opentext™

OpenText™ Documentum™ Archive Services for SAP® Solutions

Administration Guide

Configure connections to SAP, HTTP archiving services, SSL, and content-addressed storage systems using the WebAdmin tool.

EDCCOSAPAR250400-AGD-EN-01

OpenText™ Documentum™ Archive Services for SAP® Solutions
Administration Guide
EDCCOSAPAR250400-AGD-EN-01
Rev.: 2025-Oct-21

This documentation has been created for OpenText™ Documentum™ Archive Services for SAP® Solutions CE 25.4.
It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product, on an OpenText website, or by any other means.

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111
Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440
Fax: +1-519-888-0677
Support: https://support.opentext.com
For more information, visit https://www.opentext.com

© 2025 Open Text

Patents may cover this product, see https://www.opentext.com/patents.

Disclaimer

No Warranties and Limitation of Liability

Every effort has been made to ensure the accuracy of the features and techniques presented in this publication. However, Open Text Corporation and its affiliates accept no responsibility and offer no warranty whether expressed or implied, for the accuracy of this publication.

Table of Contents

Chapter 1

Documentum Archive Services for SAP solutions

1.1 Overview

Documentum Archive Services for SAP Solutions integrates the OpenText™ Documentum™ Content Management system with the SAP R/3 or ECC system. Based on the SAP HTTP ArchiveLink 4.7 interface, Documentum Archive Services for SAP Solutions provides a technology bridge between OpenText Documentum Content Management (CM) and SAP R/3 or ECC.

Documentum Archive Services for SAP Solutions provides these functions:

- Enables users to access and display documents stored in a OpenText Documentum CM repository from within a variety of SAP modules.
- Archives SAP data, reports, and documents through ArchiveLink certified interfaces in OpenText Documentum CM.
- Supports archiving attachments through GOS menu (GOS Attachments Archiving) from SAP.

1.2 Intended audience

To address the manuals to the correct audience, the following roles have been defined for users of Documentum Archive Services for SAP Solutions:

- **System Administrator** – This role covers users who install and configure Documentum Archive Services for SAP Solutions. Documentum Archive Services for SAP Solutions integrates OpenText Documentum CM and the SAP R/3 system.
- **Documentum Archive Services for SAP Solutions Administrator** – This role covers users who manage Documentum Archive Services for SAP Solutions using WebAdmin with Documentum Administrator.
- **Standard User** – This role covers users who view documents using SAP GUI.

This manual forms part of a documentation suite designed to support those who install, configure, and use Documentum Archive Services for SAP Solutions. The product and documentation suite can be found on OpenText My Support.

This document is intended for Documentum Archive Services for SAP Solutions administrators.

1.3 Architecture

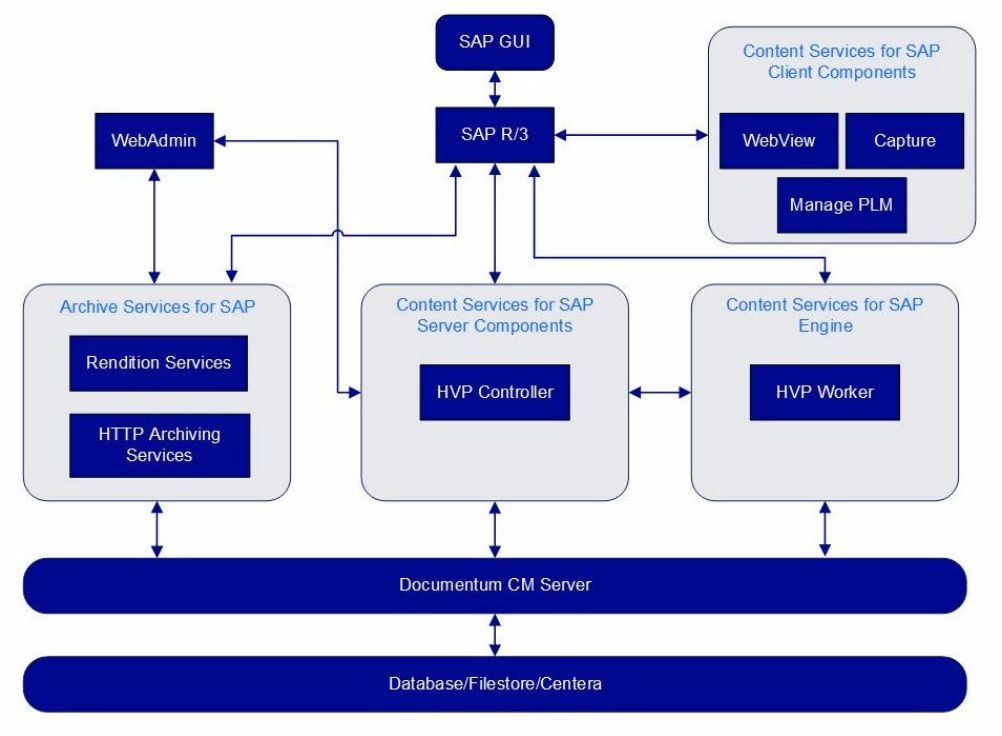

Figure 1-1: Documentum Archive Services for SAP Solutions and SAP

Note: Capture component is not available in 7.2 and later releases.

Documentum Archive Services for SAP Solutions consists of these components:

- HTTP archiving services

  A server component that, using an HTTP connection to SAP, enables you to archive reports, data, and incoming and outgoing documents from SAP to the OpenText Documentum CM repository. Documentum Archive Services for SAP Solutions is a Java servlet that communicates with SAP ArchiveLink. The reports and archived documents can later be retrieved and viewed through SAP GUI.

  Notes

  – OpenText recommends that you move from RFC- to HTTP-based archiving. No data migration is required. However, you cannot move back from HTTP archive to RFC because HTTP-archived documents are not accessible through RFC. HTTP and RFC can coexist in different archives.

  – If you migrate from RFC-based archiving to HTTP-based archiving, you do not need to convert pre-existing links from RFC to HTTP. The

migration from RFC- to HTTP-based archiving will ensure that all pre-existing links continue to work.

- WebAdmin

  An administrative tool hosted within the Documentum Administrator console that allows you to:

  – Create, configure, and manage archives.

  – Manage certificates for the archive.

  – Create repository connections for Documentum Archive Services for SAP Solutions.

  – Configure document archival for Documentum Archive Services for SAP Solutions.

The Product Compatibility Matrix (https://knowledge.opentext.com/go/matrix) contains the OpenText product requirements information for your product.

1.4 Documentum Archive Services for SAP Solutions ILM architecture

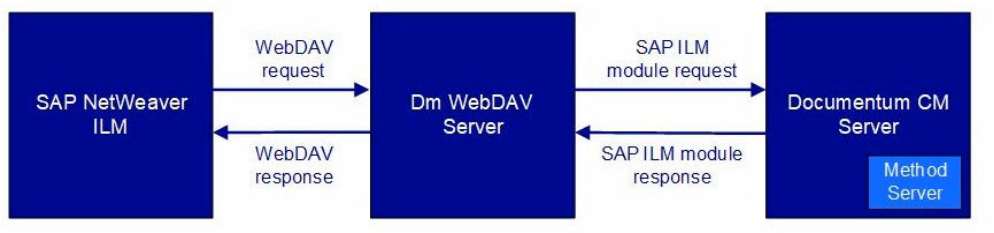

Figure 1-2: Documentum Archive Services for SAP Solutions ILM

- DM WebDAV Server: A web application, which acts as an interface between SAP ILM and OpenText Documentum Content Management (CM) Server.
- SAP Netweaver: A third party system, which provides SAP ILM capabilities.

1.5 Supported SAP document formats

OpenText Documentum CM supports the following SAP document classes or formats:

- Incoming or Scanned Documents (FAX class, Tiff format)
- Outgoing Documents (OTF class, PDF format)
- Archived Data (REO class, REO format)
- Reports or Print Lists (ALF class, ALF format)

1.6 SAP and Documentum Archive Services for SAP Solutions terms and definitions

Table 1-1: Terms and definitions

Term	Definition
AS SAP	Product that interconnects OpenText Documentum CM and SAP.
HTTP Archiving Services	Server component that, using an HTTP connection to SAP, enables you to archive reports, data, incoming and outgoing documents from SAP to the OpenText Documentum CM repository. HTTP Archiving Services is a Java servlet that communicates with SAP ArchiveLink. The reports and archived documents can later be retrieved and viewed.

Term	Definition
WebAdmin	An administrative tool hosted within the Documentum Administrator console that allows you to: • Create and manage archives • Manage certificates for the archive • Create repository connections for Documentum Archive Services for SAP Solutions
OpenText Documentum Content Management (CM)Foundation Java API	Documentum Client Library manages communication between clients and Documentum CM Server. It contains a library of API calls that are used by clients for execution on the Documentum CM Server. All client requests to the Documentum CM Server go through the Foundation Java API.
ArchiveLink	Cross-functional interface that is part of the SAP Basis System. ArchiveLink handles storing and retrieving documents and data to and from a repository external to SAP.
SAP DMS	Document Management System that is part of the SAP Basis System. Presents a logical layer to integrate with external systems such as AutoCAD or OpenText Documentum CM. Not directly related to ArchiveLink.
SAP PLM	SAP Product Life-Cycle Management (PLM) provides an integrated environment that ensures all people involved in product development, manufacturing, and service have quick and secure access to current information. It provides a set of BAPI calls that can be used by external systems. For example, OpenText Documentum CM.
SAP Master Record	A set of master data, such as customer or vendor data, which is used in the creation of SAP documents.
SAP GUI	SAP Graphical User Interface is a graphical menu/screen tool that connects a client to the SAP server.
Original Document	Paper-based version of a document. For example, an invoice may consist of two sheets of paper received from a supplier. Paper documents are scanned in and stored as electronic originals in OpenText Documentum CM.

Term	Definition
SAP Document	An electronic transactional record of header data and line items in SAP.

Chapter 2

WebAdmin

2.1 Overview

WebAdmin is a browser-based tool hosted within the Documentum Administrator that you can use to configure and administer Documentum Archive Services for SAP Solutions.

Note: Make sure that you have deployed Documentum Administrator to access the WebAdmin tool. For deployment instructions, see *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)*.

WebAdmin allows you to configure Documentum Archive Services for SAP Solutions HTTP Archiving Services as described in "Configure HTTP Archiving Services" on page 17.

2.2 Logging in to WebAdmin through Documentum Administrator

Log in to Documentum Administrator to administer Documentum Archive Services for SAP Solutions.

Note: The *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* has complete information about using Documentum Administrator.

To connect to WebAdmin through Documentum Administrator:

1. Start a web browser on a client machine.
2. Connect to the following URL, where host is the host where Documentum Administrator is installed and portnumber is a port number provided during application server installation:

   ```
   http://<host>:<portnumber>/da/
   ```

3. Type your login name and password on the login page.
4. Select a repository from the list box.

   If you change the repository, retype your password.
5. In the **Location** list (if available), select the location on your organization's network from which you are accessing Documentum Administrator.

   This allows you to access content from the nearest storage area in the network. Depending on your organization's setup, this location might be a fixed value.

6. To view additional options, click **More Options**.

   a. To connect to the repository using a particular server, select that server from the **Server** list box.

      The default is **Any Running Server**.

   b. If the repository is running in domain-required mode, type the domain name.

   c. To set the session locale to another language, select the language from the drop-down list.

   d. Do not click the **Additional Accessibility Options** link on the login page. Documentum Administrator does not support the accessibility options.

   e. To change your password in a repository, click **Change Password**, select a repository and type your old and new passwords, then click **Change Password**.

7. Click **Login**.

8. The **System Information** page appears with information about the system.

   The *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* has complete information about using Documentum Administrator and logging in to repositories available in Documentum Administrator.

2.3 Introducing the Content Services for SAP node of the WebAdmin GUI

After you have logged in to Documentum Administrator and the System Information page appears, you can select and expand the **Content Services for SAP** node located under the Administration node on the left pane.

The *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)* has complete information about using Documentum Administrator and logging in to repositories available in Documentum Administrator.

To use the following subnodes, you must have completed the installation of Documentum Archive Services for SAP Solutions. For more information, see *OpenText Documentum Archive Services for SAP Solutions - Installation Guide (EDCCOSAPAR250400-IGD)*

- ArchiveLink
- SAP

These subnodes contain additional subnodes that are used to perform these Documentum Archive Services for SAP Solutions functions:

1. **ArchiveLink**

Clicking the **ArchiveLink** subnode opens the **ArchiveLink** page in the right pane. The **ArchiveLink** page allows you to configure destination, archives, certificates, barcodes for Archive Link, and repositories.

The **ArchiveLink** subnode contains these functions:

- Archives
- Certificates
- Barcodes
- Repositories

2. **SAP**

   Clicking the **SAP** subnode opens the **SAP** page in the right pane. The **SAP** page allows you to configure the SAP Servers and Users to be used by Content Services.

   The **SAP** subnode contains these functions:

   - Query
   - Server
   - User

3. **Logout**

   Clicking **Logout** will log you out of Documentum Archive Services for SAP Solutions WebAdmin and Documentum Administrator.

Chapter 3

Configure connections to SAP

Before you can use Content Services Archive functionality, you must first configure the SAP server and user information in Documentum Archive Services for SAP Solutions.

In order to communicate with both SAP and OpenText Documentum CM, Documentum Archive Services for SAP Solutions must know the server and user login details for each system. The OpenText Documentum CM login parameters are specified when the Archives are created, as described in "Configuring, viewing, and editing archives" on page 17. When Documentum Content Services for SAP Solutions connects to Documentum CM Server, it reads the SAP server and user configuration parameters from the repository.

Documentum Content Services for SAP Solutions was designed so that you can configure multiple SAP servers and users. This allows Content Services to be used across multiple SAP application servers.

It is recommended that you create a specific user in your SAP system for use with Content Services.

The procedures in this chapter describe how to configure SAP servers and SAP users that will be used by the WebAdmin application to access SAP.

3.1 Creating, viewing, and editing connections to an SAP server

1. Connect to WebAdmin, as described in "Logging in to WebAdmin through Documentum Administrator" on page 11.
2. Click to expand the **SAP** subnode and select the **Server** subnode.

   The **SAP Server** screen appears.
3. Select **File** > **New** > **SAPServer** from the menu at the top of the **SAP Server** screen.

   The **New SAP Server** screen appears.
4. Type a name for the Server in the **New Server Name** field.
5. Do one of the following:

   - If you want to log in to an SAP server:

     Type the hostname or IP address for the server. When an SAP router is used, fill in the complete SAP router string in the following format: `/H/router1/H/<<host_name_or_IP_address>>`.

- If you want to log in to an SAP group, which is associated with an SAP R/3 server, type the following in this field:

```
MSHOST=<<message_server_host>> R3NAME=<<SAP_system_ID>> GROUP=<<SAP_group>>
```

6. Type the system name and number in the appropriate fields.
7. Click **OK** to save the SAP server configuration.

3.2 Creating, viewing, and editing an SAP user configuration

1. Connect to WebAdmin, as described in "Logging in to WebAdmin through Documentum Administrator" on page 11.
2. Click to expand the **SAP** subnode and select the **User** subnode.

   The **SAP User** screen appears.
3. Select **File** > **New** > **SAP User** from the menu at the top of the **SAP User** screen.

   The **New SAP User** screen appears.
4. Type the new username in the **New User Name** field.
5. Type the user ID in the **User ID** field.
6. Type a password for the user.
7. Type the Client Number.
8. Select the language for the user from the **Language** list box.
9. Click **OK** to save the SAP user configuration.

Chapter 4

Configure HTTP Archiving Services

4.1 Overview

This chapter describes how to configure Documentum Archive Services for SAP Solutions.

Note: SAP must be configured to work with Documentum Archive Services for SAP Solutions. Information about configuring SAP using SAPGUI is in the *OpenText Documentum Archive Services for SAP Solutions - Configuration Guide (EDCCOSAPAR250400-CGD)*.

4.2 Configuring, viewing, and editing archives

SAP uses named logical archives to specify target storage. Installations typically have a number of archives related to the different types of information that are archived:

- Archive AA may be used to archive Print Lists from SAP. As an administrator, you may want to configure the Archive Services to archive Print Lists in the following Documentum CM Server directory: /SAP/Printlists.
- Archive BB may be used to archive outgoing documents from SAP. As an administrator, you may want to configure Archive Services to archive outgoing documents in the following Documentum CM Server directory: /SAP/Outgoing.

WebAdmin allows you to specify rules for how to handle archived documents or data from SAP for each logical archive.

All configuration objects created in WebAdmin are stored within the Documentum CM Server.

Each archive configuration, such as AA or BB, can be found in the following Documentum CM Server folder: /System/DocLink/SAP/Archive.

Before configuring an archive in OpenText Documentum CM, you must create a similar archive in SAP as described in the 'OAC0 – Defining a Logical ArchiveID in SAP' section of the *OpenText Documentum Archive Services for SAP Solutions - Configuration Guide (EDCCOSAPAR250400-CGD)*. After creating an archive in SAP, WebAdmin can be used to mirror the SAP configuration and define Documentum CM Server-specific configuration options.

To configure, view or edit archives:

1. Connect to WebAdmin, as described in "Logging in to WebAdmin through Documentum Administrator" on page 11.

2. Click to expand the **ArchiveLink** subnode and select the **Archive** subnode.

   The **Archive** screen appears.

3. Select **File** > **New** > **Archive** from the menu at the top of the **Archive** screen.

   The **New Archive** screen appears.

4. Type the archive name in the **Archive Name** field.

   You can use up to 30 character long names for archives when supported by SAP.

5. The following parameters can be configured:

Table 4-1: Parameters in archives' configuration page

Field name	Description
Archive ID	Name of the SAP archive (as defined in the See OAC0 – Defining a Logical ArchiveID in SAP section in the *OpenText Documentum Archive Services for SAP Solutions - Configuration Guide (EDCCOSAPAR250400-CGD)*).
SAP Document Type	Set to NONE (HTTP provided).
Documentum Type	Specifies the OpenText Documentum CM document type, as described in "Configuring the repository Document Type" on page 19.
Workflow	Set to No Workflow.
Attribute Map	The attribute map is used to define the OpenText Documentum CM attributes of an archived document. There is a special attribute "FOLDER" that can be configured. To specify the folder path, use the following format: "FOLDER=/SAP/Archive/AA" In the Attribute map, you can also set the following attributes: • a_storage_type • a_retention_date **Note:** For more information, see "Setting Centera-related attributes in Documentum Archive Services for SAP Solutions" on page 39.

Field name	Description
Filtering	Used to define a custom filter. Used to define the output: • Text • PDF • HTML For more information, see Customizing platforms using Service-based Business Objects.

6. Click **OK** to save the archive configuration.

4.2.1 Deleting archived and linked documents

In a repository, if you delete version 1.0 of a document that is linked to SAP or archived from SAP, the link to SAP is also deleted. This is because the dm_relation object which creates the link to SAP is deleted when the parent object (which is always version 1.0) is deleted.

We recommend that you do not delete the original version of objects that are linked to SAP if you want to maintain their link to SAP. If you need to delete version 1.0 of a document, but want to keep the link to SAP, then, after deleting the document, you must relink the object to SAP, outside of Archive Services.

4.2.2 Configuring the repository Document Type

The value of the Document Type field defines the object type used to store the document in the repository. This object type must be a subtype of dm_document.

Example 4-1:

sap_print_list

4.2.3 Specifying a custom filter

(Optional) Type the name of a custom filter here.

A custom filter is usually a Docbasic or Java program that is stored as content of a specific method (dm_method) or an SBO. For example, a custom filter may parse the archived file and extract attributes from the document content. The attributes are then passed back to the Content Services Archive software and stored as custom attributes. Or, a custom filter can create queries to attach other documents (such as SOPs) as virtual components to the archived document.

Custom filters have to be marked with a leading exclamation mark if they are external executables and not dm_methods. The complete path to the executable has to be provided after the exclamation mark.

For example:

```
!C:\production\extract_keys.exe
```

SBO custom filters must be marked with a leading exclamation mark and pound sign (!#).

For example:

```
!#mySBOName
```

Customizing platforms using Service-based Business Objects provides more information.

4.2.4 Specifying a built-in filter

Using existing OpenText Documentum CM filters, you can define additional actions performed when a PrintList is archived. The following filters are currently implemented:

- *make_pdf*: A PDF rendition is generated by the Content Services software and added to the archived PrintList. To create a PDF rendition, you may want to define parameters to control how the rendition is formatted.
- *make_text*: An ASCII text rendition is generated by the Content Services Archive software and added to the archived PrintList.
- *make_html*: An HTML rendition is generated by the Content Services Archive software and added to the archived PrintList.

4.2.5 Implementing external filters

The filter mechanism allows you to customize Content Services Archive. You can write a filter program that parses the file to be archived and extracts special attributes for storage with the archived document.

The filter can be written in any programming or scripting language, such as Docbasic, C, C++, Perl, and JDK. It must be configured in the document profile with the Custom Filter Method parameter as described in Specifying a custom filter. The filter gets a number of arguments on the command line and it writes the result back to the Content Services Archive process. For performance reasons, the filter does not need to access the repository (but it is possible if really needed).

The filter is called with the following command line parameters:

```
path dm_doc_type dm_archive object_id repository_name dm_ticket
```

The parameters are:

- *path*: Full path of the ASCII text rendition of the file to be archived. Example: '/tmp/S567378.txt.'
- *dm_doc_type*: SAP document type for which this filter is defined. Example: 'ALF.'

- *dm_archive*: SAP archive ID. Example: ‘AA.'
- *object_id*: Document ID of the document created in the repository. Example: ‘09001edc800003af.'
- *repository_name*: Name of the current repository. This parameter is used when the filter has to connect to the repository.
- *dm_ticket*: Encrypted ticket string for the user.

The filter passes the result back simply by writing to the standard output. Additionally, it must return 0 (zero) when the program exits, as shown in the following table:

Table 4-2: External filters

Language	Syntax
Docbasic	print...
C	fprintf(stdout,”...”)
C++	cout << “...”)
Java	

The following parameters allow the filter to pass results back to Content Services Archive:

- *set,<any attribute name>,<value>*: Defines an attribute with a given value. The attribute must exist for the object type used. By default, the object type is ‘dm_document.' If additional attributes must be stored, you must define a new subtype of ‘dm_document' and define the attributes that the filter uses. Use the configuration parameter ‘SAP Obj Type' when using a filter with different object types.

  Example: 'set,object_name,PI Sheet 4711'
- *virtual,<obj type> where <qualification>:* Allows you to specify a query that selects documents to attach to the archived document as virtual components.

  Example: 'virtual,dm_document where title is 'SOP 4711%'
- *error,<error message>*: If the filter wants to report an error. We recommend storing the error on the first line of the file. The error message is written to the log file and the operator is notified.

  Example: 'error,Cannot open file'

4.2.5.1 Example: PI sheet

This example creates a custom filter which extracts specific attributes from archived documents. This example uses the PI Sheet filter that was installed with the Content Services Archive software. It assumes that a second filter was installed for Inspection Lots. This filter looks similar to the PI Sheet filter, but is not explained in this section. This example is already installed and configured so it is not required to perform the steps explained in this section.

The purpose of the following customization is to extract some document attributes from an archived PI sheet. These document attributes will enable standard OpenText Documentum CM queries to find the PI sheet again.

The first few lines of the archived PI sheet appear as follows:

```
------------------------------------------------------------
PI sheet            : 100000000000002128
Proc. order         : YMM_14
Plant               : 0001
CntlRecDestin.      : 01
Operating grp.      : GROUP 1
Dest.type           : 1
Test                :
Status              : 00005
Created on          : 05.01.1996
                    : 10:22:36
Changed on          : 05.01.1996
------------------------------------------------------------
```

To create a customized PI sheet filter:

1. Define a new document type named dm_pi_sheet.

   This new document type defines the attributes you wish to extract. The document type is defined with the following DQL statement:

```
CREATE TYPE dm_pi_sheet (
    proc_order char(32),plant char(32),ctrl_rec_dest char(32),
    operating_grp char(32),dest_type char(32),status char(32)
    ) WITH SUPERTYPE dm_document
```

2. Create a filter that parses the PI Sheet and defines the attributes in Docbasic:

```
Sub GetMatch(ll As String, match As String, delimiter As String, ByRef res

As String)
If InStr(ll, match) = 1 Then
        pos = InStr(ll, delimiter)
        If pos > 0 Then
            fld$ = Mid$(ll, pos + 2)
            res = Trim$(fld$)
        End If
    End If
End Sub
```

```
Sub Filter(arg_path As String, arg_dm_doc_type As String,_
             arg_dm_archive As String,_
             arg_obj_id As String, arg_docbase As String,_
             arg_user As String, arg_passwd As String)
' open file and get values into variables
    file% = FreeFile
    Open arg_path For Input As file%
    Count = 0
```

```
    Do While Not EOF(file%)
' read each line and try to find values
        Line Input #file%, ll$
        GetMatch ll$, "PI sheet", ":", pi_sheet$
        GetMatch ll$, "Proc. order", ":", proc_order$
        GetMatch ll$, "Plant", ":", plant$
        GetMatch ll$, "CntlRecDestin.", ":", ctrl_rec_dest$
        GetMatch ll$, "Operating grp.", ":", operating_grp$
        GetMatch ll$, "Dest.type", ":", dest_type$
        GetMatch ll$, "Status", ":", status$
' definitions must be within the 20 first lines
        Count = Count + 1
        If (Count > 20) Then
            Exit Do
        End If
    Loop
'write attributes and content to stdout
    Print "set,object_name," + pi_sheet$
    Print "set,proc_order," + proc_order$
    Print "set,plant," + plant$
    Print "set,ctrl_rec_dest," + ctrl_rec_dest$
    Print "set,operating_grp," + operating_grp$
    Print "set,dest_type," + dest_type$
    Print "set,status," + status$

    Exit Sub
End Sub
```

3. Create a method named dm_filter_pisheet with the following DQL statement:

```
        CREATE dm_method OBJECT set object_name='dm_filter_pisheet',
        set method_verb='dmbasic -eFilter',set timeout_min=30,
        set timeout_max=604800,set timeout_default=86400,
        set run_as_server=TRUE,set use_method_content=TRUE,
        set     method_type='dmbasic'
```

4. Use the object ID of the created method and store the Docbasic file with the following API methods.

   The DQL statement in the previous step returned the object ID of the method created:

```
        setfile,c,<ID of dm_method>,<Docbasic path>,crtext
        save,c,<ID of dm_method>
```

5. In WebAdmin, create an archive named PI. Define this archive to use folder /SAP/PI Sheets.

   Using this archive from SAP ensures that all PI Sheets are stored in this folder.

6. Configure the archive PI in SAP.

   Make sure PI Sheets are archived to this archive.

7. Create a profile object (dm_al_profile) called ALF-PI.

   This profile is applied when a document of the SAP document type ‘ALF' is archived to the archive ‘PI':

   a. Define Document Type as ‘dm_pi_sheet.'
   b. Define Document Format and SAP Retrieve Format as ‘sap_print_list.'
   c. Activate the Built-In Filter parameter as ‘make_pdf' or ‘make_html' if required.

d. Define Custom Filter Method as ‘dm_filter_pisheet.'

Note: This step is very important.

8. Test your customized filter by archiving a PI Sheet.

   Check attributes and renditions to verify that the filter implementation worked correctly.

4.2.6 Customizing platforms using Service-based Business Objects

OpenText Documentum CM Business Objects are designed to provide modular business logic to the presentation layer by hiding the underlying repository schema and by using OpenText Documentum CM core services, facilitating customization of object behavior without modifying any existing application built on Foundation Java API. Service-based Business objects (SBOs) are generalized objects that provide a specific service that may operate on different OpenText Documentum CM object types or other business objects, and are not tied to a specific OpenText Documentum CM object type. Each service-based business object provides a generalized interface to a group of related operations that need to be performed. The operations may not need access to a repository, however, content management services are the focus of OpenText Documentum CM Business Objects.

The archiving operation can be customized using a custom filter, such as an SBO. To enable OpenText Documentum CM archiving customization using SBOs, an archive configuration can specify an SBO as a custom filter. Documentum Archive Services for SAP Solutions will dynamically execute the method “doArchive (IDfPersistentObject obj,String archiveID) throws DfException” that must be defined in the SBO:

1. The SBO must have a method void doArchive (IDfPersistentObject pobj, String archiveID) throws DfException.

2. The message returned to an SAP http response, in the event of any error while executing the archive customization method, should be returned by doArchive(..) method in the exception message.

3. The call to doArchive(..) runs within the context of an archiving transaction and Documentum Archive Services for SAP Solutions will do a commit() when SBO doArchive(..) is successfully executed.

4. The SBO module need not handle any function for session management for the SessionManager passed by Documentum Archive Services for SAP Solutions. Examples are: Transactions, Session creation, or release. SBOs can obtain a session by calling getSessionManager(), getSession(), or just getSession().

5. SBOs should not release the session obtained by session management described in step 4. However, if any session manager or session is created in SBO explicitly, SBO has the responsibility to release it.

6. Documentum Archive Services for SAP Solutions will pass the IDfPersistentObject corresponding to the archived object to the doArchive(..) method of the SBO. In addition, the archive ID will be passed (if it is an archive config object).
7. Documentum Archive Services for SAP Solutions will set the SessionManager corresponding to credentials specified in a repository configuration for the repository to the SBO.

4.2.6.1 Customizing platforms using SBOs

1. Connect to WebAdmin, as described in "Logging in to WebAdmin through Documentum Administrator" on page 11.
2. Click to expand the **ArchiveLink** subnode and select the **Archive** subnode.

   The **Archive** screen appears.
3. Select **File** > **New** > **Archive** from the menu at the top of the **Archive** screen.

   The **New Archive** screen appears.
4. Type the SBO service name, prefixed with !# in the custom filter text box, and click **OK**.
5. Archive a document to the content repository from SAP.

   The customized functionality implemented in SBOs doArchive() method executes.

4.3 Efficiently handling scanned single-component SAP documents

Documentum Archive Services for SAP Solutions efficiently archives single-component, medium-sized (40–100 KB) SAP documents by processing them in memory, without using the disk. This processing method reduces the time taken to archive files.

The ability to handle the files in-memory is very useful when large volumes of single-component SAP documents need to be archived. A typical example would be when a large number of invoices are batch-scanned and then archived using Archive Services.

To configure the maximum size of files that can be processed in memory:

1. In the `al.properties` file (available here: <*Application-Installation-Root-Directory*>\webapps\archivelink\WEB-INF), locate the following attribute:

   ```
   archiving.inmemory.maxSize=10
   ```

   The default value is 10 KB.
2. Change the value of this attribute as per your needs.

The maximum size of a single-component SAP document that can be processed by Archive Services in memory is 2 GB.

Note: Before you configure Archive Services to process documents as big as 2 GB in memory, verify if the existing memory can handle such loads.

4.4 Configuring HTTP barcodes for archive linking

In the HTTP archive scenario, Agent services process "barcoded documents" and link them to SAP.

You may want to use barcodes to identify and link documents in the repository with records in SAP. You may also use a custom attribute to store the barcode. The barcode may be a unique number assigned to the document when it is received. This unique number can be written on the document in front of a barcode or in plain text. When the document is posted in SAP, the user may just type in the number or use a barcode reader.

When the document is scanned in the barcode is automatically recognized (by a third-party solution) and the value is stored in the custom barcode attribute.

Note: The document may also be scanned in before it is posted in SAP (early archiving).

For example, in late archiving, documents are scanned and stored in a OpenText Documentum CM repository after an SAP document has been processed. In other words, the SAP document is posted as usual by transferring the data from the original paper document to the system. The original paper document is forwarded to an input location, where it is scanned and then assigned to the SAP document based on a barcode.

A typical scenario for implementing barcode support is in "late archiving with barcodes."

Note: Ensure that barcodes are available for linking:

- The image is scanned.
- The barcode is recognized (by third-party software).
- The barcode is stored as a number in an object attribute (by third-party software).

To configure HTTP barcodes for archive linking:

1. Connect to WebAdmin, as described in "Logging in to WebAdmin through Documentum Administrator" on page 11.
2. Click to expand the **ArchiveLink** subnode and select the **Barcodes** subnode.

   The **Barcodes** screen appears.

3. Select **File** > **New** > **Barcode** from the menu at the top of the **Barcode** screen.

   The **New Barcode** screen appears.

4. Select the document type from the **Choose a Document Type** list box.
5. Select the barcode storage attribute from the **Barcode stored in attribute** list box.
6. Select the archive for use from the **Archive to use** list box.
7. Click **OK** to save the barcode configuration.

4.5 Working with SAP archive certificates

Documentum Archive Services for SAP Solutions uses an HTTP connection between the SAP server and the Web server (where Documentum Archive Services for SAP Solutions is installed). SAP R/3 uses this Internet-based protocol to send and receive information between R/3 and Documentum CM Server. However, before archiving can take place, a digital certificate must be generated from R/3 and installed in Documentum CM Server. This certificate is used by Documentum Archive Services for SAP Solutions to validate:

- That the request parameters have not been altered/corrupted in transmission.
- The identity of the R/3 server sending or receiving information.

If digital certificates are not used, it would be possible for non-authorized persons to spoof the Documentum CM Server into returning information that they are not allowed to access.

A different certificate is used for each archive. So, archives AA, BB, and CC would each have their own certificate that is used when transferring information between R/3 and Documentum Archive Services for SAP Solutions.

Certificates are not created directly in WebAdmin. They are passed to Documentum Archive Services for SAP Solutions (and into the Documentum CM Server) when a certificate is sent from SAP. However, before they can be used, WebAdmin must be used to activate the certificate and set an expiry date. This section describes how to transmit and activate an HTTP archive.

4.5.1 Sending certificates to HTTP Documentum Server

After creating an HTTP archive in SAP (using transaction code `oac0`), you can use SAP transaction oaht to send archive certificates to Documentum Archive Services for SAP Solutions.

Clicking **Execute** transmits the certificate to Documentum Archive Services for SAP Solutions.

If an error stating "HTTP Error: 403 Access Forbidden" is displayed, this may be because:

- The Web server is not running.
- The archive parameters are incorrect.

Note: The server may not be able to translate a hostname into an IP address. Try using the IP address instead.

If the certificate is successfully transmitted, it will be listed in the **Certificates** tab of WebAdmin.

Tips

- The first three characters of the certificate name are the system name of the SAP server that sends the certificates.
- The last two characters of the certificate name are the same as the archive name.

Note: The corresponding archive should be displayed. If this field is blank, this is probably because the archive configuration object has not been created in WebAdmin yet.

Before a certificate can be used, it must be activated and set with an expiration date. This ensures that a controlled procedure is followed before a system can archive information into Documentum CM Server.

4.5.2 Activating and customizing certificates

1. Connect to WebAdmin, as described in "Logging in to WebAdmin through Documentum Administrator" on page 11.
2. Click to expand the **ArchiveLink** subnode and select the **Certificates** subnode.

   The **Certificates** screen appears.
3. Select **File** > **New** > **Certificate** from the menu at the top of the **Certificates** screen.

   The **Certificates Properties** screen appears.
4. Right-click on a certificate and select **Properties** from the sub-menu.

Selecting **Delete** removes the Certificate from the Documentum Content Services for SAP Solutions repository.

5. Select **Activate** or **Deactivate** from the **Status** list box.
6. Select a certificate expiration date from the **Expiration** calendar menu and list boxes.
7. Click **OK** to save the certificate configuration.

4.6 Configuring HTTP repositories for archive linking

1. Connect to WebAdmin, as described in "Logging in to WebAdmin through Documentum Administrator" on page 11.
2. Click to expand the **ArchiveLink** subnode and select the **Repositories** subnode.

   The **Repositories** screen appears.
3. Select **File** > **New** > **Repository** from the menu at the top of the **Repository** screen.

   The **New Repository** screen appears.
4. Type the connection information for the new repository, as follows:

   Repository Name: Name of the new repository

   User Name: Username associated with the user of the new repository

   User Password: User password associated with the username of the user of the new repository

   Domain: Domain in which the new repository resides

   Note: Click **Test Connection** to test the connection information for the new repository.
5. Type the connection information for the global repository associated with the new repository, as follows:

   User Name: Username associated with the user of the global repository

   User Password: User password associated with the username of the user of the global repository

   Domain: Domain in which the global repository resides
6. Click **OK** to save the new repository configuration.

4.7 Managing temporary disk space in an Archive Services host

To set the available disk space limit to the local content area, use the following Foundation Java API property:

`dfc.data.local_diskfull_limit`

By default, the `dfc.data.local_diskfull_limit` value is 0. This means, there is no limit on the size of the local content area. The `getfile` error is displayed after the limit is reached.

If the limit exceeds the value configured in `dfc.data.local_diskfull_limit`, local content for the current session is purged to free up space. The `getfile` request succeeds if enough disk space is reclaimed by the purge.

Note: By default, `dfc.data.local_purge_on_diskfull` value is true.

Chapter 5

Configure SSL for Documentum Archive Services for SAP Solutions

5.1 Overview

Documentum Archive Services for SAP Solutions supports both HTTP and HTTPS protocols. This section details the configurations needed on both SAP and the Documentum Archive Services for SAP Solutions application server for Secure Socket Layer (SSL).

5.2 Prerequisites for SSL configuration

5.2.1 SAP HTTP

As of Release Web AS 6.20/SAPGUI for Windows 6.20, SSL is supported in SAPHTTP. The latest version of SAPHTTP is available on SAP Service Marketplace. The SAP Note 164203 has more information.

5.2.2 SAP cryptographic toolkit

For using SSL, the SAP Java Cryptographic Toolkit must be installed. For more information about SAP Cryptographic Library, see SAP Note 397175.

5.3 Configuring SSL for SAPHTTP

Configuring SSL for SAPHTTP requires the creation of SAPSSLC.pse and making SAPHTTP aware of the certificate.

5.3.1 Creation of SAPSSLC.pse

SAPSSLC.pse contains information for the SSL client. Copy the SAP Cryptographic Library and the sapgenpse program into the directory of SAPHTTP. Based on the certificates being Self-signed or from a Certificate authority, the following describes the details of working with the certificates.

5.3.1.1 Creating self-signed certificates

1. The following command generates SAPSSLC.pse with the name <*saphost*> in the `c:\temp\directory\`:

   ```
   sapgenpse get_pse -noreq -p c:\temp\SAPSSLC.pse CN=<saphost>
   ```

   <*saphost*> can be fully qualified host name/IP address of SAP application server. When prompted, provide a blank PIN.

2. Export the certificate for SAPSSLC.pse created using the following command:

   ```
   sapgenpse export_own_cert -p c:\temp\SAPSSLC.pse –o c:\temp\sapserver.cer
   ```

   You need to import this certificate as trusted in the Application Server keystore as detailed in the Configuring SSL on the AS SAP Application Server section of this document.

3. Import the certificate of Application Server in SAPSSLC.pse as trusted certificate using the following command:

   ```
   sapgenpse maintain_pk -a c:\temp\tomcat.cer -p c:\temp\SAPSSLC.pse
   ```

   In the command, tomcat.cer contains certificate of Application Server. Create the tomcat.cer as explained in the Configuring SSL on the AS SAP Application Server section.

   Alternatively, the certificate can also be imported using STRUST.

4. The following command lists the certificates in the PSE:

   ```
   sapgenpse maintain_pk -l -p c:\temp\SAPSSLC.pse
   ```

5. Restart the Internet Communication Manager (ICM).

5.3.1.2 Working with certificates from a Certificate Authority

You can obtain and work with certificates from a Certificate Authority of your choice such as Verisign, Thawte or Trustcenter.

To obtain a Certificate from the Certificate Authority of your choice:

1. The following command creates SAPSSLC.pse with a Certificate Signing Request (CSR):

   ```
   sapgenpse get_pse -p c:\temp\SAPSSLC.pse -r <CERT_REQUEST.csr> CN=<saphost>
   ```

2. Submit the CSR to CA (Certificate Authority) to get a certificate <CERT_RESPONSE.cer>.

3. Include the root and intermediate certificates of CA in to SAPSSLC.pse using the following command. For example, if the CA root certificate is encoded in the `c:\temp\CARoot.cer` file:

   ```
   sapgenpse maintain_pk -a c:\temp\CARoot.cer -p c:\temp\SAPSSLC.pse
   ```

   Similarly include the intermediate Certificate to SAPSSLC.pse.

4. Use the following command to import the own certificate to SAPSSLC.pse

```
sapgenpse import_own_cert -p c:\temp\SAPSSLC.pse -c <CERT_RESPONSE.cer>
```

   You can also use STRUST transaction for importing the certificate.

5. Include the root and intermediate certificates of Application Server to SAPSSLC.pse. For example, if the Application Server uses VeriSign Certificates, include VeriSign root certificate to SAPSSLC.pse:

```
sapgenpse maintain_pk -a c:\temp\TomcatRoot.cer -p c:\temp\SAPSSLC.pse
```

   Similarly include the VeriSign intermediate Certificate of Application Server to SAPSSLC.pse.

5.3.2 Configuring SAPHTTP

1. Copy the SAPSSLC.pse file to <*SYSTEM NAME*>/<*INSTANCE NAME*>/sec. SAPHTTP also requires SAPSSLS.pse. If SAPSSLS.pse is missing (for example if you do not have Web AS 6.10) in the same directory, copy SAPSSLC.pse to SAPSSLS.pse. The file named 'ticket' must also be available in the directory. If it is not available, copy this file from SAP Cryptographic Library. In addition, copy sapcrypto.dll from SAP Cryptographic Library in to this directory.
2. Copy the same files (SAPSSLC.pse, SAPSSLS.pse,ticket, sapcrypto.dll) into the SAP GUI directory and to <S*YSTEM NAME*>/SYS/exe/run directory on the SAP server.

Note: The SAP Note 506314 has more information on configuring SAPHTTP with SSL.

5.4 Configuring SSL on the Documentum Archive Services for SAP Solutions Application Server

The following steps described are for Tomcat Application Server. Apply similar changes for the other supported application servers.

5.4.1 Enabling SSL on Tomcat

To enable SSL on Tomcat, add or uncomment the following lines in "<*tomcat_home*>> \conf\server.xml"

```
<Connector port="<SSL Port>>" maxThreads="150" minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS" keystoreFile="<="<${user.home}/.keystore>"
keystorePass="<keystore password>" keyAlias="<Certificate Alias>" />
```

Note: The *Documentum CM Server* chapter in *OpenText Documentum Content Management - Server and Server Extensions Installation Guide (EDCSY250400-IGD)* contains more information about using SSL communication with Oracle JDK/ OpenJDK.

5.4.2 Creating keystore

Create a keystore using the JDK Keytool.

```
%JAVA_HOME%\bin>keytool -genkey -alias <Certificate Alias> -keyalg RSA
Enter keystore password: changeit
What is your first and last name?
[Unknown]: <enter_host_name or IP Address of host where tomcat is running>
```

Note: Record your name.

```
What is the name of your organizational unit?
[Unknown]: <enter_OU>
What is the name of your organization?
[Unknown]: <enter_Org>
What is the name of your City or Locality?
[Unknown]: <enter_city>
What is the name of your State or Province?
[Unknown]: <enter_state>
What is the two-letter country code for this unit?
[Unknown]: <enter_country>
Is CN=tomcat-host, OU=CMA, O=TEST, L=Sydney, ST=NSW, C=AU correct?
[no]: yes
Enter key password for <Certificate Alias>
(RETURN if same as keystore password):
```

Note: The private key password and keystore password should be the same. Verify that a file called `.keystore` has been created in the user home directory. For example, `C:\Documents and Settings\dmadmin\.keystore`).

5.4.3 Generating self-signed certificates from Tomcat keystore

This section describes the details of creation of a self-signed certificate from the Tomcat keystore. The certificate exported to the file would in-turn be imported to `SAPSSLC.pse`.

5.4.3.1 Export certificate from the keystore to a file

Export the certificate to a file using the following command:

```
keytool -export -alias <certificate alias> -file "C:\temp\tomcat.cer"
```

The command stores the self-signed certificate in the file `tomcat.cer`.

You need to add this certificate to the trusted list of `SAPSSLC.pse` as detailed in the Configuring SSL for SAPHTTP section.

5.4.3.2 Import SAP certificate to the keystore

Add self-signed certificate of SAPSSLC.pse to the trusted list of Tomcat keystore.

The certificate is encoded in `sapserver.cer` file. Use the following command:

```
keytool -import -alias sapserver -file C:\temp\sapserver.cer
```

5.4.4 Generating certificate from the Certificate Authority

To generate the certificate from the Certificate Authority (such as Verisign, Thawte or Trustcenter), complete the following:

5.4.4.1 Create CSR from the keystore

Create certificate request using the following command:

```
keytool -certreq -keyalg RSA -alias <Certificate Alias> -file c:\temp\certreq.csr
```

5.4.4.2 Import certificates to the keystore

1. Send the CSR to the Certificate Authority (For example, VeriSign) to get a certificate.
2. Before importing the certificate to the keystore, include root and intermediate certificates in the keystore. For example, for Verisign trial certificates.

   ```
   keytool –import -alias verisign-trial-root -trustcacerts -file c:\temp\Verisign-trial-root.txt
   ```

   ```
   keytool –import -alias verisign-trial-intermediate -trustcacerts -file c:\temp\Verisign-trial-intermediate.txt
   ```

3. Import the certificate reply to the keystore using the following command:

   ```
   keytool -import -alias <Certificate Alias> -file C:\temp\Verisign-signed-cert.txt
   ```

4. Include the root and intermediate certificates of CA from which you received the certificate of SAPSSLC.pse in the trusted list of Tomcat's keystore.

   Use the same commands which was used for importing root and intermediate certificates of VeriSign in the previous steps.

Now, both Application Server and SAPHTTP are ready to work with HTTPS protocol. Proceed with Documentum Archive Services for SAP Solutions deployment and archiving using Documentum Archive Services for SAP Solutions.

5.5 Configuring SAP Content Repository to enable SSL for archive link communication

1. In the OAC0 transaction, select the content repository on which SSL needs to be enabled.
2. Send the certificate from SAP content repository to Documentum Archive Services for SAP Solutions in the non-SSL mode.

   Note: The distribution of certificates from transaction OAC0 is intended to send the signer's certificate to the communication partner in a system landscape for an SSL application. It is used for verification of data sent through archive link using PKCS7 standard. “Send Certificate” in transaction OAC0, can be done in non-SSL mode only. It is a one time job.
3. Now edit the Content Repository to mention the SSL port. Enter %HTTPS in the transaction code field. Select HTTPS required in both HTTPS on frontend and HTTPS on backend and save the configuration.

5.6 Troubleshooting: If there is a failure while establishing secured connection between SAP and AS SAP

1. Update `CommonCryptoLib`.

   Suggested version for `CommonCryptoLib` is 8.5.36 or later.
2. Locate the file `DEFAULT.PFL`.

   By default, the file location is `/usr/sap/<sys_name>/SYS/profile`.
3. Add the following parameters in default profile (`DEFAULT.PFL`):

   ```
   ssl/ciphersuites = 135:PFS:HIGH::EC_P256:EC_HIGH
   ssl/client_ciphersuites = 150:PFS:HIGH::EC_P256:EC_HIGH
   icm/HTTPS/client_sni_enabled = TRUE
   ssl/client_sni_enabled = TRUE
   ```

Chapter 6

Configure content-addressed storage systems for Archive Services for SAP solutions

6.1 Overview

Documentum Archive Services for SAP Solutions provides dedicated support for retention management using content-addressed (CA) storage system, Centera®.

Certain industries, such as the pharmaceutical industry, are required, by law, to retain and preserve all product-related documentation for a stipulated period of time. This is a strictly-enforced, non-negotiable clause that firms are expected to comply with. To automate this process of retention management, Documentum Archive Services for SAP Solutions has been integrated with Centera.

This integration allows firms using both Centera and Documentum Archive Services for SAP Solutions to archive stipulated content:

- Based on specific attributes such as dates, and so on
- For specific periods of time, as required by law
- In a foolproof manner that ensures the content cannot be tampered with during the archival period

You can configure Documentum Archive Services for SAP Solutions to archive specific content in Centera. You can configure Documentum Archive Services for SAP Solutions to use different Centera systems for different archives. These archives map to SAP document types in SAP. This feature is particularly useful when you need to archive documents that have different retention period requirements. The integration of Documentum Archive Services for SAP Solutions with Centera allows you to automate this customized archiving process.

To configure CA storage systems for Documentum Archive Services for SAP Solutions:

1. Create the CA storage types using Documentum Administrator as described in "Creating CA storage types using DA" on page 38.
2. Set Centera-related attributes in Documentum Archive Services for SAP Solutions as described in "Setting Centera-related attributes in Documentum Archive Services for SAP Solutions" on page 39.

6.2 Creating CA storage types using DA

To configure Documentum Archive Services for SAP Solutions for Centera, you must create a CA storage type using Documentum Administrator. Before you configure Documentum Archive Services for SAP Solutions for Centera, Content Storage Services (available in Documentum CM Server 5.2.5 SP2 and later) must be enabled. For more information on enabling Content Storage Services, see the 'Using Content Assignment Policies' and 'Moving Content Files' sections in the *OpenText Documentum Content Management - Server Administration and Configuration Guide (EDCCS250400-AGD)*.

Note: The retention settings for storage types in Documentum Administrator allow you to specify only a fixed date. You cannot specify a period relative to document ingestion; such a setting would conflict with the settings in WebAdmin, as described in "Setting Centera-related attributes in Documentum Archive Services for SAP Solutions" on page 39.

For more information on creating CA storage types using Documentum Administrator, see *OpenText Documentum Content Management - Administrator User Guide (EDCAC250400-UGD)*.

6.2.1 Creating content-addressed stores

To create a content-addressable store, you must have a license for Documentum Content Services for SAP Solutions for Centera and this feature must be enabled in the Documentum CM Server installation containing the repository for which you are creating the store.

You must also know the IP address of the Centera content-addressable storage system to set up content-addressable storage.

A repository can have multiple content-addressable stores. For ease of administration, maintenance, and management, it is recommended that you use the same plug-in for all of the content-addressable stores.

To create a content-addressable store:

1. Connect to the repository for which you want to create a new content-addressed store.
2. Click **Storage**.
3. Click **File** > **New** > **Content-Addressable Storage**.
4. Type the name of the new content-addressed store.
5. Click **Edit**.
6. In the **Enter new value** field, type the IP address of the Centera content-addressable storage system.

   Do not type other parameters or values.

7. Click **Add**.
8. Click **Ok**.
9. To enable a content retention period, select **Set Retention Information**:
   a. Type in the retention attribute name.

      The value you enter must be one of the values specified as a content attribute name in step 4.
   b. Select **Application must provide value for retention attribute**; this allows a client application to supply the retention date when content is saved.
10. Click **Finish**.

6.3 Setting Centera-related attributes in Documentum Archive Services for SAP Solutions

You must set the following Centera-related attributes in Documentum Archive Services for SAP Solutions:

- a_storage_type
- a_retention_date

To set the a_storage_type and a_retention_date attributes in Documentum Archive Services for SAP Solutions:

1. Connect to WebAdmin, as described in "Logging in to WebAdmin through Documentum Administrator" on page 11.
2. Click to expand the **ArchiveLink** subnode and select the **Archive** subnode.

   The **Archive** screen appears.
3. Select **File** > **New** > **Archive** from the menu at the top of the **Archive** screen.

   The **New Archive** screen appears.
4. From the **Rule composer** drop-down list, select **a_storage_type**.
5. In the text box against the **Rule composer** drop-down list, type the name of the CA store as configured in Documentum Administrator, as described in "Creating CA storage types using DA" on page 38.
6. Move the composed rule to the **Defined map rules** field by clicking the arrow icon below the **Rule composer** drop-down list.
7. From the **Rule composer** drop-down list, select **a_retention_date**.
8. In the text box against the **Rule composer** drop-down list, type a value for **a_retention_date**.

The value assigned to the a_retention_date attribute is the desired retention period, in days, from the date of ingestion.

Example 6-1:

Type `365` in this field; this means that the documents will be stored in the archive for one year, from the date of archival.

9. Move the composed rule to the **Defined map rules** field by clicking the arrow icon below the **Rule composer** drop-down list.
10. Type appropriate values for all other fields in the archive configuration page.
11. To save the a_retention_date setting for the archive, and other archive settings, click **OK**.

    The setting is active now and will apply to all documents stored in this archive.

Appendix A. Troubleshooting

This section provides troubleshooting solutions for some of the known issues.

A.1 Archivelink repository registration issues

Unable to register repositories related to Documentum Archive Services for SAP Solutions; The registered repositories do not get displayed.

Suggested resolution

Verify the following:

- If the repository being accessed is not a GR (Global repository), then make sure the Enterprise_Integrations_Core.dar file is installed on the GR also.
- Install Documentum Archive Services for SAP Solutions (assap.war) on a supported application server.
- Specify the Global registry details of the repository in the `dfc.properties` file. Make sure that the Global registry details specified is the same in both the `dfc.properties` files of Documentum Administrator and Documentum Archive Services for SAP Solutions.

A.2 Documentum Archive Services for SAP Solutions for Korean/Japanese printlists

Unable to archive Korean/Japanese printlists or seeing garbled renditions of the archived Korean/Japanese printlists.

Suggested resolution

Archiving printlists from SAP having Japanese, Korean characters:

- If you are using Documentum Archive Services for SAP Solutions for archiving Korean or Japanese printlists, set the *`archiving.compId.decode=true`* in the al.properties file.
- Use multilingual device type for archive printer ARCHIVE.
- Default is ARCHLINK, which only supports Latin1 (cp=1100).
- Prior to R/3 Ent (MDMP system), cp=8000 must be added to ARCHLINK.
- With ECC 6.0, Unicode-aware device type ARCHUTF8 is ready to use, but not set by default.

You can change this using the following procedure:

- /nSPAD.
- Put the name *ARCHIVE* into *Output Devices* and click **Display**.

- Click **Change** to transit to change mode.
- Choose *ARCHUTF8* instead of *ARCHLINK* from the list box of **Device Type**.
- Click **Save** to save the changes.