    Internet Explorer limitation 113  
architecture  
    eDiscovery Manager 5  
attachments 81  
    open 130  
    save 130  
attributes  
    exposing LDAP attributes 110  
audit reporting  
    configuring 27

## C

case life cycle 151  
    allowed tasks 152  
case phases 151  
    allowed tasks 152  
changed features 2  
checklists  
    configuring Content Manager EE 87  
        audit configuration 97  
        collections 90  
        content management system 89  
        export formats 92  
        export settings 91  
        general settings 87  
        LDAP 98  
        logging 99  
        Lotus Domino settings 97  
        search templates 90  
        user roles 88  
    configuring FileNet P8 70  
        audit configuration 82  
        collections 74  
        content management system 73  
        export formats 76  
        export settings 76  
        general settings 71  
        LDAP 83  
        logging 84  
        Lotus Domino settings 82  
        search templates 75  
        user roles 71  
ClientUserReadOnly maximum privilege set 103, 104  
cmbicmsrvs.ini file 134  
collections  
    partitioned object stores 74

compression utilities  
    accented characters 126  
    known limitations 126  
    long file names 126  
configuration  
    gathering information 70  
    overview 69  
    recommended order of tasks 69  
configuration checklists  
    Content Manager EE 87  
        audit configuration 97  
        collections 90  
        content management system 89  
        export formats 92  
        export settings 91  
        general settings 87  
        LDAP 98  
        logging 99  
        Lotus Domino settings 97  
        search templates 90  
        user roles 88  
FileNet P8 70  
    audit configuration 82  
    collections 74  
    content management system 73  
    export formats 76  
    export settings 76  
    general settings 71  
    LDAP 83  
    logging 84  
    Lotus Domino settings 82  
    search templates 75  
    user roles 71  
configure  
    eDiscovery Manager 130  
configuring  
    eDiscovery Manager with eDiscovery Analyzer 134  
    secondary content servers 105  
    style.lex file 135  
configuring export  
    export directory name length 125  
connection methods  
    EJB protocol 50  
    IIOP protocol 50  
    WSI transport method 50  
content  
    legal holds 152  
    previewing 113  
    viewing 113  
Content Based Retrieval  
    effect on searching 136  
content management scenarios 11  
Content Manager EE  
    audit configuration 27  
Content Manager EE configuration  
    checklists 87  
        audit configuration 97  
        collections 90  
        content management system 89  
        export formats 92

Content Manager EE configuration  
    checklists (*continued*)  
        export settings 91  
        general settings 87  
        LDAP 98  
        logging 99  
        Lotus Domino settings 97  
        search templates 90  
        user roles 88  
content server data  
    deleting 204  
content servers  
    synchronizing users across 106  
cookies  
    secure 130  
custom ACL 105

## D

date attributes  
    configuring in Content Manager 134  
date range  
    partitioned object stores 74  
DB2  
    creating indexes for improved performance 43  
default item access control list 103, 104  
deleting phase 151  
DGL3757A error 175  
DGL3795A error 175  
document previewing  
    AIX systems 112  
documents  
    archiving into different item types 133  
    saving to folders 135

## E

eDiscovery administrator  
    EDMSUPERUSER privilege set 105  
    maximum privilege set 103, 104  
eDiscovery administrator password  
    changing 109  
eDiscovery Analyzer  
    scenario 14  
    working with 134  
eDiscovery group  
    ClientUserReadOnly privilege set 105  
eDiscovery Manager  
    architecture 5  
    configuring 112, 134  
    scenario 12  
eDiscovery Manager server  
    starting 68  
    stopping 68  
EDMArchiveSearcher privilege set 106  
EDMAuditor privilege set 106  
EDMCaseAdmin privilege set 106

- EDMCaseAnalyst privilege set 106
- EDMCaseReviewer privilege set 106
- EDMCaseSearcher privilege set 106
- eDMConfig\*.log 42, 62
- EDMConfigFileName setting 116, 122
- EDMExporter privilege set 106
- eDMInstallDebug\*.log 42, 62
- EDMITAdmin privilege set 106
- EDMLotusPWMgrClassPath
  - parameter 116, 122
- EDMLotusPWMgrLogFile
  - parameter 116, 122
- EDMLotusPWMgrPasswordFile
  - parameter 116, 122
- EDMMail session
  - restoring settings 68
- EDMModelItemACL 103
- EDMNativeViewer privilege set 106
- EDMRoleFolder object class 108
- EDMSecurityAdapters object class 108
- EDMSuperUser privilege set 106
- EJB protocol
  - connection methods 50
- email
  - analytics preparation
    - IBM eDiscovery Analyzer 11
    - IBM eDiscovery Manager 11
    - scenarios 11
- email notifications
  - configuring 127
  - restoring settings 68
- Exchange
  - email 120
  - PST export files 120
- export
  - configuring 119, 126
  - configuring Lotus Notes 121
  - PDF 120
- export directories
  - disabling fully qualified paths 125
  - naming recommendations 125
- Export error
  - Lotus Notes 192
- export errors
  - email attachment path name too long 125
- export file name prefixes
  - naming recommendations 125
- export subdirectories
  - naming recommendations 125
- export tasks
  - scheduling 155
- exporting 81
  - attachments 81
  - exporting 81
- exporting email attachments
  - path name too long 125
- EXTMGR\_ADDINS parameter 116, 122

## F

- FileNet P8
  - connecting by using WSI 128
  - searching special characters 135
- FileNet P8 configuration checklists 70
  - audit configuration 82
  - collections 74

- FileNet P8 configuration checklists
  - (continued)
  - content management system 73
  - export formats 76
  - export settings 76
  - general settings 71
  - LDAP 83
  - logging 84
  - Lotus Domino settings 82
  - search templates 75
  - user roles 71
- FileNet P8 server versions
  - adding version 4.5.1 131

## H

- Hebrew
  - Internet Explorer limitation 113
- holds
  - legal 152
- HTTP viewing 113
  - configuring 114

## I

- IATEMPDIR environment variable 27, 46
- IBM Connections documents
  - archived by IBM Content Collector 141
  - IBM Content Manager search options 147
  - IBM FileNet P8 search options 143
- IBM eDiscovery Manager overview 1
- IBM Legacy Content Search Engine
  - effect on searching 136
- ICMSERVER parameter 134
- IIOP protocol
  - connection methods 50
- inactive phase 151
- indexing
  - formats supported by IBM Legacy Content Search Engine 136
- Information Integrator for Content
  - installation problems 177
- installation
  - Content Manager EE 25
  - Content Manager EE environment 40
  - debug log files 42, 62
  - eDiscovery Manager 40, 60
  - FileNet P8 43
  - FileNet P8 environment 60
  - IBM Information Integrator for Content 35
  - Lotus Domino server 36, 56
  - Lotus Notes 36, 56
  - running the postinstalledm.sh script 166
  - silent 64
  - running 65
  - to connect to Content Manager EE 27
  - to connect to FileNet P8 46
  - validating 63
  - WebSphere Application Server 33, 35, 53, 55

- installation (continued)
  - WebSphere Application Server (Content Manager) 33
- installation options
  - recording 64
- installation path 25, 203
- installation program
  - improving performance 46
- installing
  - to new WAS profile 35, 55
  - to new WebSphere application server 35, 55
- item type properties
  - access control list 105

## J

- jvm.dll file 116, 122

## L

- LDAP 102
- ldapAttributes.xml file
  - Lotus Domino example 111
  - Microsoft Active Directory example 112
- legal holds 152
- legal tracing scenarios 11
- libjvm.a file 116, 122
- liblotuspwmgmra file 116, 122
- log files 181
  - Lotus Notes password manager 122
- Lotus Domino executable directory 116, 122
- Lotus Domino resource directory 116, 122
- Lotus Domino server
  - re-installing 59
  - reinstalling 39, 59
  - upgrading 39, 59
- Lotus iNotes viewing 113
  - configuring 114
  - configuring password manager 116
- Lotus Notes executable directory 116, 122
- Lotus Notes export
  - configuring 121
  - configuring password manager 122
- Lotus Notes export failure 192
- Lotus Notes password manager
  - log file 122
- Lotus Notes viewing 113
  - configuring 115
  - configuring password manager 116
- LotusPWMgr.dll file 116, 122
- LotusPWMgr.ini file 116, 122
- LotusPWMgr.log file 122

## M

- maximum privilege set 103, 104
- messages
  - format of 157
  - generic 157
  - numbered 157
- Microsoft Outlook viewing 113

monitoring 155

## N

new features 2  
non-text indexed properties  
    searching 62  
nonalphanumeric characters  
    searching as literal characters 135  
NOTES ERROR messages  
    troubleshooting 192  
notes.ini file 116, 122  
notesConnect utility 116, 122

## O

object classes  
    FileNet P8 108  
open  
    compressed attachments 130

## P

partitioned object stores  
    collections 74  
    date range 74  
password  
    changing 107  
password manager  
    configuring 116, 122  
PDF export  
    configuring 120  
    non-Latin-1 characters 120  
    true type fonts 120  
performance  
    creating DB2 indexes for  
        improving 43  
phases  
    active phase 151  
    deleting phase 151  
    inactive phase 151  
    service phase 151  
preinstallation  
    gathering information 32, 51  
prerequisite software  
    Content Manager EE 25  
    FileNet P8 43  
prerequisites 27, 46  
previewing content 113  
privilege sets  
    Content Manager EE 106  
privileges 102  
PST export files  
    configuring Exchange 120  
PublicReadACL 104

## R

reinstallation  
    Lotus Domino server 39, 59  
removing and reinstalling 199  
    Content Manager EE  
        environment 199, 200  
    FileNet P8 environment 201, 202  
    IBM FileNet P8 environment 201

removing eDiscovery Manager  
    removing privileges 203  
    turning off silent mode 203  
REPOSITORY\_UNAVAILABLE error 197  
response file  
    creating 64  
    editing 64  
roles  
    Content Manager EE 106

## S

sample configuration  
    Content Manager EE 18  
    FileNet P8  
        IBM Content Collector, IBM  
        Content Classification, IBM  
        Enterprise Records, IBM  
        eDiscovery Manager, and IBM  
        eDiscovery Analyzer 22  
    IBM Content Collector, IBM  
        eDiscovery Manager, and IBM  
        eDiscovery Analyzer 19  
    IBM Content Collector, IBM  
        eDiscovery Manager, IBM  
        eDiscovery Analyzer, and IBM  
        Enterprise Records 20  
    Planning IBM Content Collector, IBM  
        eDiscovery Manager, and IBM  
        eDiscovery Analyzer with Content  
        Manager EE 17  
save  
    compressed attachments 130  
saved document counts  
    less than search result counts 136  
saving documents 135  
scenarios  
    content management 11  
    email analytics preparation 11  
    legal tracing 11  
    organizing content 9  
    preparing for records management 8  
search  
    configuring 134  
search limitations  
    plain text files 135  
search results  
    impact of email archive 135  
    saving to folders 135  
search results counts  
    differ from saved document  
        counts 136  
search terms  
    non-English 135  
searches  
    improving performance of 62  
    on non-text indexed properties 62  
searching  
    date ranges 134  
    non-English locales 135  
    properties enabled with Content  
        Based Retrieval 136  
    special characters  
        FileNet P8 collections 135  
    when using IBM Legacy Content  
        Search Engine 136

secondary content servers  
    configuring 105  
security 107  
    object classes 108  
    secure cookies 130  
    users (FileNet P8) 108  
security adapters 109  
    FileNet P8 108  
security group  
    Content Manager EE 103  
service phase 151  
SharePoint documents  
    archived by IBM Content  
        Collector 137  
    search configuration options 138, 140  
silent installation 64  
    running 65  
silent uninstallation  
    running 206  
single sign-on 131  
special characters  
    searching as literal characters 135  
SSL  
    configuring with FileNet P8 128  
synchronizing  
    credentials 106  
    users 106

## T

tasks  
    scheduling 155  
temporary directory 27, 46  
troubleshooting 157, 181  
    ACL data and privilege set  
        exceptions 175  
    cannot connect to Content Manager  
        EE 159  
    Content Manager EE users accessing  
        eDiscovery Manager 178  
    database cannot open 187  
    database consistency 187  
    deleting eDiscovery Manager  
        data 175  
    DGL0394A 159  
    errors when installing eDiscovery  
        Manager 166  
    errors when removing eDiscovery  
        Manager 173  
    exporting Lotus Domino 180  
    exporting Lotus Domino content  
        fails 192  
    files left after uninstallation 176  
    IBM FileNet P8 connection 191  
    IBM FileNet P8 users accessing  
        eDiscovery Manager 178  
    installation errors 166  
    installation log file 168  
    installation program not  
        progressing 159  
    installing eDiscovery Manager 164  
    installing Information Integrator for  
        Content 177  
    internal error when exporting  
        content 189  
    internal error when viewing  
        content 189

- troubleshooting (*continued*)
  - Lotus Domino exports 185
  - NOTES ERROR messages 192
  - search results 135
  - searching for senders or recipients
    - by using LDAP 181
  - uninstallation errors 173
  - uninstallation program not progressing 168
  - WASX7017E exception 158
  - WASX7116E exception 158
- tuning indexes to improve performance 62
- WSI transport method
  - connection methods 50

## X

- X Window System
  - configuring 112

## U

- uninstallation
  - silent
    - running 206
- uninstallation program 204
- upgrade
  - Content Manager EE environment 40
  - eDiscovery Manager 40, 60
  - FileNet P8 environment 60
- upgrading 166
  - email notifications 68
- upgrading eDiscovery Manager 26, 44
- URLs
  - misspelled 196
- user directory
  - customizing 110
- user IDs 102
- user security
  - primary content server 103
  - secondary content server 104
- users
  - synchronizing credentials 106

## V

- viewing
  - configuring 113
  - configuring HTTP viewing 114
  - configuring Lotus iNotes
    - viewing 114
  - configuring Lotus Notes viewing 115
  - Internet Explorer limitation 113
  - Lotus iNotes viewing 113
  - Lotus Notes 113
  - Microsoft Outlook 113

## W

- Web Services Interface (WSI) transport
  - method 128
- WebSphere application profile
  - installing eDiscovery Manager to 35, 55
- WebSphere application server
  - installing eDiscovery Manager to 35, 55
- Windows
  - installation path 25, 203
- work manager 155
  - monitoring 155







Product Number: 5724-V36

GC19-1278-05

