



Gimmel
Information Management for Everyone®

Gimmel Link Installation and Administration Guide

Software Version 5.7.0

November 2021

November 12, 2021

Title: *Gimmel Link V5.7.0 Installation and Administration Guide*

© 2021 Gimmel LLC

Gimmel® is a registered trademark of Gimmel Group.

Microsoft® and SharePoint® are registered trademarks of Microsoft.

ArchiveLink® is a registered trademark of SAP.

All other trademarks are the property of their respective owners.

Gimmel LLC believes the information in this publication is accurate as of its publication date. The information in this publication is provided as is and is subject to change without notice. Gimmel LLC makes no representations or warranties of any kind with respect to the information contained in this publication, and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any Gimmel software described in this publication requires an applicable software license. For the most up-to-date listing of Gimmel product names and information, visit www.gimmel.com. All other trademarks used herein are the property of their respective owners.

If you have questions or comments about this publication, you can email TechnicalPublications@Gimmel.com. Be sure to identify the guide, version number, section, and page number to which you are referring. Your comments are welcomed and appreciated.

Contents

- 1 Introduction..... 1
 - 1.1 Who Should Read this Guide..... 2
 - 1.2 What is Included in this Guide 2
- 2 Prerequisites..... 3
 - 2.1 Prerequisite Software and Configuration..... 3
 - 2.2 Gimmel Link Component Dependencies..... 3
 - 2.3 Prerequisite Sites 3
 - 2.4 Prerequisite SAP Configuration Data..... 6
 - 2.4.1 Auto.index Update Transaction Codes..... 7
 - 2.4.2 SAPGUI Clients 7
 - 2.5 System Administrator Access Prerequisites (non-SAP)..... 7
 - 2.5.1 Core Admin Requirements 7
 - 2.5.2 Optional Admin Requirements 8
 - 2.6 Network Communications Prerequisites 8
 - 2.6.1 Connection Service 8
 - 2.6.2 Gimmel Link..... 9
 - 2.6.3 CSOM Remote Deployments..... 9
 - 2.6.4 Security Certificates 9
 - 2.8 Gimmel Link CSOM Deployment Prerequisites 10
 - Gimmel Link Software..... 10
 - Server Software Requirements..... 10
 - Optional Software 11
 - Office 365 SharePoint Online 11
 - SharePoint 2013, 2016, 2019, and SharePoint Online..... 11
 - Server Hardware 11
 - 2.9 Gimmel Link SSOM Deployment Prerequisites..... 11
 - Gimmel Link Software..... 12
- 3 Installing or Upgrading Gimmel Link..... 12

3.1	Uninstalling Older Gimmel Link Installations.....	13
3.1.1	Backing Up Existing Configuration.....	13
3.1.2	Uninstalling Gimmel Link.....	13
3.2	Installing Gimmel Link.....	14
3.3	Installing the Configuration Service.....	16
3.4	Installing the Connector Service.....	23
3.5	Installing Gimmel Link Enterprise.....	28
3.6	Installing the Document Tracking Service.....	33
3.7	Enabling Anonymous Authentication.....	41
3.8	Importing Legacy Configuration Files.....	42
3.8.1	Importing a Single Configuration File into the Configuration Service.....	45
3.9	Deploying the Gimmel Link SharePoint App into the SharePoint App Catalog.....	46
3.10	Deploying Custom SAP Transports.....	47
	Older.....	49
4	Setting Up an Gimmel Link Document Library.....	50
	(On-Premises).....	51
4.2	Deploying the iNet.DM Site Columns and Content Types in the Content Type Hub.....	53
4.3	Creating Custom Content Types Using iNet.DM Content Types.....	57
4.4	Adding Custom Content Types to iNet.DM Document Libraries.....	58
4.5	Publishing the Custom Content Types.....	62
4.6	Adding the Published Content Types to a New or Existing Document Library.....	64
4.7	(Optional) Adding Indexes to New Document Library for Use with Flat Storage Mode.....	65
5	Setting Shared Configuration Settings.....	68
5.1	Configuring the Connection Service.....	69
	Web Application.....	69
5.2	Setting Up the Configuration Service.....	69
5.2.1	Accessing the Administration Console.....	70
5.2.2	Creating a New Configuration in the Configuration Service.....	70
5.2.3	Saving Frequently.....	72
5.2.4	Specifying the Current (Active) Configuration.....	72
5.2.5	Importing a Configuration.....	73

5.2.6 Copying a Configuration	74
5.2.7 Deleting a Configuration.....	75
5.2.8 Exporting a Configuration.....	76
5.3 Setting Event Logging	77
5.4 Configuring the Web Service Security Key.....	78
5.5 Defining SAP Pools, SAP Settings, and Object Types.....	79
5.5.1 Configuring SAP Pools	80
5.5.2 Defining SAP Settings.....	86
5.5.3 Adding SAP Business Object Types.....	88
5.6 Defining SharePoint Settings.....	89
5.7 Configuring the Document Tracking Service.....	91
5.7.1 Manually Configuring Microsoft SQL Server as Database Provider.....	91
Creating Document Tracking Service Database in SQL.....	91
Creating Tracking Service Table with SQL Script	92
Assigning Permissions on SQL Database.....	93
Configuring Microsoft SQL Server as Database Provider for Document Tracking Service	95
5.8 Verifying the Connection Service.....	98
6 Configuring Content Repositories	100
6.1 Configuring a Content Repository.....	100
6.2 Configuring a Repository for SAP Security.....	102
7 Configuring CloudGate Failover Service.....	106
7.1 Enabling the CloudGate Failover Service	106
7.2 Configuring Email Notifications	107
7.3 Recovering a Repository from CloudGate Failover Service.....	108
8 Configuring SAP for Use with Document Manager	112
8.1 Configuring SAP to Use ArchiveLink.....	112
8.1.1 Creating a New Protocol (SAP T-Code OAA3)	112
8.1.2 Creating New Content Repository (SAP T-Code OAC0).....	113
8.1.3 Creating Global Document Types (SAP T-Code OAC2).....	115
8.1.4 Creating Links for Content Repositories (SAP T-Code OAC3).....	116
8.2 Using SAPOffice Attachments to Connect to Gimmel Link.....	117

8.2.1	Creating New SAP Content Repository.....	118
8.2.2	Creating New SAP Content Storage Category.....	120
8.2.3	Reconfiguring SOFFPHIO Physical Document Class.....	120
8.2.4	Configuring New Content Repository in Gimmel Link.....	121
8.2.5	Testing Attachment Using GOS Create Attachment Process.....	121
8.3	Configuring SAP to Use DMS Document Info Record Original to Connect to Gimmel Link.....	123
8.3.1	Creating New SAP Content Repository for DMS.....	124
8.3.2	Creating New SAP Content Category.....	125
8.3.3	Configuring New Content Repository in Gimmel Link.....	126
8.3.4	Testing Original Attachment Process.....	126
8.4	Using Gimmel Link with Business Document Service.....	127
8.4.1	Creating New SAP Content Repository.....	127
8.4.2	Creating New SAP Content Category.....	128
8.4.3	Configuring SAP for the Business Object and Document Type.....	129
8.4.4	Configuring New Content Repository in Gimmel Link.....	129
8.4.5	Testing Attachment Process Using Business Document Navigator.....	129
9	Validating Gimmel Link Document Manager Functionality.....	135
9.1	Assigning SAP T-Code OAAD (ArchiveLink: Administration of Stored Documents).....	135
	Web Browser.....	137
10	Sample Configuration Use Cases.....	138
10.1	Example Process: SAP Late Archival with SharePoint Metadata and Document Routing for Purchase Orders BUS2012 Using Auto.index.....	139
10.3	Example Process: SharePoint Archival (O365) with Scan.link iNet.DM Library to Start an SAP Workflow.....	141
11	Setting Up the Document Service Modules.....	142
12	Configuring Auto.index.....	143
12.1	Creating New Auto.index Instance.....	143
12.2	Indexing Business Metadata Using Auto.index.....	147
12.2.1	Indexing Using an SAP Table as Data Source.....	148
12.2.2	Indexing Using an SAP Function Module.....	152

12.2.3	Indexing Using Custom Indexers.....	156
12.2.4	Configuring Chained Indexers.....	156
12.3	Populating the Attribute Container.....	157
12.4	Writing Attributes to SharePoint.....	159
12.5	Mapping SAP Document Types to SharePoint Content Types.....	160
12.6	Configuring Auto.index Document Routing Rules.....	161
12.6.1	Configuring Read Fields from SharePoint.....	162
12.6.2	Managing Bindings in Read Fields from SharePoint.....	163
12.6.3	Setting Up Routing Rules.....	163
12.6.4	Routing Documents to SharePoint Folders.....	164
12.6.5	Setting Single Routing Rule Offering Multiple Routing Paths.....	167
12.6.6	Setting Multiple Routing Rules.....	169
12.6.7	Routing Based on Dates.....	170
12.6.8	Setting Routing Rules with Logical Operators.....	171
12.7	Testing Auto.index Configuration.....	173
13	Configuring Scan.link.....	174
13.1	Creating New Scan.link Instance.....	175
13.2	Populating the Attribute Container.....	177
13.3	Configuring Read Fields from SharePoint.....	178
13.4	(Optional) Configuring Scan.link to Perform Validation Using Indexed Metadata.....	179
13.5	Mapping SharePoint Content Types and File Extensions to SAP Document Types and Classes.....	180
13.6	Using Linkers.....	181
13.6.1	Configuring ArchiveLink Linker to Link Document to SAP Business Object.....	182
13.6.2	Configuring Barcode Linker to Associate Document with Bar-.....	184
13.6.3	Configuring Workflow Starter to Trigger a Workflow in SAP.....	185
13.6.4	Configuring RFC linker to Call Custom SAP Function Module.....	187
13.7	Testing Scan.link Configuration.....	188
14	Configuring Auto.index Update Connection.....	189
14.1	Configuring the Shared Configuration for Web Service Security.....	189
14.2	Configuring SAP Parameters for Auto.index Update.....	190

15	Changing Auto.index Update Notifications.....	193
15.1	Manually Invoking a One-Time Update.....	193
15.2	Configuring SAP to Notify Auto.index of Changes.....	195
16	Configuring the Gimmel Link Timer Service.....	201
16.1	Enabling the Timer Service for a Configuration.....	201
16.2	Stopping or Starting Timer Service.....	202
16.3	Adding a File Mover Task.....	203
16.4	Adding a File Uploader Task.....	207
17	Troubleshooting.....	212
18	FAQs.....	212
	Appendix A Additional Information.....	218
A.1	Data Flow Diagrams.....	218
A.2	Writing Expressions.....	221
A.3	Formatting Concatenated Strings.....	223
A.3.1	Examples.....	224
A.4	Function Modules Used by Document Service Modules.....	227
B	Gimmel Connection Service.....	228
B.1	Service Architecture to Support On-Premise and AzureHosted Deployment.....	228
B.2	Relationship to SAP .NET Connector 3.0.....	228
B.3	Authentication.....	229
B.4	Secure Sockets Layer.....	229
B.5	Secure Network Communications.....	229
C	Gimmel Document Tracking Service.....	230
C.1	Document Tracking Service Technical Details.....	230
C.1.1	Service Architecture.....	230
C.1.2	Provider Model for Document Tracking Data Storage.....	230
C.1.3	RESTful Endpoints.....	230
D	Information Architecture.....	231
	Information Architecture.....	231
	Business Metadata for Auto.index.....	231
	Library for Scan.link.....	232

E Configuring Auto.index Update Notifications Outside SAP Workflow 232

1 Introduction

The Gimmel Link Suite for SharePoint® and SAP is a leading provider of SAP-Microsoft interoperability solutions that enable Microsoft SharePoint as the records management/enterprise content management/document management (RM/ECM/DM) system for SAP customers. The suite includes the following components:

- **Gimmel Link Document Manager**

The SAP-certified Gimmel Link Document Manager platform creates transparency between SAP and Microsoft SharePoint so that businesses are free to define the way they want to work—inside SAP, inside SharePoint, or both—which lets businesses run better. It can leverage Archive Link, Generic Object Services (GOS), Document Management Service (DMS), or Business Document Service (BDS) to allow for archival and retrieval of content directly from the SAP interface.

- **Configuration Service**

Included with the Gimmel Link Document Manager, the **Configuration Service** provides a centralized location for the management of Gimmel Link settings. The Configuration Service is deployed as an application during the Gimmel Link installation, and it enables you to configure settings for all Gimmel Link operations from within the Gimmel Link Administration Console.

- **Gimmel Link Document Service Modules**

The Gimmel Link Document Service Modules add functionality to the Gimmel Link Document Manager platform for archiving documents against SAP business objects. They enable integration between SAP business object instances and documents archived in SharePoint. Document Service Modules process documents stored in an SAP content repository, implemented in SharePoint by Document Manager. Specifically, the Gimmel Link Document Service Modules perform the following functions:

- **Auto.index** extracts metadata from SAP for the business object that the document is attached to and adds the metadata to the SharePoint fields for the document. It can also move documents to various SharePoint locations based on metadata value-driven routing rules.
- **Auto.index Update** is a notification system for Auto.index that SAP can invoke to implement changes on SAP objects to the SharePoint documents that are linked to them. This capability allows automatic synchronization of metadata as data associated with business object changes.
- **Scan.link** invokes appropriate SAP actions when a document is dropped and/or indexed in a pre-configured SharePoint document library. SAP actions available include the following:

- Linking documents to SAP business objects, using the object IDs or bar codes
- Invoking and linking documents to an SAP workflow
- Interacting with remote SAP function modules

- **Connector Service**

The Connector Service enables inbound communications from applications written for the .NET platform to communicate with Advanced Business Application Programs (ABAPs). All communications between SAP and any .NET applications are managed by the Connector Service.

- **Gimmel Document Tracking Service**

The Document Tracking Service tracks the location of a document throughout the document lifecycle. The service supports data management in on-premise and cloudbased storage models.

1.1 Who Should Read this Guide

The intended audience for this document is an Gimmel Link administrator. The administrator must install and configure the environment according to the steps in this guide.

1.2 What is Included in this Guide

This guide contains information on how to install and configure the Gimmel Link Suite components, including the Configuration Service, the Connector Service, Gimmel Link Enterprise, and the Document Tracking Service.

2 Prerequisites

This chapter lists the prerequisites, such as software, configuration, and data, required before you can install and configure the Gimmel Link suite.

2.1 Prerequisite Software and Configuration

To install and configure Gimmel Link, you need the following software and/or configuration at a minimum:

- SharePoint installed and functional (i.e., **SharePoint 2013/2016/2019/SharePoint Client Components version 15**) (**Note:** If Gimmel Link is deployed to SharePoint Online (Office 365), no SharePoint on-premise environment is required.)
- SQL Server version 2012 or later
- Internet Information Services (IIS) version 7 or higher
- SharePoint Site Collection
- SAP .Net Connector 3.0. To access the installation files, see the SAP Service Marketplace at <http://service.sap.com/connectors>. Be sure to install the assemblies to GAC.

2.2 Gimmel Link Component Dependencies

Each Gimmel Link component has dependencies that must be met in order to deploy the component properly. When you begin the installation process (described in Chapter 3 [Installing or Upgrading Gimmel Link](#)), refer to the following table to ensure that each product's dependencies have been addressed.

Dependencies								
		Configuration Service	SAP Connector	SQL (Sql Native Client)	Sharepoint (13/16/O365)	DM/DSM	CS	DTS
Component	Configuration Service (CFG SVC)			X				
	ERP-Link Enterprise (Local) (DM/DSM)	X			X		X	
	Connector Service (CS)	X	X					
	Document Tracking Service (DTS)			X	X			

Figure 2-1 Product Installation Dependencies

2.3 Prerequisite Sites

During the installation process, the Gimmel Link installer prompts you to either specify an existing Internet Information Services (IIS) site OR create a new IIS site to which to deploy the Gimmel Link Enterprise, Configuration Service, and Connector Service. Each of these services is deployed as an IIS Web application in the IIS Web site that was created/selected.

Gimmel recommends that you create a dedicated IIS Website and application pool to deploy each of these services. A single application pool can be used for all services or a separate application pool can be created for each service for increased application isolation.

To create a new IIS website using the IIS Manager, follow these steps:

1. In IIS Manager, right-click the **Sites** node to open the context menu.

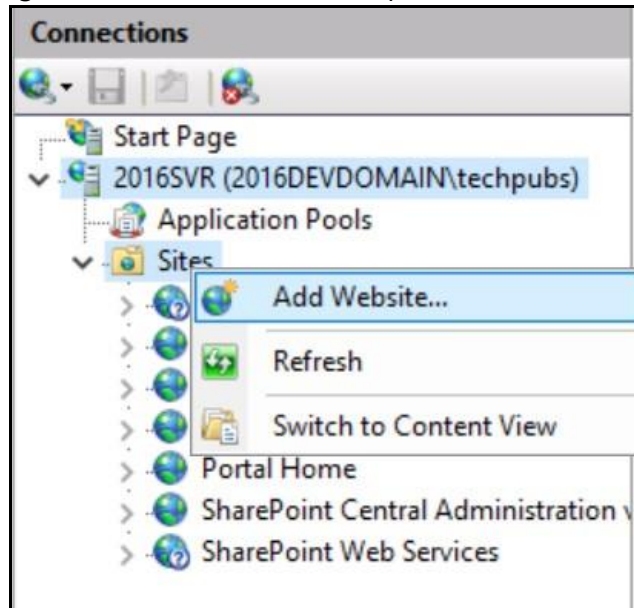


Figure 2-2 Context Menu for Sites in IIS Manager

2. Select **Add Website**. The **Add Website** dialog box displays.

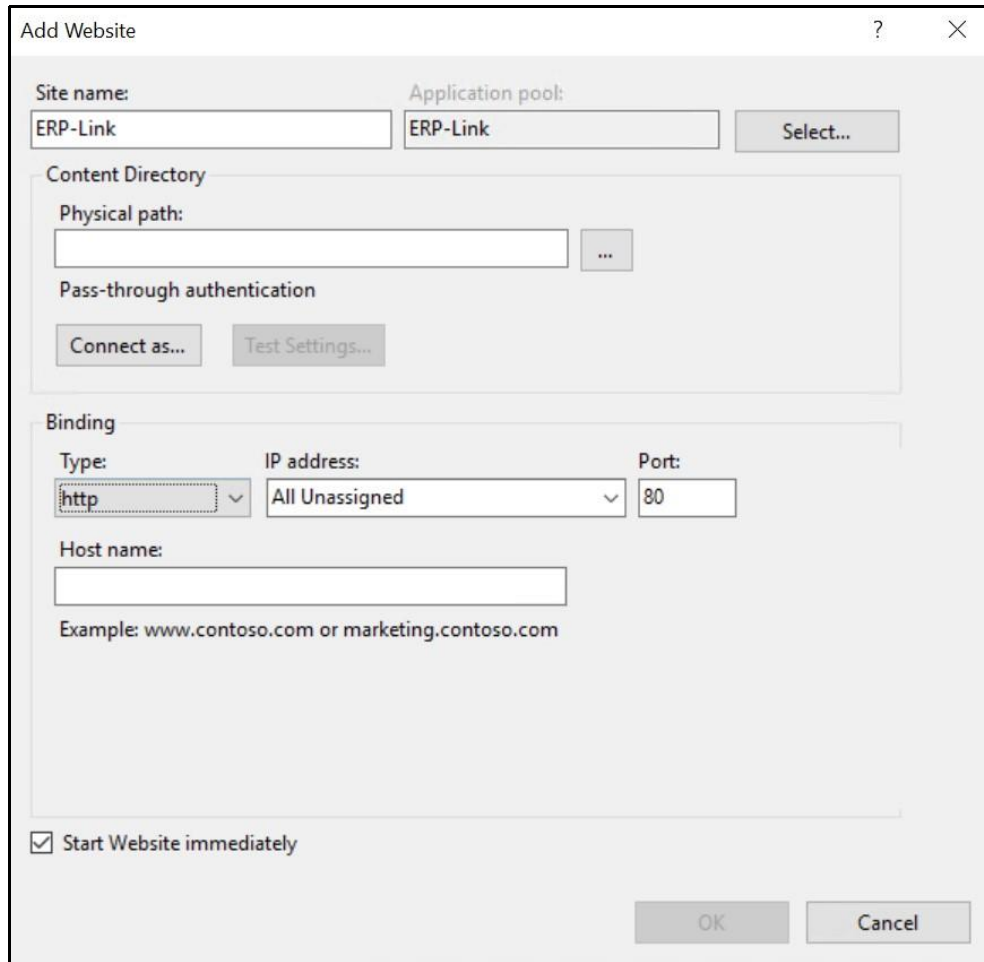


Figure 2-3 Add Website Dialog Box

3. Enter the **Site name** and **Physical path** on the server to host the Web site files, or click the **Browse** button (...) to browse to the location.

Note:

Be sure you have set up empty folders according to the path listed in the previous step so that the websites can be created.

4. In the **Pass-through authentication** section, click the **Connect as** button to display the **Connect As** dialog box.

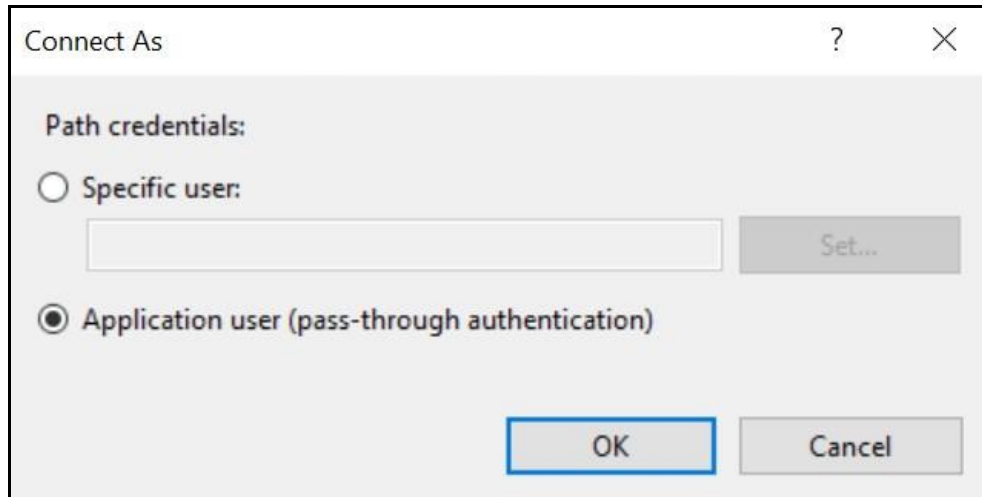


Figure 2-4 Context Menu for Sites in IIS Manager

5. Verify that the **Application user (pass-through authentication)** radio button is selected.
6. Click **OK** to save the setting and close the dialog button.

OR

Click **Cancel** to close the dialog box without saving.

7. In the **Add Website** dialog box, configure **Bindings** for the web site. Specify a **Port** and **Host name** if applicable.
8. Click **OK** to create the IIS Website.

Repeat Steps 1 to 8 for each new IIS Website that you need.

2.4 Prerequisite SAP Configuration Data

You need the following details about the configuration of the SAP system:

- __ SAP dialog user account for configuration purposes: The Gimmel team can perform the SAP configurations together with the client's SAP team member's account in a joint screen sharing session; for example, using Skype.
- __ SAP account access to RFC Create (SM59) and ArchiveLink administrator access; that is, access to the following t-codes: OAC0, OAC2, OAC3, OAA3, OAAD.
- __ Account for the Gimmel Connection Service or service such as CPIC: SAP account created that will be configured in the Gimmel Link administration console.
- __ SAP content repositories are identified.
- __ SAP object types are identified.
- __ SAP document types are identified.

2.4.1 Auto.index Update Transaction Codes

The following SAP transaction codes are needed for the optimal solution setup for Auto.index Update, which is included in the Gimmel Link Document Service Modules:

- __ SWEL: Display Event Trace
- __ SWUE: Trigger an event
- __ SWU0: Simulate event
- __ SWETYPV: Display/Maint. Event Type Linkages
- __ PFTC_DIS: Display Tasks
- __ PFTC_INS: Create Tasks
- __ PFTC_CHG: Change Tasks
- __ SWO2: BOR Browser
- __ SE37: ABAP Function Modules
- __ SE16: Data Browser

2.4.2 SAPGUI Clients

- __ SAPGUI client software SAPGUI 7.1 patch level or higher
Because of a bug in SAP's 7.0 and 7.1 SAPGUI clients, the SAPGUI client software SAPGUI 7.1 patch level or higher is required. See SAP Note #1327343 ("400 Bad Request Error with latest version of SAPHTTP".)

2.5 System Administrator Access Prerequisites (non-SAP)

You need the system administrator access prerequisites listed in this section for non-SAP installation.

2.5.1 Core Admin Requirements

- __ SSOM on-premises
 - __ SharePoint Site Collection(s) administrator
 - __ Database administrator
 - __ Local Windows server administrator access
 - __ SharePoint farm administrator for creating new SharePoint web applications and site collections
- __ CSOM on-premises
 - __ SharePoint site collection(s) administrator
 - __ Database administrator

- __ Local Windows server administrator access
- __ SharePoint farm administrator for:
 - Creating new SharePoint web applications and site collections
 - Installing and managing SharePoint Add-ins (*Apps*) in the SharePoint App Catalog (If using CSOM Certificate-Based Authentication)
- __ CSOM SaaS (Software as a Service; for example, O365 SP Online)
 - __ SharePoint site collection(s) administrator
 - __ Database administrator
 - __ Local Windows server administrator access
 - __ SharePoint tenancy administrator for installing and managing SharePoint add-ins (*Apps*) in the SharePoint App Catalog

2.5.2 Optional Admin Requirements

- __ Database administrator permissions for creating the Document Tracking Database and executing scripts to create the Document Tracking Service table
- __ A server administrator for CloudGate Failover Service (CFS) for all CSOM deployments

This administrator is only needed when the optional CFS feature is enabled and the failover files are NOT stored locally on the Gimmel Link CloudGate server's file system but rather on a network file share.

2.6 Network Communications Prerequisites

This section details the network communications prerequisites for installing Gimmel Link.

2.6.1 Connection Service

The following network ports are used with the Gimmel Link Connection Service. Although the Gimmel Link Connection Service supports bidirectional communication, it is more often used for communication from Gimmel Link residing on SharePoint (SSOM) or CloudGate (CSOM) to SAP.

- __ Port between Gimmel Link iNet applications and the Gimmel Link Connection Service hub
 - Default: 3701 (no mandatory or preferred range)
 - Port configurable during the initial install procedure, with any port number if it does not collide with existing port assignments
 - To change the port after installation, uninstall the Gimmel Link Connection Service software; then select a different port during the pre-install preparation and reinstall it.

- __ Port for inbound SAP RFC (Gimmel Link Connection Service to SAP) communication:
Ranges from 3300 to 3398
- __ Port for outbound SAP to the Gimmel Link Connection Service hub:
Default by industry standards = 514
- __ SAP .NET Connector 3.0
- __ Browsing service:
The browsing service uses the fixed UDP 40001 port. This port is used by the Gimmel Link Connection Service hub for broadcasting to listening browsing service clients.

2.6.2 Gimmel Link

- __ Network access for SAP Server:
SAP server must have network access via the appropriate HTTP(S) port to the GimmelLink server. If host headers are to be used to route traffic to the Gimmel Link server via hostname, SAP must have the necessary HOST entries added beforehand.

Note:

Typically, port 80 is used for HTTP and port 443 is used for HTTPS.

2.6.3 CSOM Remote Deployments

The following graphic explains the client-side object model (CSOM) remote deployment.

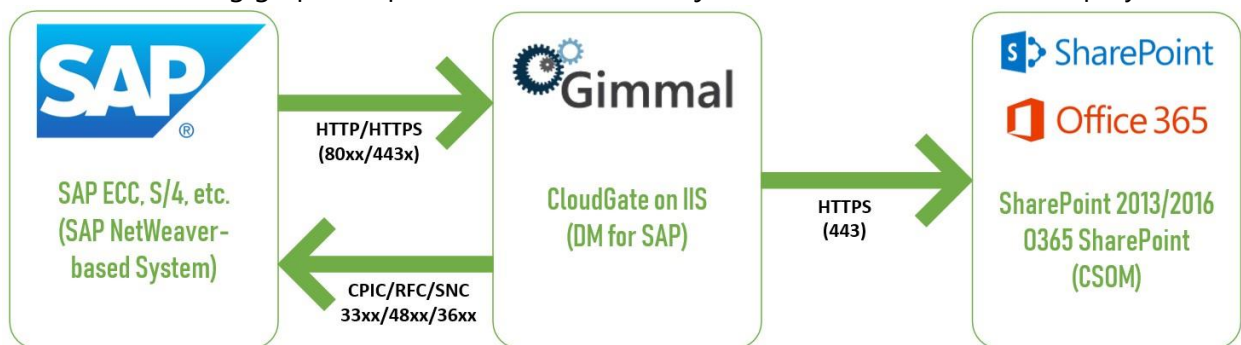


Figure 2-5 CSOM Deployment Model

2.6.4 Security Certificates

- __ Security certificates:
To enable encrypted network communications, security certificates must be deployed when SSL is used between the SAP system and the Gimmel Link CloudGate server (CSOM deployments) or between the SAP system and the SharePoint Web Front End server (SSOM deployments.)

2.7 SharePoint Prerequisites

See Appendix D [Information Architecture](#) for more information.

2.8 Gimmel Link CSOM Deployment Prerequisites

This section lists the requirements for Gimmel Link CSOM Deployment Prerequisites.

2.8.1 Software Requirements

Gimmel Link Software

- __ SharePoint app (If using CSOM Claims-Based or CSOM Certificate-Based authentication)
- __ Gimmel Link 5.7:
 - Includes Gimmel Link Administration Console
 - Includes Gimmel Link Configuration Service
- __ Gimmel Link iNet.Runtime 5.0 or higher (installed with Gimmel Link 5.7)
- __ Gimmel App Installer 5.1
- __ Gimmel Connection Service 5.7 (installed with Gimmel Link 5.7)
- __ Gimmel Document Tracking Service 5.7 (installed with Gimmel Link 5.7)

Server Software Requirements

- __ Microsoft Windows Server 2012 or higher
- __ Microsoft SQL Server 2012 or higher
- __ SAP .NET Connector
- __ .NET Framework V3.5 for the Gimmel Link Connection Service and Gimmel Document Tracking Service
- __ .NET Framework V4.8 or higher for Gimmel Link Document Manager and Document Service Modules
- __ IIS 7.0 or higher (including ASP.NET extensions):
 - Create a new domain user account (preferably) or a local server account to be associated with the new IIS web application to be created. The IUSER account cannot be used because of limited application permission assignments allowed.
- __ SharePoint Server 2016 Client Components SDK:
 - Refer to <https://www.microsoft.com/en-us/download/details.aspx?id=51679>.
- __ Microsoft.IdentityModel.Extensions.dll:
 - This library is available for download from one of the following locations.
 - o <http://download.microsoft.com/download/0/1/D/01D06854-CA0C-46F1-ADBAEBF86010DCC6/MicrosoftIdentityExtensions-32.msi>

- <http://download.microsoft.com/download/0/1/D/01D06854-CA0C-46F1-ADBAEBF86010DCC6/MicrosoftIdentityExtensions-64.msi>

Optional Software

- __ Document Tracking Service Storage Provider
 - __ Microsoft SQL Server

Office 365 SharePoint Online

- __ SharePoint App Catalog in SharePoint Online created and available
- __ Office 365 plan: Any plan E1 or greater (see [System Administrator Access Prerequisites \(non-SAP\)](#))

SharePoint 2013, 2016, 2019, and SharePoint Online

- __ Processor: 64-bit, four-core
- __ RAM
 - __ a: Minimum 8 GB for developer or evaluation user installation with database on same server
 - __ b: 10 to 24 GB PREFERRED
- __ Disk:
 - 80 GB for system drive + space for logging, debugging, memory dumps + day- today operations

2.8.2 Hardware Requirements

Server Hardware

- __ CPU and memory
 - __ Per transactional demand, recommended 8GB of RAM (min of 4GB RAM)
 - __ Recommended two core processors per transactional demand
- __ Network bandwidth per transactional demand (considering document sizes and counts, etc.) in a given time frame

Hard disk space per transactional demand and typical recovery turnaround; that is, when the CloudGate Failover Storage (CFS) feature is enabled, which temporarily stores files in the Gimmal Link CloudGate server's file system

2.9 Gimmal Link SSOM Deployment Prerequisites

2.9.1 Software Requirements

Gimmel Link Software

- __ Gimmel Link 5.7:
 - Includes Gimmel Link Administration Console
 - Includes Gimmel Link Configuration Service
 - Includes Document Tracking Service
- __ Server:
 - Should meet the minimum requirements for SharePoint 2013, SharePoint 2016, or SharePoint 2019 (Foundation or Server)

Server Software Requirements

- __ Microsoft SQL Server 2012 or higher

Optional Software

- __ Gimmel Document Tracking Service Storage Provider
- __ Microsoft SQL Server SharePoint 2013, 2016, or 2019
- __ Processor: 64-bit, four-core
- __ RAM
 - __ a: Minimum 8 GB for developer or evaluation user installation with database on same server
 - __ b: 10 to 24 GB PREFERRED
- __ Disk:
 - 80 GB for system drive + space for logging, debugging, memory dumps + day- to-day operations

3 Installing or Upgrading Gimmel Link

You can install Gimmel Link on a SharePoint Web front-end (WFE) server or on a Gimmel CloudGate server for connection to a remote SharePoint environment. The following procedures must be performed on each Gimmel Link server that is part of your implementation.

If you are upgrading to Gimmel Link 5.7 from an earlier release, you must perform the steps in section [3.1 Uninstalling Older Gimmel Link Installations](#) (including the steps in subsections [3.1.1](#) and [3.1.2](#)). Then, continue to section [3.2 Installing Gimmel Link](#) to perform the installation steps.

If you are performing a “greenfield” installation (a net new installation where no Gimmel products have previously been installed), skip to section [3.2 Installing Gimmel Link](#).

3.1 Uninstalling Older Gimmel Link Installations

The process of removing a prior version of Gimmel Link varies depending on which of the following components you already have installed:

- Gimmel Link Connection Service
- Gimmel Link iNet.DM
- Gimmel Link Document Service Modules
- Gimmel Link iNet.Runtime

3.1.1 Backing Up Existing Configuration

Before uninstalling Gimmel Link, it is recommended that you make a copy of your existing configuration files and store them in another location as a backup. The typical location where these files can be found is similar to the following.

```
c:\inetpub\wwwroot\wss\VirtualDirectories\80\iNetDM\FILES
```

The names of the configuration files have no restrictions; you can name them whatever you want. The following is an example of files you may find in prior installations:

- ContentRepositoryConfig.xml
- DSMConfig.xml
- ERPLinkConfig.xml • TimerServiceConfig.xml

3.1.2 Uninstalling Gimmel Link

To uninstall Gimmel Link from a specific server, follow these steps.

1. Launch the Windows **Control Panel** on the server.

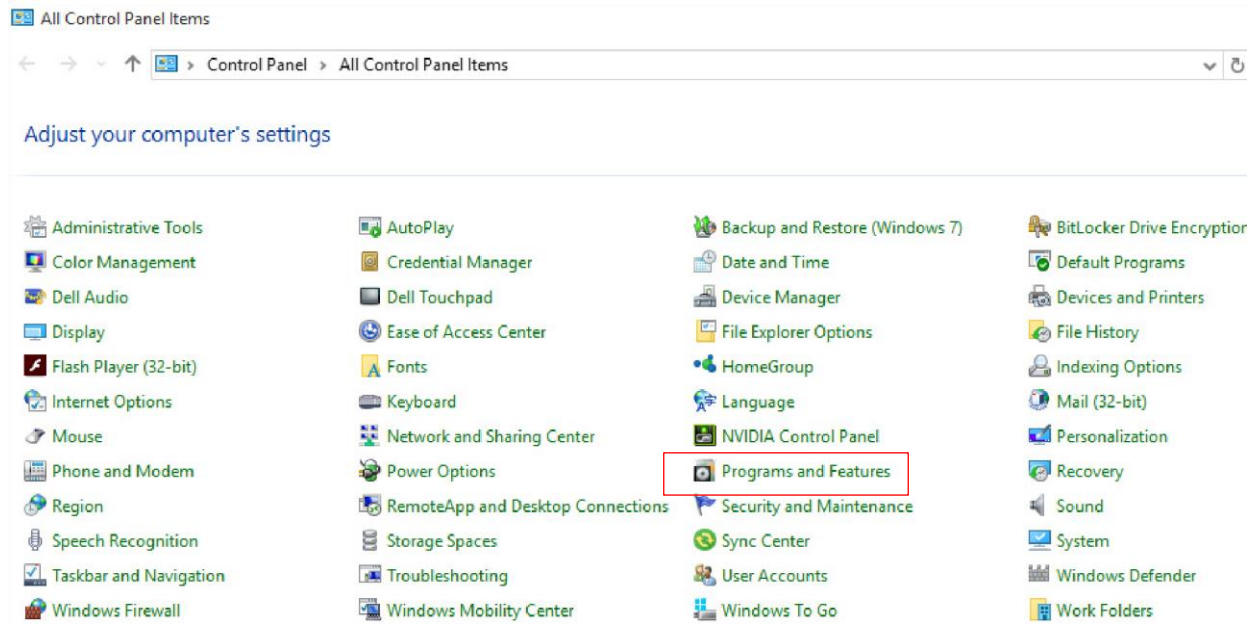


Figure 3-1 Select Programs and Features from Control Panel

2. Click **Programs and Features**.

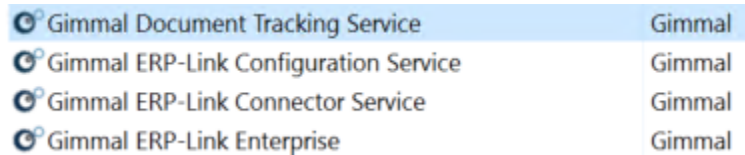


Figure 3-2 Example Gimmal Link Applications

3. On the **Programs and Features** dialog box, locate the installed Gimmal Link applications.

Note:

The names could vary from those shown, depending on the version you have installed and which features are implemented.

4. Select each Gimmal Link application, if present, and click **Uninstall**.

3.2 Installing Gimmal Link

This section provides information on how to install the following Gimmal Link components:

- Configuration Service
- Connector Service
- Gimmal Link Enterprise

- Document Tracking Service

The server where you install the Gimmel Link components must be in one of the following states:

- Clean server that never has had Gimmel Link installed on it, or
- Server that has had complete uninstall previously performed following the instructions in [3.1 Uninstalling Older Gimmel Link Installations](#)

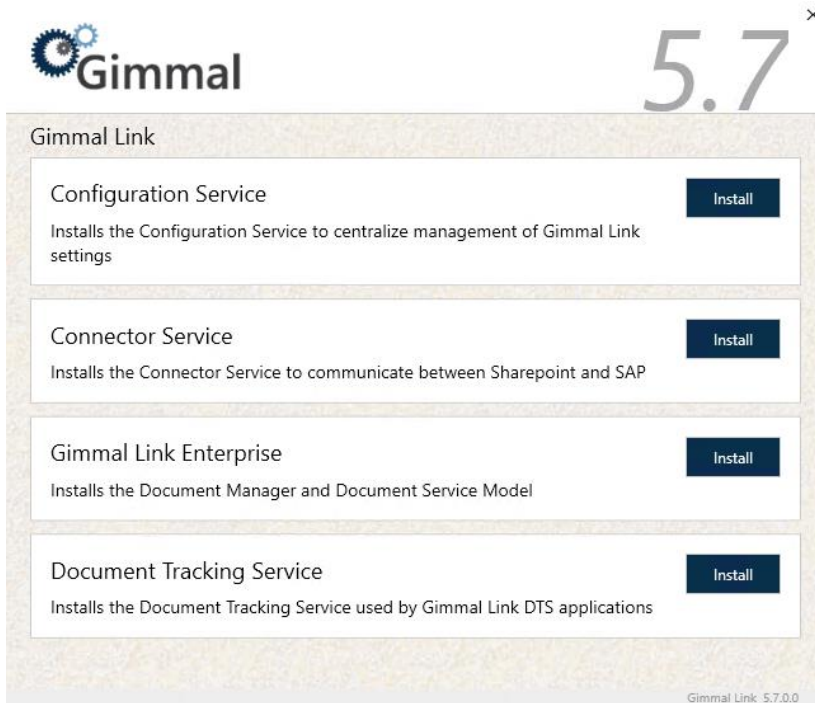
Perform the following steps to install the Gimmel Link components:

1. Download the Gimmel Link product package from [the Gimmel software download site](#) and extract it to a designated folder.
2. Navigate to the installation folder, and double-click "setup.hta" to launch the Gimmel installation splash screen.



3. On the installation splash screen, click **Core Platform** under the Install Gimmel Link section.

The main installation screen displays, listing the core platform components available for installation:



Note:

If you are upgrading, and a previous version of Gimmel Link is still installed on your system, the **Install** buttons for the Gimmel Link components will be disabled. Please uninstall the previous version and then restart the installation process.

3.3 Installing the Configuration Service

Note:

The user running the Gimmel Link installer must have the "sysadmin" role for the SQL Server instance that is being used.

-
1. On the main installation screen, click **Install** for the Configuration Service. The installer wizard opens on the "Prerequisites Verified" screen, where it verifies that all of the prerequisites have been met for the installation.



Figure 3-5 Prerequisites Verified Screen

Note

The Configuration Service installation is a prerequisite for the Connector Service and Gimmel Link Enterprise. If you attempt to install either of those components before the Configuration Service, an error message displays. For more information, see [Chapter 2.2 Gimmel Link Component Dependencies](#).

2. Click **Next**. The Website and Application Pool screen displays.
3. Indicate if you will be installing the app to a new or existing website and application pool by selecting the appropriate radio button: **New** or **Existing**.



Figure 3-6 Website/Application Pool Screen

Important!

The installation steps differ for each of these options. See the following table for detailed steps for each option.

Table 3-1 New vs. Existing Installation Steps

If you click...	Perform these Steps
-----------------	---------------------

New, then...

1. Click **Next**. The IIS Settings screen displays:



2. Enter/select the following settings:

- **Web Application Name** – Enter a name for the web application.
- **Web Application Port** – Enter a port number.
- **SSL Certificate** – Select an SSL Certificate from the drop-down list, if applicable.

When you install the Configuration Service, a new Application Pool will be created, which is used by the created web application. The following options specify the identity used for this Application Pool.

- **Username** – Enter a pre-existing username for the Application Pool Account. (**Note:** Username must be in the format of Domain\Username.)
- **Password** – Enter a pre-existing password for the Application Pool Account.

3. Continue with step 5, located below the table.

If you click...

Perform these Steps

Existing, then...

1. Click **Next**. The Select Website/Application Pool screen displays:



2. Select an existing website and application pool.

3. Click **Next**. The Database Settings screen displays.
Continue with step 4 below.

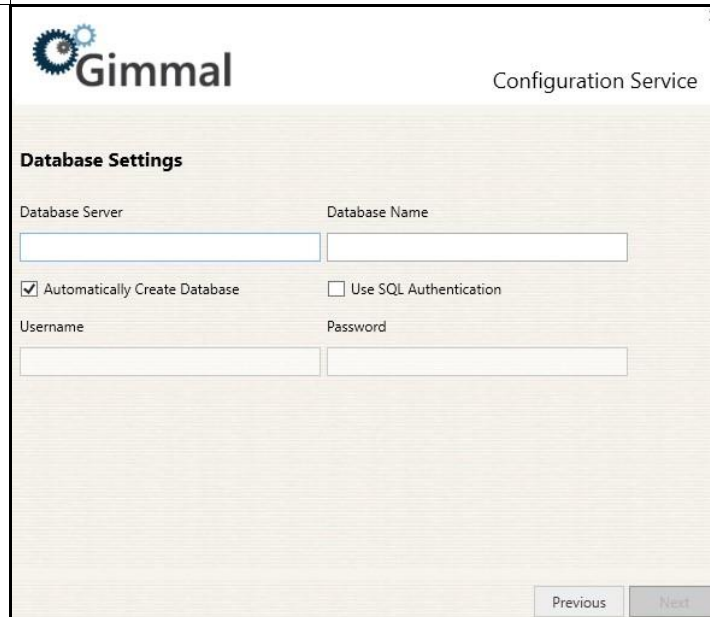


Figure 3-7 Database Settings Screen

4. On the Database Settings screen, enter/select the following database settings to determine the connection information that will be used by the Configuration Service to connect to SQL Server:

- **Database Server:** The name of the SQL Server (e.g. SERVERNAME\Instance Name)
 - **Database Name:** The name of the SQL Server database
 - **Automatically Create Database:** See description below.*
 - **Use SQL Authentication:** Specifies that the connection information should use SQL Authentication with the Username and Password indicated below
 - **Username:** The SQL Server username to use if SQL Authentication is specified
 - **Password:** The SQL Server password to use if SQL Authentication is specified
-

***Note:**

If the **Automatically Create Database** checkbox is checked, the following will happen when you click the **Next** button to advance to the next install screen. (This option requires that you have permissions to create databases and manage security in the SQL Server instance indicated.):

- If the database already exists, an error message will display.
- If the database does not already exist, then it will be created.
- The web.config connection string will be populated with the details you entered above.

If the **Automatically Create Database** checkbox is not checked, the following will happen when you click the **Next** button to advance to the next install screen:

- The web.config connection string will be populated with the details you entered above.
-

Note:

If the Identity of the chosen Application Pool is not a specific user (e.g. if it is ApplicationPoolIdentity, Local System, Local Service) then the **Use SQL Authentication** checkbox must be checked and the Username and Password fields must be completed or you will receive an error when you click the **Next** button.

If the user specified in the Username/Password fields (or the application pool identity user indicated in the table above) does not exist in the database server, a new login will be created for that user.

The user login will be assigned the following roles on the specified database: db_owner, db_datawriter, and db_datareader

If **Use SQL Authentication** is not checked, we use the identity of the Application Pool from the previous screen as the database user.

5. Click **Next**. The Installation Location screen displays.



Figure 3-8 Installation Location Screen

6. On the Installation Location screen, enter or select the installation location for the Configuration Service application. The location shown in the screenshot is the default location. To change the location, click the (...) button and navigate to and select the correct location.
7. Click **Next**. The installation process begins, indicated by a progress bar on the screen. When the installation is complete, you will see "Installed" display on the screen.



Figure 3-9 Installed Screen

8. Click **Next** to go to the Finish screen, where you will see a confirmation of the installation.



Figure 3-10 Finish Screen

9. Click **Finish** to close the installer wizard and return to the main product installation screen.
10. Continue with the next section to install the Connector Service.

3.4 Installing the Connector Service

1. On the main installation screen, click **Install** for the Connector Service. The installer wizard opens on the "Prerequisites Verified" screen, where it verifies that all of the prerequisites have been met for the installation.



Figure 3-11 Prerequisites Verified Screen

2. Click **Next**. The Website and Application Pool screen displays.

3. Indicate if you will be installing the app to a new or existing website and application pool by selecting the appropriate radio button: **New** or **Existing**.

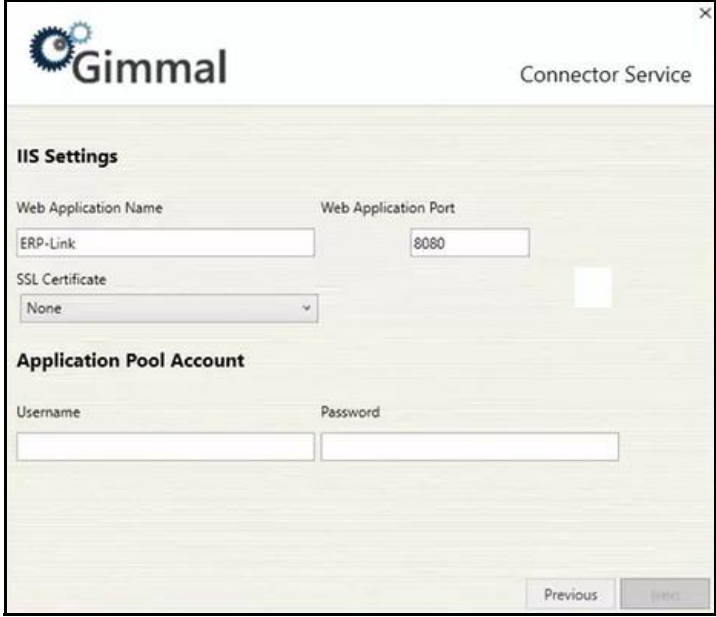


Figure 3-12 Website/Application Pool Screen

Note

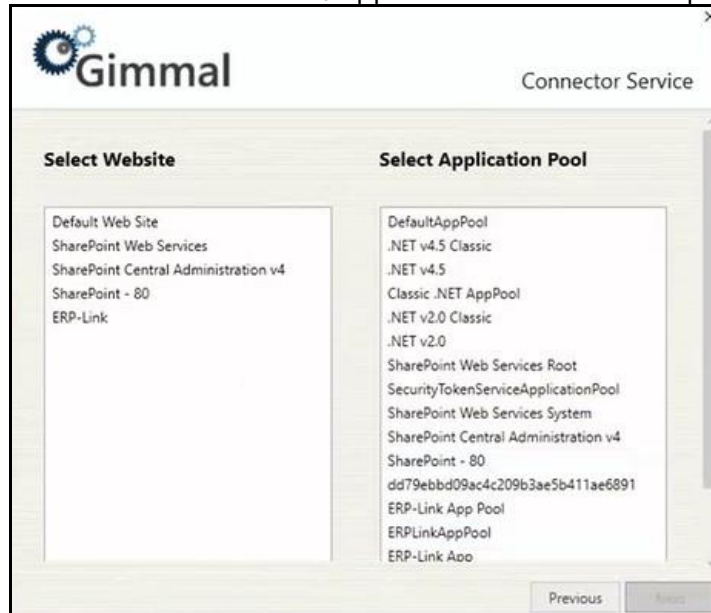
The installation steps differ for each of these options. See the following table for detailed steps for each option, and then continue with step 4 in the main body of the document.

Table 3-2 New vs. Existing Installation Steps

If you click...	Perform these Steps
<p>New, then...</p>	<p>1. Click Next. The IIS Settings screen displays:</p>  <p>2. Enter/select the following settings:</p> <ul style="list-style-type: none"> • Web Application Name – Enter a name for the web application. • Web Application Port – Enter a port number. • SSL Certificate – Select an SSL Certificate from the drop-down list, if applicable. <p>When you install the Connector Service, a new Application Pool will be created, which is used by the created web application. The following options specify the identity used for this Application Pool.</p> <ul style="list-style-type: none"> • Username – Enter a pre-existing username for the Application Pool Account. (Note: Username must be in the format of Domain\Username.) • Password – Enter a pre-existing password for the Application Pool Account. <p>3. Click Next to go to the Installation Location screen.</p>
If you click...	Perform these Steps

Existing, then...

1. Click **Next**. The Select Website/Application Pool screen displays:



2. Select an existing website and application pool.

3. Click **Next** to go to the Installation Location screen.



Figure 3-13 Installation Location Screen

4. On the Installation Location screen, enter or select the installation location for the Connector Service application. The location shown in the screenshot is the default location. To change the location, click the (...) button and navigate to and select the correct location.

5. Click **Next**. The installation process begins, indicated by a progress bar on the screen. When the installation is complete, you will see "Installed" display on the screen.



Figure 3-14 Installed Screen

6. Click **Next** to go to the Finish screen, where you will see a confirmation of the installation.



Figure 3-15 Finish Screen

7. Click **Finish** to close the installer wizard and return to the main product installation screen.
8. Continue with the next section to install the Gimmel Link Enterprise component.

3.5 Installing Gimmel Link Enterprise

1. On the main installation screen, click **Install** for Gimmel Link Enterprise. The installer wizard opens on the “Prerequisites Verified” screen, where it verifies that all of the prerequisites have been met for the installation.



Figure 3-16 Prerequisites Verified Screen

2. Click **Next**. The Website and Application Pool screen displays.
3. Indicate if you will be installing the app to a new or existing website and application pool by selecting the appropriate radio button: **New** or **Existing**.

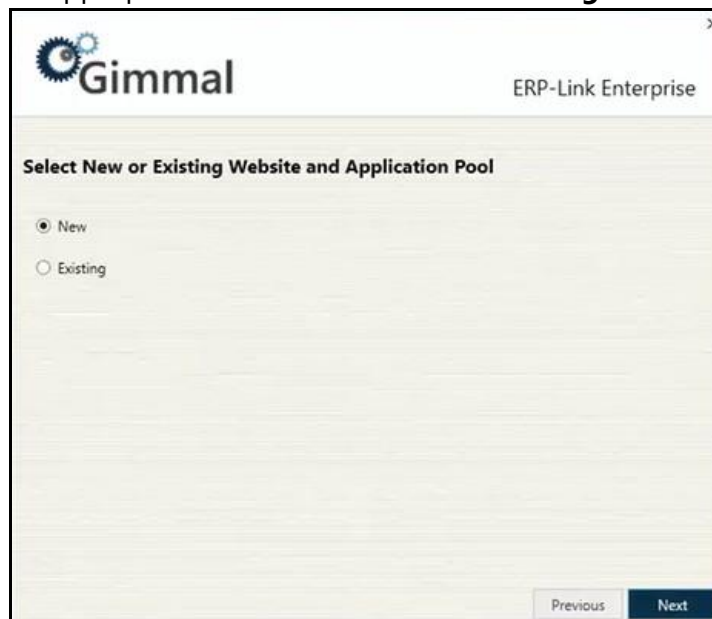


Figure 3-17 Website/Application Pool Screen

Note

The installation steps differ for each of these options. See the following table for detailed steps for each option, and then continue with step 4 in the main body of the document.

Table 3-3 New vs. Existing Installation Steps

If you click...	Perform these Steps
-----------------	---------------------

New, then...

1. Click **Next**. The IIS Settings screen displays:



2. Enter/select the following settings:

- **Web Application Name** – Enter a name for the web application.
- **Web Application Port** – Enter a port number.
- **SSL Certificate** – Select an SSL Certificate from the drop-down list, if applicable.

When you install Gimmel Link Enterprise, a new Application Pool will be created, which is used by the created web application. The following options specify the identity used for this Application Pool.

- **Username** – Enter a pre-existing username for the Application Pool Account. (**Note:** Username must be in the format of Domain\Username.)
- **Password** – Enter a pre-existing password for the Application Pool Account.


3. Click **Next** to go to the Installation Location screen.

If you click...

Perform these Steps

Existing, then...

1. Click **Next**. The Select Website/Application Pool screen displays:



2. Select an existing website and application pool.
3. Click **Next** to go to the Installation Location screen.



Figure 3-18 Installation Location Screen

4. On the Installation Location screen, enter or select the installation location for the Gimmal Link Enterprise application. The location shown in the screenshot is the default location. To change the location, click the (...) button and navigate to and select the correct location.

5. Click **Next**. The installation process begins, indicated by a progress bar on the screen. When the installation is complete, you will see "Installed" display on the screen.



Figure 3-19 Installed Screen

6. Click **Next** to go to the Finish screen, where you will see a confirmation of the installation.

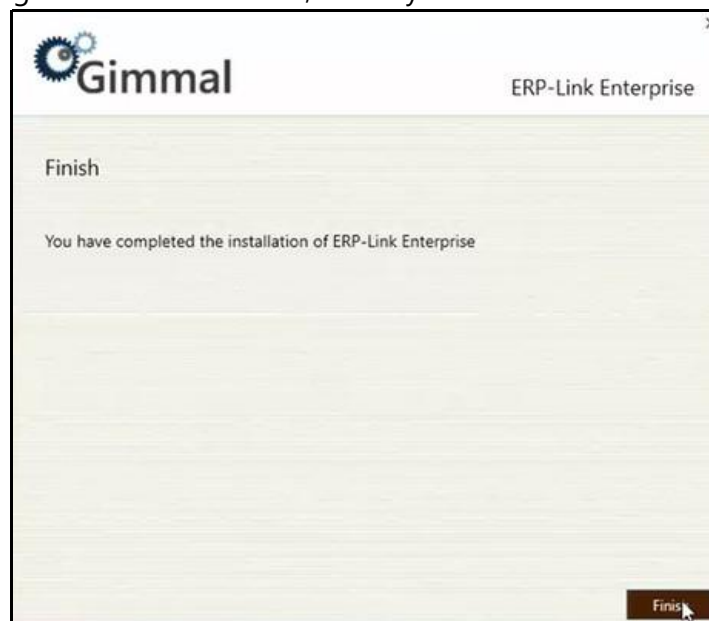


Figure 3-20 Finish Screen

7. Click **Finish** to close the installer wizard and return to the main product installation screen.
8. Continue with the next section to install the Document Tracking Service.

3.6 Installing the Document Tracking Service

1. On the main installation screen, click **Install** for the Document Tracking Service. The installer wizard opens on the "Prerequisites Verified" screen, where it verifies that all of the prerequisites have been met for the installation.

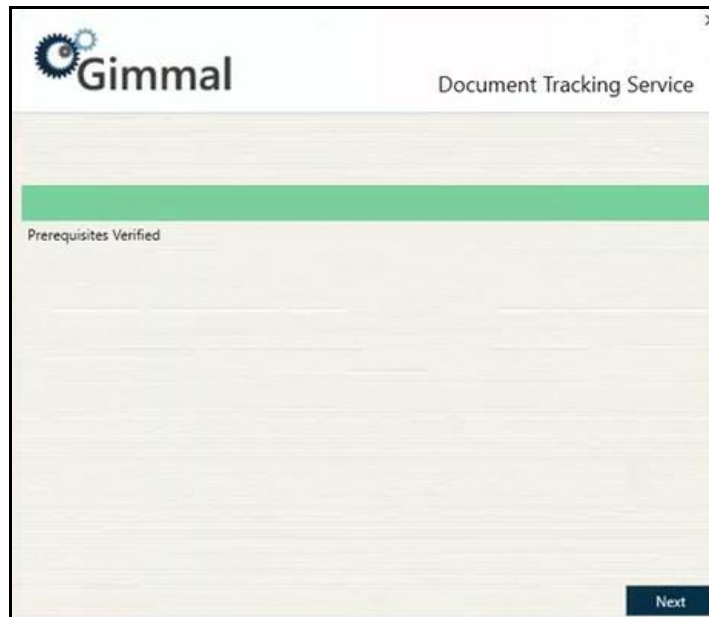


Figure 3-21 Prerequisites Verified Screen

2. Click **Next**. The Website and Application Pool screen displays.
3. Indicate if you will be installing the app to a new or existing website and application pool by selecting the appropriate radio button: **New** or **Existing**.

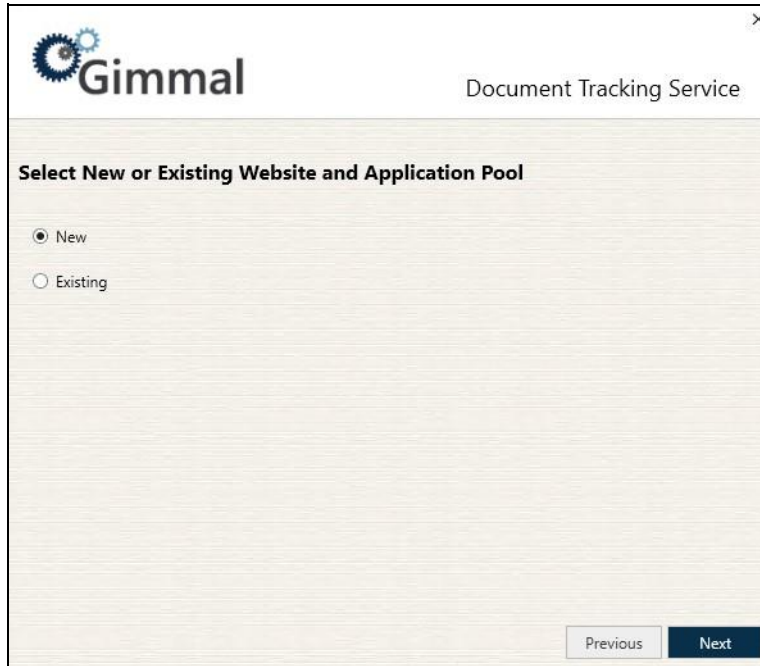


Figure 3-22 Website/Application Pool Screen

Important!

The installation steps differ for each of these options. See the following table for detailed steps for each option.

Table 3-4 New vs. Existing Installation Steps

If you click...	Perform these Steps
-----------------	---------------------

New, then...

1. Click **Next**. The IIS Settings screen displays:

2. Enter/select the following settings:

- **Web Application Name** – Enter a name for the web application.
- **Web Application Port** – Enter a port number.
- **SSL Certificate** – Select an SSL Certificate from the drop-down list, if applicable.

When you install the Configuration Service, a new Application Pool will be created, which is used by the created web application. The following options specify the identity used for this Application Pool.

- **Username** – Enter a pre-existing username for the Application Pool Account. (**Note:** Username must be in the format of Domain\Username.)
- **Password** – Enter a pre-existing password for the Application Pool Account.

3. Continue with step 5, located below the table.

If you click...

Perform these Steps

Existing, then...

1. Click **Next**. The Select Website/Application Pool screen displays:



2. Select an existing website and application pool.

Note:

The Document Tracking Service can only be installed into an existing site.

See section [2.3 Prerequisite Sites](#) for more information about the site requirements; Gimmel Link, the Connection Service, and the Document Tracking Service can all be deployed to one IIS Web site or they can each be deployed to separate IIS Web sites

3. Click **Next**. The Database Settings screen displays.
Continue with step 4 below.

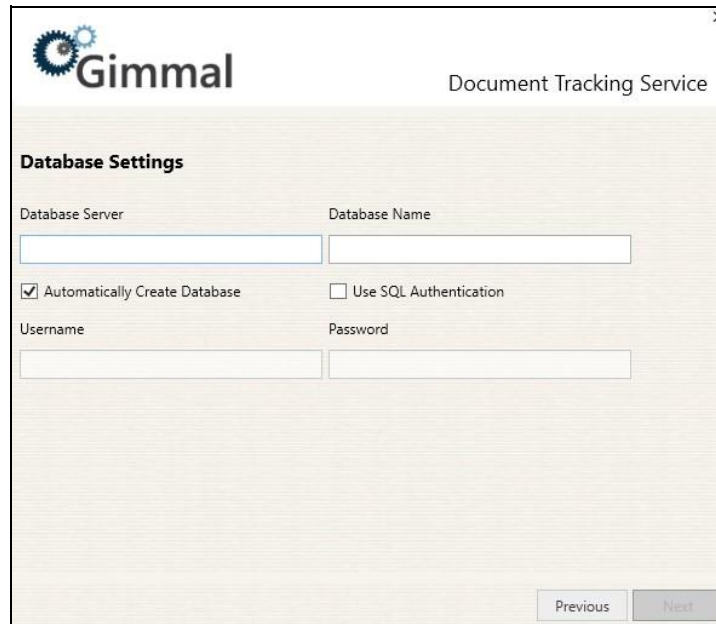


Figure 3-23 Database Settings Screen

4. On the Database Settings screen, enter/select the following database settings to determine the connection information that will be used by the Document Tracking Service to connect to SQL Server:
 - **Database Server:** The name of the SQL Server (e.g. SERVERNAME\Instance Name)
 - **Database Name:** The name of the SQL Server database
 - **Automatically Create Database:** See description below.*
 - **Use SQL Authentication:** Specifies that the connection information should use SQL Authentication with the Username and Password indicated below
 - **Username:** The SQL Server username to use if SQL Authentication is specified
 - **Password:** The SQL Server password to use if SQL Authentication is specified

***Note:**

If the **Automatically Create Database** checkbox is checked, the following will happen when you click the **Next** button to advance to the next install screen. (This option requires that you have permissions to create databases and manage security in the SQL Server instance indicated.):

- If the database already exists, an error message will display.
- If the database does not already exist, then it will be created.
- The web.config connection string will be populated with the details you entered above.

If the **Automatically Create Database** checkbox is not checked, the following will happen when you click the **Next** button to advance to the next install screen:

- The web.config connection string will be populated with the details you entered above.

Note:

If the Identity of the chosen Application Pool is not a specific user (e.g. if it is ApplicationPoolIdentity, Local System, Local Service) then the **Use SQL Authentication** checkbox must be checked and the Username and Password fields must be completed or you will receive an error when you click the **Next** button.

If the user specified in the Username/Password fields does not exist in the database server, a new login will be created for that user.

The user login will be assigned the following roles on the specified database: db_owner, db_datawriter, and db_datareader

If **Use SQL Authentication** is not checked, we use the identity of the Application Pool from the previous screen as the database user.

-
5. Click **Next**. The Database Configuration Complete screen displays once your database settings have been applied.

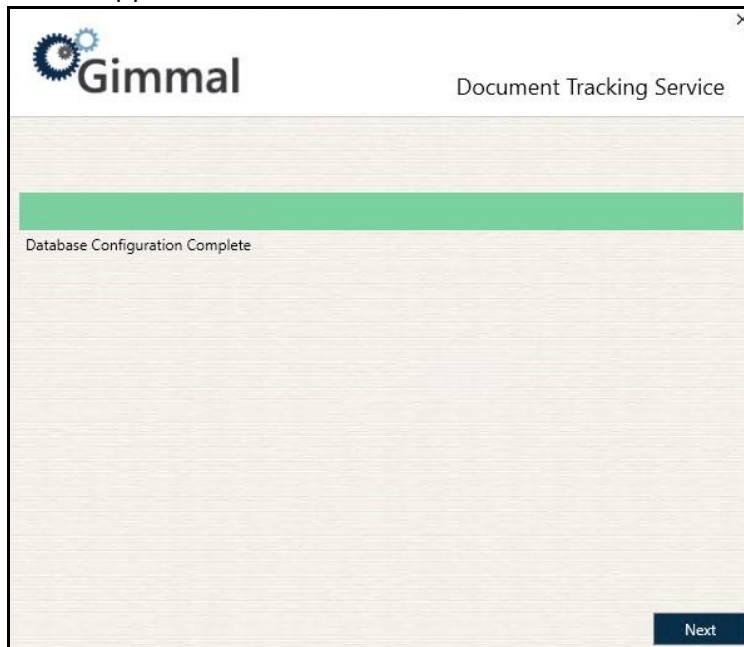


Figure 3-24 Database Configuration Complete Screen

6. Click **Next**. The Installation Location screen displays:

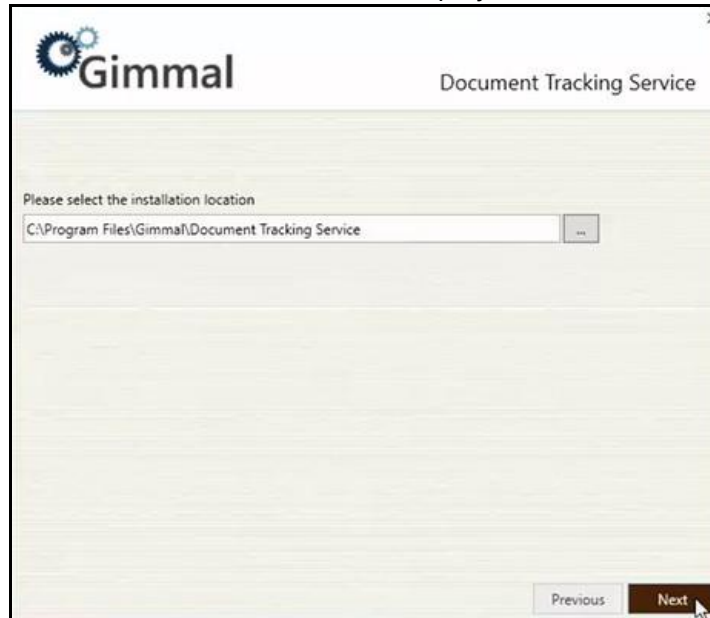


Figure 3-25 Installation Location Screen

7. On the Installation Location screen, enter or select the installation location for the Document Tracking Service application. The location shown in the screenshot is the default location. To change the location, click the (...) button and navigate to and select the correct location.
8. Click **Next**. The installation process begins, indicated by a progress bar on the screen. When the installation is complete, you will see "Installed" display on the screen.

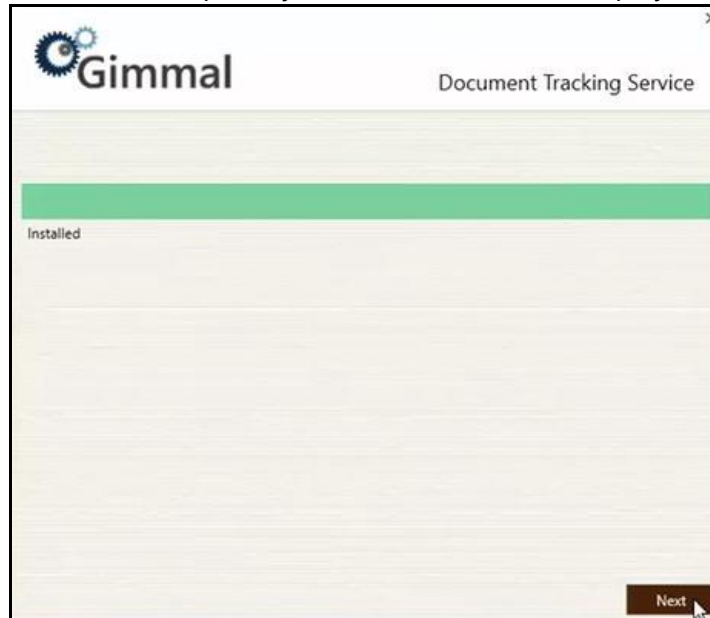


Figure 3-26 Installed Screen

9. Click **Next** to go to the Finish screen, where you will see a confirmation of the installation.



Figure 3-27 Finish Screen

10. Click **Finish** to close the installer wizard and return to the main product installation screen. This concludes the steps for installing the Gimmel Link components.

3.7 Enabling Anonymous Authentication

SAP HTTP/HTTPS communication with remote Web servers, such as DM, is performed using Anonymous Authentication. Follow these steps to enable the Anonymous Authentication for the Web application.

1. Open the IIS Manager by navigating to the Windows Control Panel, selecting **Administrative Tools**, and then selecting **Internet Information Services Manager**.

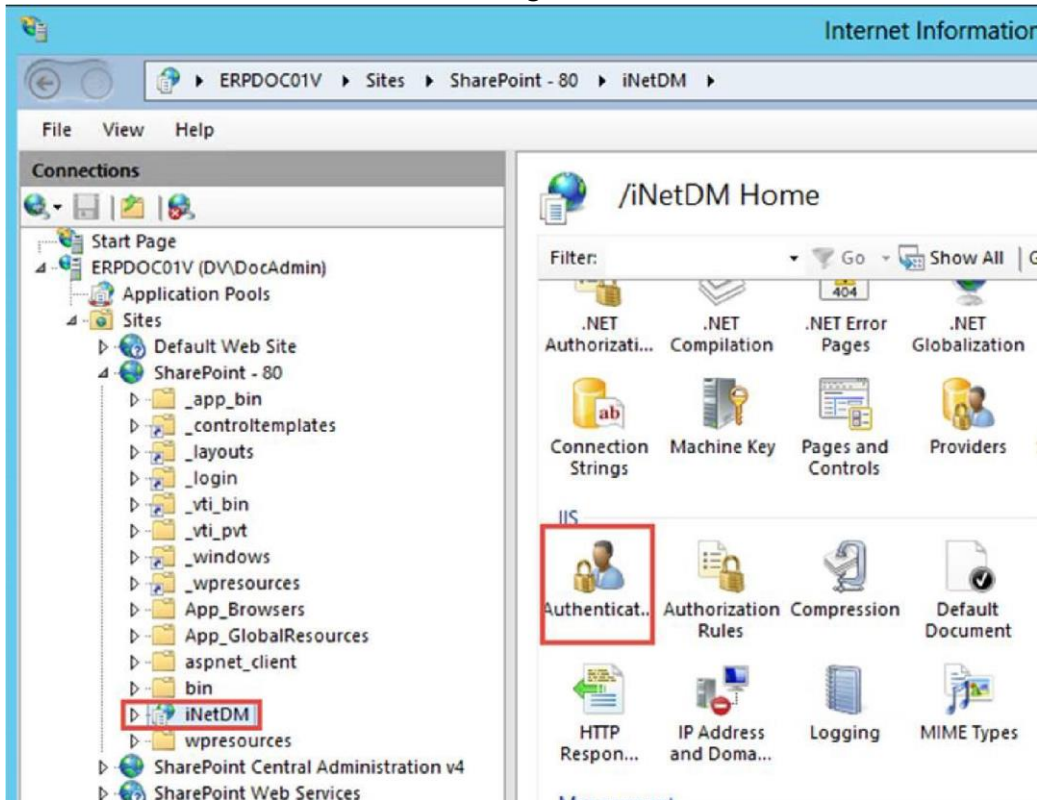


Figure 3-28 Gimmel Link iNet Software Node in IIS Manager

2. Select the same site that you selected in [Installing Gimmel Link](#).
3. Double-click **Authentication** in the right pane. The **Enable Authentication** pane displays.

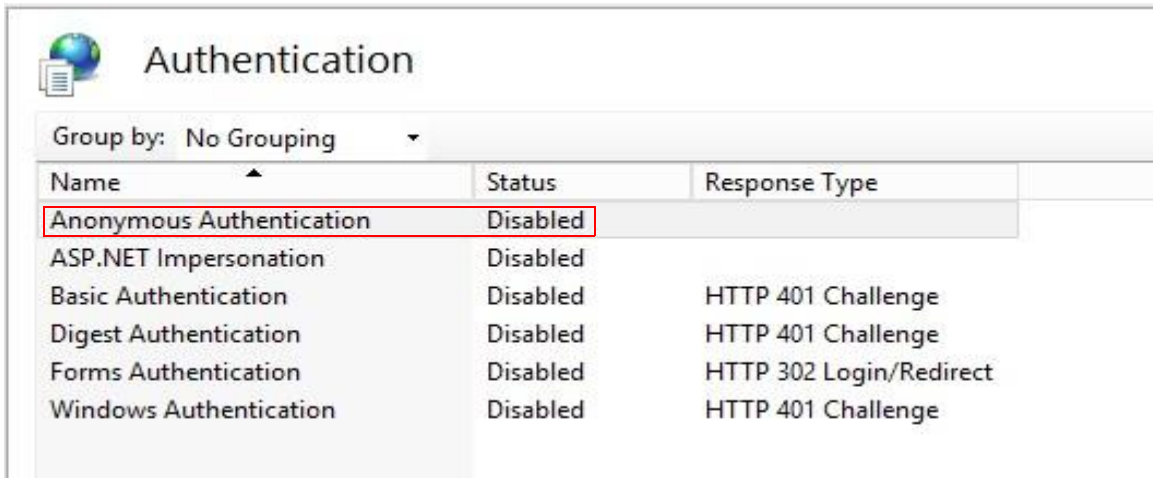


Figure 3-29 Enable Authentication Pane

4. Select **Anonymous Authentication** and ensure that **Enabled** displays in the **Status** column.

If **Disabled** displays, right-click it and select **Edit** from the dropdown menu that displays. The **Edit Anonymous Authentication Credentials** dialog box displays.

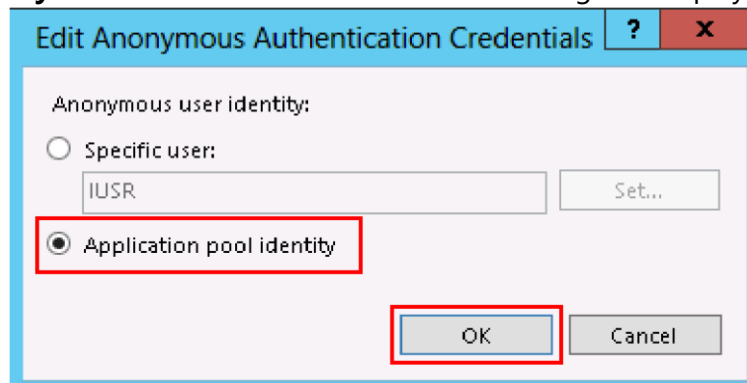


Figure 3-30 Enable Authentication Dialog Box

5. Select **Application pool identity** and click **OK**.

3.8 Importing Legacy Configuration Files

Note:


In versions of Gimmel Link prior to version 4.2.x, several configuration files were used to configure the various components in an installation. In Gimmel Link 4.2.x and later, a single configuration file is used.

"Legacy files" are files for versions prior to version 4.2.x, such as

ContentRepositoryConfig.xml, DSMConfig.xml, and TimerServiceConfig.xml.

If you are upgrading from Gimmel Link version 4.2.x or later, jump to section [3.8.1](#) to add your single configuration file to the new Configuration Service.

To import legacy configuration files into the Configuration Service, follow these steps.

1. Click the Windows Start button () and scroll through the alphabetical list on the left.
2. Click the **Gimmel Link** folder, and then **Gimmel Link Administration Console**. The console window opens.
3. Click **File > Open** to open the Configuration Service.
4. Create a new configuration. (For information on how to create a new configuration, see [5.2.2 Creating a New Configuration in the Configuration Service](#).)
5. Open this configuration in the Administration Console.
6. From the **Tools** menu, select the **Import Legacy Configuration** option.

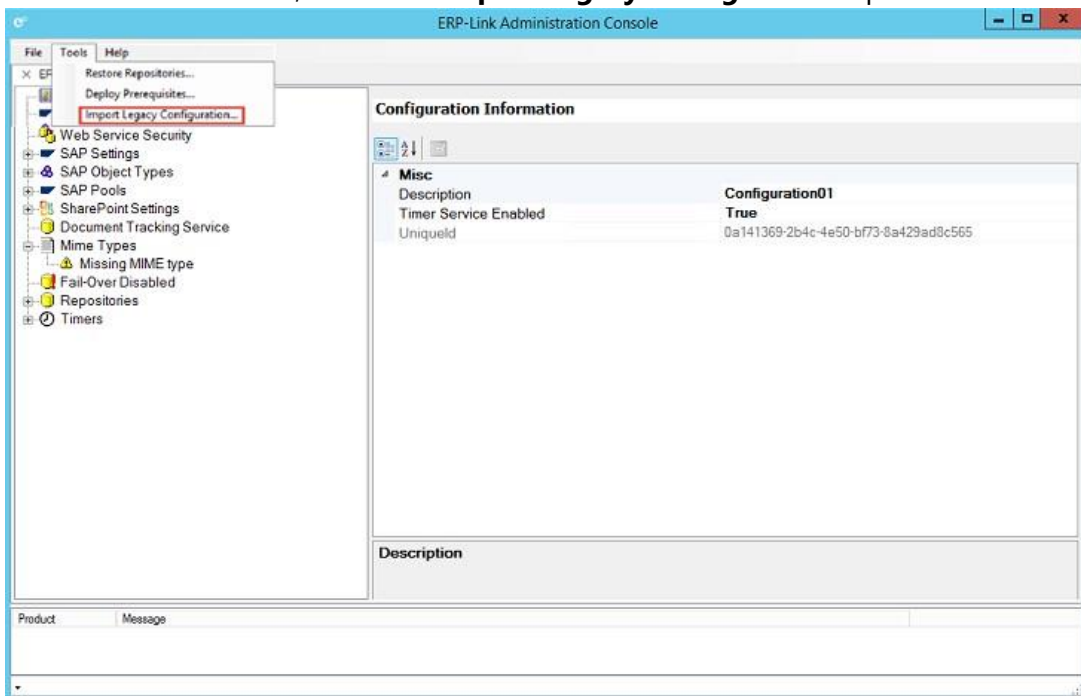


Figure 3-31 Gimmel Link Administration Console

The **Import Legacy Configuration** dialog box displays.

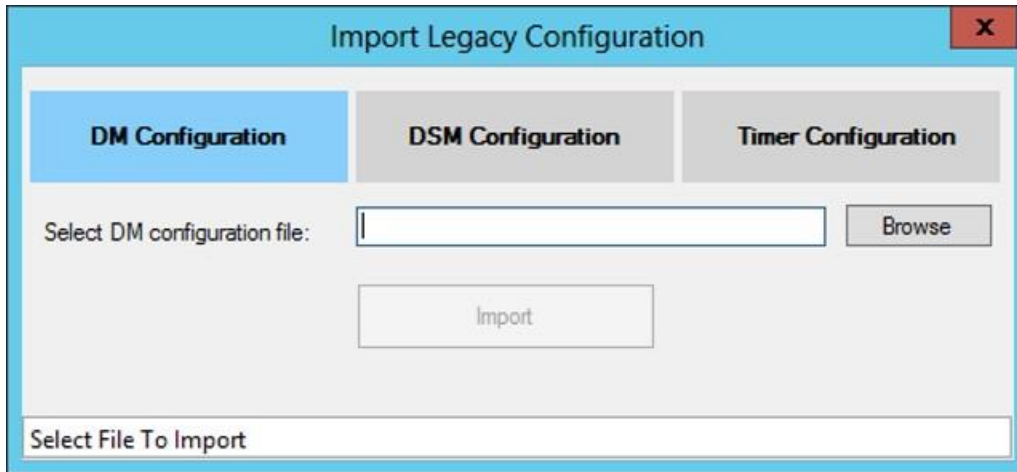


Figure 3-32 Import Legacy Configuration Dialog Box

7. Click the type of file that you want to import, browse to the configuration file that you backed up in [3.1 Uninstalling Older Gimmel Link Installations](#), select it, and click the **Import** button. The message appears at the bottom of the box that the configuration loaded successfully.

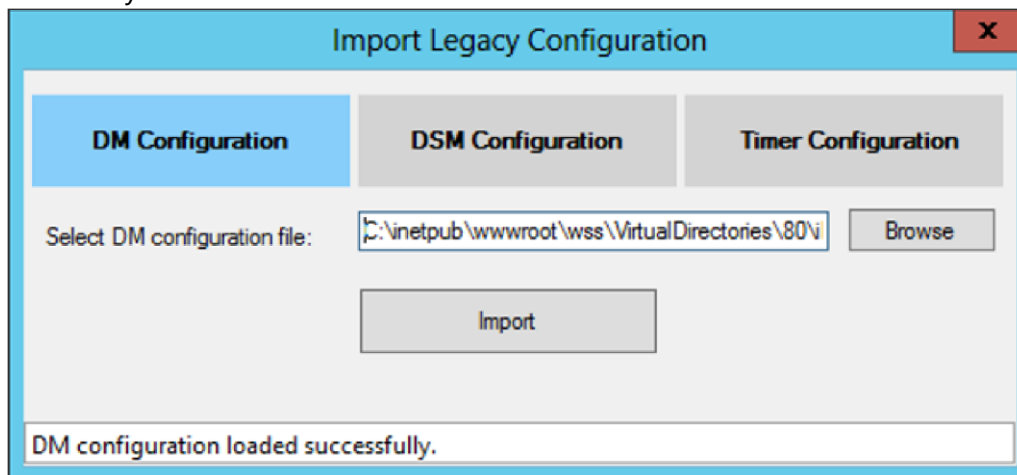


Figure 3-33 Import Successful Message

8. Repeat Steps 2 and 3 for each file. You can import as many files as you want to.
9. Click **X** at the top right corner when you have imported all the desired files.

Note:

If you did not have Gimmel Link Document Service Modules in the previous installation, there will not be any **DSM Configuration** file to import. If you do not currently own Gimmel Link Enterprise, you can import a **DSM Configuration** file, but when you attempt to enable Auto.index, errors will occur.

When the import completes, the Gimmel Link Administration Console contains all the configuration information that was set in the imported files. For example, the three files imported into the console that display in the following figure contain a complete configuration.

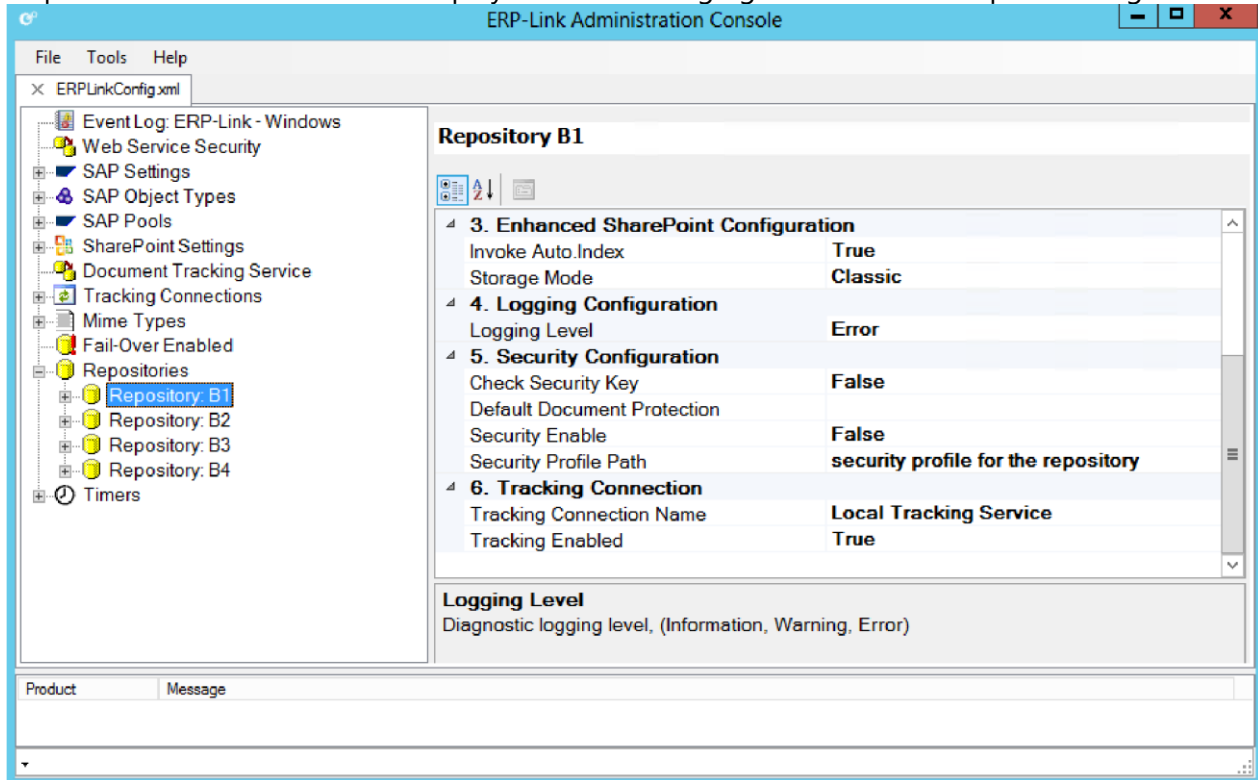



Figure 3-34 Example Console after Importing Configuration Files from Previous Installation

10. Click **File > Save** to save the configuration. This action causes the configuration to remain in the Configuration Service when you close the application.

3.8.1 Importing a Single Configuration File into the Configuration Service

If you are upgrading Gimmel Link from version 4.2.x or later, perform the following steps to import a configuration file into the Configuration Service:

1. Click the Windows Start button () and scroll through the alphabetical list on the left.
2. Click the **Gimmel Link** folder, and then **Gimmel Link Administration Console**. The console window opens.
3. Click **File > Open** to open the Configuration Service.
4. Select **Import** from the **Config** drop-down menu.

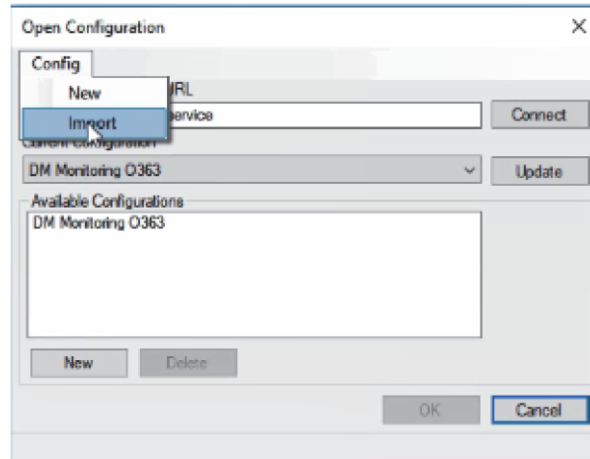


Figure 3-35 Selecting Import from the Config Menu

A file browser dialog opens.

5. Browse to the location of the configuration file you want to import and select it.
6. Click **OK**.
7. The imported configuration displays in the Administration Console. You may change the default name in the Description Field of the information window.
8. Click **File > Save** save the configuration. This action causes the configuration to remain in the Configuration Service when you close the application.

3.9 Deploying the Gimmel Link SharePoint App into the SharePoint App Catalog

The Gimmel Link app is installed in the Office365 tenant to enable secure access to the SharePoint environment from Gimmel Link. Gimmel Link uses an OAuth token passing flow to authenticate to SharePoint in the app context, and uses the clientID and client secret of the app to securely authenticate through Azure Access Control Services.

You must install the Gimmel Link SharePoint app under the following conditions:

- You are creating a CSOM Claims-Based Authentication setup with SharePoint Online/O365, or
- You are creating a CSOM Certificate-Based Authentication setup with SharePoint onpremises

No other configurations require that you install the SharePoint app.

Review <https://msdn.microsoft.com/en-us/library/office/fp142384.aspx> to understand more about SharePoint Add-On security model.

If you are using CSOM Claims-Based authentication mode to connect to SharePoint Online/O365 or using CSOM Certificate-Based Authentication to connect to SharePoint on-premises, then the Gimmel Link App Add-On must be installed to access SharePoint contents by performing the following steps:

1. Download the ERP-Link App 1.0 from [the Gimmel software download site](#).
2. Download version 5.1 of the Gimmel App Installer and the associated documentation from [the Gimmel software download site](#).

Note:

You must use v5.1 of the Gimmel App Installer. Earlier versions will not work with this version of Gimmel Link.

3. Follow the steps in the documentation to add the app to the SharePoint App Catalog in the target environment.
4. Install the app on any site collection that you want to use with Gimmel Link for archival and retrieval processes.

3.10 Deploying Custom SAP Transports

Gimmel Gimmel Link Enterprise leverages a custom SAP Transport as part of the Auto.index functionality. If you have Gimmel Link Enterprise, you must deploy the transport.

1. Navigate to the location where the Gimmel Link software was installed and find the **ERP-Link Transports.zip** file as shown in the following image.

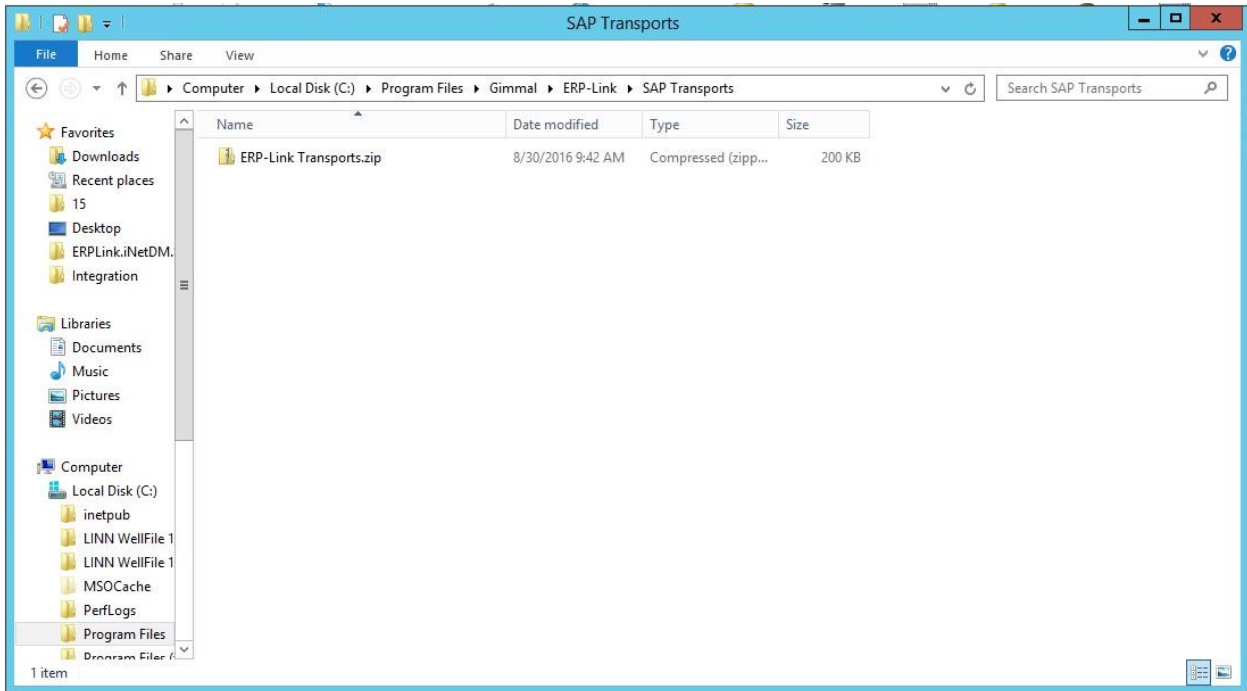


Figure 3-36 Location of Gimmel Link Transports File

2. Extract the zip file. It extracts into two folders that contain the exported SAP transports.

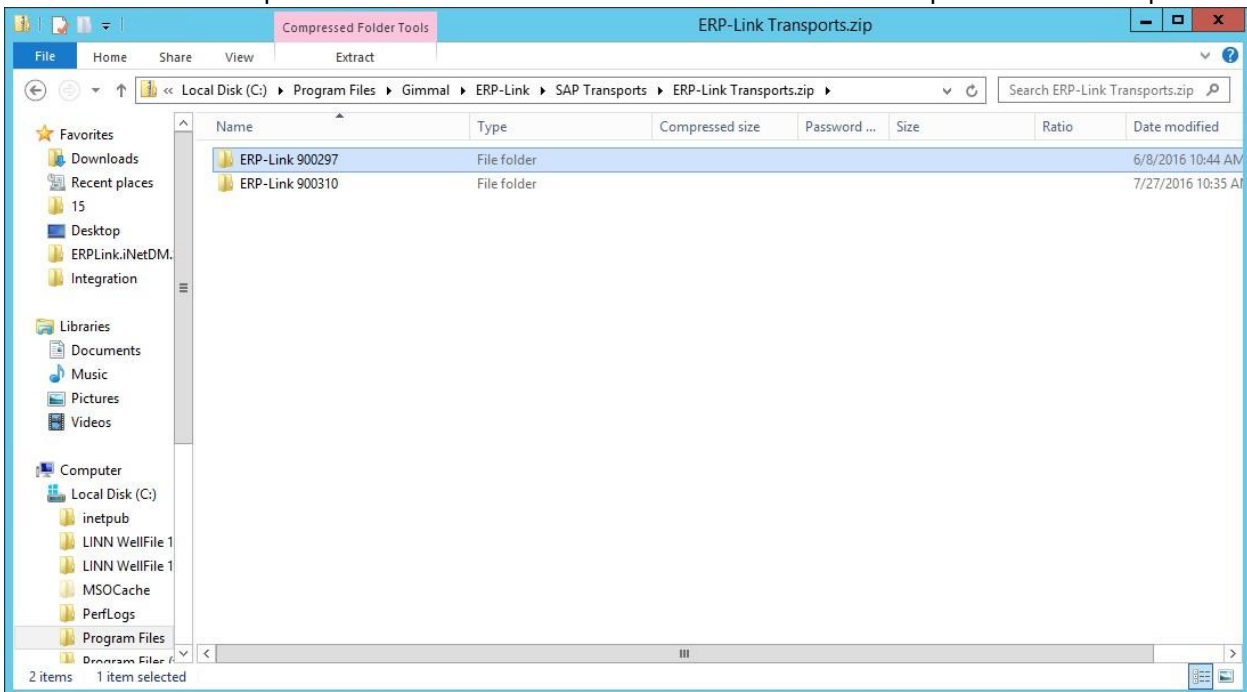


Figure 3-37 Example Folders with Exported SAP Transports

3. Import each transport into SAP.

3.11 Populating Document Tracking Service if Upgrading from v4.x or Older

Note:

All content repositories must be configured before performing this task or Document Tracking Service will not properly function.

If you are upgrading to Gimmel Link 5.2 from V4.x or older, you need to run the Document Tracking Service Migration Utility after executing the Gimmel Link 5.1 installation, importing the Gimmel Link configuration files, and completing of all Gimmel Link 5.1 configuration.

The Document Tracking Service Migration Utility iterates the Gimmel Link 5.1 configuration file, identifies all primary and secondary document repository locations, and crawls these document repository locations in SharePoint. Therefore, any content repositories that are not configured in the Gimmel Link configuration will not be crawled and references for documents in these repositories are not created in the Document Tracking Service. Additionally, users will not be able to retrieve documents in SAP from these content repositories until they are configured in the Gimmel Link configuration.

3.11.1 Configure Settings for the Document Tracking Service Migration Utility

The Document Tracking Service Migration Utility enables population of document locations and metadata in the Document Tracking Service through crawling of content repositories configured in Gimmel Link 5.1. The Document Tracking Service Migration Utility iterates the Gimmel Link 5.1 configuration file, identifies all primary and secondary document repository locations, and crawls these document repository locations in SharePoint. The document location and metadata for documents in the primary or secondary document repositories are added as entries in the Document Tracking Service during the crawl.

The Document Tracking Service Migration Utility is a command line executable. To configure settings for the Document Tracking Service Migration Utility:

1. Navigate to the Document Tracking Service Migration Utility folder C:\Program Files\Gimmel\Gimmel Link\DTS Migration\.
2. Open the configuration file ERPLink.DTSMigrationUtility.exe.Config in a text editor such as Notepad.
3. Edit the DocumentTrackingServiceURL key value to the URL of the Document Tracking Service configured in the Gimmel Link Administration Console.

```
<add key="DocumentTrackingServiceURL"  
value="http://yourserverurl/DocumentTrackingService/" />
```

4. Edit the ERPLinkConfigPath key value to the UNC path of the Gimmel Link Configuration File.

```
<add key="ERPLinkConfigPath" value="C:\Program Files\Gimmel\ERPLink\iNetDM\Website\FILES\ERPLinkConfig.xml" />
```
5. Save the ERPLink.DTSMigrationUtility.exe.Config to the same location.

3.11.2 Executing the Document Tracking Service Migration Utility

The Document Tracking Service Migration Utility must be executed with an account that has read permissions to all primary and secondary document repositories in the Gimmel Link configuration file. This account can be the SharePoint farm or web application service accounts, service account for the iNet.DM web application, or other domain account that has appropriate permissions.

To execute the Document Tracking Service Migration Utility:

1. Launch a Windows command prompt with an account that appropriate permissions.
2. Navigate to the Document Tracking Service Migration Utility folder `C:\Program Files\Gimmel\Gimmel Link\DTS Migration\` in the Windows command prompt.
3. Type `'ERPLink.DTSMigrationUtility.exe'` and press the **ENTER** key.
4. The executable creates a log file in the Logs folder. The log file is named `ERPLink_DTSMigration_mmddyy_hhmm.log`, where `mmddyy_hhmm` is the month, day, year, hour, and minute the log file is created.

4 Setting Up an Gimmel Link Document Library

Gimmel Link requires that specific site columns be present in the content types used in iNet.DM repositories to archive, index, and retrieve content. SharePoint provides several ways to implement this approach. The recommended approach uses a Content Type hub to publish custom content types to all site collections. This approach is best because it allows for centralized management of the content types and publishing to support re-use across the entire SharePoint farm. This approach is especially important for complex environments where content could be spread across many site collections.

To deploy iNet.DM-dependent site columns and content types to SharePoint according to best practices, follow this process:

1. [Creating and Configuring a SharePoint Content Type Hub \(On-Premises\)](#)
2. [Deploying the iNet.DM Site Columns and Content Types in the Content Type Hub](#)
3. [Creating Custom Content Types Using iNet.DM Content Types](#)
4. [Publishing the Custom Content Types](#)

5. [Adding the Published Content Types to a New or Existing Document Library](#)
6. [\(Optional\) Adding Indexes to New Document Library for Use with Flat Storage Mode](#)

4.1 Creating and Configuring a SharePoint Content Type Hub (On-Premises)

To create and configure a SharePoint content type hub, follow these steps.

1. Create a new site collection in Central Administration.
2. Navigate to the newly created site collection.
3. Click the **Settings** button and select the **Site Settings** option.
4. In the **Site Settings** pane, click **Site Collection Administration** and then click **Site Collection Features**.
5. In the **Site Collection Features** pane, activate the **Content Type Syndication Hub** feature.

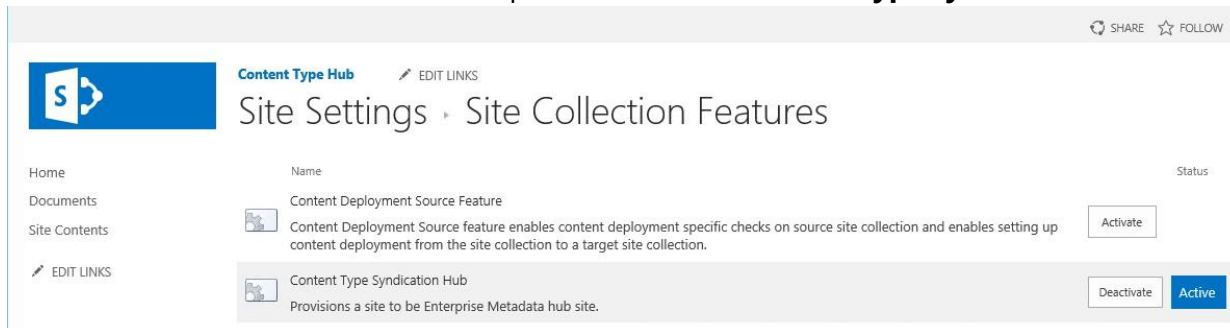


Figure 4-1 Activated Content Type Syndication Hub Feature

6. To add the content type hub syndication site to the Managed Metadata service application:
 - a. In the **Central Administration** home page, click **Application Management** and then click **Manage Service Applications**.

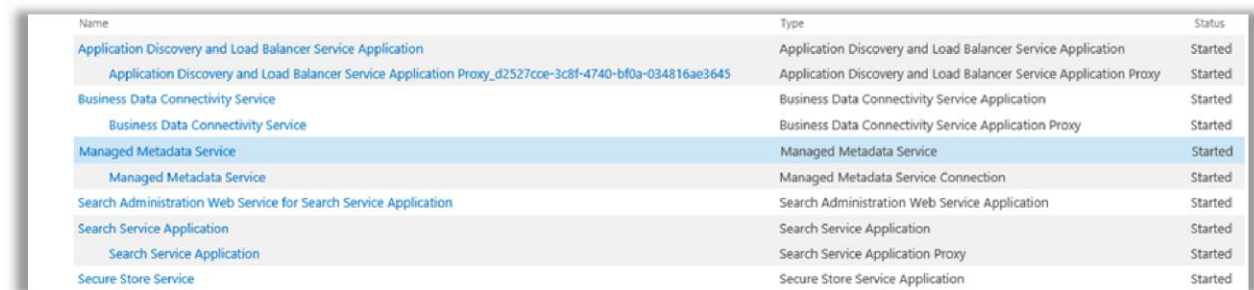


Figure 4-2 Managed Metadata Service Option in Service Applications Pane

- b. On the **Service Applications** page, select the **Managed Metadata Service** by clicking on the row for that item.

- c. Click **Properties** in the ribbon.

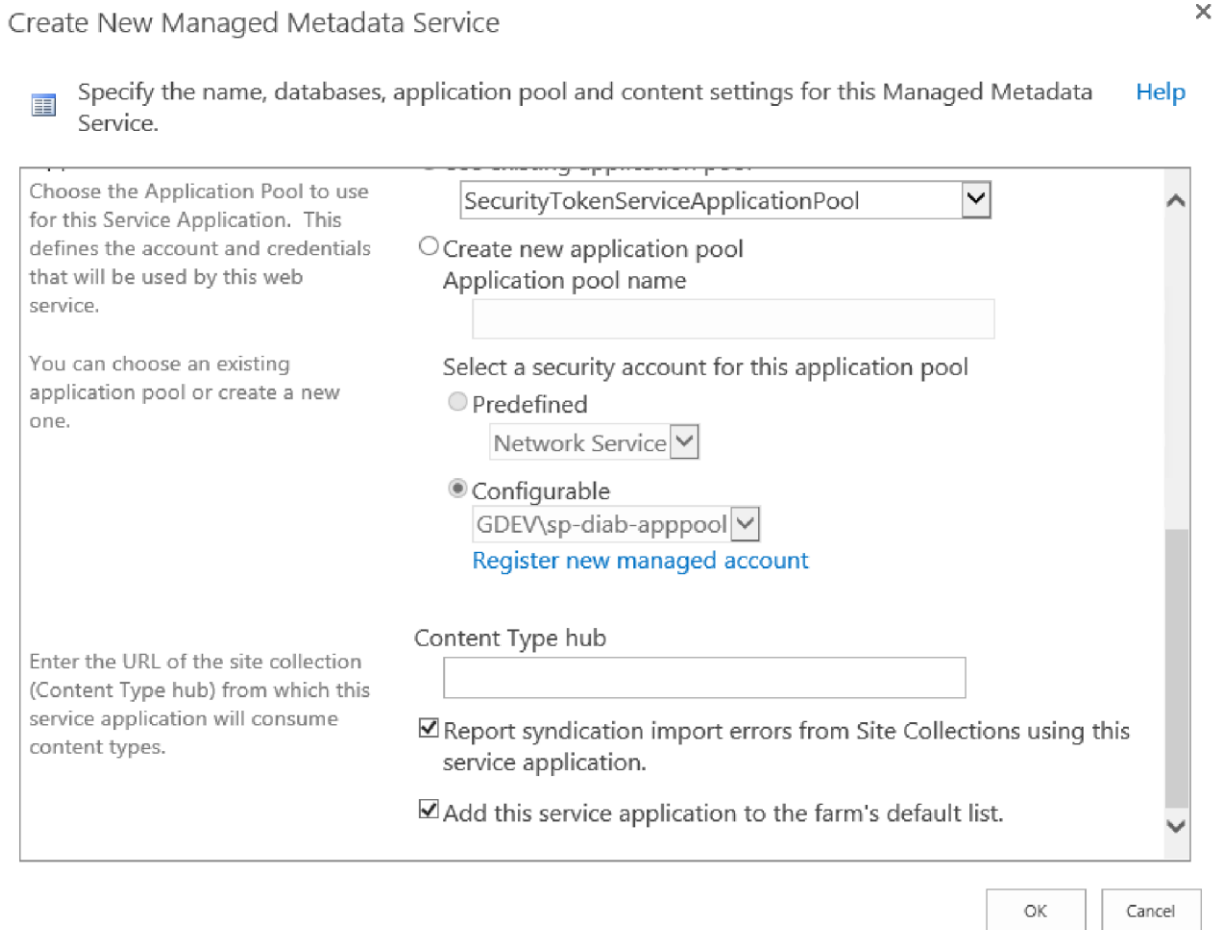


Figure 4-3 Create New Managed Metadata Service Dialog Box

- d. In the **Create New Managed Metadata Service** dialog box, enter the URL to the site collection that implements the content type hub.
 - e. Click **OK** to save this configuration.
7. To configure the **Managed Metadata Service Connection**, follow these steps.
- a. Navigate to the **Service Applications** pane.
 - b. On the **Service Applications** page, select the **Managed Metadata Service Connection** by clicking on the row for that item.

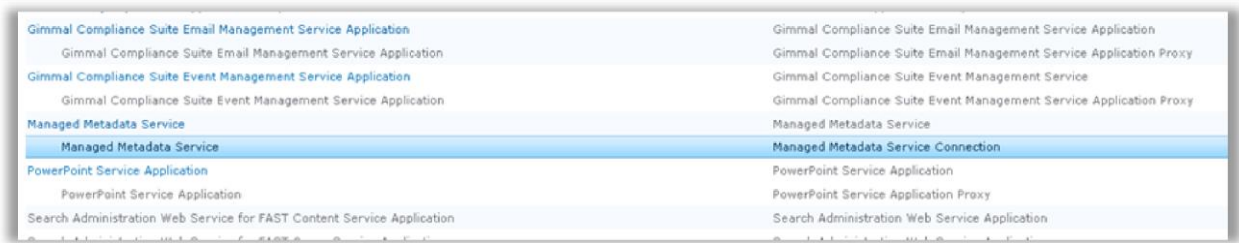


Figure 4-4 Managed Metadata Service Connection in Service Applications Pane

- c. Click **Properties** in the ribbon.
- d. On the **Properties** dialog box, select the **Consumes content types from the content type gallery at http://*SiteURL*** checkbox.
- e. Click **OK** to save the configuration.

The content type hub is configured and can be used to publish to all other site collections.

4.2 Deploying the iNet.DM Site Columns and Content Types in the Content Type Hub

Deploy the iNet.DM site columns and content types to the content type hub by following these steps.

1. Launch the **Gimmel Link Administration Console**.

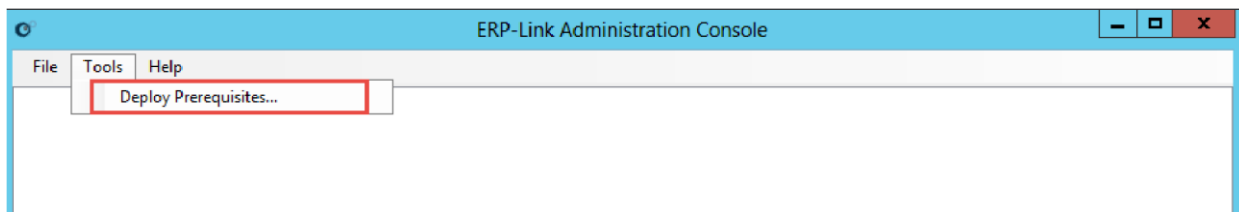


Figure 4-5 Gimmel Link Administration Console

2. From the **Tools** menu, select Deploy Prerequisites.

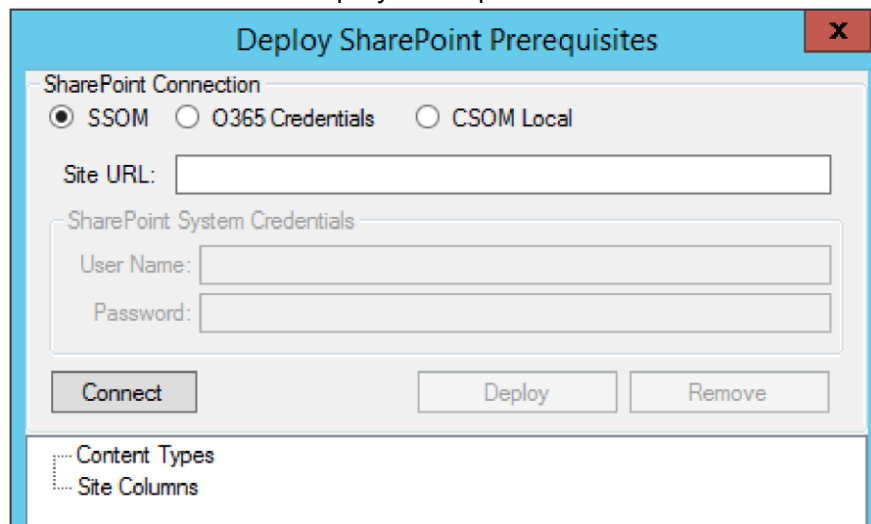


Figure 4-6 Deploy SharePoint Prerequisites Dialog Box

3. Make sure the correct selection is made for the SharePoint Connection.
 - By default, the Deploy SharePoint Prerequisites feature attempts to connect to the SharePoint site collection using SSOM.

- For a deployment to O365 using the Client-Side Object Model, select O365 Credentials and specify the user name and password for an O365 account able to make changes to the site collection.
 - Select CSOM Local when the connection is on the same system as the SharePoint server. For SharePoint on-premise deployments, you must select CSOM Local.
4. Enter the **Site URL** of the SharePoint site collection that implements the content type hub created in [Creating and Configuring a SharePoint Content Type Hub \(On-Premises\)](#). This SharePoint site collection is where the iNet.DM site columns and content types will be created.

Note:

For SSOM or CSOM mode, the credentials in the **Deploy SharePoint Prerequisites** must at a minimum have Full Control permissions to the Content Type Hub implemented in the Site URL in this dialog box.

-
5. Click **Connect**. If the connection is successful; then the deployment status of the iNet.DM site columns and content types displays in the text area.

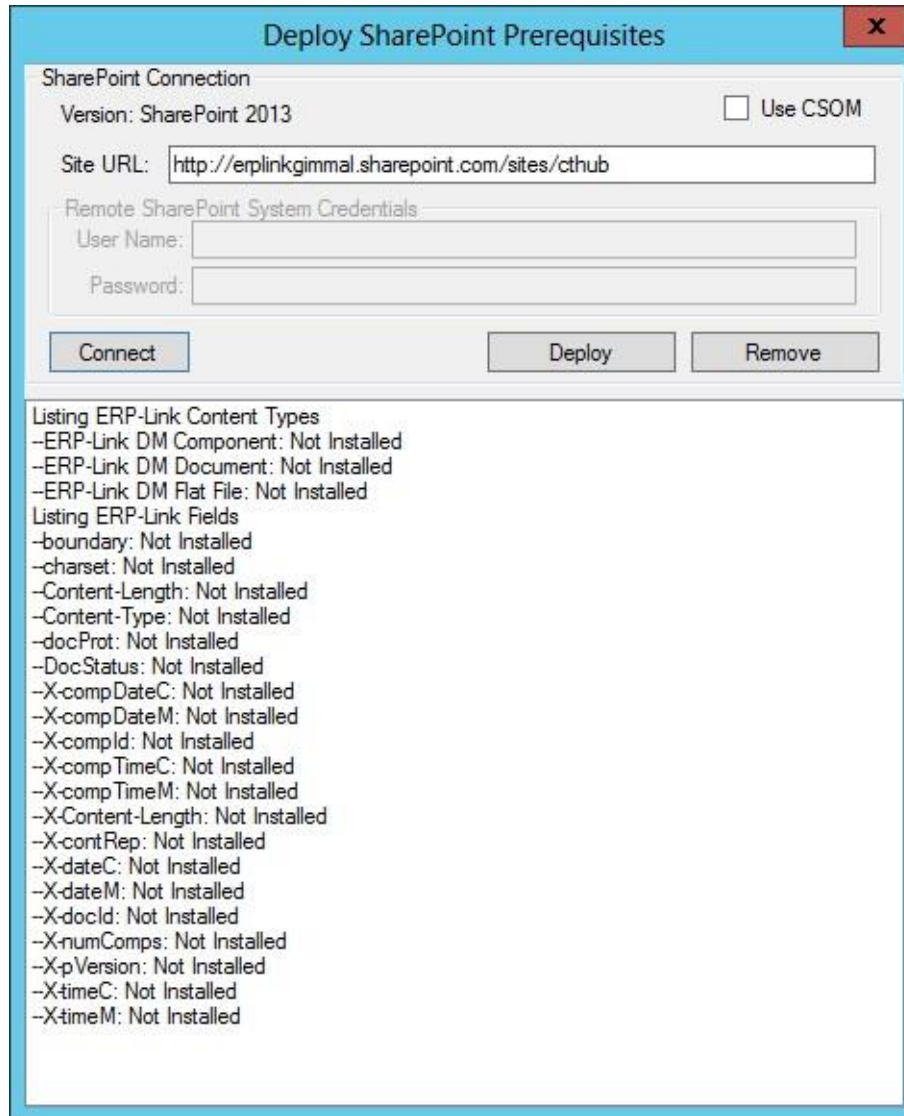


Figure 4-7 Status of iNet.DM-Dependent Site Columns and Content Types in Content Hub

- The text area displays the deployment status of the iNet.DM-dependent site columns and content types. The site columns and content types that exist in the site collection display a status of **Installed**.

If any of the statuses are **Not Installed**, click **Deploy** to deploy all iNet.DM-dependent site columns and content types to the site collection.

- Click **Remove** if you want to remove all iNet.DM-dependent site columns and content types from the site collection.
- Navigate to the SharePoint site collection where the iNet.DM dependent site columns and content types were deployed.
- Click the **Settings** button and select the **Site Settings** option.

- Click **Site Columns** to verify that all iNet.DM site columns and content types were successfully deployed to the site collection.

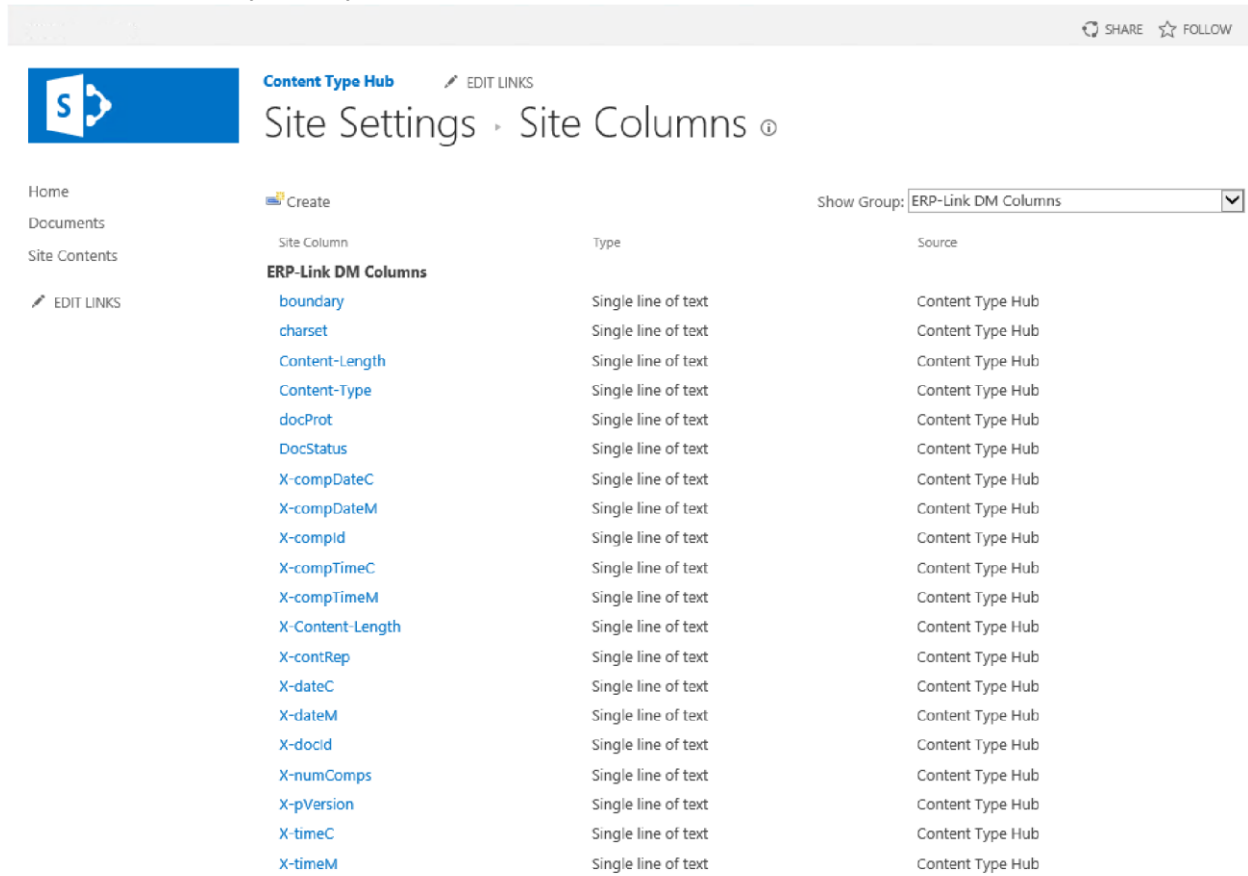


Figure 4-8 Deployed Gimmel Link iNet.DM-Dependent Site Columns

- Click **Site Content Types** to view the deployed content types.

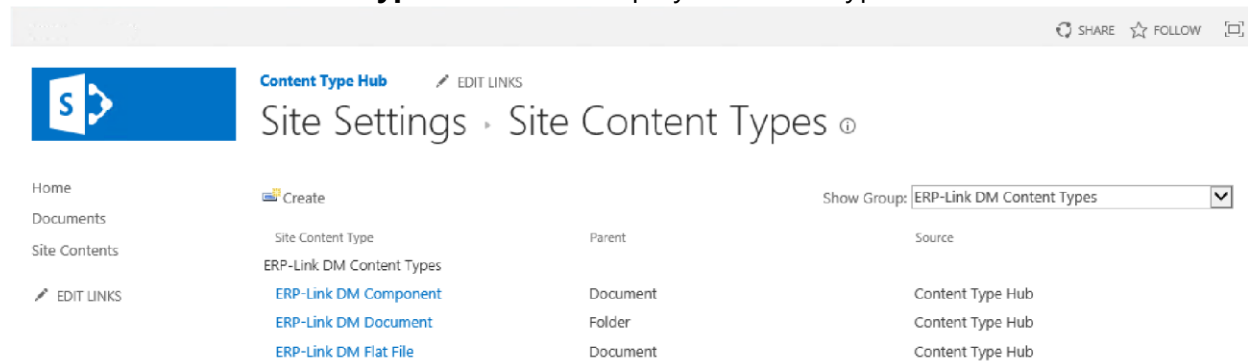


Figure 4-9 Deployed Gimmel Link iNet.DM-Dependent Site Content Types

4.3 Creating Custom Content Types Using iNet.DM Content Types

After you deploy the iNet.DM-dependent site columns and content types to the SharePoint site collection, you can create custom content types that are derived from the iNet.DM-dependent content types. The custom content types include the iNet.DM-dependent site columns. These custom content types can define specific document types that relate to SAP business objects such as Purchase Order or Invoice. These custom content types are added to the iNet.DM document libraries and associated with specific document types for iNet.DM archiving, indexing, and routing.

To create a custom content type for use by iNet.DM, follow these steps.

1. Navigate to the content type hub site collection.
2. Click the **Settings** button and then select the **Site Settings** option.
3. On the **Site Settings** pane, click **Site Collection Administration** and then click **Site Content Types**.
4. On the **Site Content Types** dialog box, click **Create**.

Site Content Types · New Site Content Type ⓘ

Name and Description
Type a name and description for this content type. The description will be shown on the new button.

Name:

Description:

Parent Content Type:
Select parent content type from:
ERP-Link DM Content Types ▼

Parent Content Type:
ERP-Link DM Component ▼

Description:
Create a new document.

Group
Specify a site content type group. Categorizing content types into groups will make it easier for users to find them.

Put this site content type into:

Existing group:
Custom Content Types ▼

New group:
ERP-Link Content Types x

OK Cancel

Figure 4-10 New Site Content Type Dialog Box with Correct Entries

5. Type a **Name** for the new content type.
6. From the **Select parent content type from** menu, select **Gimmel Link DM Content Types**.
7. From the **Parent Content Type** menu, select **Gimmel Link DM Component content type**.
8. Select the **Group** parameter that fits your situation.
9. Click **OK** to create the content type.

Site Content Types ▸ Site Content Type

Site Content Type Information

Name: Purchase Order
Description:
Parent: ERP-Link DM Component
Group: ERP-Link Content Types

Settings

- Name, description, and group
- Advanced settings
- Workflow settings
- Delete this site content type
- Document Information Panel settings
- Information management policy settings
- Manage publishing for this content type

Columns

Name	Type	Status	Source
Name	File	Required	Document
Title	Single line of text	Optional	Item
charset	Single line of text	Optional	ERP-Link DM Component
Content-Length	Single line of text	Optional	ERP-Link DM Component
Content-Type	Single line of text	Optional	ERP-Link DM Component
docProt	Single line of text	Optional	ERP-Link DM Component
X-compDateC	Single line of text	Optional	ERP-Link DM Component
X-compDateM	Single line of text	Optional	ERP-Link DM Component
X-compId	Single line of text	Optional	ERP-Link DM Component

Figure 4-11 New Content Type Information

10. You can add more site columns to the custom content type by clicking **Add from existing site columns** or **Add from new site column** at the bottom of the dialog box.

4.4 Adding Custom Content Types to iNet.DM Document Libraries

The published custom content types should be added to iNet.DM document libraries in the site collections that implement iNet.DM repositories so that these content types can be assigned to specific document types archived in the iNet.DM repository.

1. Navigate to the site that contains the document library to add the content type to.

Note:

This site can be the root site of a site collection or any subsite.

2. Open the document library to add the content type to.
3. Click the **Library** tab in the ribbon.

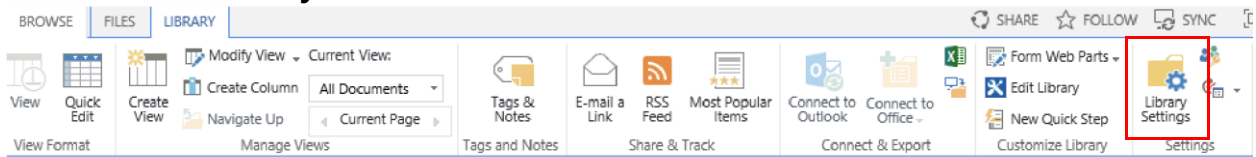


Figure 4-12 Library Ribbon

4. Verify that the document library is configured to support content types by clicking **Library Settings** in the ribbon.

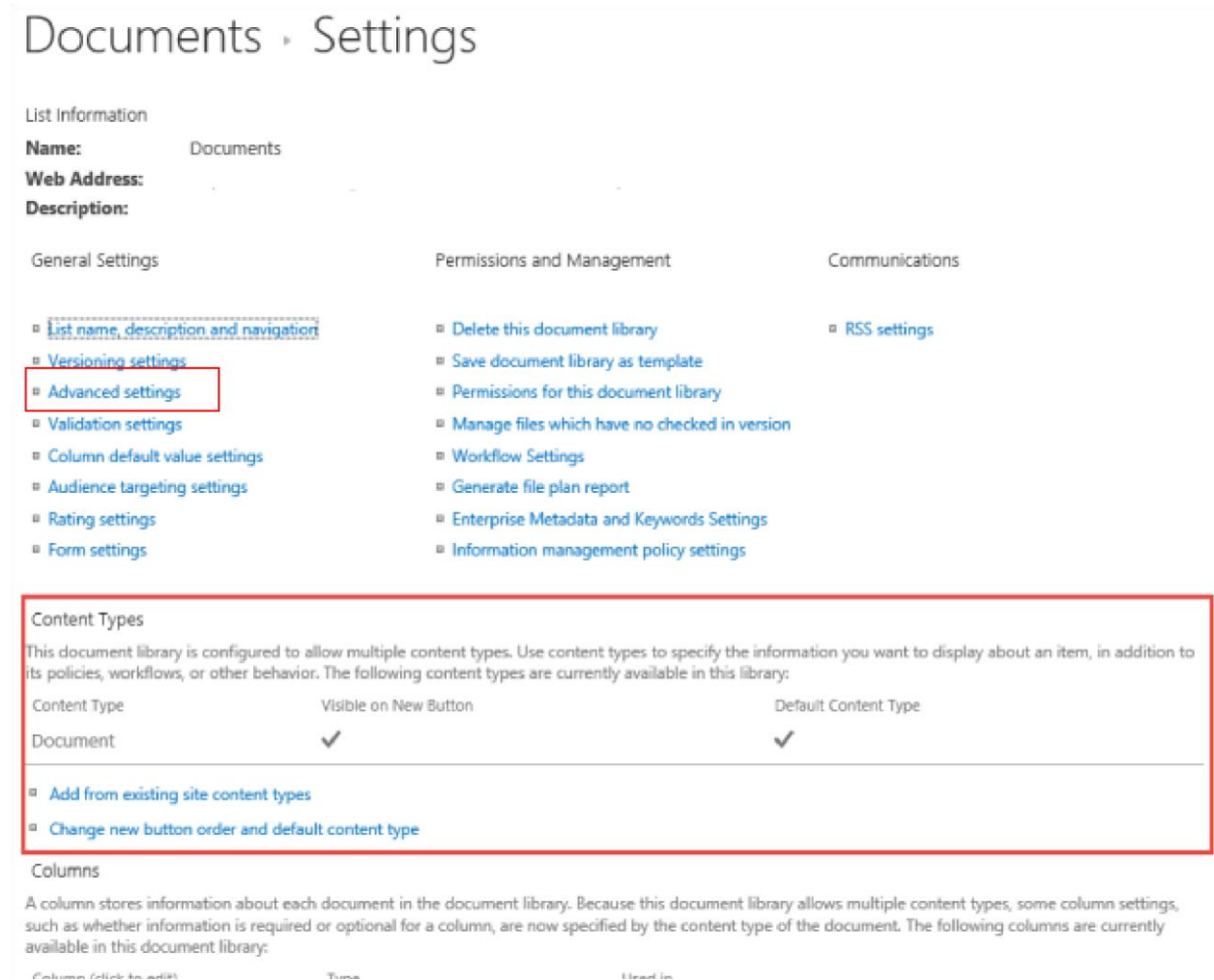


Figure 4-13 Documents Settings Page Showing Content Types Enabled

- If content types are enabled, the **Document Settings** dialog box displays a section for content types and displays all content types that have been added to the document library.

If content types are enabled, skip to step 7.
- If content types are not enabled in the document library, follow these steps to enable them.

- a. Click **Advanced Settings**.

Settings ▸ Advanced Settings

Content Types

Specify whether to allow the management of content types on this document library. Each content type will appear on the new button and can have a unique set of columns, workflows and other behaviors.

Allow management of content types?

Yes No

Document Template

Type the address of a template to use as the basis for all new files created in this document library. When multiple content types are enabled, this setting is managed on a per content type basis. [Learn how to set up a template for a library.](#)

Template URL:

Shared Documents/Forms/template.dotx

Figure 4-14 Advanced Settings Pane

- b. In the **Advanced Settings** page, select **Yes** for **Allow management of content types?**
- c. Click **OK** to save the configuration.

- 7. Add the published custom content type to the document library.

- a. Click **Add from existing content types**.

Settings ▸ Add Content Types ⓘ

Select Content Types

Select from the list of available site content types to add them to this list.

Select site content types from:

ERP-Link Content Types

Available Site Content Types:

[Empty list box for Available Site Content Types]

Add >

< Remove

Content types to add:

Purchase Order

Description:
None

Group: ERP-Link Content Types

OK

Cancel

Figure 4-15 Add Content Types Page

- b. Select the published content type group from the **Select site content types from** menu.
- c. In the **Available Site Content Types** field, select content types that are to be added to the document library.
- d. Click **Add** to move the content type to the **Content types to add** field.

When all desired content types have been moved to the **Content types to add** box, click **OK** to save the configuration.

4.5 Publishing the Custom Content Types

To publish the custom content types to SharePoint site collections that implement iNet.DM repositories, follow these steps.

1. Navigate to the content type hub site collection.
2. Click the **Settings** button and select **Site Settings**.
3. In the **Site Settings** pane, click **Site Collection Administration** and then click **Site Content Types**.
4. On the **Site Content Types** pane, find the content type that you want to publish and click the link of the name for that content type.

Site Content Types › Site Content Type

Site Content Type Information

Name: Purchase Order
Description:
Parent: [ERP-Link DM Component](#)
Group: ERP-Link Content Types

Settings

- [Name, description, and group](#)
- [Advanced settings](#)
- [Workflow settings](#)
- [Delete this site content type](#)
- [Document Information Panel settings](#)
- [Information management policy settings](#)
- [Manage publishing for this content type](#)

Columns

Name	Type	Status	Source
Name	File	Required	Document
Title	Single line of text	Optional	Item
charset	Single line of text	Optional	ERP-Link DM Component
Content-Length	Single line of text	Optional	ERP-Link DM Component
Content-Type	Single line of text	Optional	ERP-Link DM Component
docProt	Single line of text	Optional	ERP-Link DM Component
X-compDateC	Single line of text	Optional	ERP-Link DM Component
X-compDateM	Single line of text	Optional	ERP-Link DM Component
X-compId	Single line of text	Optional	ERP-Link DM Component

Figure 4-16 Site Content Type Information Pane

5. Click **Manage publishing for this content type**.

Content Type Publishing: Purchase Order

Content Type Publishing

Publish
Make this content type available for download for all Web Applications (and Site Collections) consuming content types from this location.

Unpublish
Make this content type unavailable for download for all Web Applications (and Site Collections) consuming content types from this location. Any copies of this content type being used in other site collections will be unsealed and made into a local content type.

Republish
If you have made changes to this content type, the content type needs to be "republished" before the changes are available for download to Web Application consuming content types from this location.

Publishing History
The date on which one or more service applications have successfully published this content type.

Last successful published date:

OK Cancel

Figure 4-17 Content Type Publishing Dialog Box

6. Click **OK** to initiate the publishing process.

Note:

The publishing process is managed by SharePoint timer jobs. Depending on the configured interval for your environment, publishing could take up to an hour for the published content type to appear in the target site collection. To expedite the process, you can execute the Content Type Hub timer job and once it completes, execute each of the Content Type Subscriber timer jobs.

4.6 Adding the Published Content Types to a New or Existing Document Library

Add the content types to the library as you normally would in SharePoint.

Note:

If you wish to use SharePoint's Document ID feature with your Document Libraries, this is fully supported. If more than one site collections has this feature enabled, the documents will maintain the Document ID that was first assigned. During routing, this Document ID will persist across site collections with the Document ID feature enabled, as well as site collections with the Document ID feature disabled.

4.7 (Optional) Adding Indexes to New Document Library for Use with Flat Storage Mode

This optional procedure adds a query index that is necessary to use flat storage libraries with a quantity of items that exceeds the SharePoint List View Item threshold. This procedure also improves performance in these conditions.

1. Launch SharePoint.

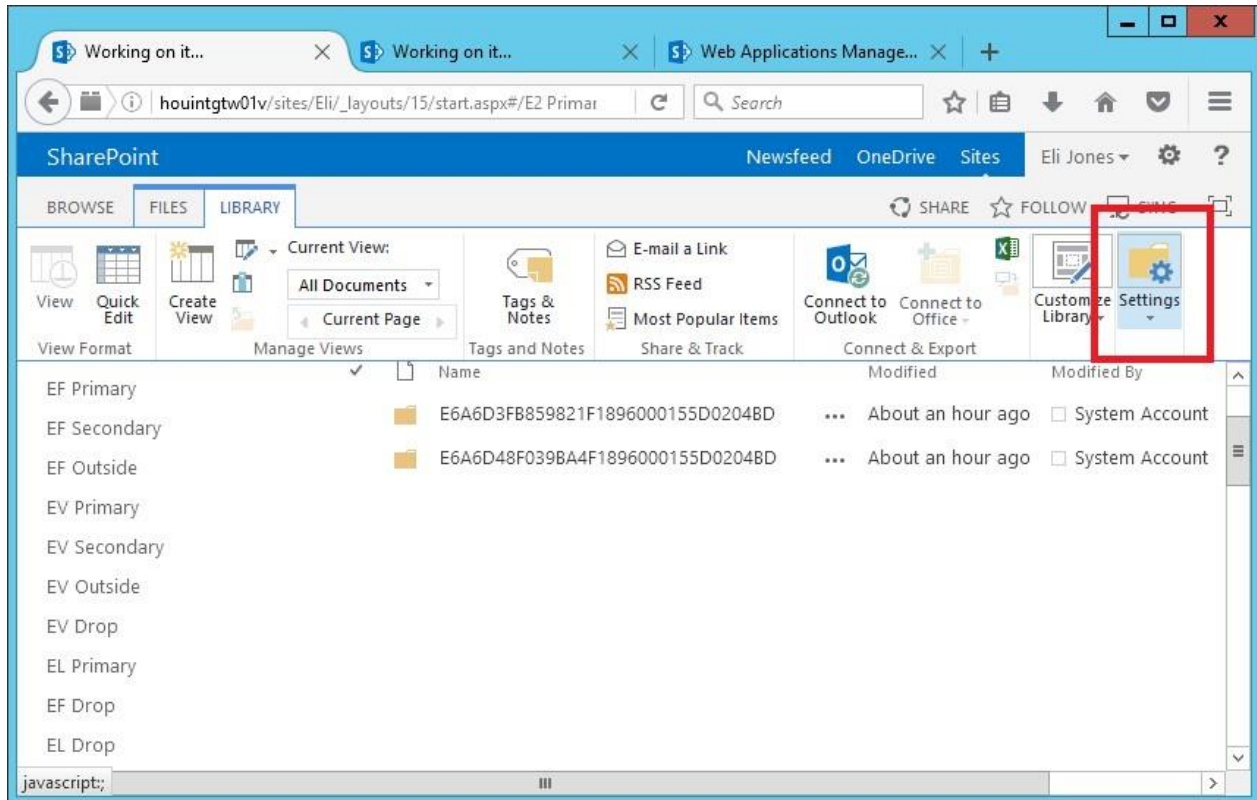


Figure 4-18 Initial SharePoint Window

2. From the **Library** view, select **Settings**.

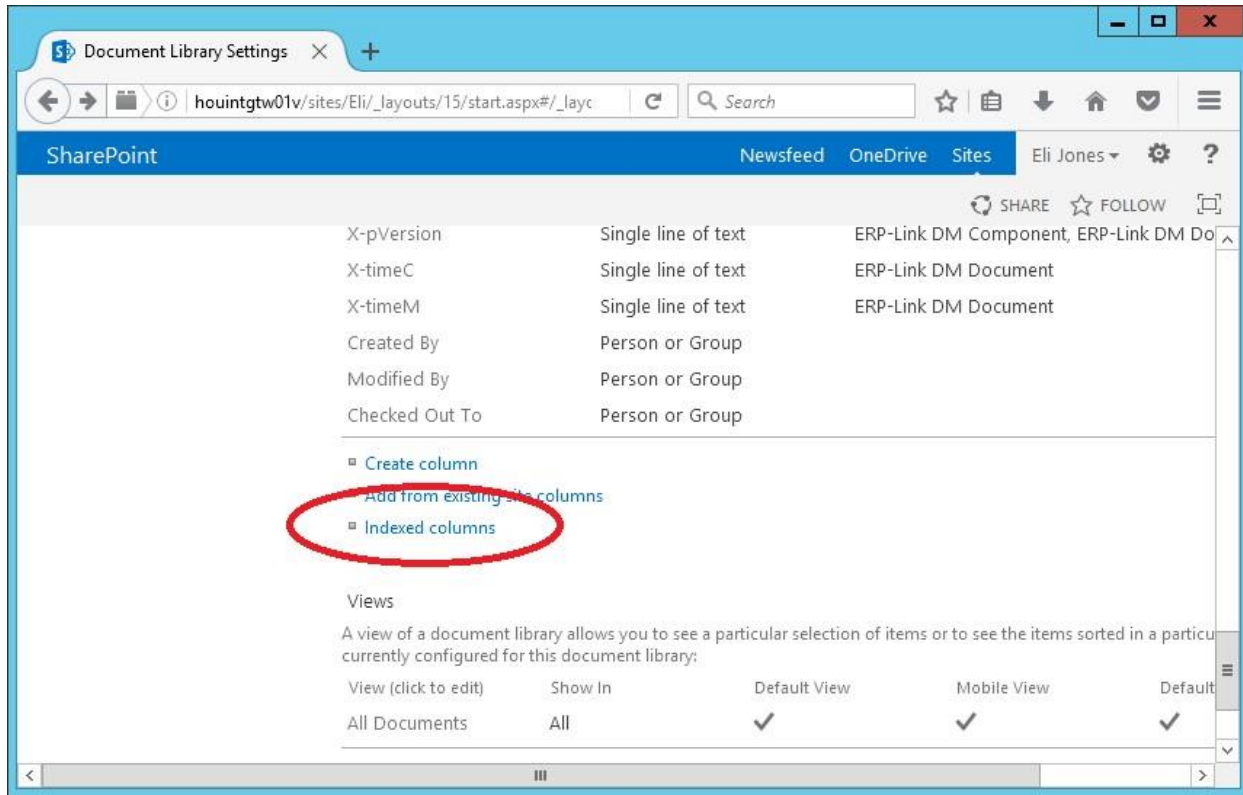


Figure 4-19 Settings Window in SharePoint

3. Under the **Columns** heading, click **Indexed columns**.

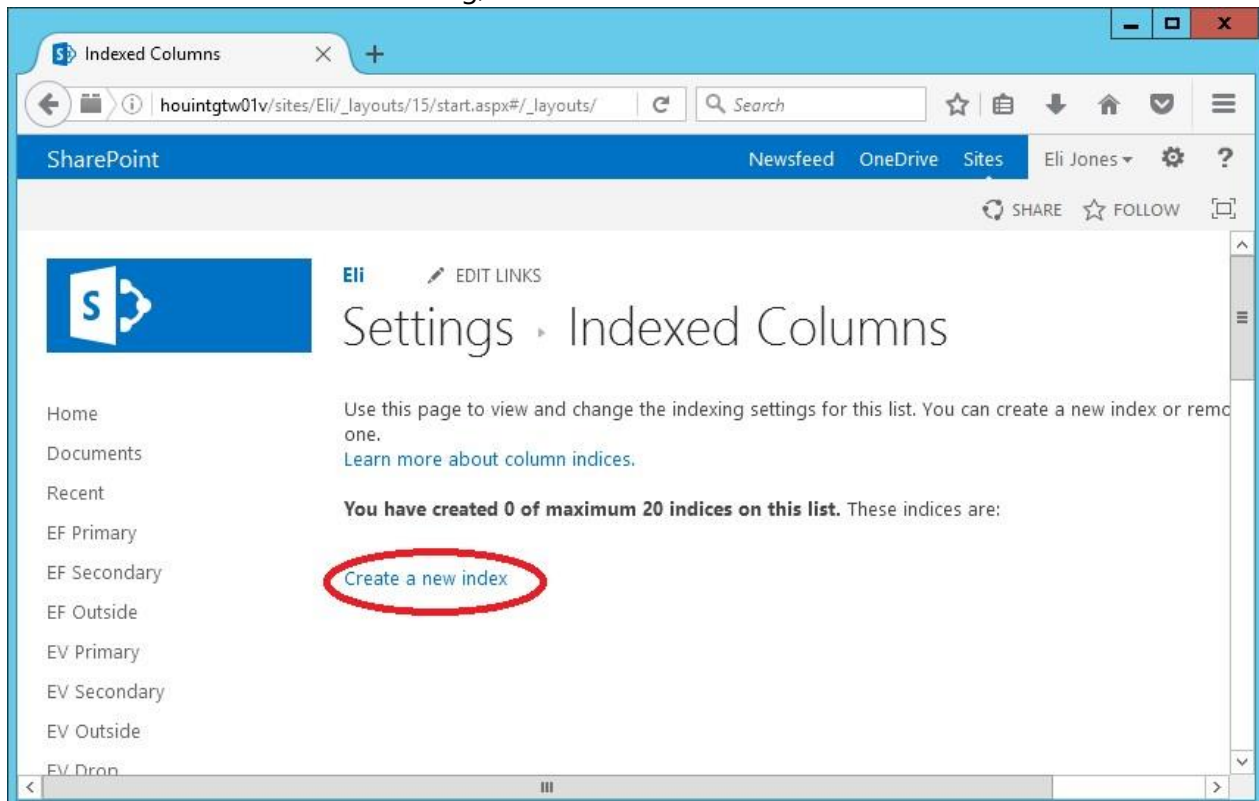


Figure 4-20 Indexed Columns Window

4. Click **Create a new index**.

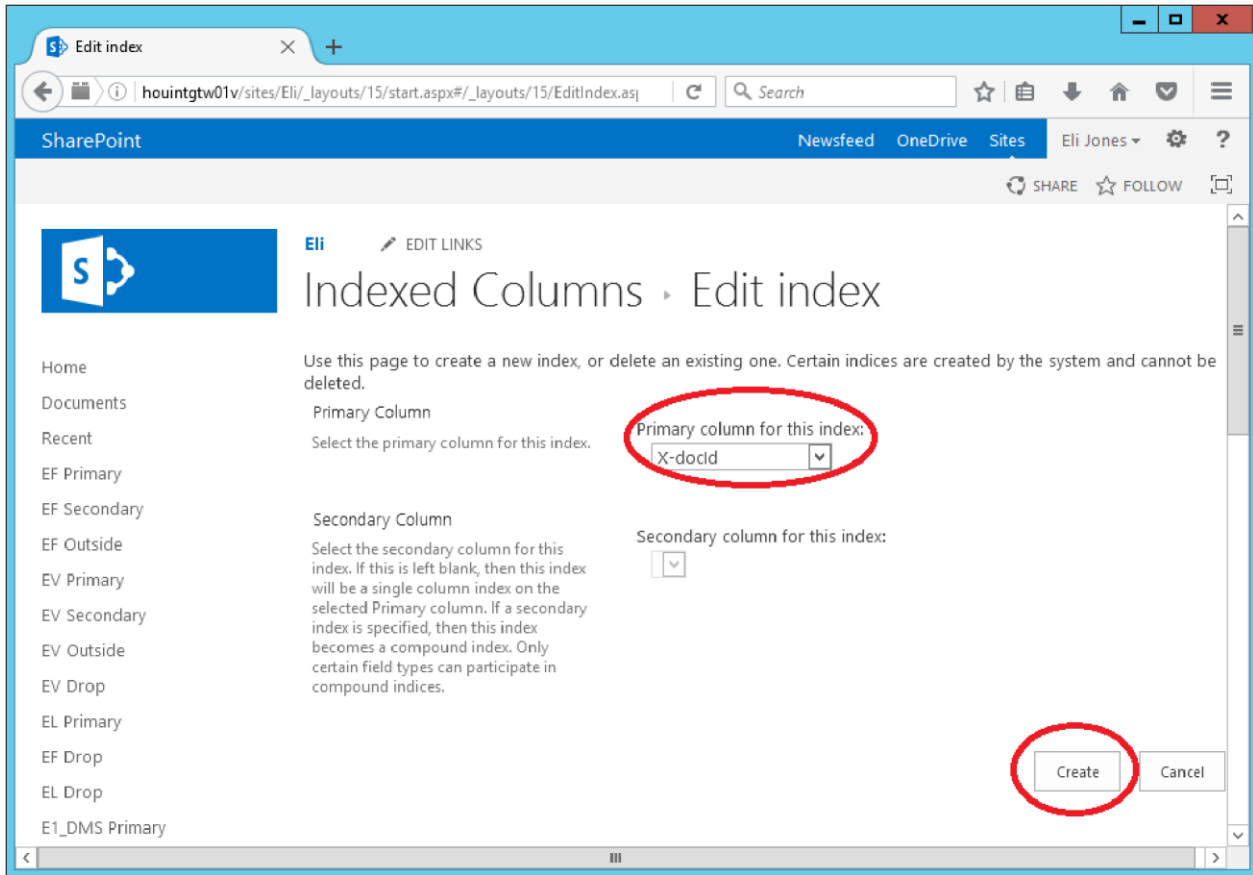


Figure 4-21 Edit Index Window

5. For **Primary** column, select **X-docid** and then click **Create**. The column X-docid should have been created in [4.2 Deploying the iNet.DM Site Columns and Content Types in the Content Type Hub](#).

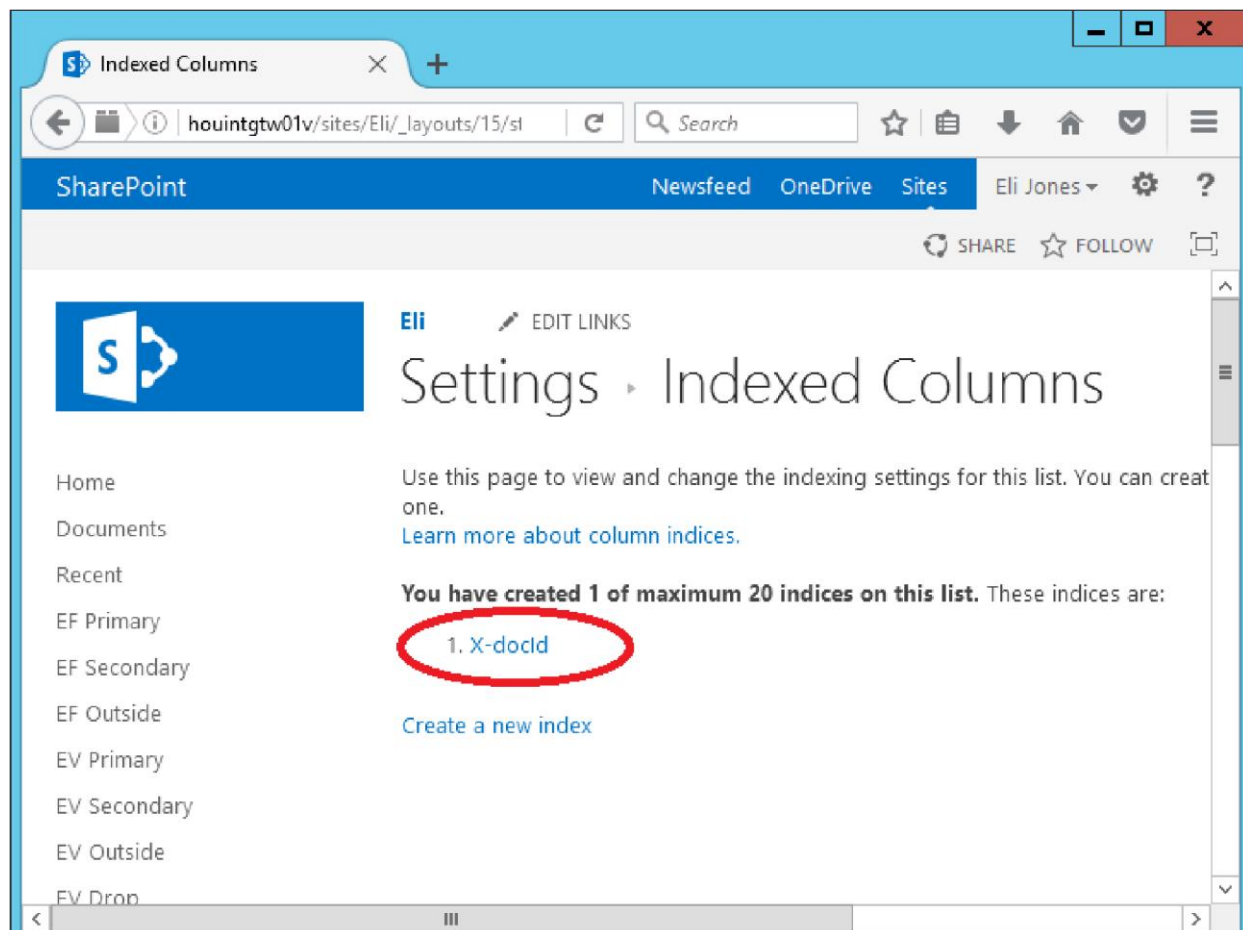


Figure 4-22 Index Appearing under Indexed Columns

The index **X-docid** should appear under **Indexed Columns**.

5 Setting Shared Configuration Settings

This chapter contains information on how to configure the Gimmal Link Administration Console and its components. It includes the following:

- [5.2 Setting Up the Configuration Service](#)
- [5.3 Setting Event Logging](#)
- [5.4 Configuring the Web Service Security Key](#)
- [5.5 Defining SAP Pools, SAP Settings, and Object Types](#)
- [5.6 Defining SharePoint Settings](#)
- [5.7 Configuring the Document Tracking Service](#)
- [5.8 Verifying the Connection Service](#)

5.1 Configuring the Connection Service

For technical information about the Gimmel Link Connection Service, refer to Appendix [B Gimmel Connection Service](#). See the following section for information on configuring the SSL certificate, which is required for the Connection Service.

5.1.1 Configuring Secure Socket Layers (SSL) for Connection Service Web Application

You need to choose a certificate. A browser usually verifies the following in a server certificate:

- Current date and time is within the Valid from and Valid to date range on the certificate
- Certificate's Common Name (CN) matches the host header in the request. For example, if the client is making a request to `http://www.contoso.com/`; then the CN must also be `http://www.contoso.com/`
- Issuer of the certificate is a known and trusted Certificate Authority (CA)

If one or more of these verifications fails, the browser prompts the user with warnings. For production deployments of Gimmel Link and the Connection Service 5.1, it is recommended that you request and obtain a certificate from a known CA such as VeriSign or GeoTrust.

Self-signed certificates are certificates created on your computer. They are useful in environments where it is not important for an end user to trust your server, such as a development or test environment. For information to request an Internet Server Certificate, refer to: [https://technet.microsoft.com/en-us/library/cc732906\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc732906(v=ws.10).aspx).

5.2 Setting Up the Configuration Service

The Gimmel Link Configuration Service stores configuration data in a SQL database, which is accessible through a web service. This service supersedes the storage of configuration data in XML files on the file system.

The following sections describe how to use the Configuration Service to manage and configure your Gimmel Link settings from one central location.

Note:


The Configuration Service only allows one active configuration at a time. You can set up other configurations, but only the active configuration is used by your Gimmel Link instance.

Gimmel Link must be either configured or the configuration from a prior installation must be imported before it can be used.

5.2.1 Accessing the Administration Console

The Configuration Service is accessible from the Gimmel Link Administration Console. You must launch the Administration Console and open the Configuration Service as described below. From there, you can configure the Gimmel Link settings/components for your configurations.

To access the Administration Console, follow these steps:

1. Click the Windows Start button () and scroll through the alphabetical list on the left.
2. Click the **Gimmel Link** folder, and then **Gimmel Link Administration Console**. The console window opens.

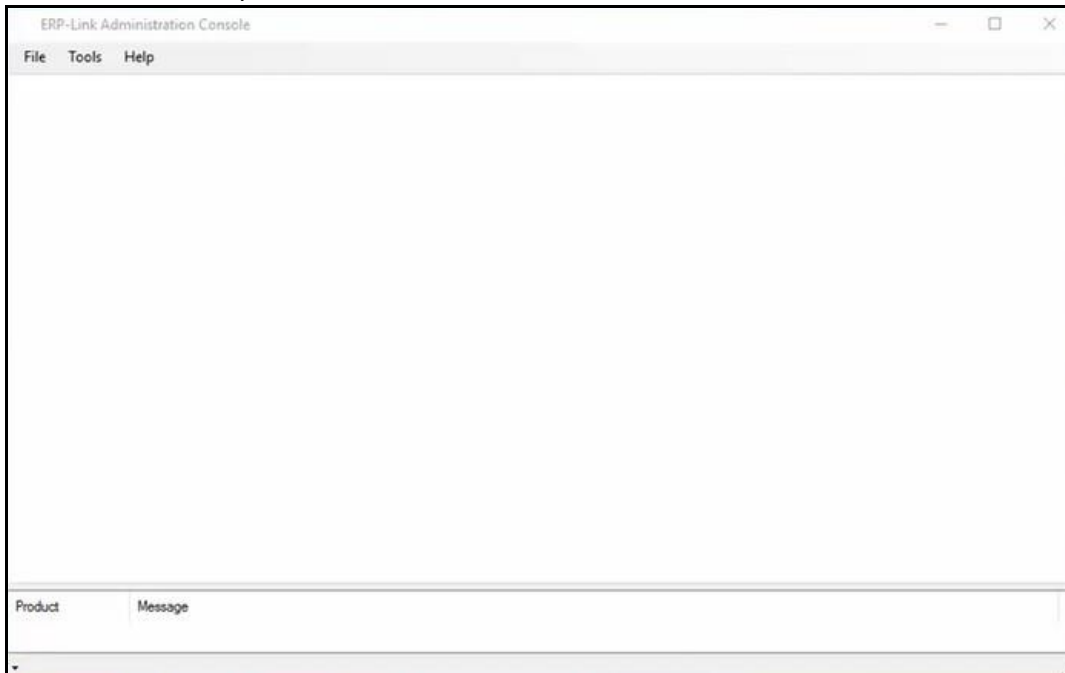


Figure 5-1 Gimmel Link Administration Console

Note:

You must create a new configuration or import an existing configuration from a prior installation before you can use the Configuration Service. See the following sections for information on how to create a new configuration or import a configuration.

5.2.2 Creating a New Configuration in the Configuration Service

Follow these steps to create a new configuration in the Configuration Service. A configuration provides a centralized location where you can configure and manage your Gimmel Link settings.

1. In the Gimmel Link Administration Console, click **File > Open** from the drop-down menu to open the Configuration Service. The Open Configuration dialog displays.

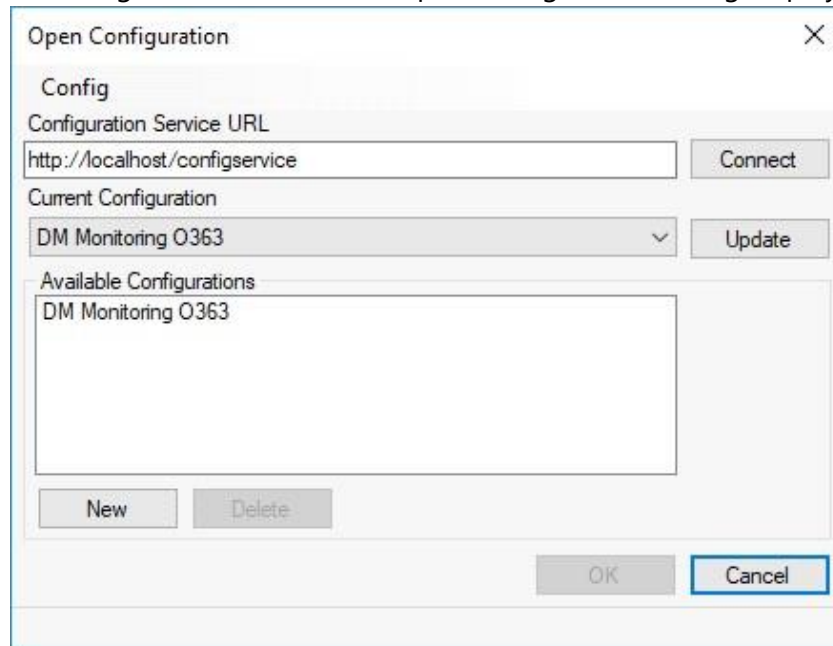


Figure 5-2 Open Configuration Dialog

2. Enter the URL of the Configuration Service web page you created during the installation process and click **Connect**. This links the Configuration Service to your configuration database. (**Note:** This only has to be done the first time you open the Configuration Service.)
3. Click **New** below the **Available Configurations** area on the Open Configuration dialog. The New Configuration dialog displays.

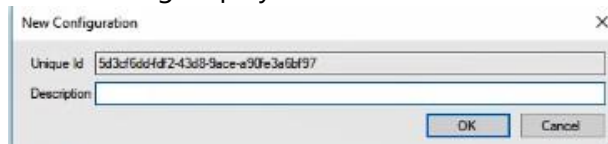


Figure 5-3 New Configuration Dialog

4. Enter the **Description** for the configuration and click **OK**.
5. The New configuration displays in the Administration Console.
6. Click **File > Save** to save the configuration. This action causes the configuration to remain in the Configuration Service when you close the application.

Note:

When you create a new configuration, it is **not** added as an entry into the database until it's saved for the first time.

A configuration can only be saved if the assigned user has the proper permissions assigned.

5.2.3 Saving Frequently

Gimmal Link does not automatically save the configuration file when you make changes to it and no mechanism exists to create a backup if a crash or network issue occurs. Therefore, during the configuration of the Administration Console components, remember to save frequently following this step.

- From the top menu in the **Gimmal Link Administration Console**, select **File** and then select **Save**.

You can save a configuration with a new file name by following these steps:

1. Activate the tab with the configuration that you want to save.
2. From the top menu in the **Gimmal Link Administration Console**, select **File** and then select **Save As**.
3. Type a **File name**.
4. Click **OK**.

Note:

A configuration can only be saved if the assigned user has the proper permissions assigned.

The file corresponding to the active tab is saved under the name you typed.

5.2.4 Specifying the Current (Active) Configuration

After setting up a new configuration, you must specify the configuration for Gimmal Link to actively use. Gimmal Link calls in every 30 seconds to check for an updated configuration.

Follow these steps to specify the configuration for Gimmal Link to use:

1. Log onto the Gimmal Link Administration Console.
2. Click **Open**. The Open Configuration dialog displays.

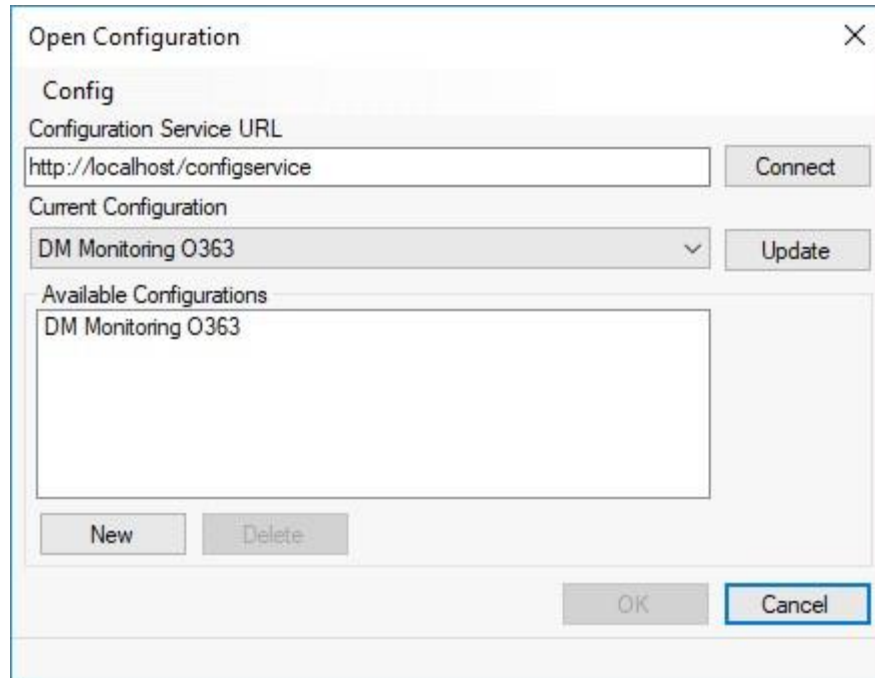


Figure 5-4 Open Configuration Dialog

3. Select the configuration from the **Current Configuration** drop-down and click **Update**. After you click **Update**, you will receive two prompts.
4. Confirm both prompts for your Current Configuration to be updated.

Repeat these steps if you want to switch to a different configuration.

5.2.5 Importing a Configuration

You can import an existing configuration into the Gimmel Link Configuration Service.

Follow these steps to import an existing configuration:

1. Launch the Gimmel Link Administration Console, and then click **File > Open**.
2. Select **Import** from the **Config** drop-down menu.

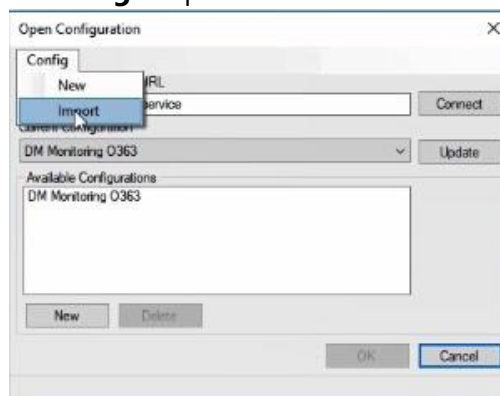


Figure 5-5 Selecting Import from the Config Menu

A file browser dialog opens.

3. Browse to the location of the configuration file you want to import and select it.

Note:

You can only import .XML files into the Configuration Service.

4. Click **OK**.
5. The imported configuration displays in the Administration Console. You may change the default name in the Description Field of the information window.
6. Click **File > Save** to save the configuration. This action causes the configuration to remain in the Configuration Service when you close the application.

Note:

You can change the title of the configuration by opening it in the Administration Console, clicking on the title in the left pane to display the configuration information screen, and editing the description field.

5.2.6 Copying a Configuration

You can copy an existing configuration from Gimmel Link to another location.

Follow these steps to copy an existing configuration:

1. Launch the Gimmel Link Administration Console.
2. Select **Open** from the **File** menu. The Open Configuration dialog displays.
3. Select the configuration that you want to copy in the **Available Configurations** section.
4. Either right-click the configuration or click **Config** to display the drop-down menu and select **Copy**.

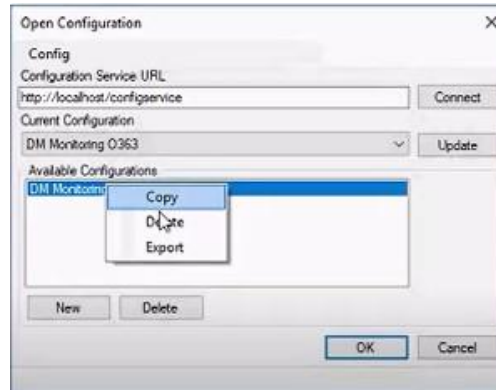


Figure 5-6 Copying a Configuration

A copy of the configuration displays in the **Available Configurations** section, with the format "Copy of <Name of copied configuration>".

Note:

You can change the title of the configuration by opening it in the Administration Console, clicking on the title in the left pane to display the configuration information screen, and editing the description field.

5.2.7 Deleting a Configuration

You can delete an existing configuration from Gimmel Link.

Follow these steps to delete an existing configuration:

1. Launch the Gimmel Link Administration Console.
2. Select **Open** from the **File** menu. The Open Configuration dialog displays.
3. Select the configuration that you want to delete in the **Available Configurations** section.
4. Either right-click the configuration or click **Config** to display the drop-down menu and select **Delete**.

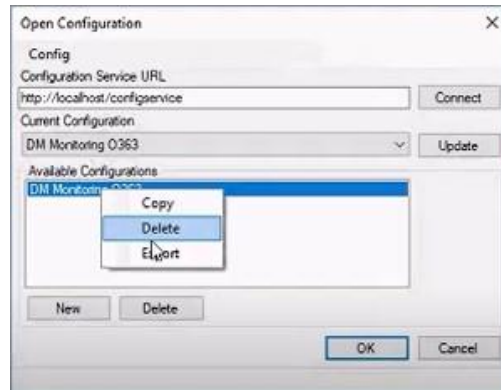


Figure 5-7 Deleting a Configuration

A confirmation dialog displays.



Figure 5-8 Confirm Deletion 5.

Click **Yes**. The Deletion Successful dialog displays.

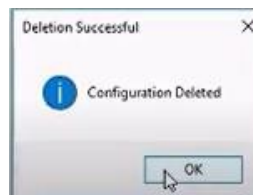


Figure 5-9 Deletion Successful

6. Click **OK**.

5.2.8 Exporting a Configuration

If you have created a configuration for Gimmel Link that you want to use in another application, you can export the configuration. This is also very useful for any troubleshooting or Service engagements, if they arise.

Follow these steps to export an existing configuration:

1. Launch the Gimmel Link Administration Console.
2. Click **File > Open**. The Open Configuration dialog displays.
3. Select the configuration that you want to export in the **Available Configurations** section.

4. Either right-click the configuration or click **Config** to display the drop-down menu and select **Export**.

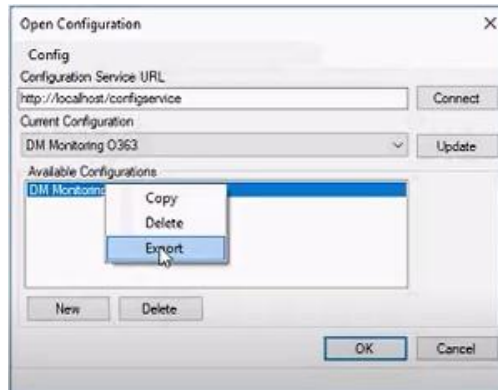


Figure 5-10 Selecting Export from the Config Drop-Down Menu

A file browser dialog opens.

5. Browse to the location you want to export the configuration file to.
6. Click **OK**.

5.3 Setting Event Logging

Event logging is very useful for troubleshooting. Event logging takes place during program execution in the security context of the SharePoint application. This term means that the process identity is that of the application pool hosting the SharePoint application (typically the SharePoint service account).

To set the Event logging level for all the Document Service Modules, follow these steps:

1. Launch the Gimmel Link Administration Console.

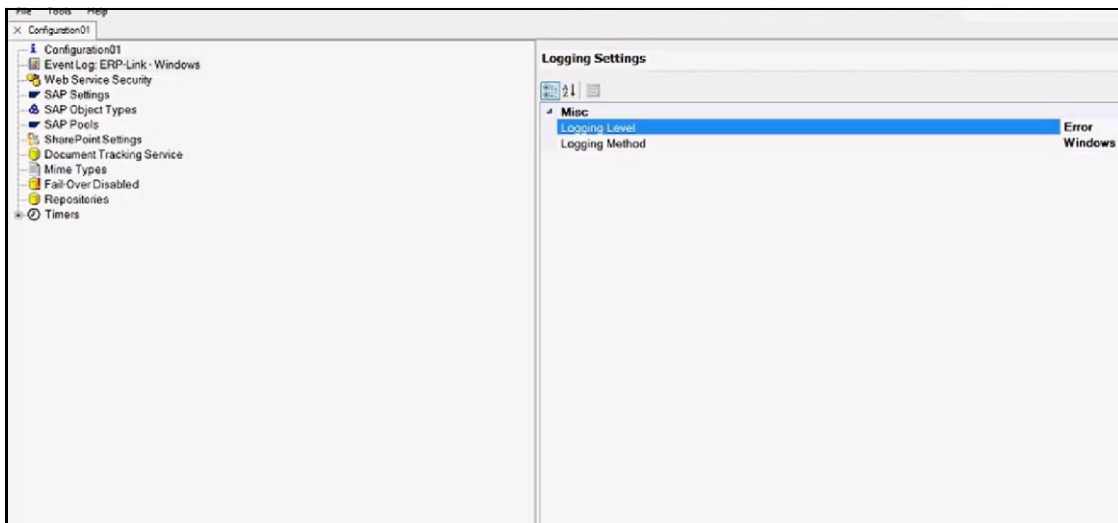


Figure 5-11 Example Event Log Settings Dialog Box

2. Click **Event Log: Gimmel Link - Windows** in the left pane.
3. Complete the information in the right pane. [Table 5-1](#) describes each field. *Table 5-1 Event Log Settings*

Field Title	Description
Logging Level	Can be set to define what types of events are logged
Logging Method	Specifies the method of logging that will be used. Currently only the Windows option is available to log to the Windows Event Viewer.

Note:

Recent versions of Windows have restricted access to the Windows Event Log. You must make sure that the appropriate process identity has full permissions to the event log and event source, or the Document Service Module fails with *Access Denied* errors when it attempts to write to the event log. Using `regedit`, navigate to the `HKLM\System\CurrentControlSet\Services\EventLog\\` registry key and ensure that the application pool identity has full access.

5.4 Configuring the Web Service Security Key

The Web Service Security Key is a common security key that is used for web service communication between Gimmel Link and the Connector Service and Document Tracking Service. It is a key that is known by both the sender and the receiver. If the key doesn't match what the receiver is expecting, the request is ignored. You must configure the Web Services Security Key for the Shared Connection Service and DTS to work properly.

Note:

You can find the Web Security Key in the Document Tracking Service `web.config` file. You can set this key as desired, as long as the field in the DTS `web.config` and the key field in the Administration Console match.

Follow these steps to configure Web Service Security for the Shared Configuration:

1. In the Gimmel Link Administration Console, select **Web Service Security** in the left pane. The Web Service Security information displays on the right.

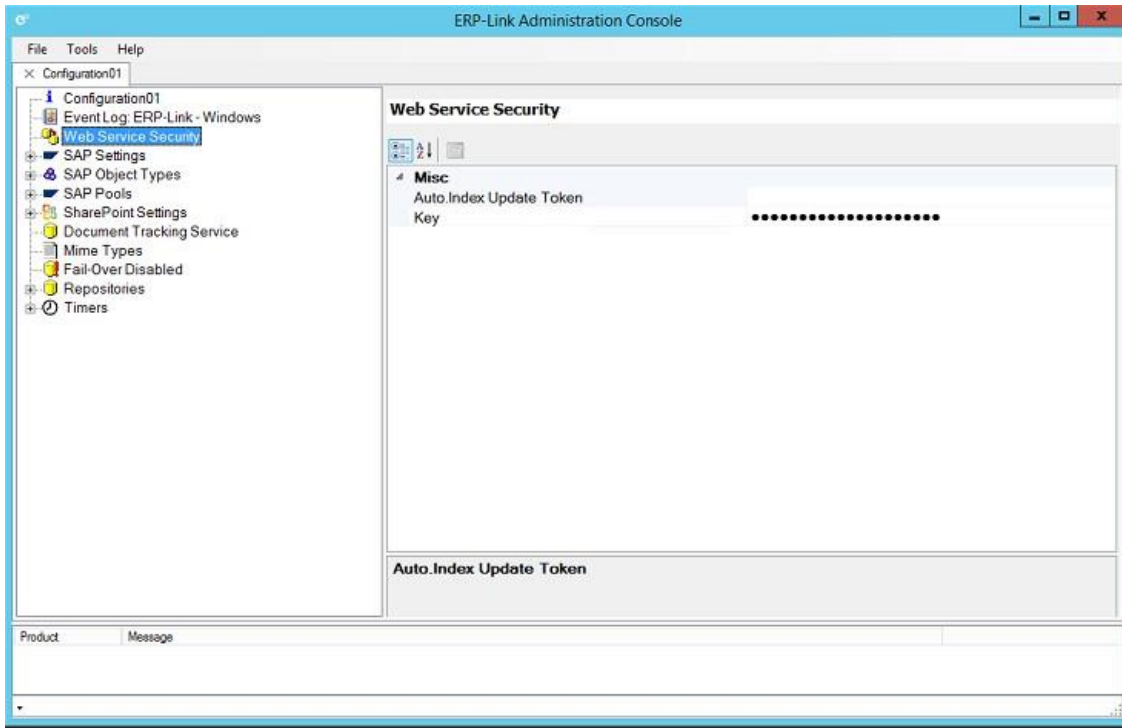


Figure 5-12 Entering the Web Service Security Key

2. Enter the **Key** to use for the shared connection service and DTS.

Note:

See Chapter [14 Configuring Auto.index Update Connection](#) for instructions on configuring the Auto.Index Update Token.

3. Click **Save**.

5.5 Defining SAP Pools, SAP Settings, and Object Types

This section describes how to define the SAP Pools, SAP Settings, and Object Types so you can establish the physical connection to SAP from Gimmel Link.

Note:

SAP Settings cannot be completely configured unless the SAP Pool(s) are configured.

5.5.1 Configuring SAP Pools

Follow these steps to configure an SAP Pool. You can configure multiple pools if you have multiple SAP environments.

1. From the Gimmel Link Administration console, right-click **SAP Pools** and then click **Add SAP Pool**.

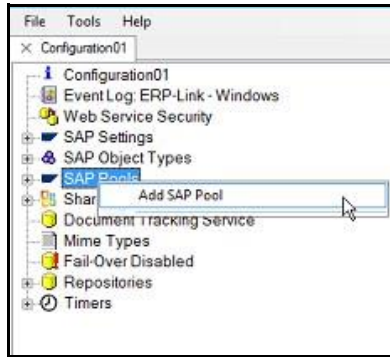


Figure 5-13 Selecting SAP Pools

The SAP Pool Information pane displays on the right, along with five sections that contain various properties. These properties are described in the tables below.

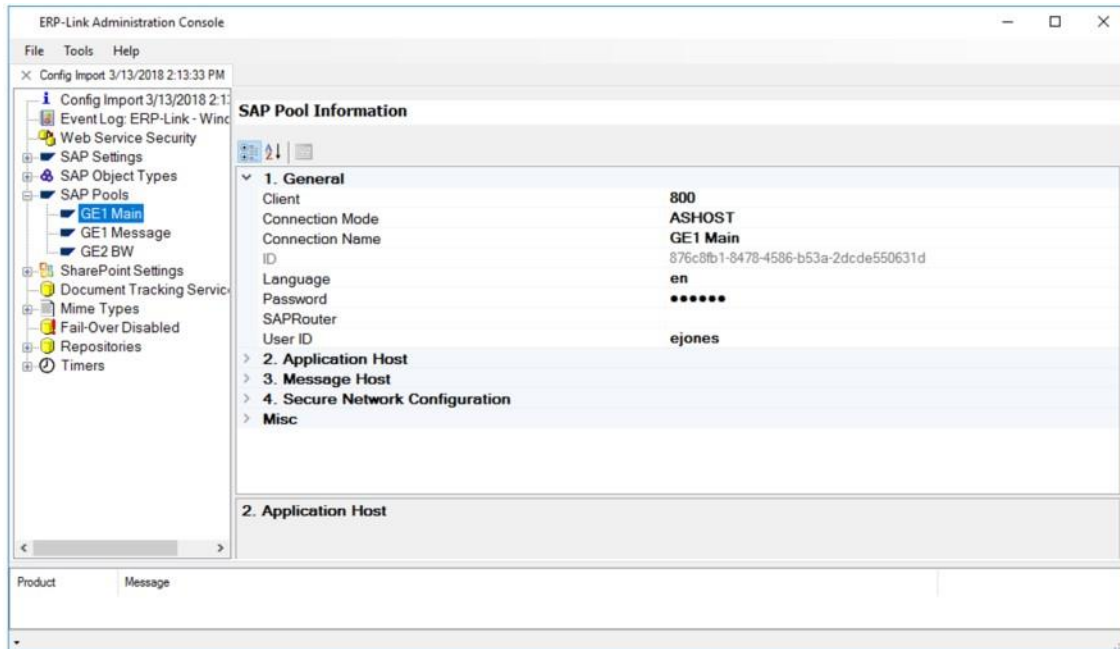


Figure 5-14 SAP Pool Information - **General** Properties

2. Expand the **General** section and complete the fields as required. [Table 5-2](#) describes the properties.

Table 5-2 SAP Pool Information – General Properties

Property	Description
Client	Three-digit SAP client number
Connection Mode	<p>ASHOST = The pool specifies a connection to an application host and expects the values under the Application Host properties (after General section) to be specified</p> <p>MSHOST = The pool specifies a connection to a message host and expects values under the Message Host properties (after Application Host section) to be specified</p>
Connection Name	Unique connection name, describing the connection pool
ID	Read-only field that displays the identifier for the connection pool
Language	The standard language abbreviation for the language set up in your SAP environment
Password	Password that corresponds to the user ID entered below for your SAP environment
SAPRouter	If the connection needs to be made through a firewall via an SAPRouter, specify the SAPRouter parameters here
User ID	The user ID to use when the pool connects to your SAP environment

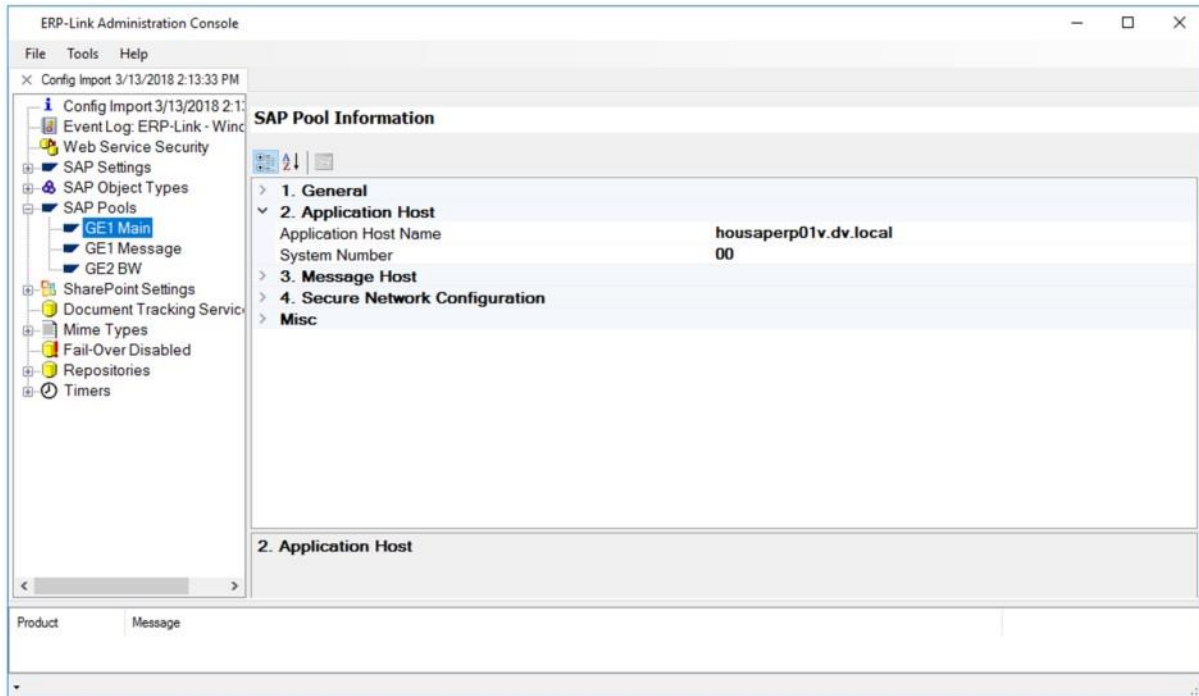


Figure 5-15 SAP Pool Information - **Application Host** Properties

- Expand the **Application Host** section and complete the fields as required. [Table 5-3](#) describes the parameters.

Note

The Application Host fields apply only if the **Connection Mode** is set to **ASHOST**. (See step #2 above.)

Table 5-3 SAP Pool Information – Application Host Properties

Property	Description
Application Host Name	The host name or IP address of the SAP application host to be used
System Number	The system number for the SAP application host

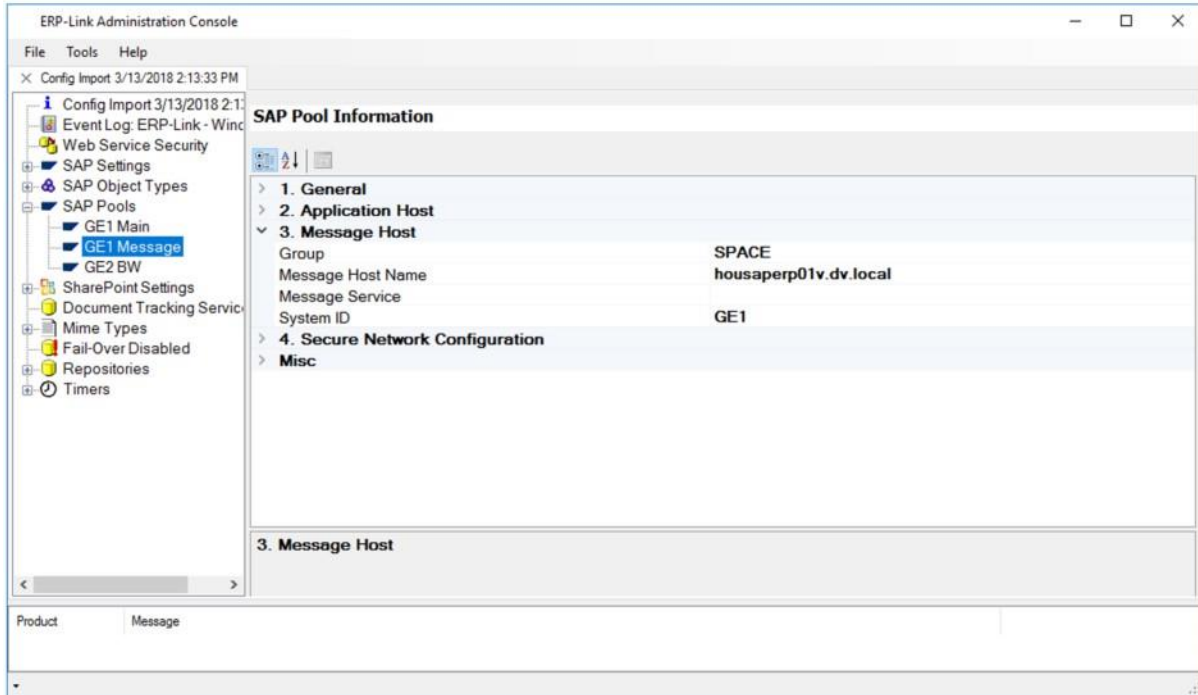


Figure 5-16 SAP Pool Information - **Message Host** Properties

- Expand the **Message Host** section and complete the fields as required. [Table 5-4](#) describes the parameters.

Note

The Message Host fields apply only if the **Connection Mode** is set to MSHOST. (See step #2 above.)

Table 5-4 SAP Pool Information – Message Host Properties

Property	Description
Group	The logon group for connecting to the SAP Message Server
Message Host Name	The host name or IP address for the message server
Message Service	The service name or the port number that the message server is listening to for load-balancing requests; can be omitted if System ID is specified

System ID	The SAP system's three-letter system ID
-----------	---

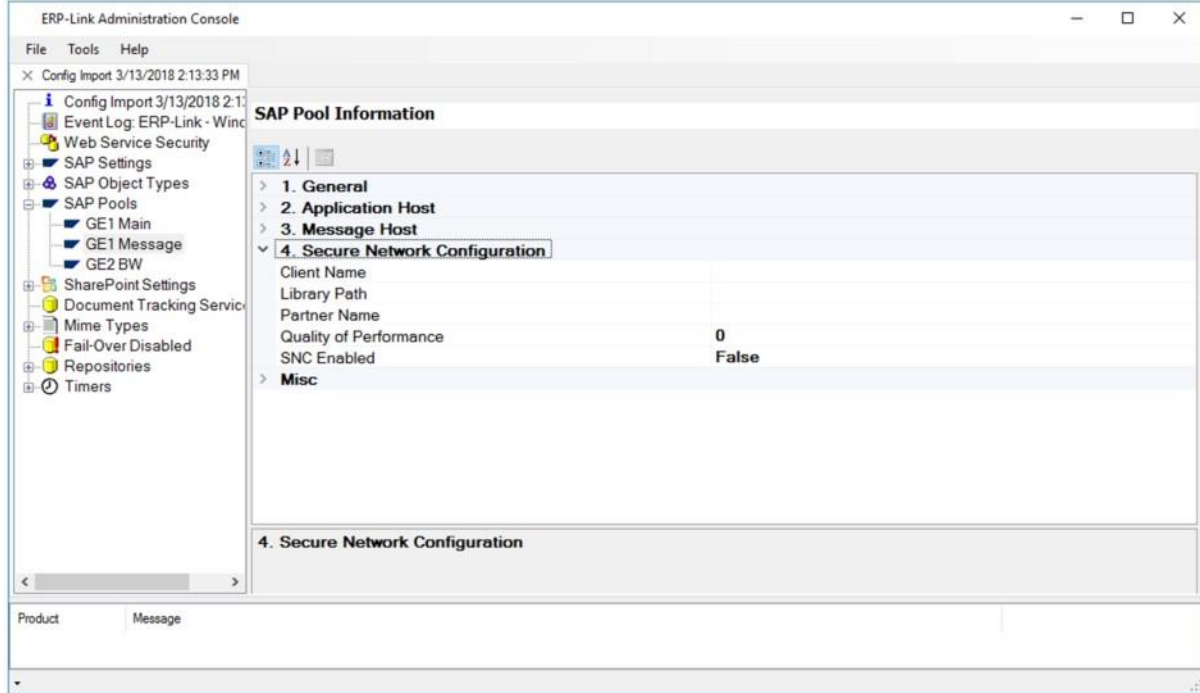


Figure 5-17 SAP Pool Information - **Secure Network Configuration** Properties

- Expand the **Secure Network Configuration** section and complete the fields as required. [Table 5-5](#) describes the parameters.

Table 5-5 SAP Pool Information – **Secure Network Configuration** Properties

Property	Description
Client Name	Appropriate string for the connection user
Library Path	Full path and name of the SNC shared library to be used
Partner Name	The back end's SNC name

<p>Quality of Performance</p>	<p>The Quality of Service to be used for SNC communication of this particular destination/server; use one of the following values:</p> <p>0 = No SNC security 1 = Digital signature 2 = Digital signature and encryption 3 = Digital signature, encryption, and user authentication 8 = Default value defined by back-end system 9 = Maximum value that the current security product supports</p>
<p>SNC Enabled</p>	<p>"True" indicates the connection pool will attempt to encrypt communications to SAP through the Secure Network Configuration (SNC)</p>

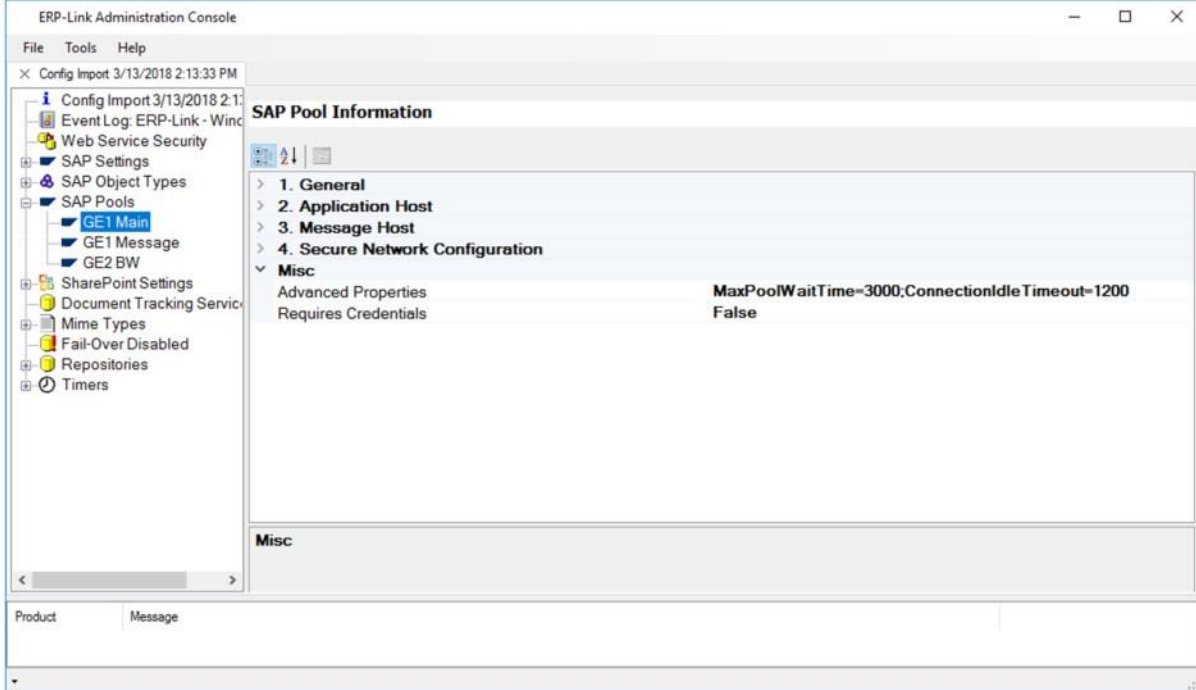


Figure 5-18 SAP Pool Information - **Misc** Properties

- Expand the **Misc** section and complete the fields as required. Table 5-6 describes the parameters.

Table 5-6 SAP Pool Information – Misc Properties

Property	Description
<p>Advanced Properties</p>	<p>Allows specification of additional connection parameters supported by the SAP .NET Connector 3.0 API via a semi-colon delimited name=value string. For more information, see the following SAP support page: https://support.sap.com/en/product/connectors/msnet.html</p>

Requires Credentials	True/False setting usually set to False. Typically only set to True if you have additional connection settings for custom applications and want to require that they provide alternate credentials at runtime to connect to SAP
----------------------	---

5.5.2 Defining SAP Settings

SAP settings are used to define Connection Services to SAP that are used by the Document Service Modules. Each connection should be uniquely named so it can be differentiated in the configuration process.

Note

Each content repository must refer to a single SAP environment.

To add SAP settings, follow these steps:

1. Right-click **SAP Settings** > **Add SAP Setting**.
2. Select the newly created setting. The fields on the right appear.

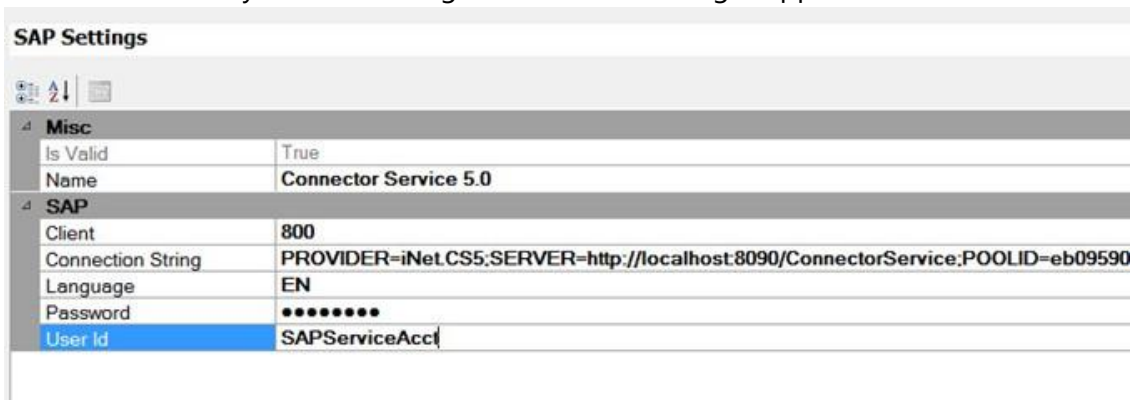


Figure 5-19 SAP Settings Pane

3. Complete the fields in the right pane. [Table 5-7](#) describes the parameters.

Table 5-7 SAP Settings

Field Title	Description
IsValid	Indicator of the validity of the connection. Defaults to "False" and changes to "True" when setting is successfully configured.
Name	The name of the SAP setting.
Client	Three-digit SAP client number.

Table 5-7 SAP Settings

Field Title	Description
<p>Connection String</p>	<p>The iNet.CS connection string to the target SAP system, consisting of the name of the server hosting the iNet.CS remote connection server and the connection pool to use when communicating with it.</p> <p>The Connection String property can be directly entered in this field, or you can use the Select Connection Pool dialog box to configure the string and test the connection to the database.</p> <p>To display the Select Connection Pool dialog box, click the ellipses at the right of the Connection String field.</p> <div data-bbox="597 583 1279 1388" data-label="Image"> </div> <p style="text-align: center;"><i>Example Select Collection Pool Dialog Box</i></p> <p>The following rows describe the fields in this dialog box.</p>

Table 5-7 SAP Settings

Field Title	Description
-------------	-------------

Provider	<p>The iNET Connection service provider version installed with the iNet Connection Service.</p> <p>The menu displays only providers that have been installed. The iNET Connection service provider iNETCS.5 is installed with Gimmel Link 5.1.</p> <p>The iNETCS3.1 continues to be supported in Gimmel Link 5.1.</p> <p>The iNETCS2 and iNETCS3 connection providers are no longer supported and have been removed.</p>
Server	<p>After you select the Provider, this field displays. Enter the URL of the Connection Service, for example: http://YourServerURL/ConnectionService.</p>
Connect	<p>After you select the Provider, this field displays. Click Connect to connect to the selected remote machine. The Select Pool field populates with options.</p>
Select Pool	<p>Expand the tree and select the correct SAP Pool ID.</p>
Description	<p>This field is populated when a connection pool is selected from the available connection pools.</p>
Client, User, Password, and Language	<p>All this data was entered when the connection service was set up in Gimmel Link Connection Service and you cannot change it or add it here or in the right pane of the primary window.</p>

5.5.3 Adding SAP Business Object Types

Any SAP business object types that the Document Service Modules reference must be added to the SAP Object Types. To configure the SAP business object types, follow these steps.

1. Right-click **SAP Object Types** in the left pane and from the context menu select **Add SAP Object Type**.
2. Enter the **SAP Object Type** and **Description** (optional). [Table 5-8](#) describes the fields.

Table 5-8 Add SAP Business Object Dialog Box Settings

Field Title	Description
SAP Business Object type	The SAP business object type that is available to the Document Service Modules as a remote function call.
Description	An optional description of the SAP business object type; for example, <i>Financial document</i> .

3. Click **OK**.

5.6 Defining SharePoint Settings

To define a SharePoint connection that is available to use in Gimmel Link processes, follow these steps.

1. Right-click the **SharePoint Settings** option in the left pane and select **Add SharePoint Connection** from the context menu. A new node displays under SharePoint Settings, indicating that you must enter a connection name.
2. Click the new connection tree node.
3. Enter the information. [Table 5-9](#) explains the options. *Table 5-9 SharePoint Connection Settings*

Field Title	Description	
Connection name	A description for this connection that reflects the type of connection (Scan.link, Auto.index, etc.). This name must be unique.	
Select mode of operation	SSOM on SharePoint Web Front End	Server Side Object Model on SharePoint Web Front End. Gimmel Link.NET assemblies are deployed to the Global Assembly Cache on each SharePoint server. Supported for on-premise SharePoint deployment only. Revision history of a document routed by Auto.index is preserved only in this mode.
	CSOM using local authentication	Client-Side Object Model calls that authenticate to a local SharePoint instance using elevated privileges. This mode can be used to support an on-premise implementation of SharePoint 2016.
	CSOM using claims-based authentication*	Client Side Object Model using claims-based authentication for O365-based SharePoint repository. Revision history of a document routed by Auto.index is not preserved in this mode. When using CSOM with Claims-based authentication in the Misc pane, enter the Clientid and ClientSecret that you saved from the installation of the SharePoint app.
	CSOM using certificatebased authentication*	Client-Side Object Model using certificate-based authentication for on-premise or Azure-hosted SharePoint repository. Revision history of a document routed by Auto.index is not preserved in this mode.
Client ID	Gimmel Gimmel Link.app Client ID. Used when installing the Gimmel Gimmel Link SharePoint App.	

Table 5-9 SharePoint Connection Settings

Field Title	Description
Client Secret	Gimmel Gimmel Link.app Client Secret. Used when installing the Gimmel Gimmel Link SharePoint app.
Certificate Password	Client signing certificate password for certificate-based authentication
Certificate Path	Client signing certificate path for certificate-based authentication
Issuer ID	Issuer ID for certificate-based authentication
Request Timeout**	Request timeout (in milliseconds) for CSOM requests.

4. Save your changes.

*Important!

When using CSOM claims-based authentication or certificate-based authentication, you must have a different SharePoint setting for each SharePoint Online tenant (if using claims-based authentication) or SharePoint farm (if using certificate-based authentication).

**Note

IIS limits the maximum size of a request which imposes a limitation on the maximum file size that can be uploaded and processed by Gimmel Link. During installation of the Gimmel Link components, the IIS request limits are set to the following. These values can be changed post-installation by editing the request limits located in the IIS Manager at **<Site> > Request Filtering > Edit Feature Settings**. They can also be changed by editing the requestLimits section of the web.config file for the site directly.

Maximum allow content length: 2147483647

Maximum URL length: 4096

Maximum query string: 2048

SharePoint and SAP have their own limitations that differ, depending on the version of SharePoint or SAP being used. These limitations are outside of Gimmel's control.

5.7 Configuring the Document Tracking Service

The Document Tracking Service tracks the location of a document through the document lifecycle. For technical details, refer to [Appendix C Gimmel Document Tracking Service](#).

Note:

Set up of the Document Tracking Service database is now handled automatically through the Gimmel Link installation process. If you would like to configure DTS manually, you may perform the following steps

5.7.1 Manually Configuring Microsoft SQL Server as Database Provider

Follow the steps in the sections below to configure Microsoft SQL Server as the database provider and set it up for the Document Tracking Service in Gimmel Link.

- [Configuring Microsoft SQL](#)
 - [Creating Document Tracking Service Database in SQL](#)
 - [Creating Tracking Service Table with SQL Script](#)
 - [Assigning Permissions on SQL Database](#)
- [Entering the Tracking URL](#)

Creating Document Tracking Service Database in SQL

The Document Tracking Service database can be hosted on SQL versions 2012 and later. The database name can be set to whatever value required by your organization.

- Use the SQL server to configure the database as shown in [Figure 5-20](#)

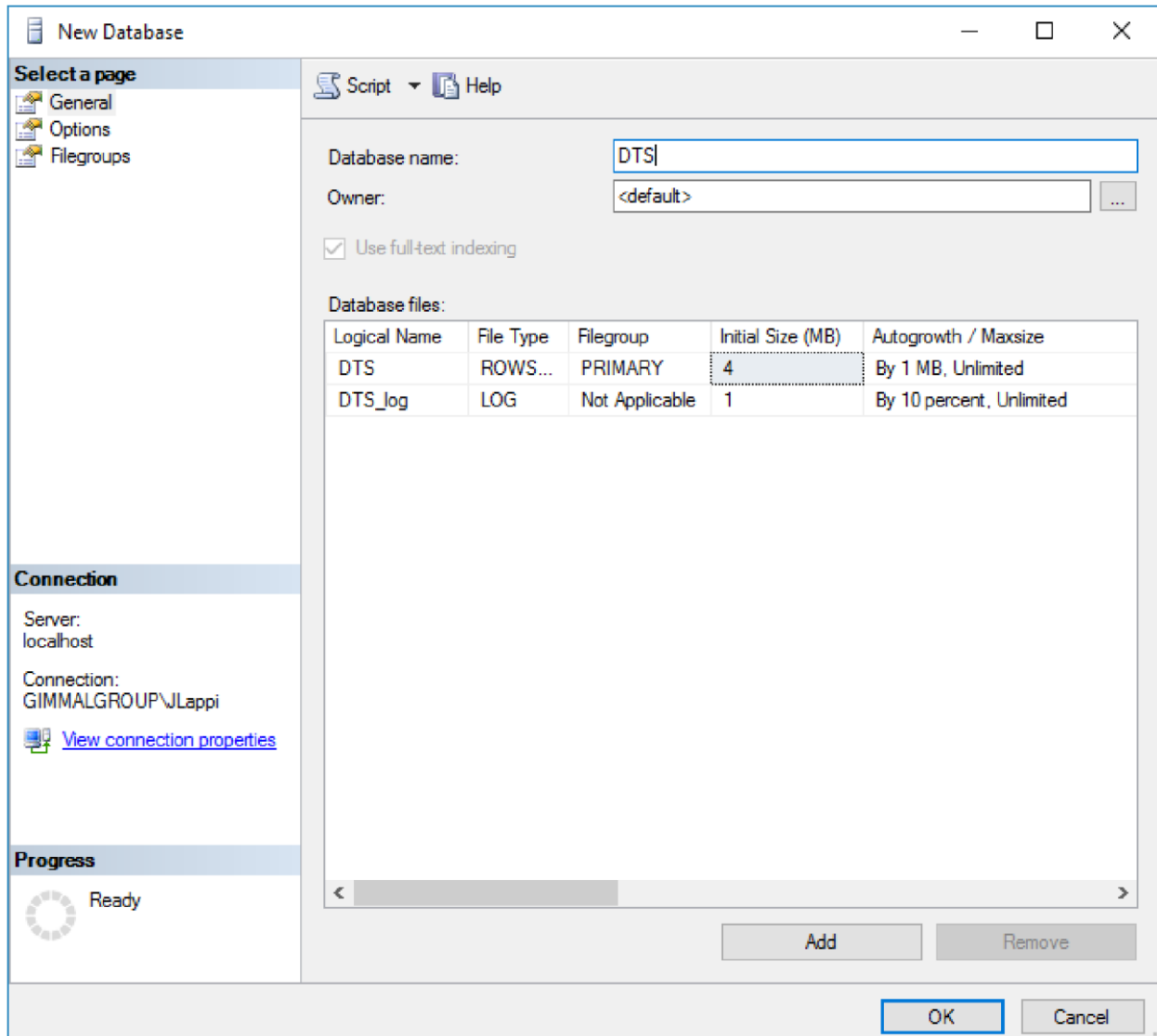


Figure 5-20 Configuring a Document Tracking Service Database in SQL

Creating Tracking Service Table with SQL Script

The Document Tracking Service table creation script is located at `C:\Program Files\Gimmel\DTS\scripts` when the default installation path is used.

- Execute this script to create the table for DTS.

Note:

This table name cannot be changed.

When you execute the script, it creates a table for the DTS database called *TrackingDetails*. The table contains the following columns:

- **ID**: Unique identifier for a particular row
- **Application ID**: Application key of the application using the service.
- **Url**: Current location of the document
- **Key1 (required)**: Used to identify the document
- **Key2 (required)**: Used to identify the document
- **Key3 (required)**: Used to identify the document
- **Key4 (required)**: Used to identify the document
- **Key5 (required)**: Used to identify the document
- **History**: Contains the history of document movements
- **Information**: Contains information used by Gimmel Link
- **LastModifiedDate**: Timestamp of last update

Assigning Permissions on SQL Database

SQL permissions can be set to either use Integrated Security or SQL user authentication.

When using Integrated Security, the configured user for the Document Tracking Service IIS application pool must be set to a user that has at least data reader and data writer authorization. This account can be a domain level account if necessary. The following figures demonstrate correct configuration. For additional information, see <https://msdn.microsoft.com/en-us/library/bsz5788z.aspx>.

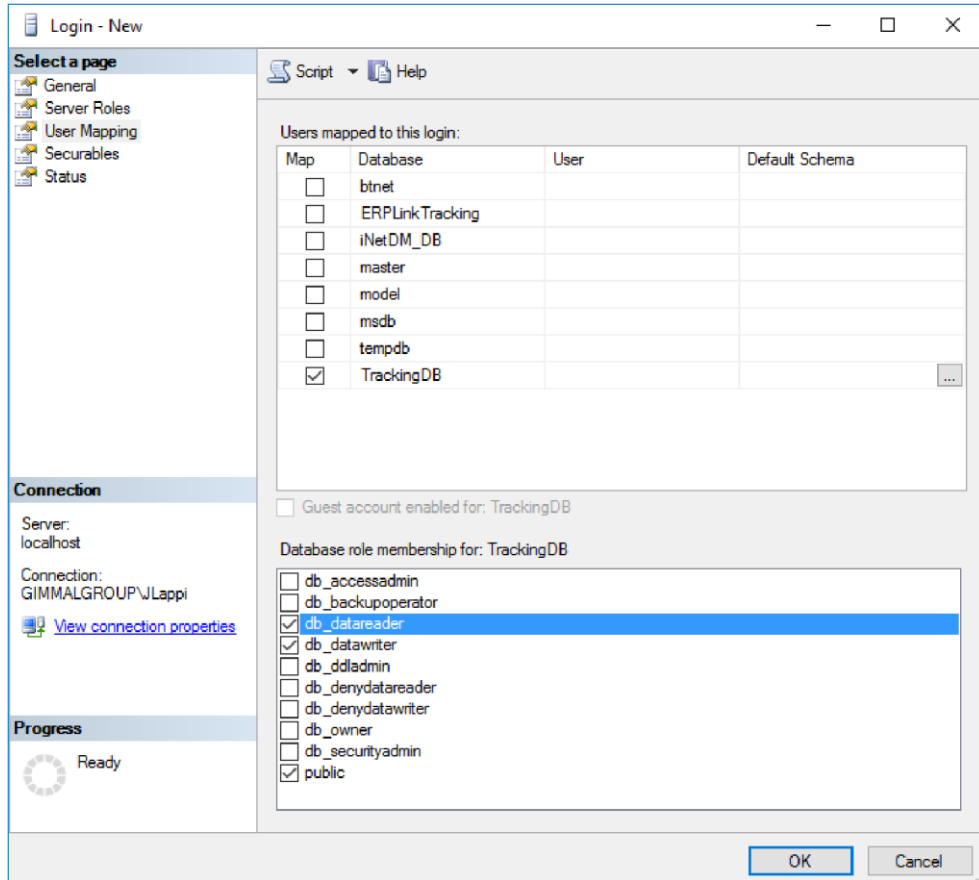


Figure 5-21 Setting Data Reader and Data Writer Permissions

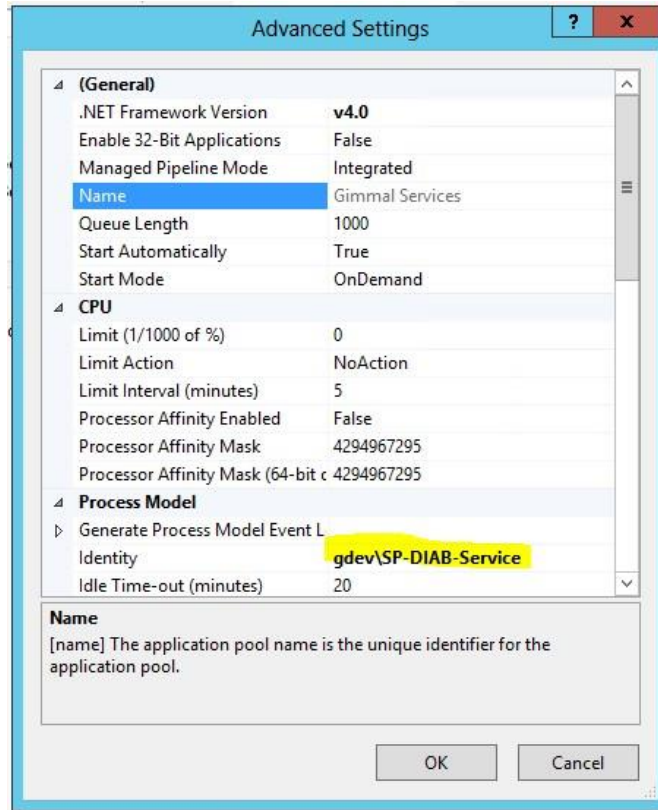


Figure 5-22 Setting IIS Application Pool Advanced Settings to Use Domain-Level Account

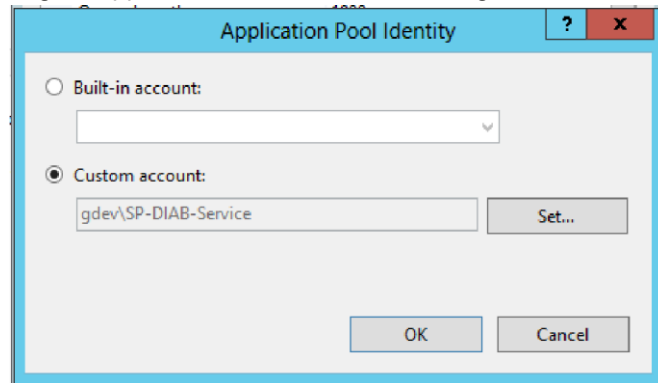


Figure 5-23 Setting Application Pool Identity

Configuring Microsoft SQL Server as Database Provider for Document Tracking Service

To configure your Document Tracking Service, follow these steps.

1. Open the web.config file for the Document Tracking Service. (The file is located, by default, at C:\Program Files\Gimmel\DTS\Web Files.)
2. Find the ConnectionString and enter the following parameters:

- a. **Server** - the SQL server the Document Tracking Service database is located on
 - b. **Database** - the name of the Document Tracking Service database
 - c. **User Id** - the SQL username used to connected to the database
 - d. **Password** - the password for the SQL user Id
 - e. **Persist Security Info** - this should always be set to "False"
 - f. **Trusted Connection** - should be set to true if using integrated security
 - i. This is only required with integrated security, if this is set to "True" no User ID or Password is required.
3. Save the web.config file.

Note

Before you proceed to the next section, refer to section [5.4 Configuring the Web Service Security Key](#) to update the web security key.

5.7.2 Entering the Tracking URL

Gimmel Link supports multiple tracking connections in the Administration Console. To add a new connection, follow these steps.

1. Launch the Gimmel Link Administration Console.
2. Click the **Document Tracking Service** node in the left pane. The Document Tracking Service screen displays.

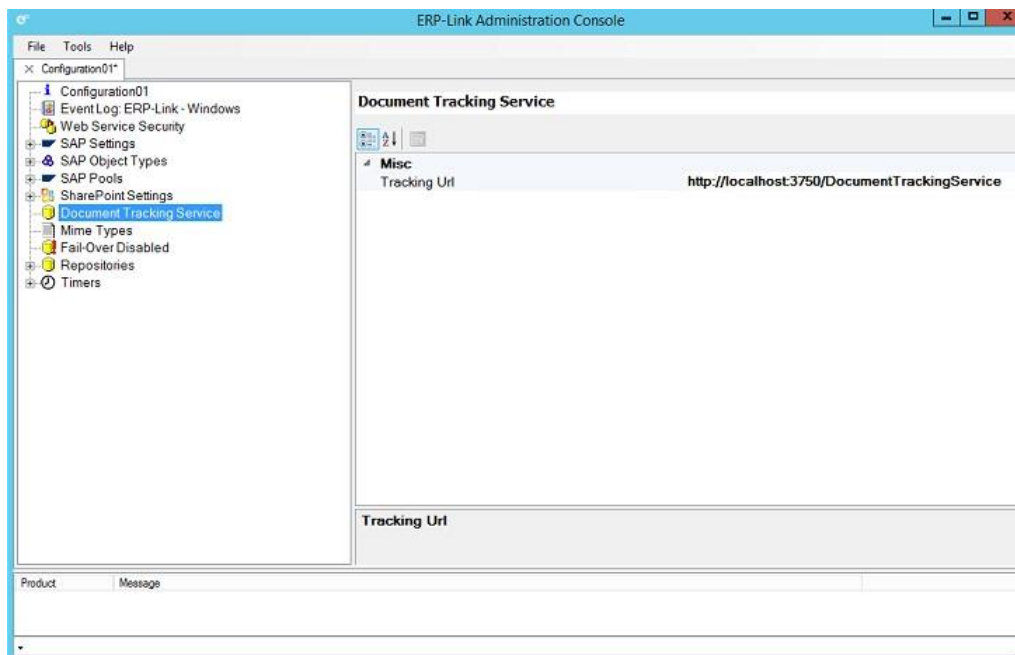


Figure 5-24 Enter the Tracking URL

3. Click in the **Tracking Url** field on the right side and enter the URL for the tracking service.
4. Save the configuration file.

5.7.3 Verifying the Document Tracking Service Connection

To verify the Document Tracking Service (DTS) connection to the database, perform the following steps:

1. Enter the URL to the DTS website.
2. Verify that the Connection Test field is Successful. If the connection test fails, repeat the steps in sections [“Configuring Microsoft SQL Server as Database Provider for Document Tracking Service”](#) on page 96 and [“Entering the Tracking URL”](#) on page 97.

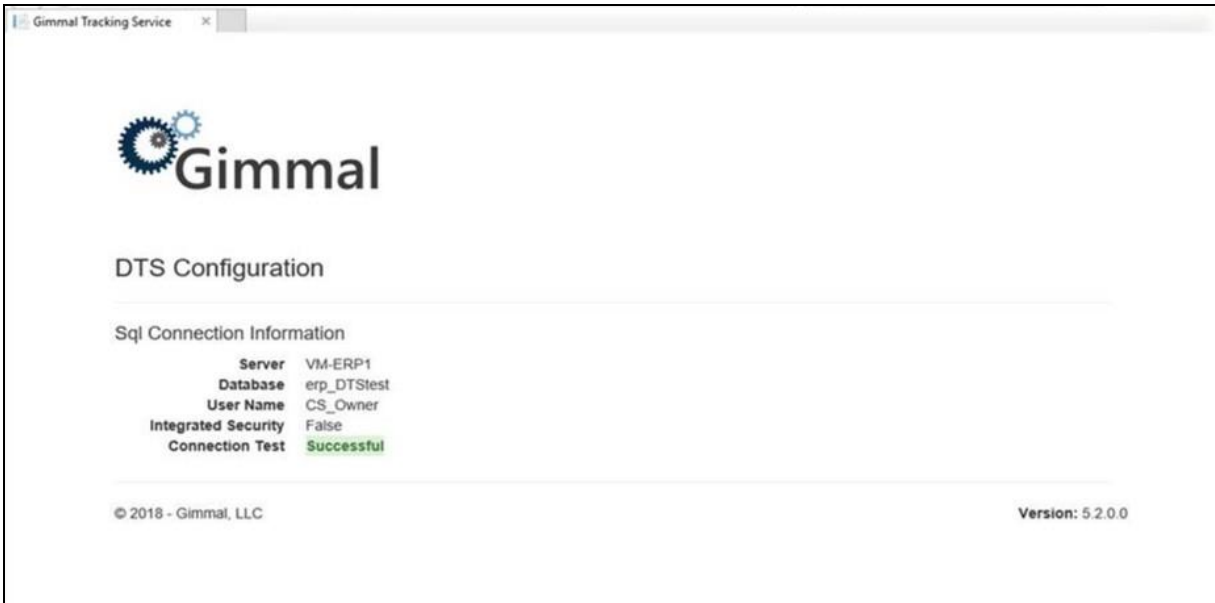


Figure 5-25 Successful DTS Connection

5.8 Verifying the Connection Service

After configuring the SAP Settings and SAP pools, you can verify the configuration of the Connection Service by issuing a ping from the Connection Service Web application to the configured SAP system.

Navigate to the Connection Service URL in the browser; for example, <https://yourserverurl/ConnectionService>.

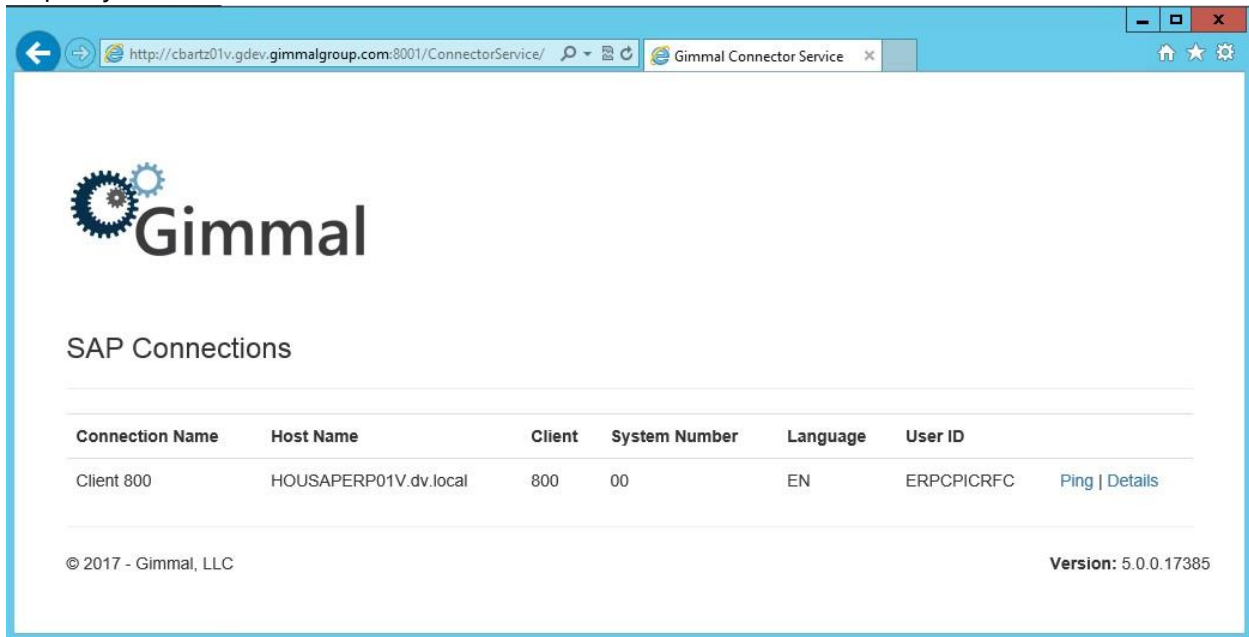


Figure 5-26 Connection Service Page Displaying SAP Connections

3. Click the **Ping** link in the **Gimmal SAP Connections** page. The **Ping Results** page displays.

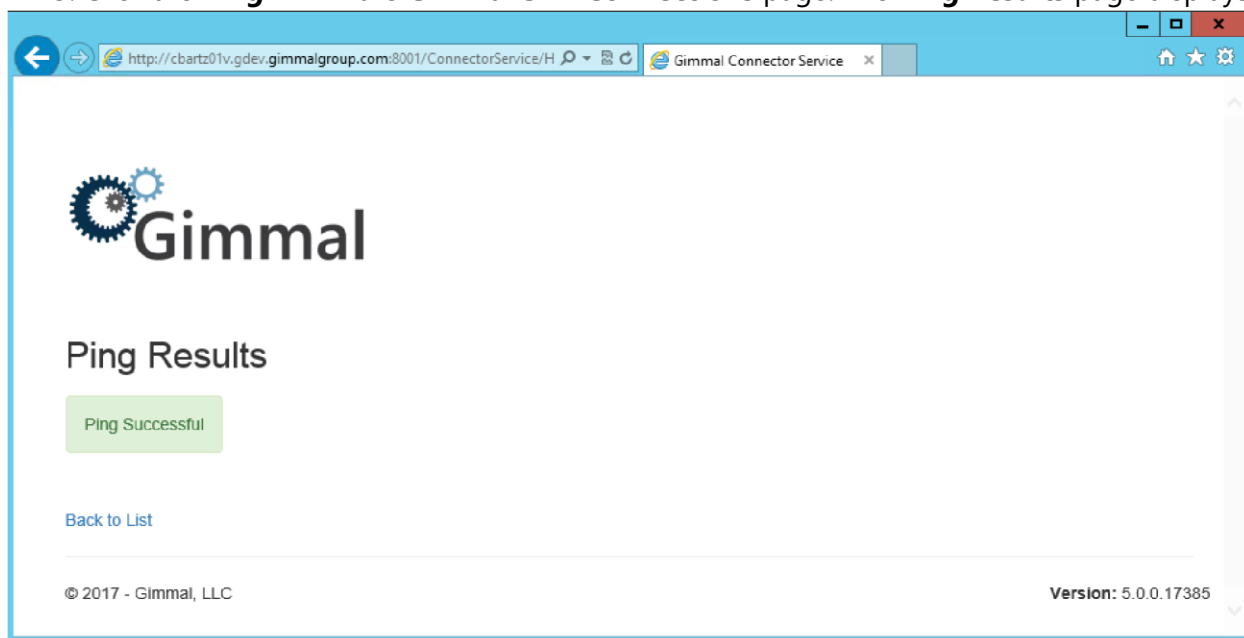


Figure 5-27 Ping Results

The **Connection Service** page displays the SAP Connections configured in the Gimmal Link SAP Settings.

If the ping is unsuccessful, refer to Chapter [5.1 Configuring the Connection Service](#) and Appendix [B Gimmal Connection Service](#).

For technical information about the Gimmal Link Connection Service, refer to Appendix [B Gimmal Connection Service](#).

For the remaining settings in the Administration Console: **Repositories**, **Fail-Over**, and **Timers**, see the following chapters:

- [6 Configuring Content Repositories](#)
- [7 Configuring CloudGate Failover Service](#)
- [16 Configuring the Gimmal Link Timer Service](#)

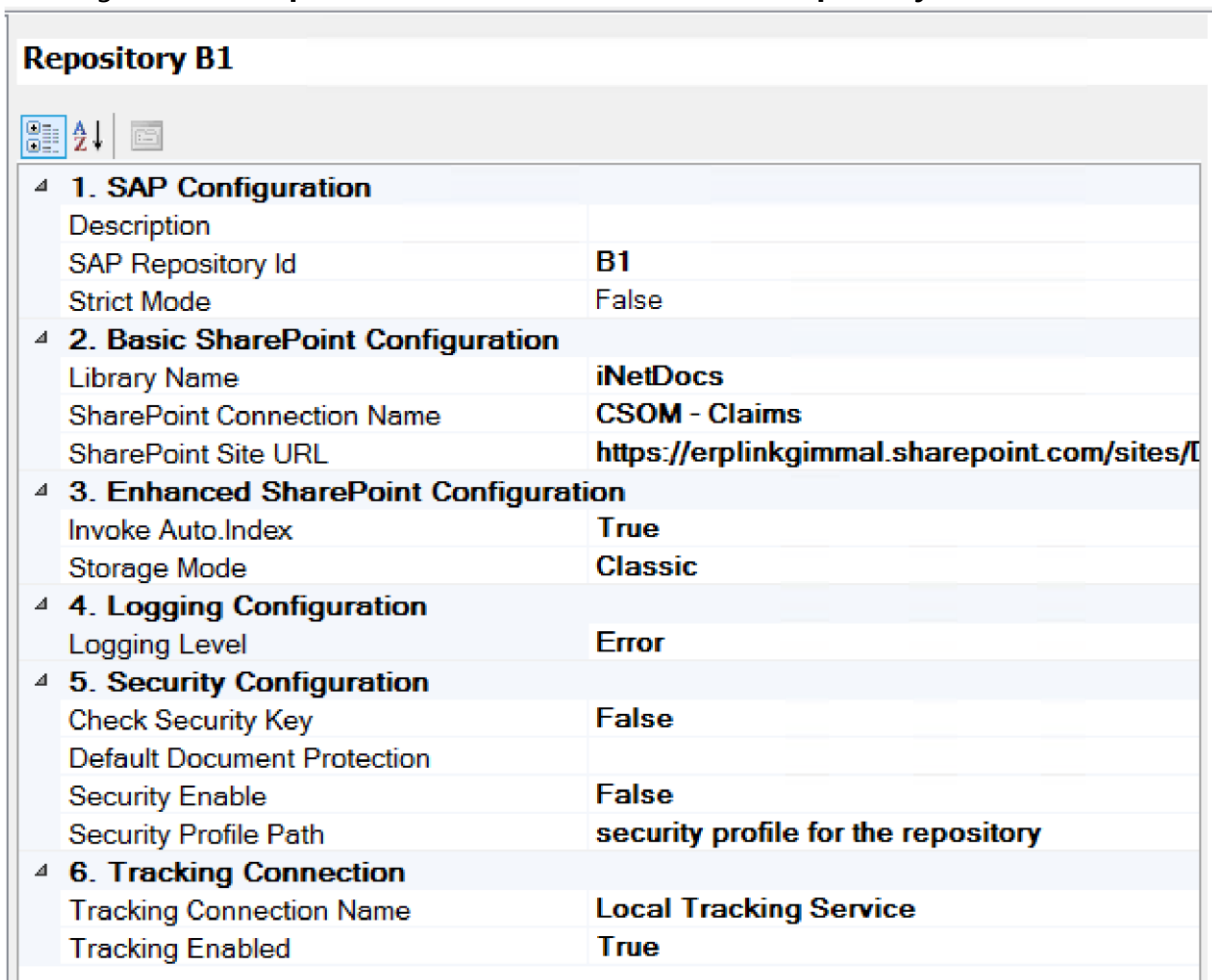
6 Configuring Content Repositories

This section contains steps for configuring Gimmel Link Document Manager with the Gimmel Link Administration console.

6.1 Configuring a Content Repository

Follow these steps to configure the Gimmel Link Document Manager content repository:

1. From the Gimmel Link Administration Console, with the current configuration open, rightclick the **Repositories** node and select **Add New Repository**.



The screenshot shows a configuration window titled "Repository B1" with a toolbar at the top. The configuration is organized into six numbered sections, each with a collapse/expand icon (a small triangle) to its left. The sections and their parameters are as follows:

1. SAP Configuration	
Description	
SAP Repository Id	B1
Strict Mode	False
2. Basic SharePoint Configuration	
Library Name	iNetDocs
SharePoint Connection Name	CSOM - Claims
SharePoint Site URL	https://erplinkgimmel.sharepoint.com/sites/
3. Enhanced SharePoint Configuration	
Invoke Auto.Index	True
Storage Mode	Classic
4. Logging Configuration	
Logging Level	Error
5. Security Configuration	
Check Security Key	False
Default Document Protection	
Security Enable	False
Security Profile Path	security profile for the repository
6. Tracking Connection	
Tracking Connection Name	Local Tracking Service
Tracking Enabled	True

Figure 6-1 Setting Up a Repository in the Gimmel Link Administration Console

2. Click the newly created repository node and in the right pane enter the following parameters.

Table 6-1 Repository Parameters

Field Title	Description
Description	The detailed description of the content repository.
SAP Repository ID	This SAP Content Repository ID for the repository being configured, for example, <i>B1</i> .
Strict Mode	The default is False to improve archive performance. If the value is True , a document retrieval is performed after archiving a document to validate the archival. Enabling Strict Mode is useful for archive validation and certification, but should be disabled to improve archive performance because the document retrieval increases the overall archive time.
Library Name	The name of the primary SharePoint library associated with the content repository.
SharePoint Connection Name	Select a configured SharePoint connection that will be used for all operations for the content repository.
SharePoint Site URL	The URL of the SharePoint site that contains the library specified in the Library Name property.
Invoke Auto.Index	<p>Specifies whether to execute the Auto.index configuration if it is configured for the content repository. This allows for an easy way to disable the Auto.index capability without having to remove the configuration completely.</p> <hr/> <p>Note:</p> <p>This entry should only be turned on for installations that have Enterprise licensing and have a configured Auto.index configuration for the content repository.</p> <hr/>
Storage Mode	<p>Specifies whether to use <i>Classic</i> or <i>Flat</i> storage modes for archiving documents in a content repository.</p> <ul style="list-style-type: none"> ● Classic storage leverages foldering for storing all documents. The folder name will leverage the SAP Document ID. ● Flat storage will store all documents at the root level of the content repository. If this is selected, all document libraries used by the content repository should have the x-Docid column index applied to them.

Logging Level	Specifies the logging level to utilize for archival and retrieval processes against the content repository. The values that can be specified include <i>Information</i> , <i>Warning</i> , and <i>Error</i> .
---------------	---

Table 6-1 Repository Parameters

Field Title	Description
Check Security Key	Specifies whether to enable usage of the SAP security certificates to prevent unauthorized access.
Default Document Protection	If SAP does not provide a document protection property on archival or update, the default document protection value configured in this setting is used. The Document Protection value can be any combination of <i>c</i> (Create), <i>r</i> (Read), <i>u</i> (Update), or <i>d</i> (Delete).
Security Enable	Specifies the security status on the SAP repository. If security is enabled in the SAP environment, then this field should be set to <i>True</i> ; otherwise, it should be set to <i>False</i> . Refer to 6.2 Configuring a Repository for SAP Security .
Security Profile Path	Specifies the full path and filename to the security certificate that is specific for the content repository.
Tracking Connection Name	Specifies the configured Document Tracking Service connection to use for logging tracking entries for the content repository.
Tracking Enabled	Specifies whether to enable saving of tracking entries to the Document Tracking Service.

3. From the **File** menu, select **Save**.

6.2 Configuring a Repository for SAP Security

This section describes how to use iNet.DM's SAP security integration in conjunction with an SAPSECU encryption certificate.

1. Create a folder named *c:\SAPCert*.
2. Set permissions on the folder.

The account iNet.DM runs under must be able to modify files in this directory. In the example below, **Authenticated Users** have *Modify* access. The access can be more restricted, but this level should work.

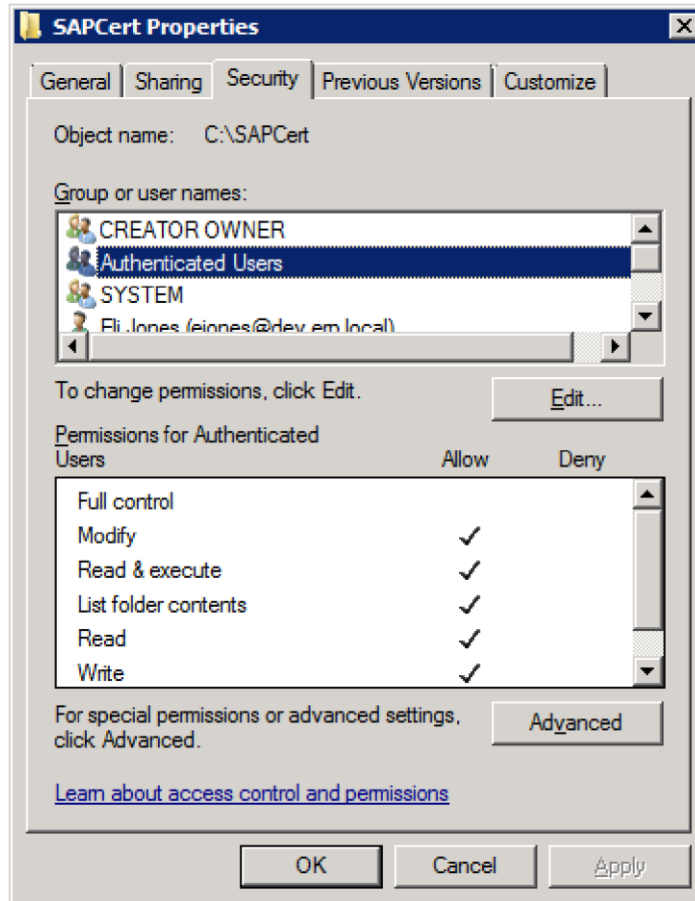


Figure 6-2 Security Settings

3. Open the current configuration in the Gimmel Link Administration Console.

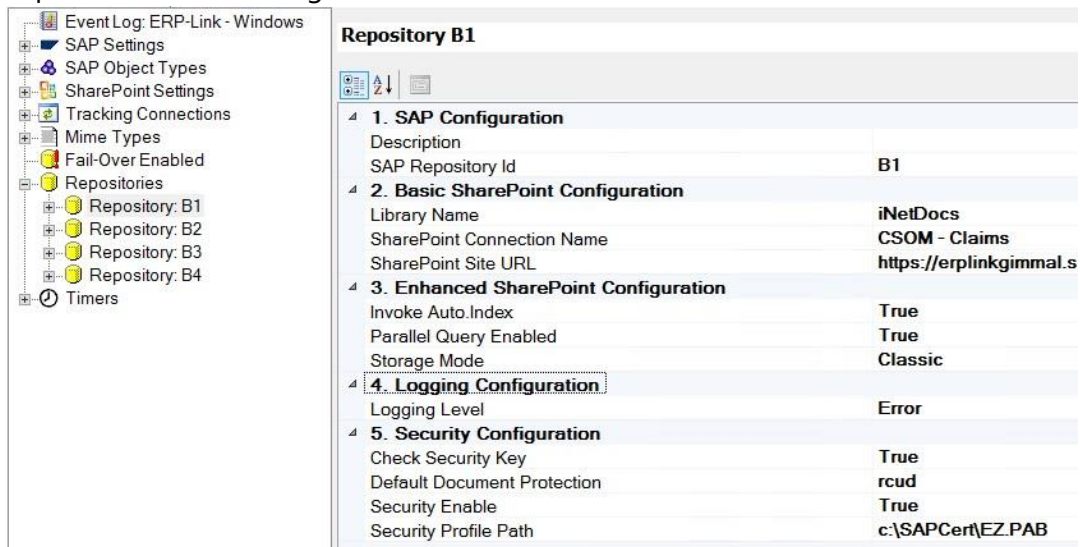


Figure 6-3 Editing Configuration File

4. In the left pane, click the repository that you want to set the parameters for and then in the right pane set the following values for that repository:
 - **Check Security Key** = *True*
 - **Default Document Protection**= *rcud*
 - **Security Enable** = *Yes*
 - **Security Profile Path**: The path and filename for the security certificate. In this example, we specified the directory created in Step 1, the content repository ID as the filename, and PAB as the extension.
5. Save the configuration file and restart iNet.DM.
6. Open the content repository in SAP.

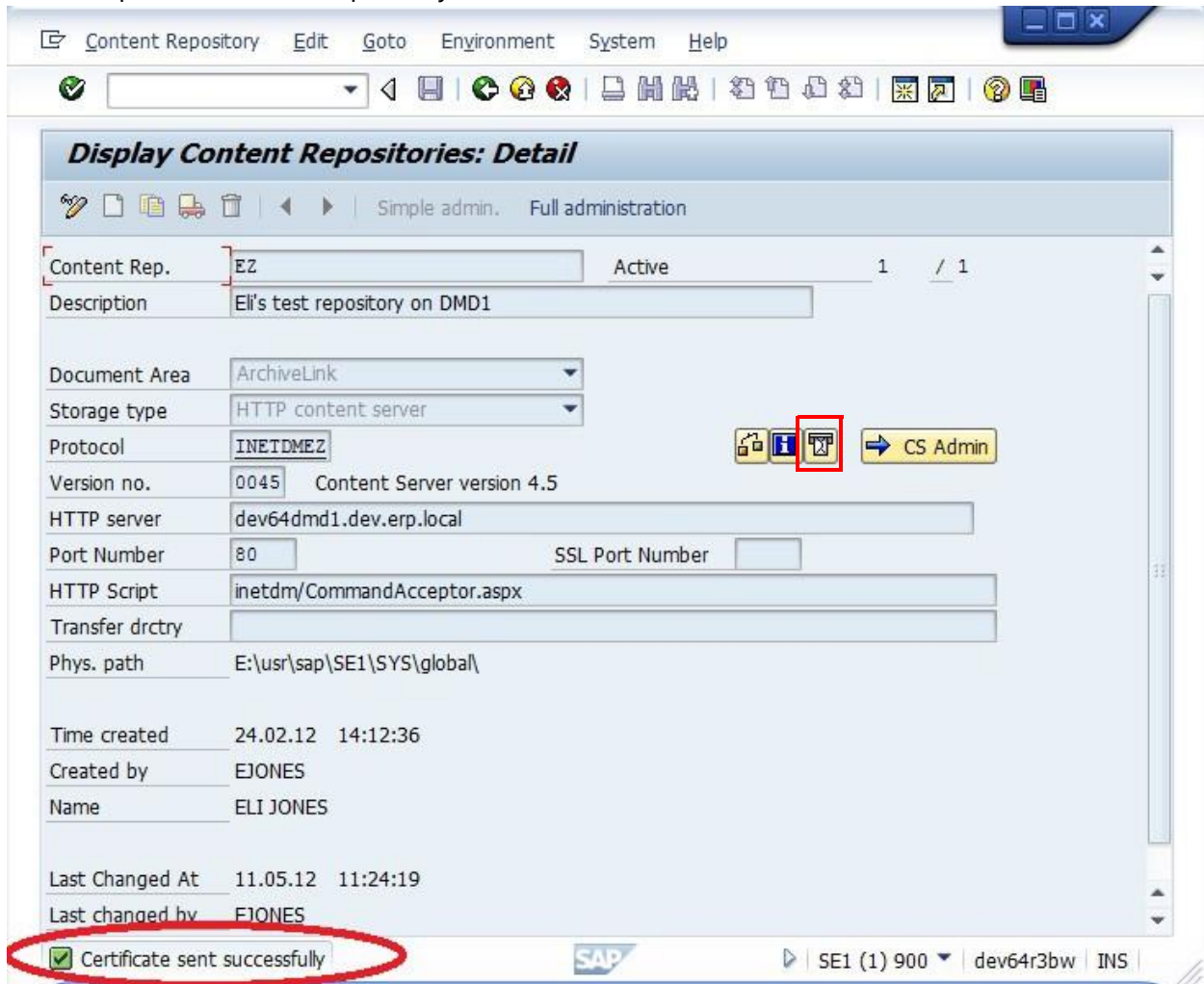


Figure 6-4 Content Repositories Detail in SAP

7. Click **Send Certificate**. The message that it was sent successfully displays in the lower left corner.
8. Test archival and retrieval.

- a. If the archival and retrieval are successful, the settings are correct.
- b. If you see a message such as the following:
unable to add certificate - (iNetDMSecurity)
CCertificateVerifier::AddCertificateToProfile - Function @ file:
..\iNetDMSecurity\CertificateVerifier.cpp, line: 101 returned an error:
7

Either the path to where the security certificate should be added is incorrect.

or

The security permissions are not sufficient to write to the location.

7 Configuring CloudGate Failover Service

Gimmel Link iNet.DM uses the CloudGate server that runs on IIS to receive document requests from

SAP. The CloudGate server communicates with O365 SharePoint Online (or with any remote SharePoint system) to fulfill the document requests from SAP. When a remote SharePoint environment is unavailable, Gimmel Link's CloudGate Failover Service (CFS) provides a single failover location for temporarily storing newly archived documents. This provision ensures that archival processes are not interrupted during short-term outages of remote SharePoint environments such as O365.

While in failover mode, the new documents stored in the failover location are still accessible by SAP users; however, any previously archived documents that reside in SharePoint are unavailable. In addition to logging failover events, CFS supports configuring email notifications when the status of the remote SharePoint connectivity changes; that is, notifications occur any time CFS mode is entered or exited.

A failover location to store the documents while in failover mode must be configured for CloudGate Failover Services. Email notification of failover mode can be configured, which will send an email to administrators when CloudGate failover mode occurs.

7.1 Enabling the CloudGate Failover Service

CloudGate Failover Service configuration will be in effect for all content repositories that are configured in a content repository configuration file. Perform these steps to enable CFS.

1. From the Gimmel Link Administration Console, open the current configuration.
2. Select the **Fail-Over** node in the navigation pane.

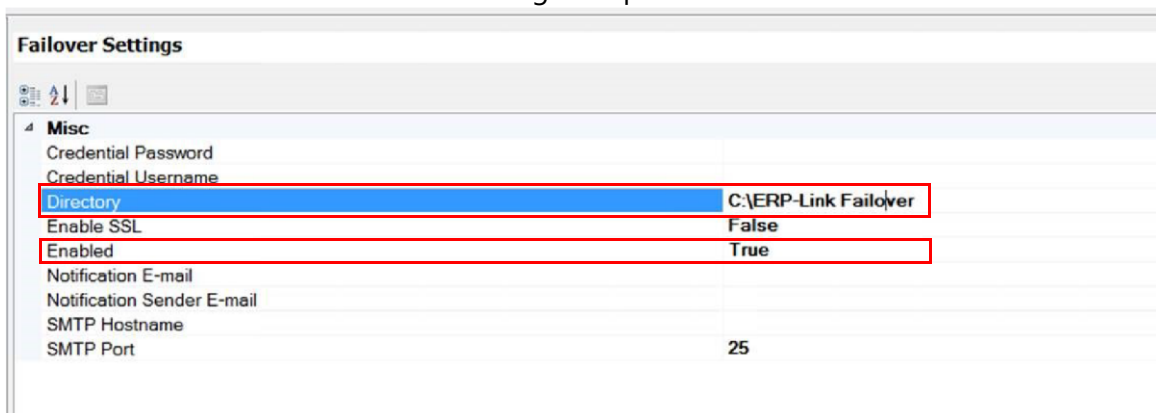


Figure 7-1 Failover Settings Pane

3. In the **Directory** field, enter a single directory location where files can be stored. Verify that this folder has the appropriate permissions assigned so that files can be written and retrieved from this location by iNet.DM.

4. In the **Enabled** field, select *True* to enable CFS for this configuration. Click **File** on the top menu and select **Save**.

7.2 Configuring Email Notifications

To configure CFS to support email notifications, follow these steps.

1. From the Gimmel Link Administration Console, open the current configuration.
2. Select the **Fail-Over** node in the left pane.
3. In the **Notification E-mail** field, enter the address of the administrators who will receive the notification emails.
4. In the **Notification Sender E-mail** field, enter the sending email address for notification emails.
5. In the **SMTP Hostname** field, enter the IP or resource name to use as the SMTP server for the emails.
6. In the **SMTP Port** field, enter the port that the SMTP server is configured to use. This is typically port 25 (Non-SSL) or 587 (SSL). Check with your email administrator for the appropriate values.
7. In the **Enable SSL** field, specify whether SSL should be used for communications to the SMTP server.
8. In the **Credential Username** field, specify the username for the user account being used to authenticate to the SMTP server.
9. In the **Credential Password** field, specify the password for the user account being used to authenticate to the SMTP server.
10. Click **File** on the top menu and then select **Save**.

When Gimmel Link enters into CFS failover mode, an email will be sent to the configured email recipients that is similar to the following.

Dear Gimmel Customer:

Gimmel's ERP-Link Suite has ENTERED failover storage mode.

ERP-Link CloudGate Server: ERPDOC01V
Remote SharePoint System: <https://erplinkgimmel.sharepoint.com/sites/DocSite>

The ERP-Link CloudGate server is responsible for communication from SAP to the remote SharePoint system (e.g. O365 SharePoint Online).

Please note that all new SAP archived documents [and serviced through this ERP-Link CloudGate server] are now stored in the configured failover file system location (e.g. a network share location). Please visit the ERP-Link Administration Console to determine the configured failover file system location and to perform document recovery from the configured failover location to the remote SharePoint system. It is important to first restore connectivity to the remote SharePoint system, and then perform document recovery with the administration console.

The ERP-Link software will check the availability of the remote SharePoint system upon every document archival attempt from SAP and will store documents in the remote SharePoint system if it detects that SharePoint connectivity is restored. The ERP-Link Suite will EXIT the failover storage mode once SharePoint connectivity is restored and a document is successfully stored in the remote SharePoint system.

Documents stored in the failover file system location are NOT automatically recovered and need to be manually recovered using the ERP-Link Administration Console.

Sincerely,

ERP-Link Product Team, Gimmel LLC

Figure 7-2 Sample Email Notifying Administrators that Failover Mode Entered

When connectivity to the remote SharePoint environment is available and CloudGate has resumed its normal storage mode, an email is sent to the configured email recipients that is similar to the following.

Subject: ATTENTION: ERP-Link Is In Failover Storage Mode

Dear Gimmel Customer:

Gimmel's ERP-Link Suite has ENTERED failover storage mode.

ERP-Link CloudGate Server: JDONOVAN/04
Remote SharePoint System: <https://isdev2.sharepoint.com/sites/erplink>

The ERP-Link CloudGate server is responsible for communication from SAP to the remote SharePoint system (e.g. O365 SharePoint Online).

Please note that all new SAP archived documents [and serviced through this ERP-Link CloudGate server] are now stored in the configured failover file system location (e.g. a network share location). Please visit the ERP-Link Administration Console to determine the configured failover file system location and to perform document recovery from the configured failover location to the remote SharePoint system. It is important to first restore connectivity to the remote SharePoint system, and then perform document recovery with the administration console.

The ERP-Link software will check the availability of the remote SharePoint system upon every document archival attempt from SAP and will store documents in the remote SharePoint system if it detects that SharePoint connectivity is restored. The ERP-Link Suite will EXIT the failover storage mode once SharePoint connectivity is restored and a document is successfully stored in the remote SharePoint system.

Documents stored in the failover file system location are NOT automatically recovered and need to be manually recovered using the ERP-Link Administration Console.

Sincerely,

ERP-Link Product Team, Gimmel LLC

Figure 7-3 Sample Email Notifying Administrators that Failover Mode Exited

7.3 Recovering a Repository from CloudGate Failover Service

When a target SharePoint environment goes offline, the CloudGate CFS stores documents in the folder created for failover document storage. The documents remain in this folder until the

environment is accessible and the documents can be routed to the appropriate iNet.DM repositories.

Note:

When multiple iNet.DM servers are used, the content stored by CFS must be located and restored from a single location, either local storage or a file share.

Restore the repositories from a single iNet.DM server by following these steps.

1. Using the **Gimmel Link Administration Console**, open the current configuration.

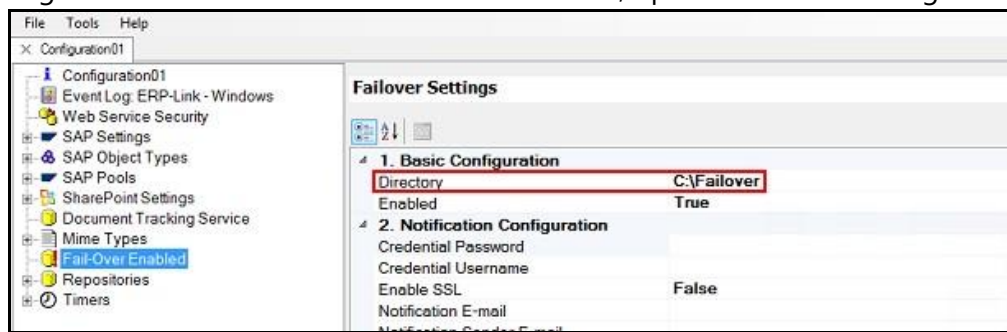


Figure 7-4 Location to Restore Documents From

2. Verify that the CFS directory is configured to point to the location where all of the documents will be restored from.
3. From the menu at the top of the Administration Console, select **Tools** and then select **Restore Repositories**.

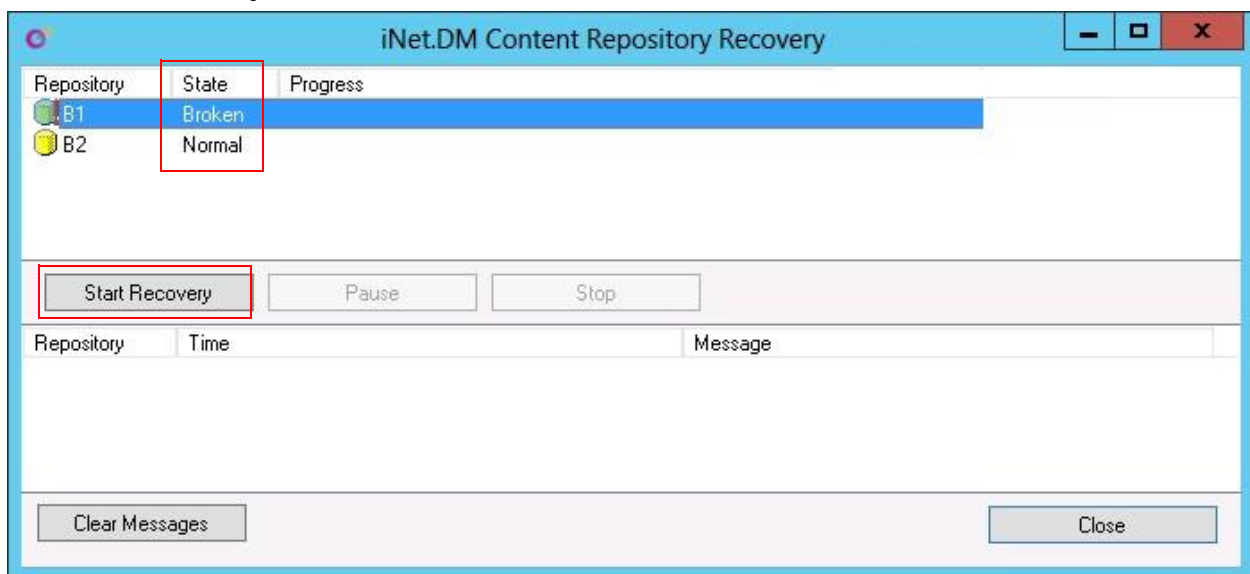


Figure 7-5 iNet.DM Content Repository Recovery Dialog Box

In the iNet.DM Content Repository Recovery dialog box, you can view the state of the repositories.

- **Broken:** The status of SharePoint connection is unknown, but it was broken at one time and documents were stored in the failover location. The repository must be recovered.
- **Normal:** The SharePoint connection is available and no documents are stored in the failover location. This repository does not need to be recovered.
- **Invalid:** The SharePoint connection is unavailable but no documents are stored in the failover location. This repository does not need to be recovered.

4. Select the **Broken** repository to be recovered. You can hold the **Ctrl** button and select multiple repositories.
5. Click the **Start Recovery** button.

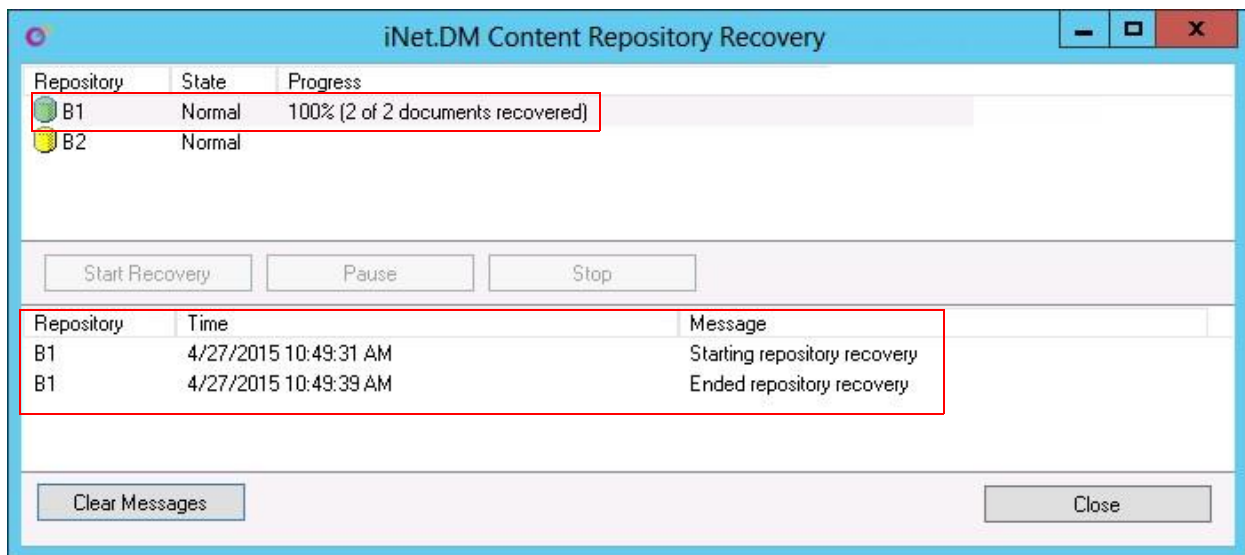


Figure 7-6 Status of Repository Recovery

When the repository has been recovered from a *Broken* state, The **State** field displays the state of the repository, and the **Progress** field displays 100% and the number of documents recovered. The start and stop times of recovery display in the message pane.

Note:

The files are recovered individually, but repositories are recovered in parallel. If a file fails to be recovered, the repository will remain in a *Broken* state after the recovery finishes.

6. To verify that the files were recovered, navigate to the failover storage location. The stored files should not display in the failover location.

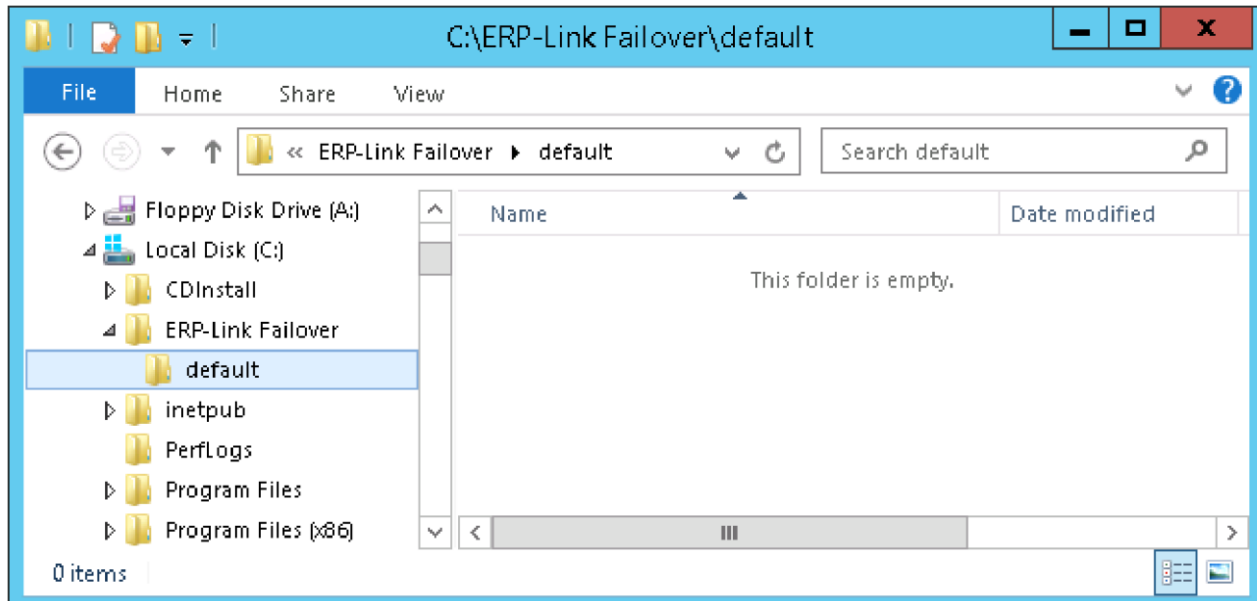


Figure 7-7 All Files Recovered from Failover Storage Location

8 Configuring SAP for Use with Document Manager

This section contains the procedures necessary to configure SAP for use with Gimmel Link Document Manager.

- [8.1 Configuring SAP to Use ArchiveLink](#)
- [8.2 Using SAPOffice Attachments to Connect to Gimmel Link](#)
- [8.3 Configuring SAP to Use DMS Document Info Record Original to Connect to Gimmel Link](#)
- [8.4 Using Gimmel Link with Business Document Service](#)

8.1 Configuring SAP to Use ArchiveLink

This section contains instructions to configure SAP to connect to Gimmel Link Document Manager with ArchiveLink.

8.1.1 Creating a New Protocol (SAP T-Code OAA3)

Follow these steps to create a new protocol.

1. Launch SAP.



Figure 8-1 SAP Ribbon

2. In the ribbon, type `/noaa3`; then press **Enter**.

ArchiveLink: Communications Interface Administration

Protocol	Version	Description	Used in st. systems
ERPLINK	0045	ERP-LINK INET.DM PROTOCOL	Used B1 C0 C1 C2 C3 E0 ET F1 F
ERPLTEST	0045	TEST	Used SI
ERPOBJ	0045	ERPLINK W/ CLIENT COMPONENT	Used DC I2
NEWERP	0045	SAMPLE	Not used in any st. system
SAPHTTP	0045	SAPHTTP 0045	Used EP VG
SAPMA	0046	PROTOKOLL FÜR CREP MA	Used MA
SAPRFC	0031	SAPRFC	Not used in any st. system

Figure 8-2 Create Protocol Button 3.

Click **New Protocol** at the top left of the ribbon.

Create New Protocol

Protocol: ERPLINK

Version: 0045

Description: ERP-LINK INET.DM PROTOCOL

[OK] [Cancel] [X]

Figure 8-3 Create New Protocol Dialog Box with Example Entries

- In the **Create New Protocol** dialog box, enter the parameters.

Note:

The **Version** field represents the HTTP Content Server interface version that is to be used.

- Click the **Save** button.

8.1.2 Creating New Content Repository (SAP T-Code OAC0)

Follow these steps to create the content repository.

- In the ribbon (Figure 8-1 SAP Ribbon), type `/noac0`; then press **Enter**.

Content Repository	Document...	Storage type	Ver...	Description
/OSP/O01	SRM	SAP System Data...	0045	DB Storage for Customer Content
/OSP/O02	SRM	SAP System Data...	0045	DB Storage for Customer Content

Figure 8-4 Change Content Repositories

2. On the ribbon, click the **Change/Display** button and then click **Create**.

Change Content Repositories: Detail

Simple admin. **Full administration**

Content Rep.

Description

Document Area

Storage type

Protocol

Version no.

HTTP server

Port Number SSL Port Number

HTTP Script

Basic Path

Figure 8-5 Content Repository Details with Example Entries

- On the **Detail** page, click **Full Administration** and enter the parameters.
 - Content Rep: Enter the defined Content Repository ID, which will match that identified in the Gimmel Link DM configuration XML file (e.g., ContentRepositoryConfig.xml). In the example above, it is B1.
 - Description: Type any free form text description.
 - Document Area: Select the *ArchiveLink* option.
 - Storage Type: Select the *HTTP Content Server* option.
 - Protocol: Type the protocol created in OAA3 ().
 - Version no: Type the version of the Content Server that is to be used.

- HTTP Script: Type the server name or IP address of the server where Gimmel Link is installed. In a load-balanced installation, this would be the load balancer server.
- Port Number: Type the network port number that the Gimmel Link DM Web application is using to receive SAP document requests.
- HTTP Script: Type *iNetDM/CommandAcceptor.aspx*.

4. Click **Save**.

8.1.3 Creating Global Document Types (SAP T-Code OAC2)

Follow these steps to create Global Document Types.

1. Launch SAP.
2. In the ribbon, type `/noac2` to create SAP ArchiveLink Document Types.

Change View "Global document types": Overview				
Global document types				
Document...	Description	Document Class	Status	
ABAP	Reports	BIN	<input type="checkbox"/>	
AMIDOCUM	Asset accounting documents	FAX	<input type="checkbox"/>	
ARCHIVE	Archive files R/3 application data	REQ	<input type="checkbox"/>	
BDS_ATTACH	Attachment	DOC	<input checked="" type="checkbox"/>	
BDS_HTMLT	HTML template	HTM	<input type="checkbox"/>	
BDS_IMAGE	Image	TIF	<input checked="" type="checkbox"/>	

Figure 8-6 Global Document Types Page

3. On the **Global Document Types: Overview** page, click **New Entries**.

New Entries: Overview of Added Entries				
Global document types				
Document type	Description	Document Class	Status	
Z_B1_PDF	DocAdmin - iNet.DM PDF for SAP Rep - B1	PDF	<input checked="" type="checkbox"/>	

Figure 8-7 New Entries Page

4.

Enter the requested values for each Document type that you want to define.

Document...	Description	Document Class	Status
Z_B1_DOC	DocAdmin - iNet.DM DOC for SAP Rep - B1	DOC	<input checked="" type="checkbox"/>
Z_B1_DOCX	DocAdmin - iNet.DM DOCX for SAP Rep - B1	DOCX	<input checked="" type="checkbox"/>
Z_B1_JPG	DocAdmin - iNet.DM JPG for SAP Rep - B1	JPG	<input checked="" type="checkbox"/>
Z_B1_PDF	DocAdmin - iNet.DM PDF for SAP Rep - B1	PDF	<input checked="" type="checkbox"/>

Figure 8-8 Example Document Types Defined

5. Click **Save**.

8.1.4 Creating Links for Content Repositories (SAP T-Code OAC3)

Follow these steps to create links for content repositories.

1. Launch SAP.
2. In the ribbon, type /noac3.

ObjectType	Doc. Type	L Link	Retent.Period
/XFT/EPA04	HRICERTIFI	X TOA01	

Figure 8-9 Links for Content Repository Page

3. Click the **Change/Display** button; then click **New Entries**.

4.

Object Type	BUS2012
Document type	Z_B1_PDF
Link Status	<input checked="" type="checkbox"/> X
Storage system	B1
Link	TOA01
Retention per.	

Figure 8-10 New Entries Dialog Box with Example Parameters

On the **New Entries: Details** dialog box, enter the requested parameters.

- Object type: The SAP Object Type name
- Document type: The SAP Document Type that you created in previous steps
- Link status: Checked indicates that the link is active
- Storage system: The name of the SAP Content Repository you recently created
- Link: Any SAP link table
- Retention Per: Can be blank

5. Click **Save**. The new Content Repository displays in the Display View.

Object Type	Doc. Type	L Cont.Rep.ID	Link	Retent.Period
BUS2012	Z_B1_DOC	X B1	TOA02	0
BUS2012	Z_B1_DOCX	X B1	TOA02	0
BUS2012	Z_B1_JPG	X B1	TOA02	0
BUS2012	Z_B1_PDF	X B1	TOA02	0
BUS2012	Z_B1_TXT	X B1	TOA02	0

Figure 8-11 Display View of Links

8.2 Using SAPOffice Attachments to Connect to Gimmel Link

SAPOffice attachments (GOS/GOS Documents/SAPOffice Documents) use a single target location system-wide. Therefore, only one SAP content repository can be configured to use as an SAPOffice repository, and the same repository is used with all SAP transactions and all files types when storing documents as attachments.

4.

It is highly recommended to **not** use SAPOffice attachments for storing general-purpose business documents because the attachment functionality is difficult to manage at transaction and user levels and doesn't provide many capabilities offered by ArchiveLink, BDS, or DMS for more robust content management solutions.

When use of SAPOffice attachments is unavoidable, because of application limitation or business requirements, consider enabling this attachment functionality only for some very specific business cases.

To configure SAP to use SAPOffice attachments to connect to Gimmel Link, follow the instructions in the following sections.

1. [8.2.1 Creating New SAP Content Repository](#)
2. [8.2.2 Creating New SAP Content Storage Category](#)
3. [8.2.3 Reconfiguring SOFFPHIO Physical Document Class](#)
- [8.2.4 Configuring New Content Repository in Gimmel Link](#)
5. [8.2.5 Testing Attachment Using GOS Create Attachment Process](#)

8.2.1 Creating New SAP Content Repository

To create a new SAP content repository, follow these instructions.

1. In the ribbon (Figure 8-1 SAP Ribbon), type `/noac0`; then press **Enter**.

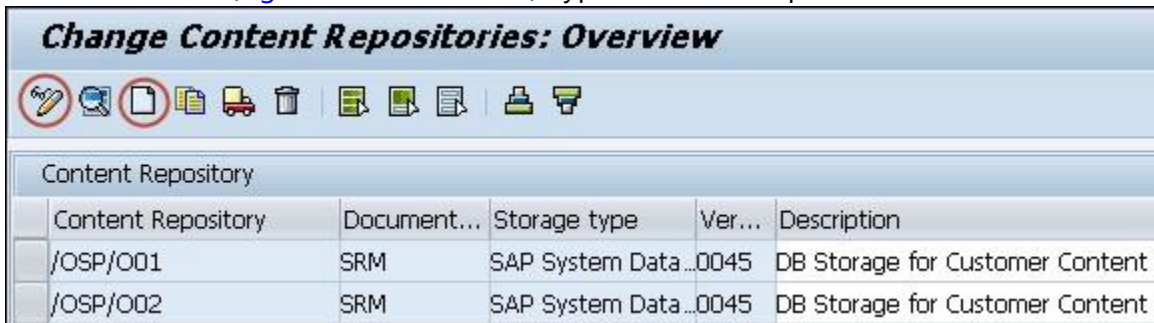


Figure 8-12 Change Content Repositories

2. On the ribbon, click the **Change/Display** button and then click **Create**.

4.

Change Content Repositories: Detail	
Simple admin. Full administration	
Content Rep.	B1 New
Description	iNet.DM Documentation Server
Document Area	ArchiveLink
Storage type	HTTP content server
Protocol	ERPLINK CS Admin
Version no.	0045
HTTP server	erpd0c01v-inet.dv.local
Port Number	80 SSL Port Number
HTTP Script	iNetDM/CommandAcceptor.aspx
Basic Path	

Figure 8-13 Content Repository Details with Example Entries

3. On the **Detail** page, click **Full Administration** and enter the parameters.
 - Content Rep: Enter the defined Content Repository ID, which will match that identified in the Gimmel Link DM configuration XML file (e.g., ContentRepositoryConfig.xml). In the example above, it is B1.

- Description: Type the description of the Content Repository.
- Document Area: Select the *ArchiveLink* option.
- Storage Type: Select the *HTTP Content Server* option.
- Protocol: Type the protocol created in OAA3 ().
- Version no: Type the version of the Content Server that is to be used.
- Port Number: Type the network port number that the Gimmel Link DM Web application is using to receive SAP document requests.
- HTTP Script: Type *iNetDM/CommandAcceptor.aspx*.

4. Click **Save**.

8.2.2 Creating New SAP Content Storage Category

To create a new SAP content storage category, follow these steps.

1. In SAP, enter T-Code *OACT*.

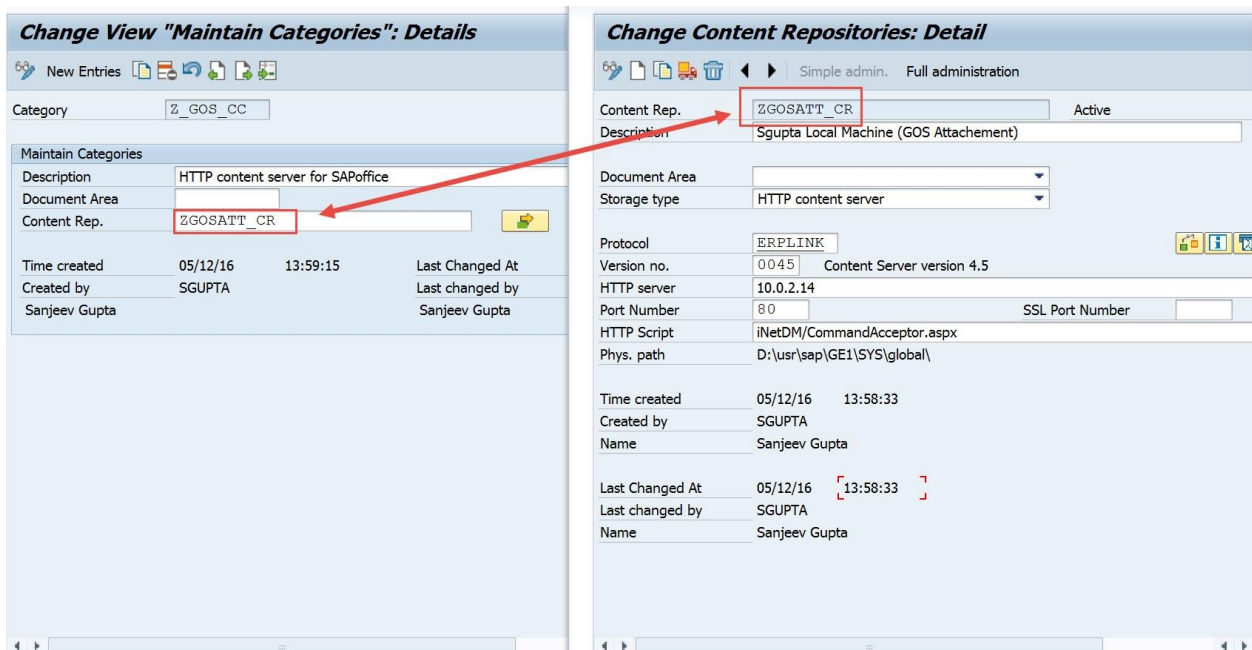


Figure 8-14 Creating New Content Category

2. Create a new **Content Category** using the content repository defined in [8.2.1 Creating New SAP Content Repository](#).

8.2.3 Reconfiguring SOFFPHIO Physical Document Class

To reconfigure the SOFFPHIO physical document class, follow these instructions.

1. In SAP, enter T-code *SKPR08*.

2. Select **New** and then select **Create Attachment**.

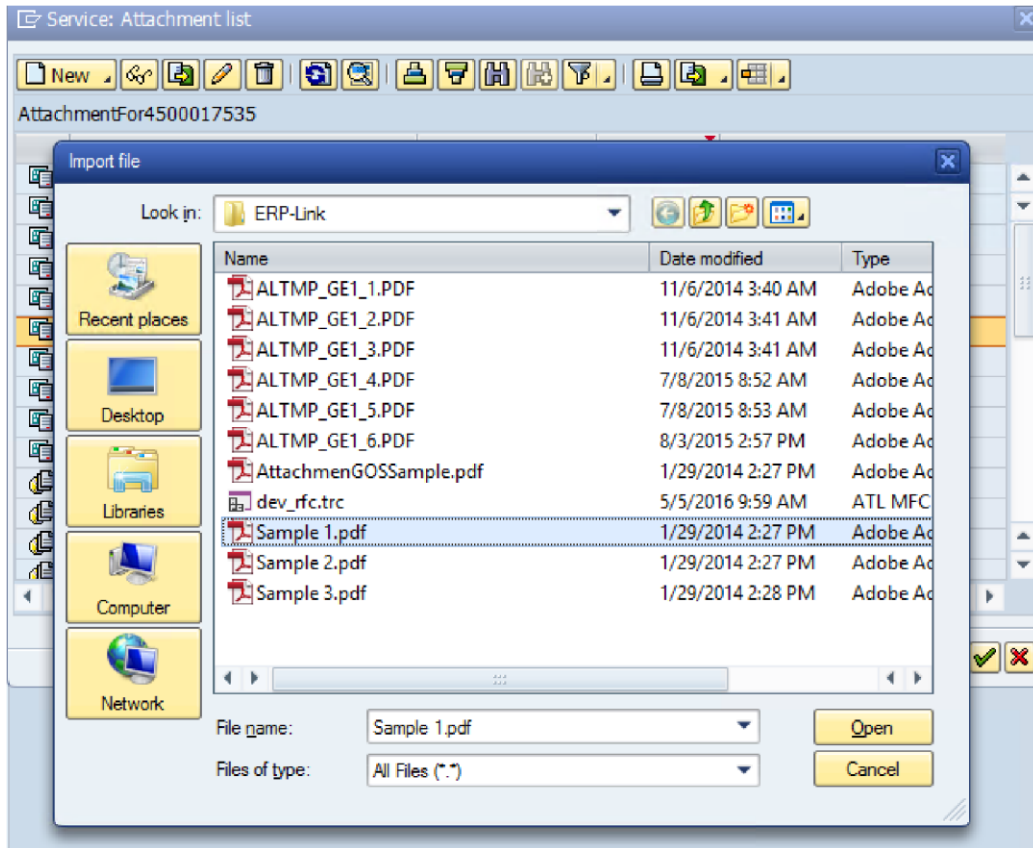


Figure 8-17 Selecting an Attachment

Note:

Text files (.txt) will not show up in your HTTP server repository when using GOS. They will instead be stored in SAP's database. Gimmel recommends that you do **not** use text (.txt) files to test. Use .PDF files instead.

-
3. Select the attachment and click **Open**.

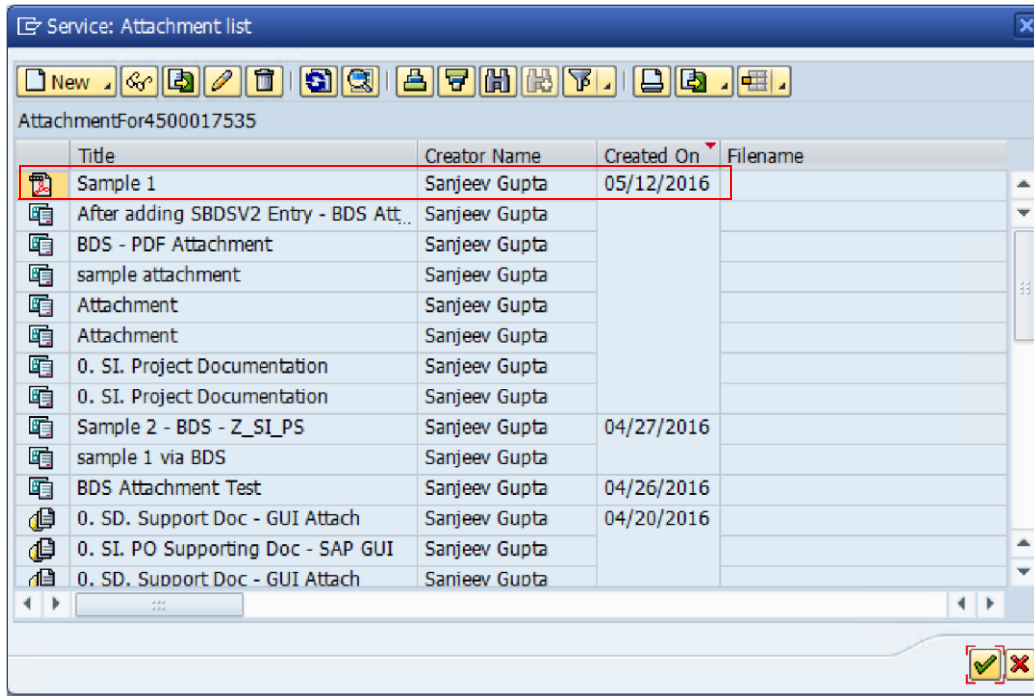


Figure 8-18 Attachment Appearing in List of Service Attachments

4. Confirm that the attachment correctly appears in the **Service Attachments** list.
5. To verify that the content was archived properly, navigate to the target SharePoint library.

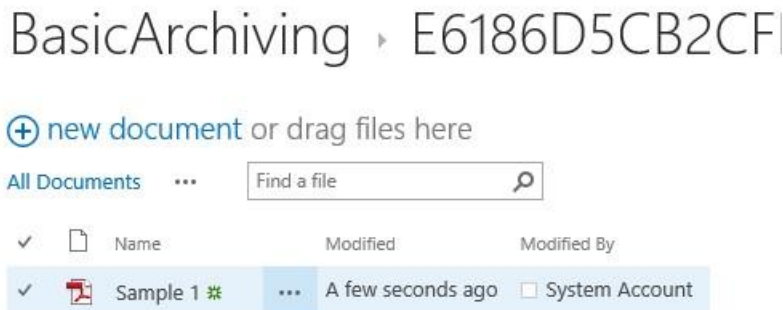


Figure 8-19 Content Correctly Archived in SharePoint Library

8.3 Configuring SAP to Use DMS Document Info Record Original to Connect to Gimmel Link

To use Gimmel Link with DMS document information record originals (DIRs), you must first perform the tasks in the following sections:

- [8.3.1 Creating New SAP Content Repository for DMS](#)

- [8.3.2 Creating New SAP Content Category](#)
- [8.3.3 Configuring New Content Repository in Gimmel Link](#)
- [8.3.4 Testing Original Attachment Process](#)

8.3.1 Creating New SAP Content Repository for DMS

To create a new SAP content repository to use DMS, follow these steps.

1. In the ribbon (Figure 8-1 SAP Ribbon), type `/noac0`; then press **Enter**.

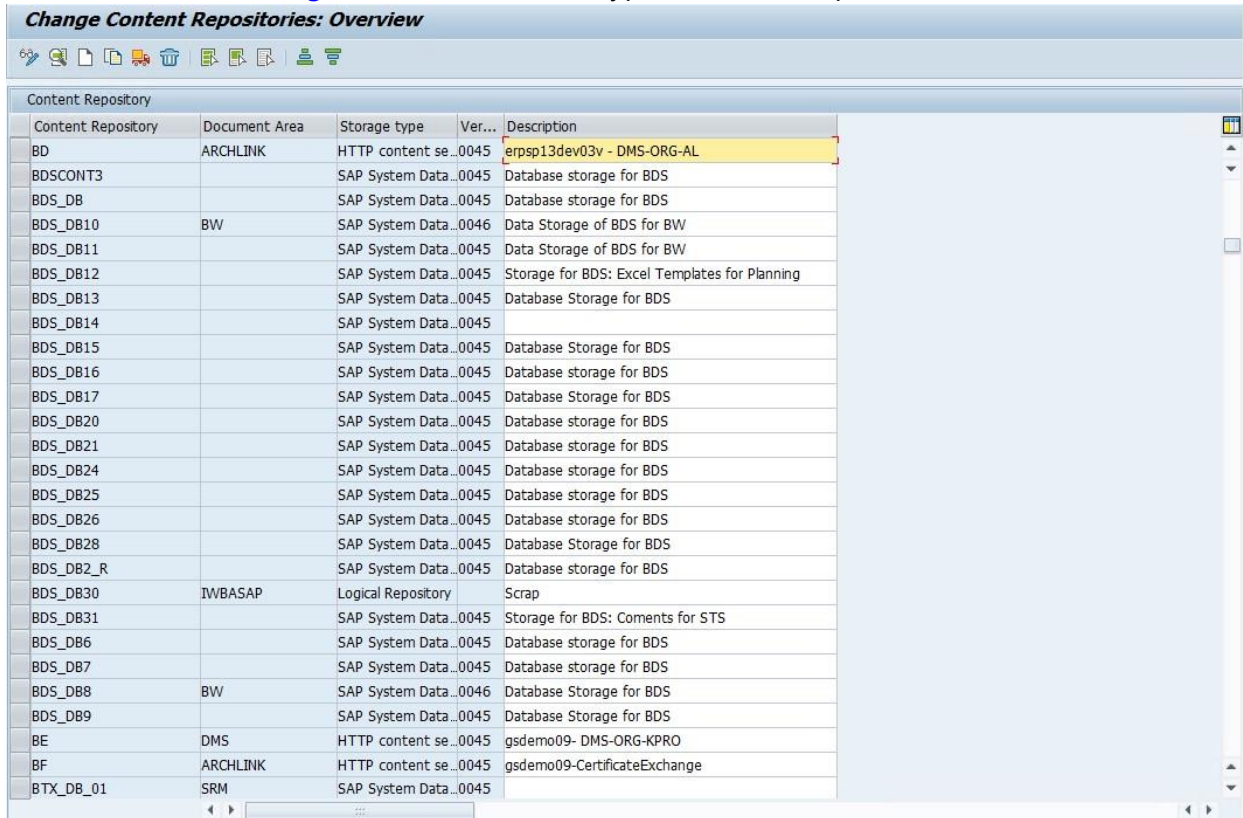


Figure 8-20 Change Content Repositories

2. On the ribbon, click the **Change/Display** button and then click **Create**.

Change Content Repositories: Detail

Simple admin. **Full administration**

Content Rep.

Description

Document Area

Storage type

Protocol

Version no.

HTTP server

Port Number SSL Port Number

HTTP Script

Basic Path

Figure 8-21 Content Repository Details with Example Entries

3. On the **Detail** page, click **Full Administration** and enter the parameters.
 - **Content Rep:** Enter the defined Content Repository ID, which will match that identified in the Gimmel Link DM configuration XML file (e.g., ERPLinkConfig.xml). In the example above, it is B1.
 - **Description:** Type the description of the Content Repository.
 - **Document Area:** Select the **Document Management System** option or leave it blank.
 - **Storage Type:** Select the **HTTP Content Server** option.
 - **Protocol:** Type the protocol created in OAA3 ().
 - **Version no:** Type the version of the Content Server that is to be used.
 - **Port Number:** Type the network port number that the Gimmel Link DM Web application is using to receive SAP document requests.
 - **HTTP Script:** Type *iNetDM/CommandAcceptor.aspx*.
4. Click **Save**.

8.3.2 Creating New SAP Content Category

To create a new SAP content category for use with Gimmel Link, follow these steps.

1. Enter T-code *OACT*.

Change View "Maintain Categories": Details

New Entries [Print] [Refresh] [Save] [Cancel] [Help]

Category: ZBDS_BE

Maintain Categories					
Description	DMS ORG Test - Tied to BE repository				
Document Area	DMS				
Content Rep.	BE				
Time created	05/19/16	14:17:04	Last Changed At	05/19/16	14:17:04
Created by	SGUPTA		Last changed by	SGUPTA	
Sanjeev Gupta			Sanjeev Gupta		

Figure 8-22 Creating a New SAP Content Category

2. Create a new SAP Content Category (also called *Storage Category*) using the content repository defined in [8.3.1 Creating New SAP Content Repository for DMS](#); that is, use the same **Document Area** that you defined in that step.

8.3.3 Configuring New Content Repository in Gimmel Link

Follow the instructions in [6.1 Configuring a Content Repository](#) for associating the SAP content repository to a SharePoint library.

8.3.4 Testing Original Attachment Process

To test the process, follow these steps.

1. Create a new directory (cv01n) or change an existing (cv02n) DIR.
2. Add an **Original**.
3. Click the **Originals** tab.
4. Click the **Create original** button.
5. Specify the file and click **OK**.
6. Check in the original.
 - a. Right-click the document.
 - b. Click **Check-in**.
 - c. Select the **Storage Category** defined previously.
7. Click the **Save** button on the top to save the DIR.
8. To verify that the content archived correctly, navigate to the target SharePoint library.

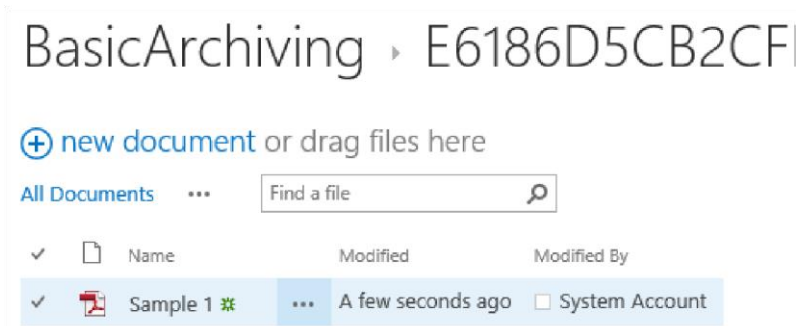


Figure 8-23 Content Archived Correctly in SharePoint Library

8.4 Using Gimmel Link with Business Document Service

To use Gimmel Link with Business Document Service (BDS), you must first perform the tasks in the following sections:

1. [8.4.1 Creating New SAP Content Repository](#)
2. [8.4.2 Creating New SAP Content Category](#)
3. [8.4.3 Configuring SAP for the Business Object and Document Type](#)
4. [8.4.4 Configuring New Content Repository in Gimmel Link](#)
5. [8.4.5 Testing Attachment Process Using Business Document Navigator](#)

8.4.1 Creating New SAP Content Repository

To create a new SAP content repository, follow these steps.

1. In the ribbon ([Figure 8-1 SAP Ribbon](#)), type `/noac0`; then press **Enter**.

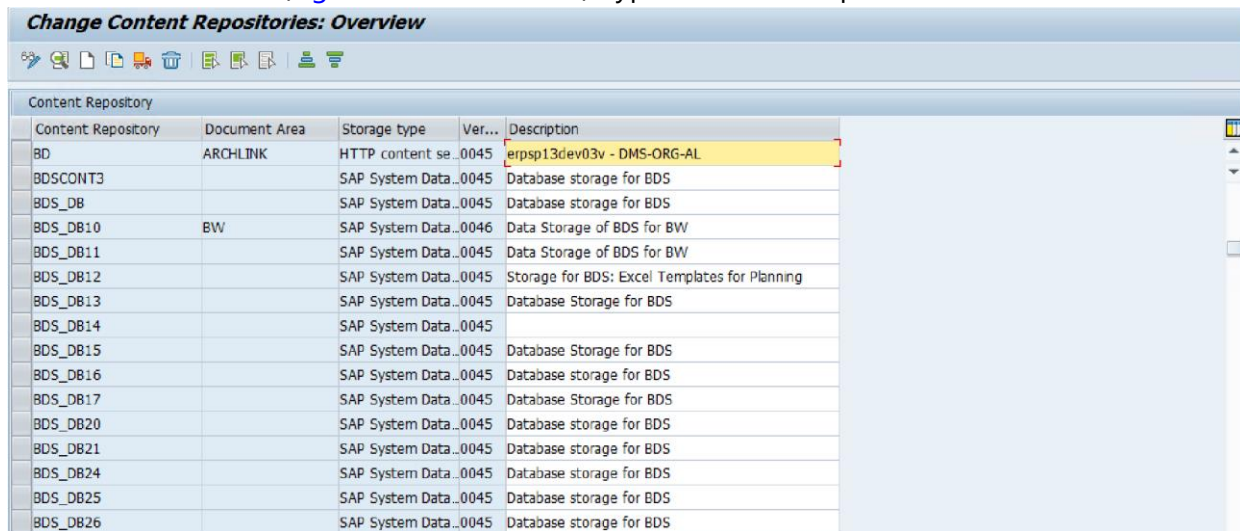


Figure 8-24 Change Content Repositories

- On the ribbon, click the **Change/Display** button and then click **Create**.

Change Content Repositories: Detail

Simple admin. **Full administration**

Content Rep. New

Description

Document Area

Storage type

Protocol CS Admin

Version no.

HTTP server

Port Number SSL Port Number

HTTP Script

Basic Path

Figure 8-25 Content Repository Details with Example Entries

- On the **Detail** page, click **Full Administration** and enter the parameters.
 - Content Rep:** Enter the defined Content Repository ID, which will match that identified in the Gimmel Link DM configuration XML file (e.g., ERPLinkConfig.xml). In the example above, it is B1.
 - Description:** Type the description of the Content Repository.
 - Document Area:** Select the *Business Document Services* option.
 - Storage Type:** Select the *HTTP Content Server* option.
 - Protocol:** Type the protocol created in OAA3 ().
 - Version no:** Type the version of the Content Server that is to be used.
 - Port Number:** Type the network port number that the Gimmel Link DM Web application is using to receive SAP document requests.
 - HTTP Script:** Type *iNetDM/CommandAcceptor.aspx*.
- Click **Save**.

8.4.2 Creating New SAP Content Category

To create a new SAP content category, follow these instructions.

- In SAP, enter T-Code *OACT*.

Change View "Maintain Categories": Details

New Entries

Category: ZBDSTEST

Maintain Categories					
Description	Content Rep for BDS test				
Document Area					
Content Rep.	ZBDSTEST1				
Time created	04/27/16	10:57:11	Last Changed At	04/27/16	
Created by	SGUPTA		Last changed by	SGUPTA	
Sanjeev Gupta	Sanjeev Gupta				

Figure 8-26 Creating New SAP Content Category

2. Create a new SAP content category using the content repository defined in [8.4.1 Creating New SAP Content Repository](#); be sure to use same **Document Area** that you used in that step.

8.4.3 Configuring SAP for the Business Object and Document Type

To configure SAP for the business object and document type, follow these instructions.

1. In SAP, enter T-Code *SBDSV2*.
2. Create a new entry in **BDS Class Definition**, for each unique combination of **Business Object**, **Doc. Type** and **Content Category**. Document Types listed here are Global *Document Types* (T-code: OAC2). Make sure that the Content Category for this entry is same one that you defined in [8.4.2 Creating New SAP Content Category](#).

8.4.4 Configuring New Content Repository in Gimmel Link

Follow the instructions in [6.1 Configuring a Content Repository](#) for associating the SAP content repository to a SharePoint library.

8.4.5 Testing Attachment Process Using Business Document Navigator

To test the attachment process using Business Document Navigator, follow these steps.

1. In SAP, open the Business Document Navigator by entering T-code *OAOR*.

Identification of application object	
Class name	BUS2012
Class type	BO
Object key	4500017535
Attributes	
Description	

Figure 8-27 Business Document Navigator

2. Provide the relevant Business Object and Business Object ID.
3. Click the **Create** tab in the Business Document Navigator.

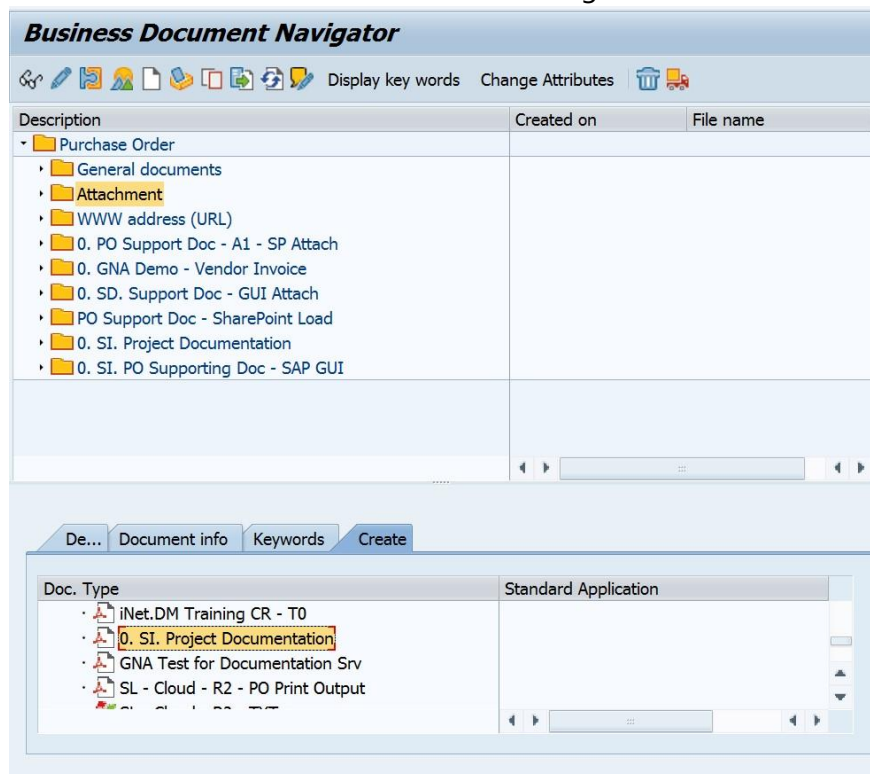


Figure 8-28 Create Tab in Business Document Navigator

4. New documents can be created in one of two ways:
 - **Standard Doc Types.** These are not maintained in the context of Business Object/ Document Type in OAC3 or SBDSV2, but are available in Global Document Types (OAC2). To create a new document, select **Standard Doc Types** to display the Business Document Navigator File Selection dialog box.

- **Doc. Types for Object.** The Doc Types are maintained in the context of the selected Business Object/Document Type in OAC3 or SBDSV2). To create a new document, In the **Create** tab, select the appropriate document type for the document to display the Business Document Navigator File Selection dialog box.
5. Select the document to add to the Business Document Navigator and click the **Open** button to upload the document.

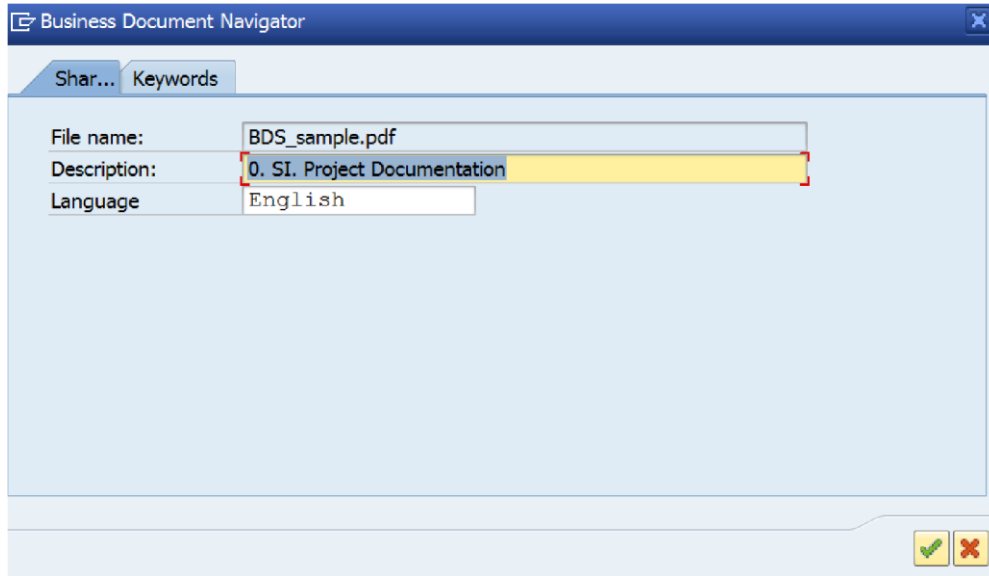


Figure 8-29 Document Info Dialog Box

6. Provide relevant values for the **File Name**, **Description**, and **Language** and click the green check mark.
The document is displayed in the Business Document Navigator under the selected doc type node for documents created using **Standard Doc Types**.

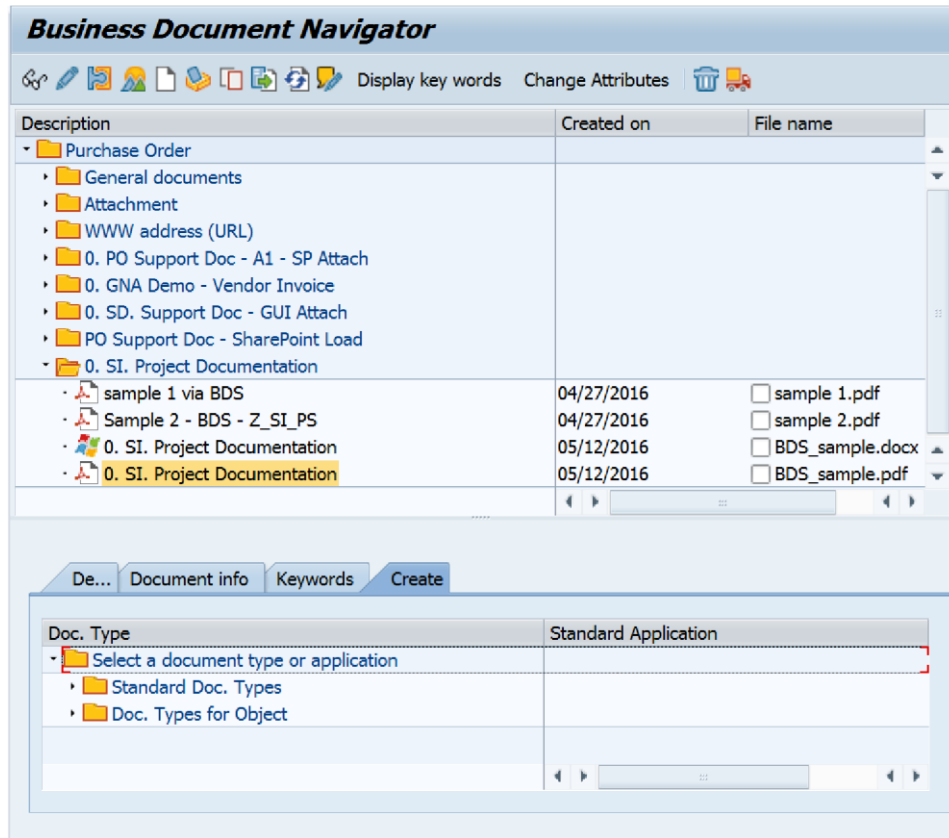


Figure 8-30 Document Displayed in BDN Under Selected Doc Type Node

The document is displayed in the Attachment List for the business object for documents created using **Doc Types for Object**.

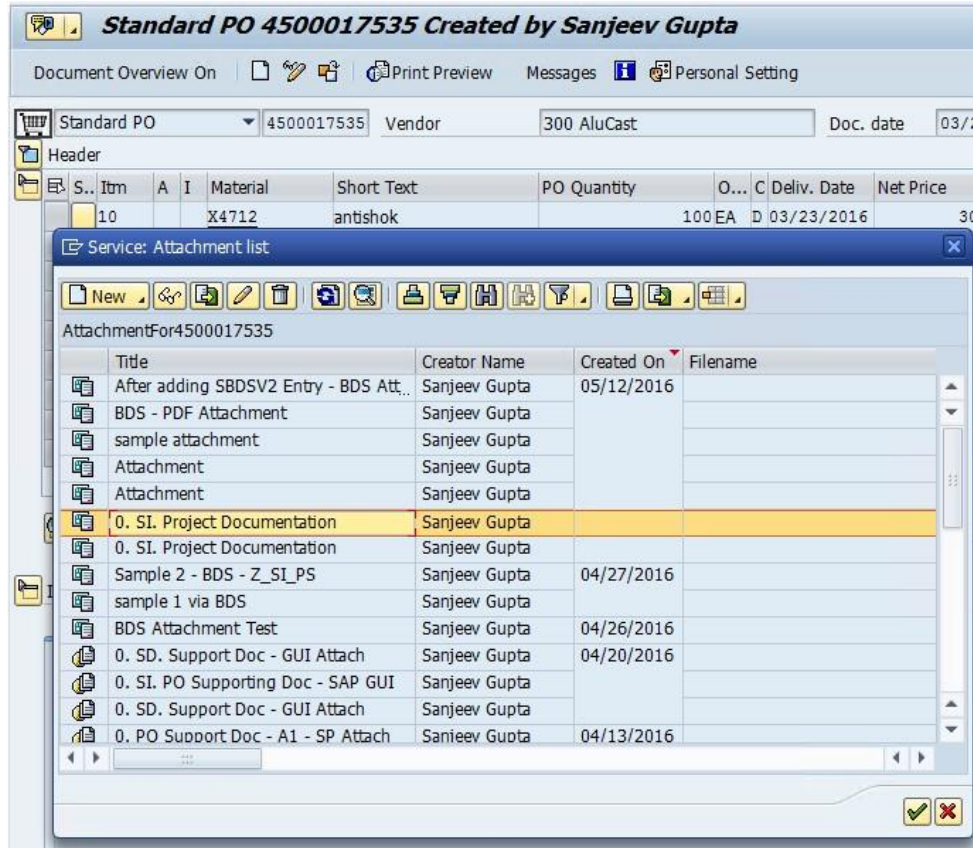
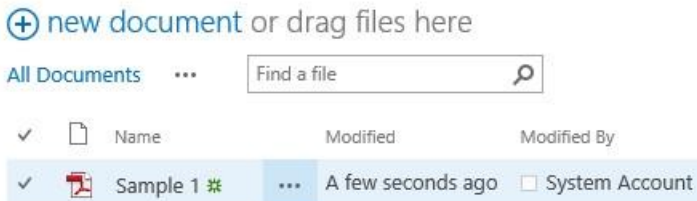


Figure 8-31 Document in Attachment List

7. To verify that the content was archived properly, navigate to the target SharePoint library and validate that the document was uploaded to the library.

BasicArchiving ▸ E6186D5CB2CF



-

Figure 8-32 Content Correctly Archived in SharePoint

9 Validating Gimmel Link Document Manager Functionality

This section contains steps to validate basic Gimmel Link Document Manager functionality.

[9.1 Assigning SAP T-Code OAAD \(ArchiveLink: Administration of Stored Documents\)](#)

[9.2 Validating Gimmel Link Document Manager Service Through Web Browser](#)

9.1 Assigning SAP T-Code OAAD (ArchiveLink: Administration of Stored Documents)

Follow these steps to store and assign a document.

1. Launch SAP.
2. In the ribbon, type `/nOAAD`.

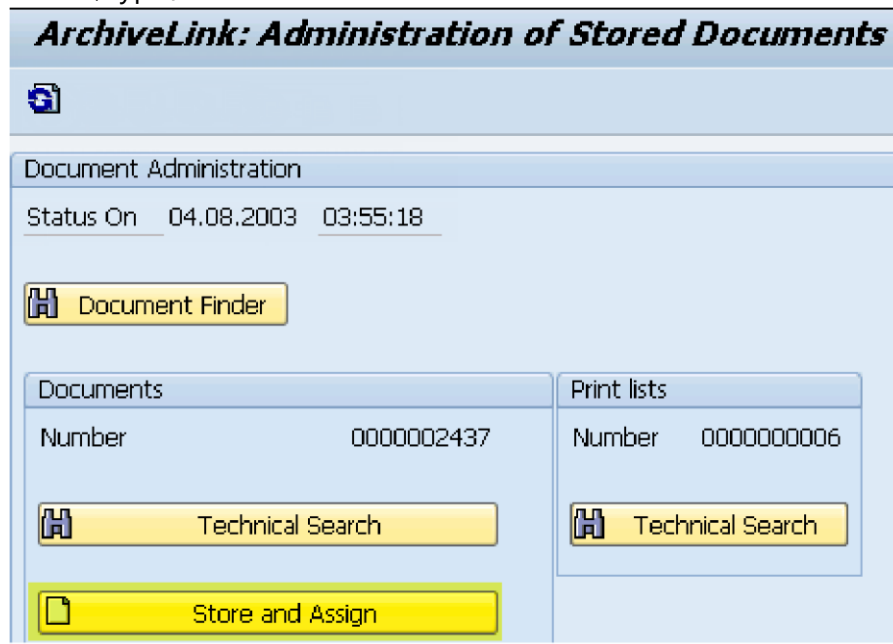


Figure 9-1 Administration of Stored Documents Page

3. On the **ArchiveLink: Administration of Stored Documents** page, click **Store and Assign**.

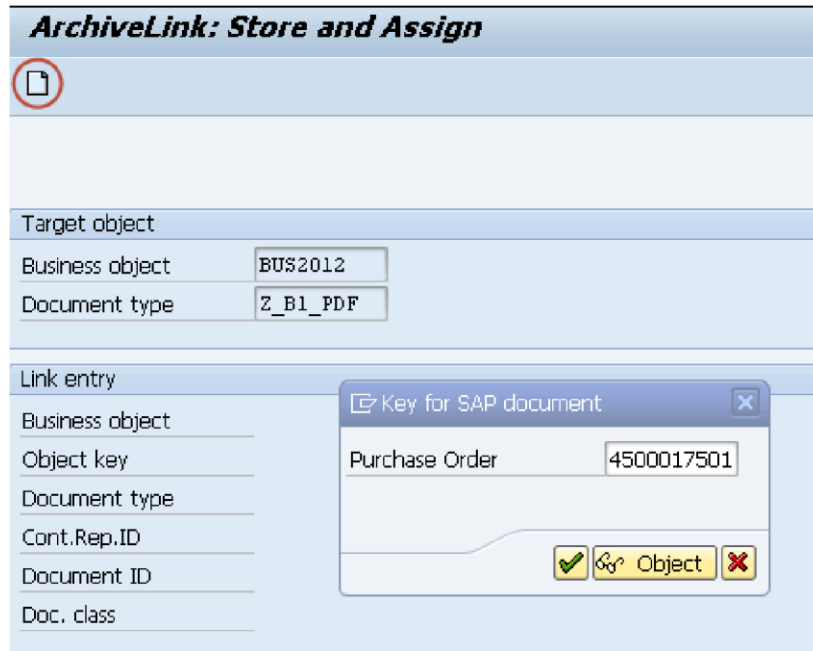


Figure 9-2 Store and Assign Page with Example Entries

4. On the **Store and Assign** page, select the **SAP Business Object Type**.
5. Click the **Create** button in the upper left corner and look up the desired purchase order number for the document attachment operation in the next step.
6. Click **Accept**.

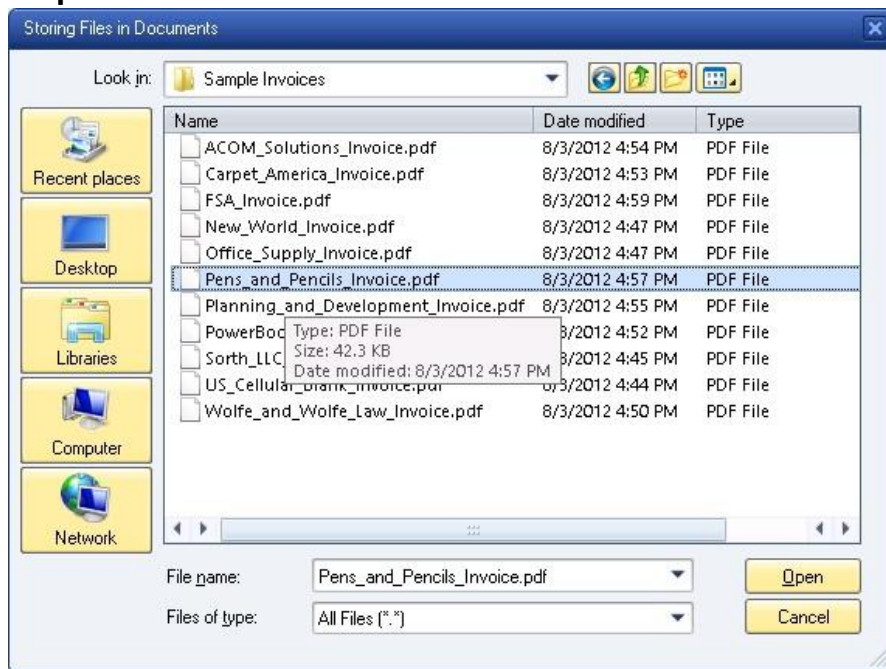


Figure 9-3 Storing Files in Documents Dialog Box

7. From the **Storing files in document** dialog box, locate the document and then click **Open**.

8. In SharePoint, navigate to the Document Library where the iNetDM documents from SAP will be stored.

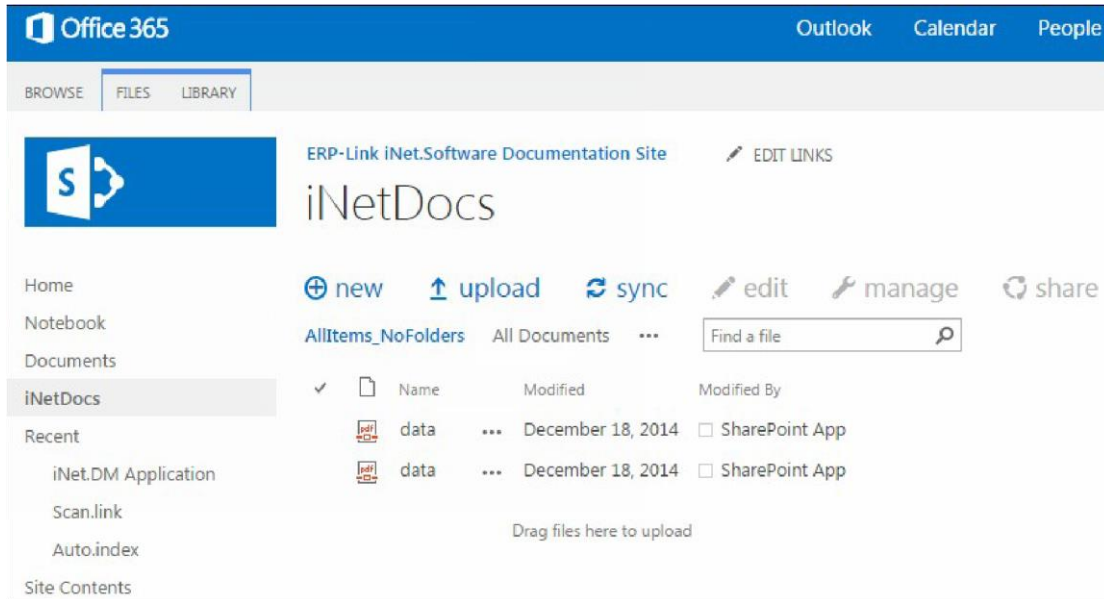


Figure 9-4 iNetDocs Library

9.2 Validating Gimmel Link Document Manager Service Through Web Browser

Follow these steps to validate the Gimmel Link DM service through a Web browser:

1. Go to the Gimmel Link Document Manager interface.
2. Click the **Command Acceptor** button.



ERP-Link Document Manager

Command Acceptor

Content Repositories

Repository	Description	Site Url	Library Name	Secondary Libraries
D3		http://portal.iatham.com/departments/hr	ERP-Link Classic Storage	1

SAP Connections

Name	Version	Ping
GimmelSAP-CS	5	Ping Failed
SAP Setting	3.1	Not supported with this utility

© 2017 - Gimmel, LLC

Version: 5.0.0.17412

Figure 9-5 Gimmel Link Document Manager Interface

- With a successful test, the sample text shown in [Figure 9-6 Sample Text](#) returns.

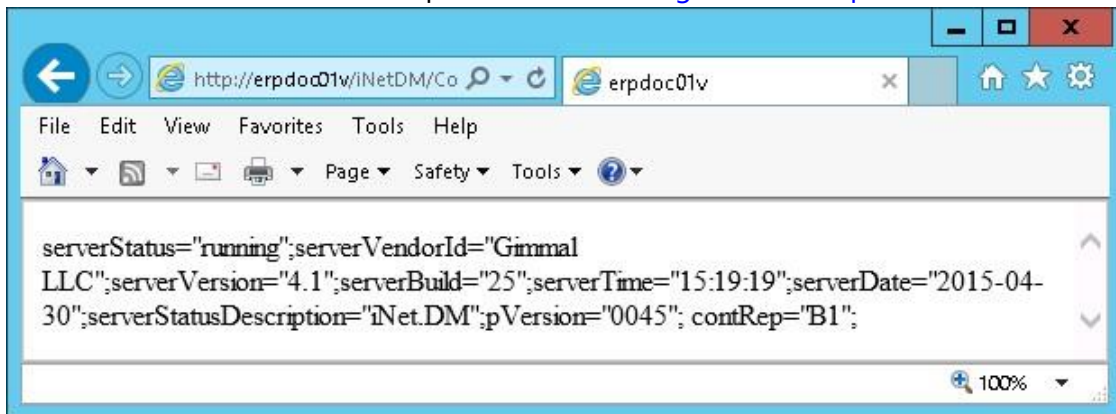


Figure 9-6 Sample Text

10 Sample Configuration Use Cases

The actual configuration is unique to your site. The following are sample configuration workflows that cover some of the most common situations. Additional information in the next chapter helps customize your site’s configuration. Be sure that the installation and configuration described in [2.1 Prerequisite Software and Configuration](#) is present and have the information specified in [2.2 Gimmel Link Component Dependencies](#) available.

The following sections provide configuration instructions for three of the most common situations.

- [10.1 Example Process: SAP Late Archival with SharePoint Metadata and Document Routing for Purchase Orders BUS2012 Using Auto.index](#)
- [10.2 Example Process: SharePoint Late Archival with SharePoint Metadata and Document Routing for Accounting Invoice ID BKPF Using Auto.index and Scan.link](#)
- [10.3 Example Process: SharePoint Archival \(O365\) with Scan.link iNet.DM Library to Start an SAP Workflow](#)

10.1 Example Process: SAP Late Archival with SharePoint Metadata and Document Routing for Purchase Orders BUS2012 Using Auto.index

This example process performs the following:

1. Checks a SharePoint folder for newly added documents intended for attachment to an existing SAP business object BUS2012.
2. Retrieves the metadata for each document from SAP.
3. Archives the document in the correct SharePoint repository, *iNetDocs* in this example, with all the correct metadata from the SAP business object.

To configure the Document Service Modules to carry out the process, follow these steps.

Document Service Modules Shared Configuration

- [5 Setting Shared Configuration Settings](#)

Auto.index

- [12.1 Creating New Auto.index Instance](#)
 - Select *BUS2012* as the **SAPObjectType**.
- [12.3 Populating the Attribute Container](#)
- [12.4 Writing Attributes to SharePoint](#)
- [12.2.2 Indexing Using an SAP Function Module](#)
- [12.4 Writing Attributes to SharePoint](#)
- [12.5 Mapping SAP Document Types to SharePoint Content Types](#)
- [12.6 Configuring Auto.index Document Routing Rules](#)
- [12.7 Testing Auto.index Configuration](#)

10.2 Example Process: SharePoint Late Archival with SharePoint

Metadata and Document Routing for Accounting Invoice ID BKPF Using Auto.index and Scan.link

This example process performs the following:

1. Monitors a SharePoint document library for documents to be attached to SAP business objects; in this example an invoice with SAP object id BKPF.
2. Retrieves the metadata for each SAP business object referenced and indexes the documents with the metadata.
3. Archives the document in the correct SharePoint repository.
4. Attaches each document to the business object in SAP.

To configure the Document Service Modules to carry out the process, follow these steps.

Document Service Modules Shared Configuration

- [5 Setting Shared Configuration Settings](#)

Auto.index

- [12.1 Creating New Auto.index Instance](#)
 - Select *BKPF* as the **SAPObjectType**.
- [12.3 Populating the Attribute Container](#)
- [12.4 Writing Attributes to SharePoint](#)
- [12.2.2 Indexing Using an SAP Function Module](#)
- [12.4 Writing Attributes to SharePoint](#)
- [12.5 Mapping SAP Document Types to SharePoint Content Types](#)
- [12.6 Configuring Auto.index Document Routing Rules](#)
- [12.7 Testing Auto.index Configuration](#)

Scan.link

- [13.1 Creating New Scan.link Instance](#)
- [13.2 Populating the Attribute Container](#)
- [13.3 Configuring Read Fields from SharePoint](#)
- [13.4 \(Optional\) Configuring Scan.link to Perform Validation Using Indexed Metadata](#)
- [13.5 Mapping SharePoint Content Types and File Extensions to SAP Document Types and Classes](#)
- [13.6.3 Configuring Workflow Starter to Trigger a Workflow in SAP](#)
- [13.6.1 Configuring ArchiveLink Linker to Link Document to SAP Business Object](#) •
 - [13.7 Testing Scan.link Configuration](#)

Gimmel Link Timer Service

- [16 Configuring the Gimmel Link Timer Service](#)

10.3 Example Process: SharePoint Archival (O365) with Scan.link iNet.DM Library to Start an SAP Workflow

This example process performs the following:

1. Checks a SharePoint folder for newly added documents.
2. Kicks off a workflow in SAP.

To configure the Document Service Modules to carry out the process, follow these steps.

Document Service Modules Shared Configuration

- [5 Setting Shared Configuration Settings](#)

Scan.link

- When defining a provider, select an O365 provider
- [13.1 Creating New Scan.link Instance](#)
- [13.2 Populating the Attribute Container](#)
- [13.3 Configuring Read Fields from SharePoint](#)
- [13.4 \(Optional\) Configuring Scan.link to Perform Validation Using Indexed Metadata](#)
- [13.5 Mapping SharePoint Content Types and File Extensions to SAP Document Types and Classes](#)
- [13.6.3 Configuring Workflow Starter to Trigger a Workflow in SAP](#)
- [13.7 Testing Scan.link Configuration](#)

Gimmel Link Timer Service

- [16 Configuring the Gimmel Link Timer Service](#)

11 Setting Up the Document Service Modules

The following chapters present instructions for tasks that you can use to configure your organization's unique work process.

- [12 Configuring Auto.index](#)
- [13 Configuring Scan.link](#)
- [16 Configuring the Gimmel Link Timer Service](#)

It is assumed that you have already configured Gimmel Link as described in the preceding chapters.

12 Configuring Auto.index

Early archival occurs when documents are archived before a corresponding Transactional Record is created in SAP. In early archival, the incoming document drives creation of the SAP transaction record. An example of an early archival is when documents arrive in the archive because Scan.link performed an automated archival, but the document is not linked to an SAP transactional record nor does Auto.index index the document with the metadata.

Late archival occurs when documents are archived after the SAP transaction record is created. An example of a late archival is when an SAP user attaches a document image to an SAP business object instance and the document is managed in the iNet.DM archive in SharePoint.

The Auto.index event listener processes documents arriving in the iNet.DM library whether they result from an early or a late archival. Auto.index's primary function is to index the documents in SharePoint with metadata obtained from the SAP system, which it can only do if the document can be linked to a transaction (late archival). It can also route documents from the iNet.DM library to an archive library or another library or folder in either an early or late archival, although Scan.link is more commonly used to perform this task.

12.1 Creating New Auto.index Instance

To add a new instance of Auto.index, follow these steps.

1. In the **Gimmal Link Administration Console**, expand the desired **Content Repository**.

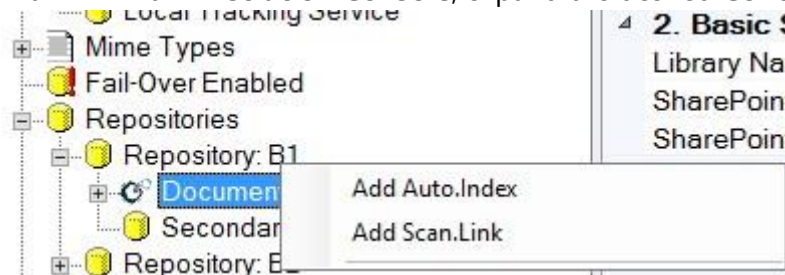


Figure 12-1 Content Repository Pane

2. Right-click **Document Service Modules** in the left pane and select **Add Auto.index**. The new Auto.index instance displays under the Document Service Modules.

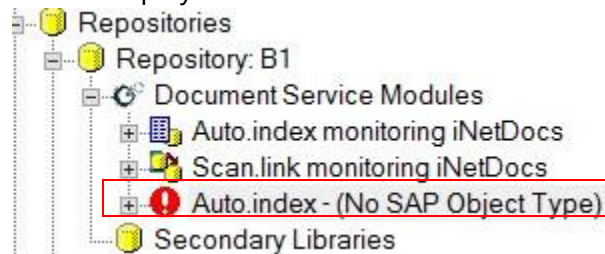


Figure 12-2 New Unconfigured Auto.Index Instance

- Click the new Auto.index instance to view the configuration pane.

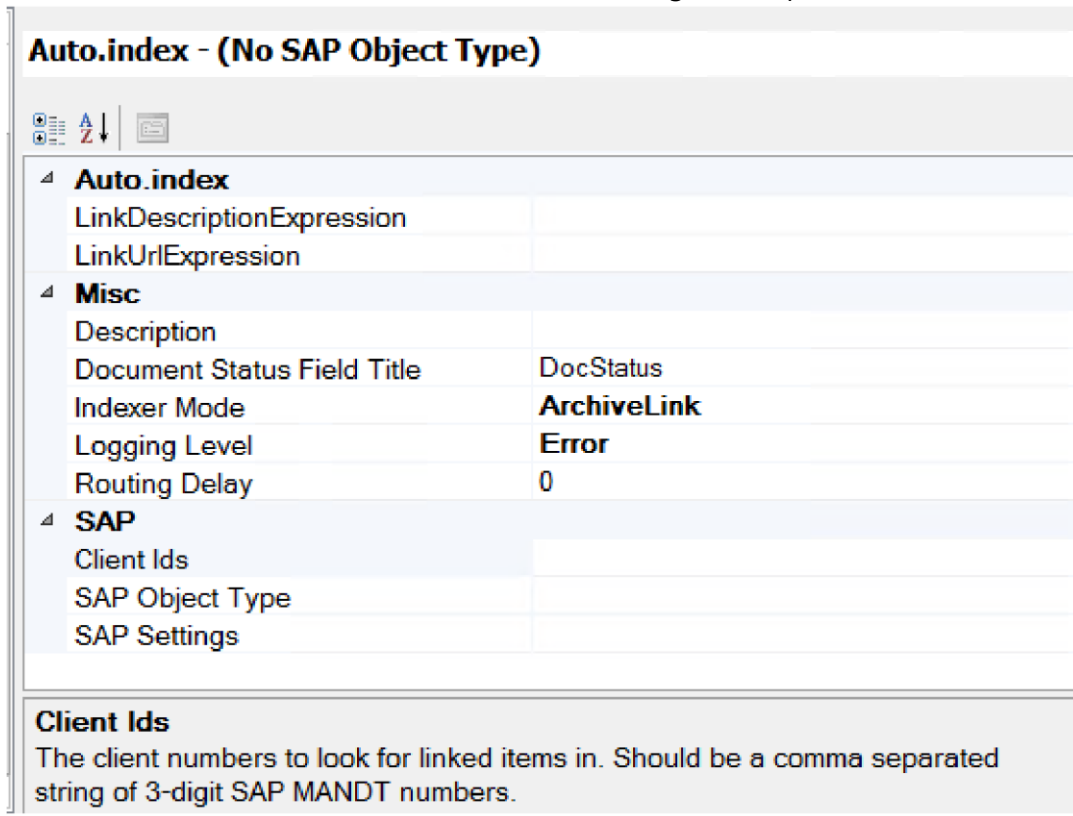


Figure 12-3 Configuration Pane for Auto.index Instance

- Modify the parameters in the right pane. The name of the Auto.index entry automatically adjusts to indicate which SharePoint iNet.DM library this Document Service Module monitors. [Table 12-1](#) describes all the fields.

Table 12-1 Auto.index Configuration Pane Settings

Field Title	Description
-------------	-------------

<p>LinkDescriptionExpression</p>	<p>If not blank, and the <code>LinkUrlExpression</code> property is set, this property is evaluated to generate a description (or title) that is visible to the SAPGUI user. The format strings refer to the attributes obtained from the SAP object using the syntax <code>\$<property name>\$</code>, while properties from the SharePoint document are obtained using the syntax <code>[<property name>]</code>.</p> <p>Example: If the SAP object being indexed supplied the key-value pairs (VENDOR_NAME, <i>Bob's Welding Company</i>), (VENDOR_ID, <i>009112</i>), and the SharePoint document contained the property <i>Title</i> with the value <i>Doc</i>, the URL and description format strings would be:</p> <p>LinkDescriptionExpression = Details for \$VENDOR_NAME\$ from [Title] LinkUrlExpression = http://test.server/item.aspx?vnd=\$VENDOR_ID\$</p> <p>Results in the following URL and Description being attached to the SAP</p> <p>Description = Details for Bob's Welding Company from Doc URL = http://test.server/item.aspx?vnd=009112</p>
<p>LinkUrlExpression</p>	<p>If not blank, this property is evaluated to generate a URL that attaches to the linked SAP business object. The format strings refer to the attributes obtained from the SAP object using the syntax <code>\$<property name>\$</code>, while properties from the SharePoint document are obtained using the syntax <code>[<property name>]</code>.</p> <p>Example: If the SAP object being indexed supplied the key-value pairs (VENDOR_NAME, <i>Bob's Welding Company</i>), (VENDOR_ID, <i>009112</i>), and the SharePoint document contained the property <i>Title</i> with the value <i>Doc</i>, the URL and description format strings would be:</p> <p>LinkDescriptionExpression = Details for \$VENDOR_NAME\$ from [Title] LinkUrlExpression = http://test.server/item.aspx?vnd=\$VENDOR_ID\$</p> <p>Results in the following URL and Description being attached to the SAP</p> <p>Description = Details for Bob's Welding Company from Doc URL = http://test.server/item.aspx?vnd=009112</p>

Description	A descriptive comment for this Document Service Module instance.
Document Status Field Title	Title of the field in SharePoint in which the Document Service Module document status is stored.

Table 12-1 Auto.index Configuration Pane Settings

Field Title	Description
Indexer Mode	<hr/> <p>Important!</p> <p>The Indexer Mode for Auto.index must match the archiving mode configured in SAP for the content repository. For example, if the repository is configured to archive content via GOS, the Indexer Mode in Auto.index must be set to GOS as well.</p> <hr/> <p>Connect with SAP using one of the following choices:</p> <ul style="list-style-type: none"> • ArchiveLink: Assigns stored documents to a business object through GOS [Generic Object Services] Create Business Document • GOS (SAPOffice): Attachment of document through GOS Create Attachment • DMS: SAP Document Management Service • BDS: Business Document Service <p>Select the field and click the arrow on the right to view the menu.</p> <hr/> <p>Note:</p> <p>When ArchiveLink is selected as the Indexer Mode, if a document reference is deleted from the SAP business object, any archived documents are deleted from the SharePoint library.</p> <p>When GOS is selected as the Indexer Mode, if a document reference is deleted from the SAP business object, any archived documents are NOT deleted from the SharePoint library.</p> <hr/>
Routing Delay	Delay time, in milliseconds, before performing routing on an item.
Logging Level	Level of messages that are logged to the event log for this Auto.index instance. Valid levels are Error, Warning, and Information.

Table 12-1 Auto.index Configuration Pane Settings

Field Title	Description
Client IDs	<p>The ID of the client that Auto.index connects to. You can configure one or multiple clients. Auto.index searches each SAP client for the index record in the same order that they appear in the ClientID field.</p> <ol style="list-style-type: none"> 1. Configure Auto.index to connect to the primary client; for example, client 800. 2. In the ClientID field on the Auto.index root node, enter the additional clients on the same SAP system separated by commas; for example, clients 800 and 810. 3. Make sure that the SAP user configured in the iNet.CS connection pool also has rights to connect to the additional clients or Auto.index receives Access Denied errors. <hr/> <p>Note:</p> <p>RFC function modules (see A.4 Function Modules Used by Document Service Modules) and SAP table validation require the MANDT (client) field in SAP for multiple clients to work correctly.</p> <hr/>
SAP Object Type	The SAP business object type to which documents are linked and/or from which indexing properties are fetched.
SAP Settings	The SAP connection to use to communicate to the SAP server.

12.2 Indexing Business Metadata Using Auto.index

Auto.index can obtain metadata from SAP for a particular business object and then populate the fields for related documents in the SharePoint folders with that information. To fetch the SAP Business object attributes for a given archived document when it arrives into a content repository managed by iNet.DM, the Document Service Module instance consults the SAP application server to obtain the SAP object type and the object ID of the linked object. The Document Service Module instance then fetches the attributes from the SAP business object instance using an **indexer**. The attribute values that are mapped to SharePoint properties are then populated into the document properties.

The Document Service Modules use three kinds of indexers.

- **Indexing Using an SAP Table as Data Source:** Table indexers are the simplest of the indexers. They simply look up an item directly in an SAP relational table and retrieve the attributes from the table record. However, in many cases, a table indexer might not be able to fetch the required attributes. For example, the desired attributes might not be available in a single SAP table, but scattered across multiple SAP tables. Corporate

policy may restrict remote access to the RFC_READ_TABLE function module, on which Table Indexers depend. Table Indexer support is therefore provided for user convenience, but not recommended for production use.

- **Indexing Using an SAP Function Module:** Standard SAP remote-enabled function modules (see [A.4 Function Modules Used by Document Service Modules](#)) are typically available; when called, they can retrieve all the desired attributes. If such a standard function module is not available, a custom remote-enabled function module can be written to retrieve the attributes (see [Indexing Using Custom Indexers](#)).
- **Indexing Using Custom Indexers:** If the signature of a custom function module matches certain criteria, it can be called by the RFC indexer with minimal configuration.

12.2.1 Indexing Using an SAP Table as Data Source

To configure an Auto.index instance to use an SAP table as its data source for indexing, follow these steps:

1. Expand the Document Service Module instance that you want to configure.

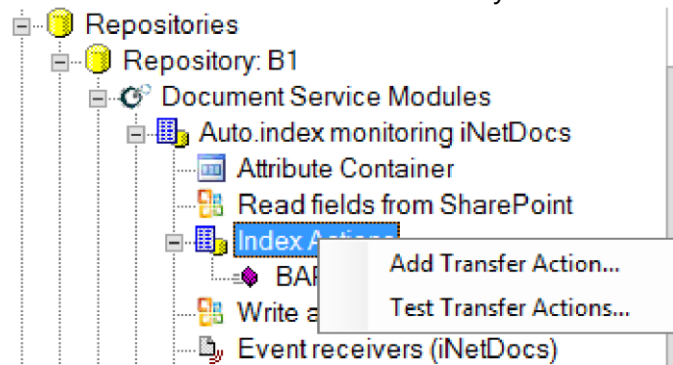


Figure 12-4 Add Transfer Action Option from Auto.index Tree

2. Right-click **Index Actions** in the left pane and select **Add Transfer Action**.

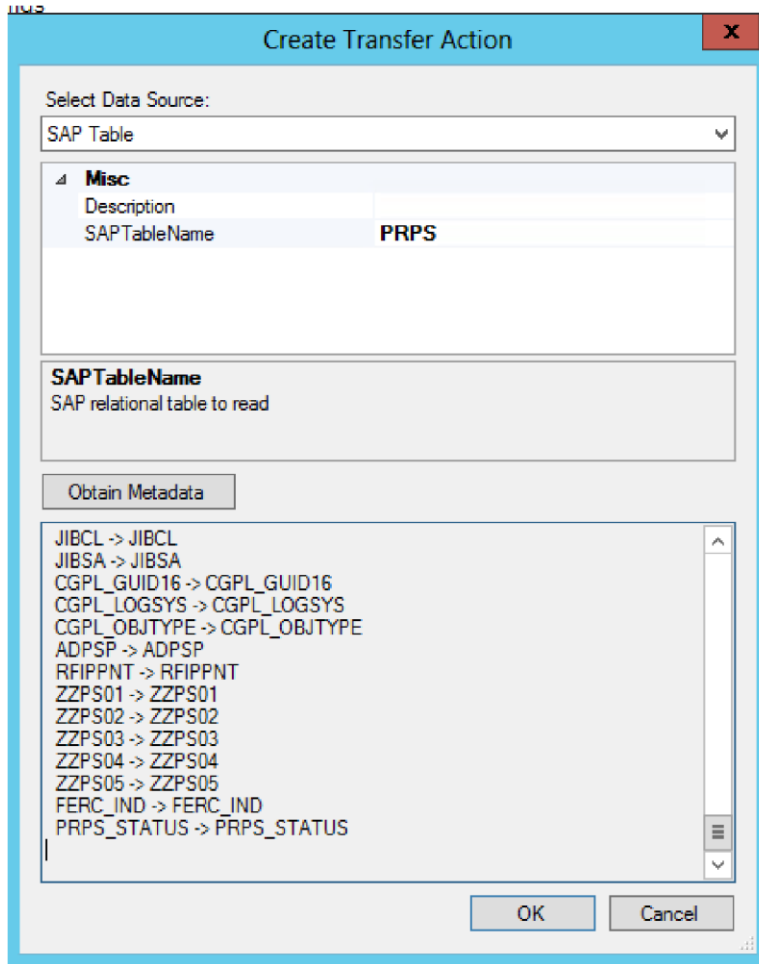


Figure 12-5 Example Create Transfer Action Using SAP Table

3. Select **SAP Table** in the **Create Transfer Action** dialog box as the data source.
4. Enter a **Description** and define the **SAP TableName**. This example called the PRPS table. [Table 12-2](#) describes the fields for this pane.

Table 12-2 Properties Fields

Binding	Description
Properties: Description	Descriptive text for the SAP data table.
Properties: SAPTable-Name	SAP data table that this Document Service Module will query for the metadata.

5. Click **Obtain Metadata** to see all the data that this function can retrieve.
6. Click **OK**.
7. Click the **Request Bindings** tab. The request bindings specify how the SAP business object ID that is retrieved from the ArchiveLink table is used as a key in the SAP relational table.

The request bindings specify the key **FieldBindings** collection and the **SourceExpression** specifies the SAP object ID format.

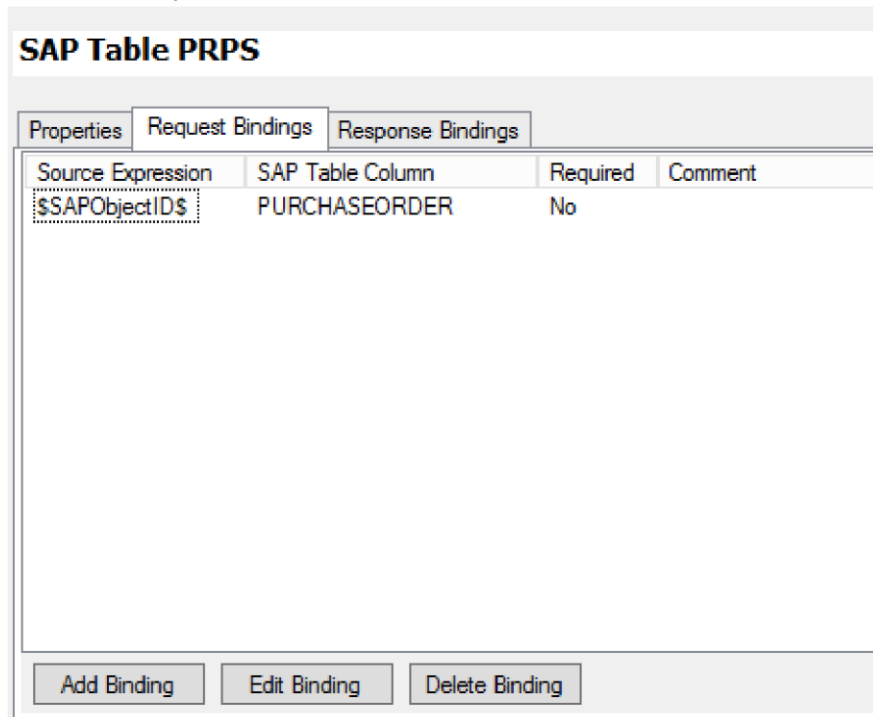


Figure 12-6 Example Request Bindings Tab in SAP Data Table Pane

8. To manually enter bindings, follow these steps.
 - a. Modify the list by using the **Add Binding**, **Edit Binding**, and **Delete Binding** buttons. [Table 12-3](#) describes the fields for this tab.

Table 12-3 Request Bindings Fields

Binding	Description
Request Bindings: Source Expression	Source expression that maps to SAP table column in the request query. Also see Writing Expressions for more detailed information.
Request Bindings: SAP Table Column	SAP table column for the request query.
Request Bindings: Required	Specifies if the request binding is a required field. If the request binding is required and the source expression is empty, then the query is not executed.
Request Bindings: Comment	Descriptive comment for the request binding mapping.

- b. Refer to [Formatting Concatenated Strings](#) for more information about creating bindings.

- c. Click the **Response Bindings** tab.

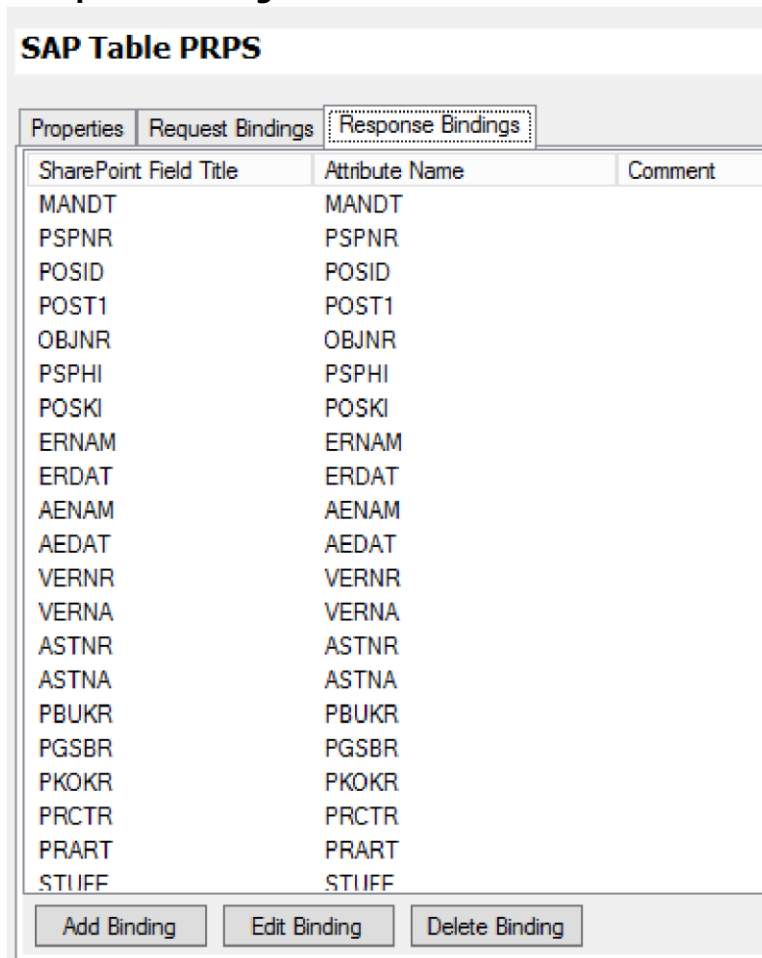


Figure 12-7 Example Response Bindings Tab in SAP Data Table Pane

The response bindings define how the **SAP Output Parameter Names** (fields returned from the request to SAP) are mapped to attributes defined in the Attribute Container.

- d. Click the **Add Binding**, **Edit Binding**, or **Delete Binding** buttons to create the list that you want. [Table 12-4](#) describes the fields for this tab.

Table 12-4 Response Bindings Fields

Binding	Description
Response Bindings: SAP Output Parameter Name	The name of the output parameter from the SAP request. The SAP Output Parameter is mapped to an attribute in the Attribute Container.
Response Bindings: Attribute Name	Output attribute name from the request query that maps to the SharePoint field.

Response Bindings: Comment	Optional descriptive comment for the response binding
-------------------------------	---

Note:

SAP places a 512K limit on the data that is returned to Gimmel Link from SAP when using an SAP table. It is recommended that unnecessary bindings be deleted.

12.2.2 Indexing Using an SAP Function Module

You can configure Auto.index to index the documents using a function module in SAP (see [A.4 Function Modules Used by Document Service Modules](#)). The SAP function module might have one or more input parameters, which are specified in the request bindings of the function module configuration.

1. Right-click **Index Actions** in the left pane under the Document Service Module instance that you are configuring and select **Add Transfer Action**.
2. Select *Remote Function Module* as the data source.

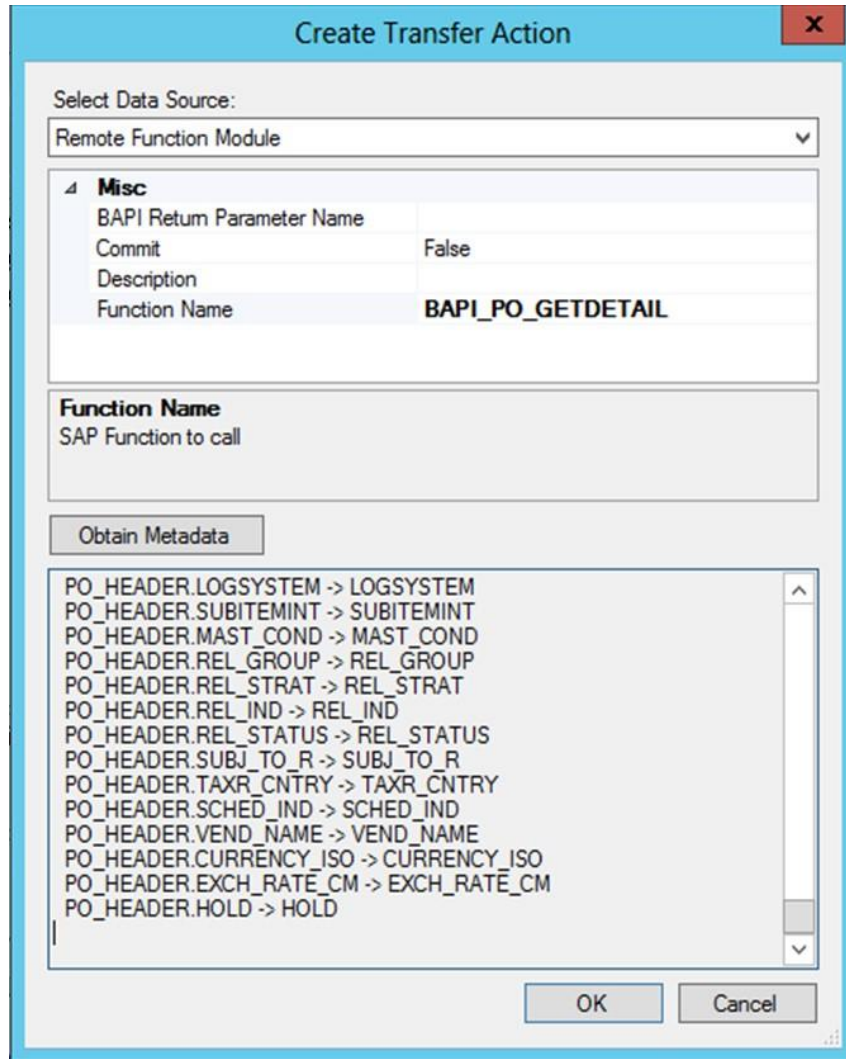


Figure 12-8 Example Create Transfer Action Dialog Box for a Remote Function Module

- Complete the fields in the **Create Transfer Action** dialog box. Table 12-5 describes the fields for this pane.

Table 12-5 Create Transfer Action Dialog Box Fields

Binding	Description
BapiReturnParameter-Name	Name of the export parameter that contains a BAPIRETURN structure, if any.

Commit	<p>If set, will cause an extra call to BAPI_TRANSACTION_COMMIT to be issued after the current function module finishes executing.</p> <hr/> <p>Note:</p> <p>If you use this setting, your connection pool must be in user mode.</p> <hr/>
Description	Can be used to store documentation or explanatory comments.
Function Name	SAP function module to call.
Obtain Metadata	Click Obtain Metadata to see the metadata that this function retrieves.

4. Click **OK**.
5. Click the **Request Bindings** tab. All the **Source Expressions** list in the **Create Transfer Action** dialog box after you click **Obtain Metadata**. The Source Expressions are the SharePoint parameter that are available to be sent to BAPI_PO_GETDETAIL on the SAP side. In this example, SharePoint queries SAP about a purchase order. You can send many parameters, but the only mandatory one for this particular function is the purchase order number.

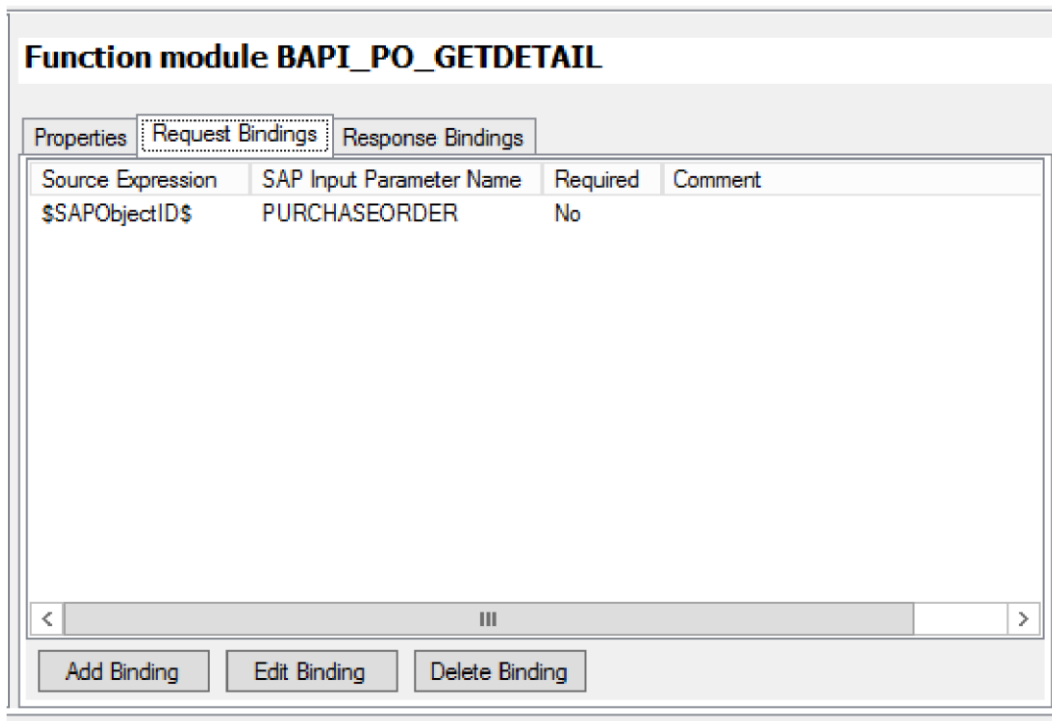


Figure 12-9 Example Request Bindings Tab in Function Module Pane

- In the **Request Bindings** tab, click **Add Binding**, **Edit Binding**, or **Delete Binding** to create the lists that you want. [Table 12-6](#) describes the fields.

Table 12-6 Fields to Add Bindings

Binding	Description
Request Bindings:Source Expression	The Source Expression is mapped to an SAP Input Parameter of the function module.
Request Bindings: SAP Input Parameter Name	The SAP name for the input parameter for the remote function module call.
Request Bindings: Required	Specifies if the request binding is a required field. If the request binding is required and the source expression is empty the query is not executed.
Request Bindings: Comment	A descriptive comment about the request binding mapping.

- Click the **Response Bindings** tab. The response bindings define how the **SAP Output Parameter Names** (fields returned from SAP) are mapped to attributes defined in the Attribute Container.

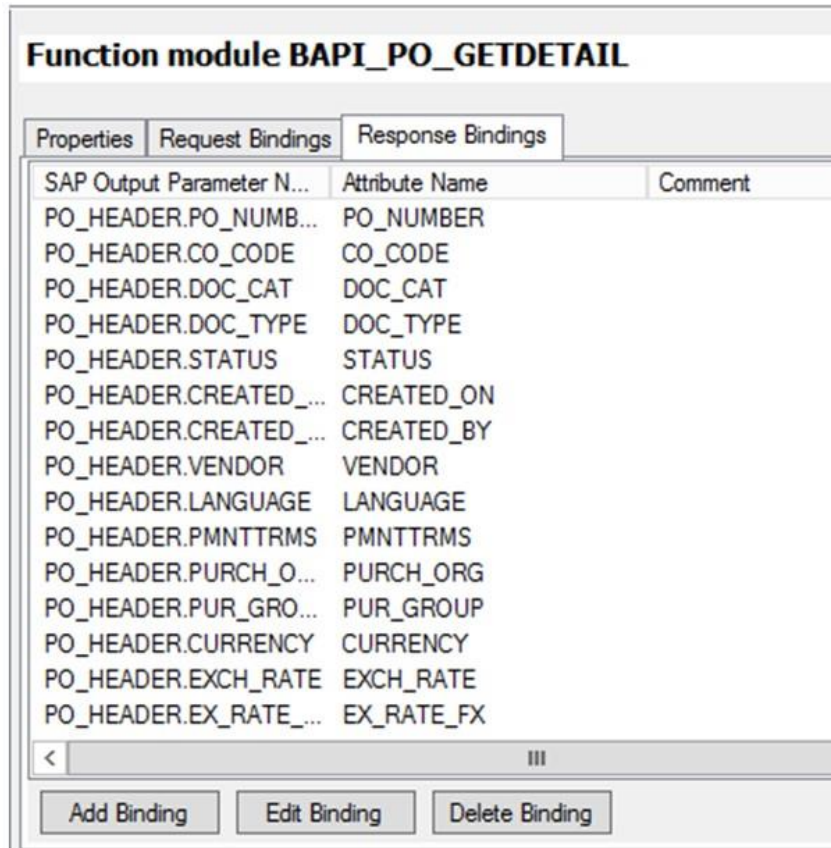


Figure 12-10 Example Response Bindings Tab in Function module Pane

8. In the **Response Bindings** tab, click **Add Binding**, **Edit Binding**, or **Delete Binding** to create the lists that you want. [Table 12-7](#) describes the fields.

Table 12-7 Fields to Add Bindings

Binding	Description
Response Bindings: SAP Output Parameter Name	SAP name of the output parameter of the RFC call
Response Bindings: Attribute Name	Attribute from the Attribute Container that is mapped to the SAP Output Parameter
Response Bindings: Comment	A descriptive comment about the response binding

12.2.3 Indexing Using Custom Indexers

Custom indexers are highly specialized indexers where the extraction of data from the SAP system is complex; for example, where data extraction might require complex joins, consultation with external third-party systems, or other scenarios. Contact Gimmel support if you think that you need to implement a custom table indexer.

12.2.4 Configuring Chained Indexers

Sometimes attributes need to be retrieved from several sources. For example, the Auto.index instance might need to retrieve some attributes of a purchase order and then use the SAP company code of the purchase order to retrieve additional details on the SAP company code. Another example would be when the desired data is located in two or more SAP data tables.

In situations like these, Gimmel recommends creating an ABAP custom function module that retrieves both sets of attributes and returns them in a single call. Such a custom function module could then be used by an RFC indexer. However, it might not be possible or practical to implement a custom function module. In those cases, the indexers in Auto.index can be *cascaded*, or *chained*.

- Cascaded indexers can be any one of the three indexer types described above
- Auto.index executes each of the indexers in order
- After each indexer completes, Auto.index saves the retrieved properties in the attribute container
- The next indexer uses the values in the attribute container written by the previous indexers as key values for its own operation

This cascading process proceeds until all indexers have completed.

Note:

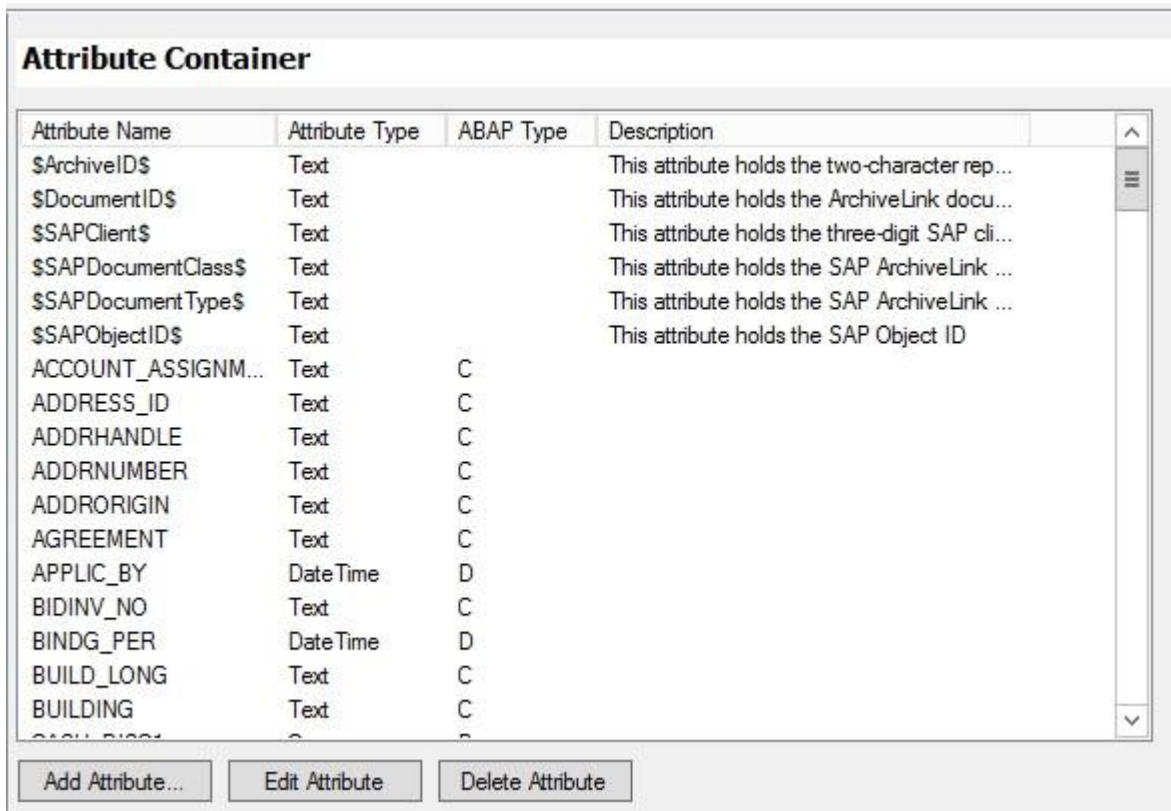
Cascading indexers offer convenience at the expense of performance. Each indexing operation requires $1 + nIndexer$ round-trip calls to the SAP application server, where $nIndexer$ is the number of indexers. Depending on the rate of documents being archived, having cascading indexers may become an avoidable load on the SAP application system. Consider developing a custom remote function module to use with a Remote Function Module indexer instead.

12.3 Populating the Attribute Container

The **Attribute Container** lists the attributes that can be extracted from SAP business objects. The attributes are used in the Document Service Modules as either input parameters or to provide mapping to or from SharePoint fields. Mapping of SAP attributes to Sharepoint fields is implemented in the **Read fields from Sharepoint** and **Write fields to Sharepoint** panes.

To populate the Attribute Container, follow these steps.

1. Select **Attribute Container** under the Document Service Module instance that you are configuring in the left pane. The Attribute Container information appears in the right pane.



The screenshot shows the 'Attribute Container' window with a table listing various attributes. The table has four columns: Attribute Name, Attribute Type, ABAP Type, and Description. Below the table are three buttons: 'Add Attribute...', 'Edit Attribute', and 'Delete Attribute'.

Attribute Name	Attribute Type	ABAP Type	Description
\$ArchiveID\$	Text		This attribute holds the two-character rep...
\$DocumentID\$	Text		This attribute holds the ArchiveLink docu...
\$SAPClient\$	Text		This attribute holds the three-digit SAP cli...
\$SAPDocumentClass\$	Text		This attribute holds the SAP ArchiveLink ...
\$SAPDocumentType\$	Text		This attribute holds the SAP ArchiveLink ...
\$SAPObjectID\$	Text		This attribute holds the SAP Object ID
ACCOUNT_ASSIGNM...	Text	C	
ADDRESS_ID	Text	C	
ADDRHANDLE	Text	C	
ADDRNUMBER	Text	C	
ADDRORIGIN	Text	C	
AGREEMENT	Text	C	
APPLIC_BY	DateTime	D	
BIDINV_NO	Text	C	
BINDG_PER	DateTime	D	
BUILD_LONG	Text	C	
BUILDING	Text	C	

Figure 12-11 Example Entries in Attribute Container

Some predefined attributes are always present in the Attribute Container (Table 12-8).

Table 12-8 Predefined Attributes in Attribute Containers

Attribute	Description
\$SAPObjectID\$	SAP object ID of the business object whose attributes are being extracted. Note: Not all attribute bindings involve an SAP field. Such bindings leave the SapFieldName blank.
\$SAPClient\$	SAP Client ID (MANDT) of the SAP application server.
\$ArchiveID\$	ArchiveLink archive ID.
\$DocumentID\$	ArchiveLink document ID.
\$SAPDocument-Class\$	SAP ArchiveLink document class of the document being processed.
\$SAPDocument-Type\$	SAP ArchiveLink document type of the document being processed.

- To populate the Attribute Container with the attributes that you want, use the **Add Attribute**, **Edit Attribute**, and **Delete Attribute** buttons. Table 12-9 describes all the fields.

Table 12-9 Fields to Add Attribute

Name	Description
Attribute Name	Name of the attribute as displayed in the SAP field.
Attribute Type	SharePoint attribute type. Only attributes of the following types are support in the attribute container. <ul style="list-style-type: none"> • Text • Currency • Date Time • Integer

ABAP Type	ABAP attribute type: <ul style="list-style-type: none"> ● C: character data ● N: numerical character data ● P: packed numeric data ● D: date ● I: 32-bit integer
Description	An optional description of this attribute.

12.4 Writing Attributes to SharePoint

Write attributes to SharePoint enables the attributes provided from the SAP business object (for example, BAPI_PO_GETDETAIL) to be mapped to SharePoint fields in the document library. The **Source Expression** is added from the attributes populated in the Attribute Container. To configure this function, follow these steps.

1. Click **Write attributes to SharePoint** in the left pane under the instance of Auto.index that you want to configure. Only the attributes listed in the **Request Bindings** tab are written to the SharePoint columns.

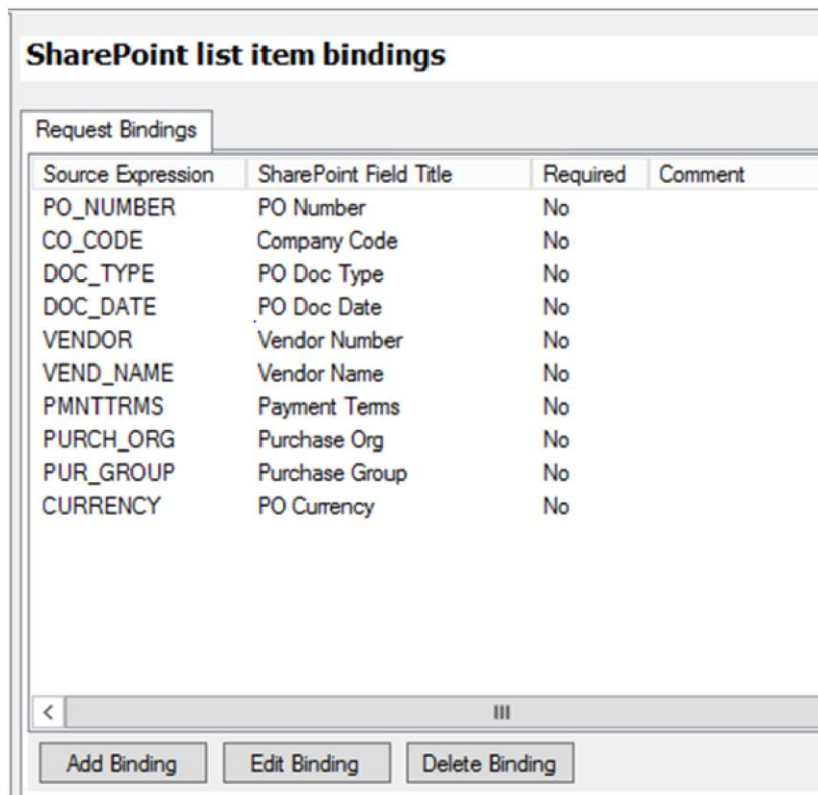


Figure 12-12 SharePoint list item bindings

Table 12-10 describes the fields.

Table 12-10 Fields to Add Request Bindings

Binding	Description
Source Expression	Source expression that maps to the SAP field in the attribute container, SAP return parameter or SAP table column.
SharePoint Field Title	Title of SharePoint field that the source expression is mapped to. Note: The SharePoint Field Title uses SharePoint's display names.
Required	Specifies if the source expression is a required field. If the source expression is required and the source expression is empty, then the attributes are not written to the SharePoint fields. Select <i>Yes</i> or <i>No</i> .
Comment	Optional descriptive comment for the source expression mapping.

2. For the **Source Expression**, enter a name that is already present in the Attribute Container.
3. To create the request bindings, follow these steps.
 - a. To add a binding, click **Add Binding**. A field opens in the **Request Bindings** column.
 - b. Select a name from the list or type a new name for the **Source Expression**.
 - c. Press **Tab** to go to the next field.
 - d. Select from the SharePoint Field Title list for the **Attribute Name**.
 - e. Press **Tab** and type in a **Comment**.
 - f. Use the **Edit Binding** and **Delete Binding** buttons to make changes to existing bindings.

12.5 Mapping SAP Document Types to SharePoint Content Types

You can assign content types by following the steps in [12.4 Writing Attributes to SharePoint](#). Auto.index can assign a SharePoint content type to the archived document based on the SAP document type and class. Content type is assigned by creating rules in the Auto.index **Content Type Mappings** pane. Each rule consists of an SAP document type, an SAP document class, and a SharePoint content type name. If the SAP document Type and class match, then the document is assigned the corresponding SharePoint content type.

To map the SAP document types to the SharePoint content types, follow these steps.

1. Click **Content Type Mapping** under the Auto.index instance in the left pane.
In the example in [Figure 12-13](#), all **SAP Document Types** and **SAP Document Classes** are associated to **Purchase Orders** in **SharePoint Content Type**. Auto.index processes the rules from top to bottom as they appear in the **Content Type Mappings** editor. Specifying an asterisk (*) or an empty string in either the SAP Document Type or SAP Document Class is equivalent to *match anything* and specifies a default rule after all

previous rules have been tried. If at runtime, no rule matches, no content type is assigned to the document and a warning is issued in the Event log.

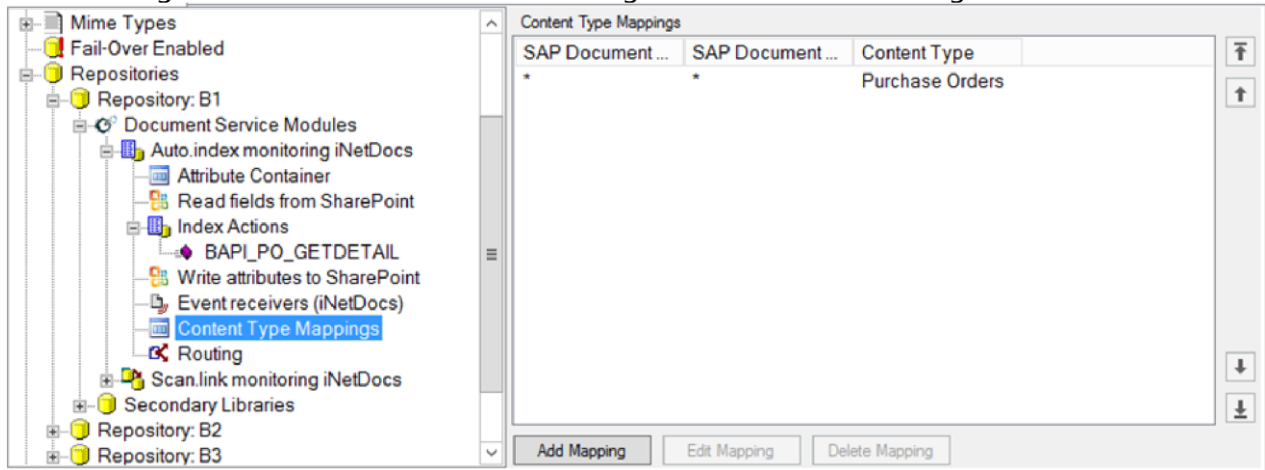


Figure 12-13 Example of Mapping the SAP Document Types and Classes to the SharePoint Content Type

2. Click **Add Mapping**, **Edit Mapping**, or **Delete Mapping** as necessary to create the list of mapping that you want. [Table 12-11](#) describes the fields.

Table 12-11 Fields in SAP Document Type Mapping Pane

Binding	Description
SAP Document Type	SAP document type
SAP Document Class	SAP document class
(SharePoint) Content Type	The SharePoint Content Type that the SAP document type and class will be mapped to

12.6 Configuring Auto.index Document Routing Rules

iNet.DM supports storing archived documents from one logical ArchiveLink archive in one or more physical SharePoint document libraries. A common reason for doing this is that the different document libraries can be assigned differing access permissions. Often, access to a document needs to be controlled depending on some property associated with the document.

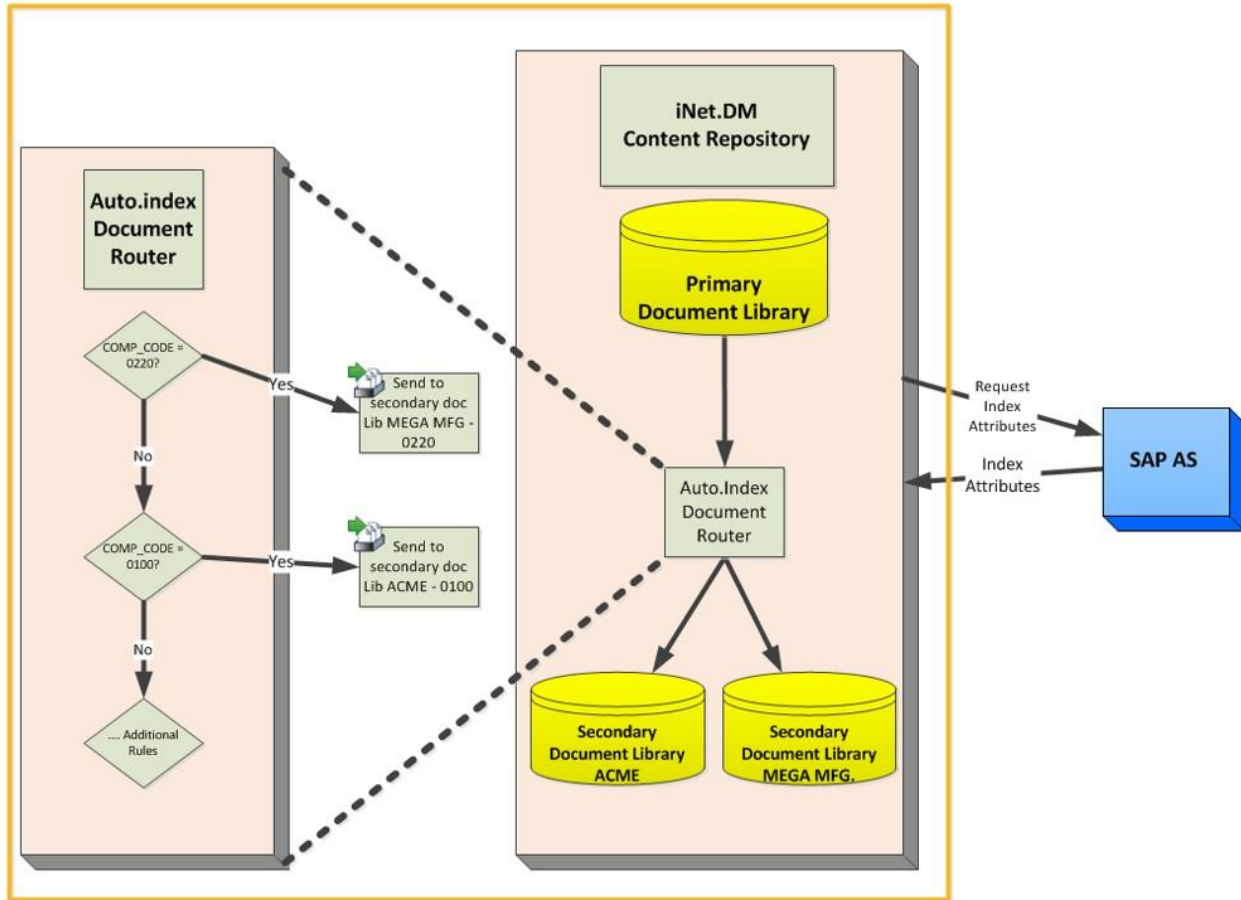


Figure 12-14 Document Routing

Auto.index document routing can move a document from an archive library to another library or folder based on attributes retrieved from the SAP object and populated to the Sharepoint document properties. Sharepoint does not have these extended properties until they are indexed from SAP.

The Auto.index Document Service Module offers simple document routing based on attributes retrieved by the indexers. The administrator can configure routing rules that specify which attribute value should be compared to which constant value, and to which document library the document should be moved if the rule is met.

12.6.1 Configuring Read Fields from SharePoint

Note:

Complete these instructions only if you are using a SharePoint field for Auto Routing.

The **Read Fields from Sharepoint** pane maps fields from the Sharepoint site to attributes in the Attribute Container. The response bindings of this mapping are used in the Index Actions that you configure ([12.4 Writing Attributes to SharePoint](#)).

To configure the fields to read from SharePoint, follow these steps.

1. Click **Read Fields from SharePoint** under the Document Service Module instance that you want to configure. The Sharepoint list item bindings display in the right pane.
2. Select the **SharePoint Field Titles** from a drop-down list of available fields.
3. Select the **Attribute** name from the drop-down list of available attributes, or you can create a new attribute.

12.6.2 Managing Bindings in Read Fields from SharePoint

To manage bindings, follow these steps:

1. Click **Read Fields from SharePoint**.
2. Click **Add Binding** to create a new binding.
3. Click **Edit Binding** to edit the selected binding.
4. Click **Delete Binding** to delete the selected binding.

[Table 12-12](#) describes the fields.

Table 12-12 Fields to Add Attribute

Binding	Description
SAP Document Type	SAP document type
SAP Document Class	SAP document class

Table 12-12 Fields to Add Attribute

Binding	Description
(SharePoint) Content Type	The SharePoint Content Type that the SAP document type and class will be mapped to

12.6.3 Setting Up Routing Rules

Before you start executing the **Routing Rule** functionality, make sure that Auto.index and the SAP Object Type have been configured successfully.

To navigate to the **Routing Rule** pane, follow these steps.

1. Expand the **Auto.index Monitoring** section in the tree on the left side.
2. Click the **Routing** item to see the **Routing Rules** in the right pane.

Routing Rules				
Routing condition	Site URL	Destination Libr	Folder path	File n...
=[VENDOR] = "0000001000"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000		Inv-
=[VENDOR] = "0000003902" O...	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000		
=[VENDOR] = "0000000015" A...	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000	/Invoice	
=[VENDOR]="0000003815"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Format("VEND...		

Destination Library	Folder path	File n...
mal.sharepoint.com/sites/DocSite	Vendor_1000	Inv-
mal.sharepoint.com/sites/DocSite	Vendor_1000	
mal.sharepoint.com/sites/DocSite	Vendor_1000	/Invoice
mal.sharepoint.com/sites/DocSite	Format("VENDOR-{0}"; [VENDOR_ID])	

Figure 12-15 Routing Rules Displayed in Gimmel Link Administration Console

The following sections explain how different rules can be set up.

Note:

When using DMS, additions to the document container in SAP will trigger an update event for all documents in that container. If new routing rules have been entered since the first archival of the documents, they will be routed in accordance with the new rules.

12.6.4 Routing Documents to SharePoint Folders

You can create folders in a repository and route documents directly to the correct folder. For example, follow these instructions.

1. Create a folder in the SharePoint repository named *Invoice*.
2. Set the **Routing Rule** as follows:

Routing Condition - [VENDOR] = "00000000015".

Site URL- <http://erplinkgimmel.sharepoint.com/sites/DocSite>.

Destination Library- Vendor_1000

Folder Path- /Invoice.

Routing Rules				
Routing condition	Site URL	Destination Library	Folder path	File name prefix
=[VENDOR] = "0000001000"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000		Inv-
=[VENDOR] = "0000003902" O...	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000		
=[VENDOR] = "0000000015" A...	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000	/Invoice	
=[VENDOR]="0000003815"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Format("VENDOR-{0}"; [VEN...		

Figure 12-16 Routing Rule to Route Documents from Vendor 1000 to Folder Fold_1

3. Archive document from SAP with vendor number 1000.

4. Verify the event logs.

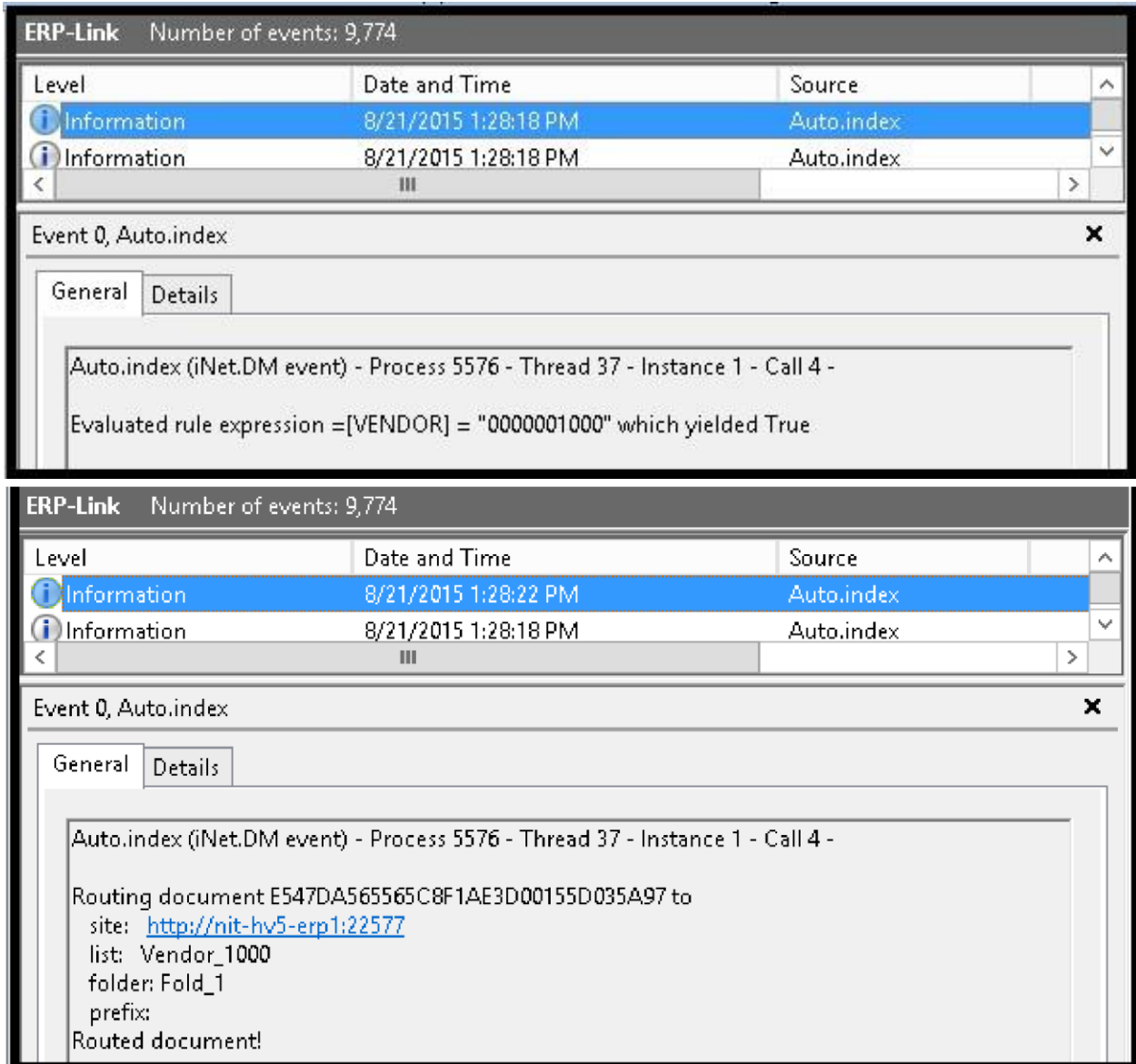


Figure 12-17 Event Logs Showing Correct Handling of Document with Vendor 1000

5. Now go to SharePoint and verify that document was successfully routed to Fold_1.



Figure 12-18 Document Correctly Routed to Fold_1

12.6.5 Setting Single Routing Rule Offering Multiple Routing Paths

You can create a routing rule with a **Site URL** that drives different documents to different locations based on the content's metadata. A single document can only be routed to a single location. Create the rule according to the following parameters and examples.

- Syntax of rule in Auto.index
 - Routing Condition: True
 - Site URL: `http://test.com/sites/{CompanyCode}`
 - Destination `{LibraryVendorName}`
 - Folder: `{VendorNumber}`
 - File Name Prefix: `{PONumber}`
 - Document Stored At:
`http://test.com/sites/{CompanyCode}/{VendorName}/{VendorNumber}/{PONumber}_xxxx.xxx`
- Special considerations
 - Routing Condition: This is a logical condition with True or False result.
 - Site URL: the site must pre-exist. Routing rule does not create site. If the **evaluate site** value does not exist, the routing rule will fail.
 - Destination Library: The destination library must pre-exist. Routing rule does not create site. If the **evaluated document library** does not exist, the routing rule will fail.
 - Folder: If the Folder exists, files are copied into the existing folder. If the Folder does not exist, it **will be created** by the routing rule. If the Site URL and the Destination Library exist, this value does not cause a routing rule failure.
 - File Name Prefix: No special consideration exists for this parameter.

- Document Stored At:
 http://test.com/sites/Site_{CompanyCode}/{VendorName}_{VendorNumber}/{PONumber}_xxxx.xxx • Evaluated Routing Condition: True
- Evaluated Site URL: http://test.com/sites/1000
 - Evaluated Destination Library: 2022
 - Evaluated Folder: 2000
 - Evaluated File Name Prefix: 45000002
 - Document Stored At: http://test.com/sites/Site_1000/2022_2000/45000002_data.pdf

12.6.6 Setting Multiple Routing Rules

You can set multiple rules to manage the document routing. Auto.index looks at each rule in order and executes the first rule that is true. For example, if a document matches all three rules in the following example, then Auto.index executes the first rule and routes the document to Vendor_1000.

Routing condition	Site URL	Destination Lib
= [VENDOR] = "0000001000"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
= [VENDOR] = "0000003902" OR [PO_NUMBER] = "4500014364"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
= [VENDOR] = "0000000015" AND [PO_NUMBER] = "4500014483"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
= [VENDOR] = "0000003815"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Format("VEND

Figure 12-19 Multiple Routing Rules in Auto.index

In the following example, when the first rule is false, then Auto.index moves to the next rule. In this example, the second rule is true; therefore, it executes and the document is routed to Vendor_3000.

Routing condition	Site URL	Destination Lib
=[VENDOR] = "0000001000"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR] = "0000003902" OR [PO_NUMBER]="4500014364"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR] = "0000000015" AND [PO_NUMBER]="4500014483"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR]="0000003815"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Format("VEND

Figure 12-20 Auto.index Executes Second Rule

If the first two rules executes false, and the third rule executes true, then the third rule execute and the document is routed to the Exception_Library repository.

Routing condition	Site URL	Destination Lib
=[VENDOR] = "0000001000"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR] = "0000003902" OR [PO_NUMBER]="4500014364"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR] = "0000000015" AND [PO_NUMBER]="4500014483"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR]="0000003815"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Format("VEND

Figure 12-21 Auto.index Executes Third Rule

If all the rules are executed as false, then the document is not moved from the iNet.DM library.

12.6.7 Routing Based on Dates

Gimmel Link enables routing based on **DateTime** fields from SharePoint. After binding a DateTime SharePoint Field to an attribute, you can set up routing rules to compare dates that are accurate to the day.

As shown below, the format to compare against is yyyyMMdd. So 07/24/2018 (MM/dd/yyyy) becomes 20180724.

Examples:

1. Route all documents from 07/24/2018 to the Folder "OnThisDay".

Routing Condition "[TDATE] = 20180724" Site URL= "http://server/sites/SharePointSite"
Destination Library= "Docs" Folder path= "OnThisDay"

2. Route all documents after 07/24/2018 to the Folder "AfterThisDay".

Routing Condition "[TDATE] > 20180724" Site URL= "http://server/sites/SharePointSite"
Destination Library= "Docs" Folder path= "AfterThisDay"

3. Route all documents before 07/24/2018 to the Folder "BeforeThisDay".

Routing Condition "[TDATE] < 20180724" Site URL= "http://server/sites/SharePointSite"
Destination Library= "Docs" Folder path= "BeforeThisDay"

4. Route all documents on or after 07/24/2018 to the Folder "OnOrAfterThisDay".

Routing Condition "[TDATE] >= 20180724" Site URL= "http://server/sites/SharePointSite"
Destination Library= "Docs" Folder path= "OnOrAfterThisDay"

5. Route all documents on or before 07/24/2018 to the Folder "OnOrBeforeThisDay".

Routing Condition "[TDATE] <= 20180724" Site URL= "http://server/sites/SharePointSite"
Destination Library= "Docs" Folder path= "OnOrBeforeThisDay"

6. Route all documents except those from 07/24/2018 to the Folder "NotOnThisDay".

Routing Condition "[TDATE] <> 20180724" Site URL= "http://server/sites/SharePointSite"
Destination Library= "Docs" Folder path= "NotOnThisDay"

7. Route all documents from the year 2018 to the Folder "2018"

Routing Condition "=(TDATE] > 20180000) AND ([TDATE] < 20190000)" Site URL= "http://server/sites/SharePointSite" Destination Library= "Docs" Folder path= "2018"

12.6.8 Setting Routing Rules with Logical Operators

You can set the **Routing Rules** using the following logical operators and expressions:

=

<>

>

<

>=

<=

AND

OR

NOT

Beginswith(sourceString, searchString)

Endswith(sourceString, searchString)

Contains(sourceString, searchString)

SubStr(string, startIndex, length)

RemovePrefix(string, startIndex)

Format(format, stringToFormat)

Pad(value, fieldSize, padChar, justification)

The following examples demonstrate how to route rules using the AND and OR operators.

1. When you set the **Routing Rules** with an AND operator as in the following example, the document is routed to the destination library (Vendor_1000 in this case) if and only if both the conditions ({VENDOR} = "0000001000" AND {PO_NUMBER} = "4500014476") are matched.

Routing Rules		
Routing condition	Site URL	Destination Lib
=[VENDOR] = "0000001000"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR] = "0000003902" OR [PO_NUMBER]="4500014364"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR] = "0000000015" AND [PO_NUMBER]="4500014483"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR]="0000003815"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Format(VEND

Figure 12-22 Logical Operator AND in Routing Rules

2. When you set the **Routing Rules** with an OR operator as in the following example, the document is routed to the destination library if only one of the conditions ({VENDOR} = "0000001000" OR {PO_NUMBER} = "4500014476") is matched. Of course, it is also routed to the destination library if both conditions are met, too.

Routing condition	Site URL	Destination Lib
=[VENDOR] = "0000001000"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR] = "0000003902" OR [PO_NUMBER]="4500014364"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR] = "0000000015" AND [PO_NUMBER]="4500014483"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Vendor_1000
=[VENDOR]="0000003815"	https://erplinkgimmel.sharepoint.com/sites/DocSite	Format(VEND

Figure 12-23 Logical Operator OR in Routing Rules

12.7 Testing Auto.index Configuration

To verify that Auto.index is working correctly, a late archival operation can be initiated from within SAP. The way to do this can vary widely depending on the **SAP Object Type** and business scenario in question. Once the archival is complete, a document should appear in the iNet.DM content repository: this is the normal operation of iNet.DM. Then, after a few seconds, attributes values should appear in the document properties.

1. You can also manually place a document with the expected properties, such as Company Code, in a SharePoint iNet.DM library configured with Auto.index.
2. Wait a few seconds and check the iNet.DM library to see if the metadata has been added.
3. If the routing was configured in the Auto.index instance, check the destination SharePoint library to see if the document was moved to it, and check that the metadata has been added.
4. If the Auto.index operation fails, consult the Windows event log for diagnostic error messages.

13 Configuring Scan.link

Early archival occurs when documents are archived before a corresponding Transactional Record is created in SAP. In early archival, the incoming document drives creation of the SAP transaction record. An example of an early archival is when documents arrive in the archive because Scan.link performed an automated archival, but the document is not linked to an SAP transactional record nor does Auto.index index the document with the metadata.

Late archival occurs when documents are archived after the SAP transaction record is created. An example of a late archival is when an SAP user attaches a document image to an SAP business object instance and the document is managed in the iNet.DM archive in SharePoint.

Scan.link is a Document Service Module that automates SAP document archival processes in SharePoint without requiring users to log into the SAP system.

A sample Scan.link process could look like the following.

1. User/process drops a document into iNet.DM document library.
2. Scan.link checks all documents in this library at the time interval set in the Timer Service.
3. Scan.link checks for one or more required properties. If any of the required properties are not present, Scan.link considers the document incomplete; that is, not ready for processing, and does no further processing. The administrator can use this feature to prevent *early archival* by configuring one of the required properties to be the SAP transactional record number; for example, a Purchase Order number. Scan.link can, however, perform early archival if that is what it is configured to do.
4. If all the required properties are present on the document, Scan.link can invoke one of the linking actions:
 - Link document to SAP business objects using ArchiveLink with object ID: Used to create ArchiveLink link inside SAP system
 - Link document to SAP business object using ArchiveLink with bar codes: Used to create a bar code entry inside SAP
 - Invoke an SAP workflow: Used to start a workflow using SharePoint site columns and document link as parameters to workflow
 - Interact with any remote enabled SAP function module: Used to create a more complex scenario to invoke SAP actions based on SharePoint document properties and document ID
5. After a linking action successfully finishes, Scan.link can move the document and any properties on it to an iNet.DM content repository.

13.1 Creating New Scan.link Instance

To add a new instance of Scan.link, follow these steps.

1. Using the **Gimmel Link Administration Console**, open the Gimmel Link configuration file.
2. Right-click **Document Service Modules** in the left pane and select **Add Scan.link**.
3. Click the newly created Scan.link instance in the left pane and modify the parameters in the right pane similarly to this example. You can complete additional fields to this example, but the critical fields are shown. The name of the Scan.link instance automatically adjusts to indicate which SharePoint iNet.DM library (MonitoredListTitle) this instance monitors.

Scan.link monitoring iNetDocs	
<ul style="list-style-type: none"> Messages <ul style="list-style-type: none"> Missing Document Type Error Message Misc <ul style="list-style-type: none"> Description Document Status Field Title: DocStatus Logging Level: Information SAP <ul style="list-style-type: none"> Client Ids SAP Object Type: BUS2012 SAP Settings: SAP Setting 1 Scan.link <ul style="list-style-type: none"> Library Name: iNetDocs Required Field Titles: String[] Array Timer Task <ul style="list-style-type: none"> Enabled: True Interval: 5 Minimum Age: 20 Validation <ul style="list-style-type: none"> Invalid Text Perform Validation: False Valid Text Validation Status Field Title 	

Figure 13-1 Example Configuration for Scan.link Instance

4. Complete the information in the right pane. The example in [Figure 13-1](#) includes the critical parameters. [Table 13-1](#) describes all the fields.

Table 13-1 Scan.link Configuration Pane Settings

Field Title	Description
Messages	

Missing Document Type Error Message	Message shown in Doc Status field if Scan.link is unable to determine the SAP document type and class from the content type and/or file extension of the uploaded file.
Misc	
Description	Descriptive comment for this instance of a Document Service Module.

Table 13-1 Scan.link Configuration Pane Settings

Field Title	Description
DocStatusFieldTitle	Title of the SharePoint field in which the Document Service Module document status is stored.
SAP	
SAP Settings	The SAP connection to use to communicate to the SAP Server.
SAP Object Type	the SAP business object type to which documents are linked and/or from which indexing properties are fetched.
Scan.Link	
Library Name	Name of the SharePoint document library that is managed by iNet.DM. The name of the Scan.link instance automatically changes to reflect the text you enter in this field.
Required Field Titles	Titles of the SharePoint fields that must have a value for the linking to occur. Note: The Required Field Titles field expects SharePoint's internal name for the column you want to use.
Timer Task	
Enabled	Indicates whether the timer will be executed by the service. Refer to 16 Configuring the Gimmel Link Timer Service for more information about setting the Timer Service.
Interval	Timer interval in seconds. Must be >5 seconds.
Minimum Age	Specifies how old documents must be before they are processed by the Scan.link timer task. Negative numbers are not allowed.
Validation	
Invalid Text	Text to display in the validation status field if validation fails.

Perform Validation	If <i>True</i> , Scan.link calls the SAP system to validate the business object whose ID is stored in the field specified in the SAObjectType.
Validation Status Field Title	Result of the validation is stored in a field with this name.
Valid Text	Text to display in the validation status field if validation was successful.

13.2 Populating the Attribute Container

The **Attribute Container** lists the attributes that can be extracted from SAP business objects. The attributes are used in the Document Service Modules as either input parameters or to provide mapping to or from SharePoint fields. Mapping of SAP attributes to Sharepoint fields is implemented in the **Read fields from Sharepoint** and **Write fields to Sharepoint** panes.

To populate the Attribute Container, follow these steps.

1. Select **Attribute Container** under the Document Service Module instance that you are configuring in the left pane.

The screenshot shows the 'Attribute Container' interface. It contains a table with the following data:

Attribute Name	Attribute Type	ABAP Type	Description
\$ArchiveID\$	Text		This attribute holds the two-character repository ID
\$DocumentID\$	Text		This attribute holds the ArchiveLink document ID
\$SAPClient\$	Text		This attribute holds the three-digit SAP client number
\$SAPDocumentClass\$	Text		This attribute holds the SAP ArchiveLink document class of the d
\$SAPDocumentType\$	Text		This attribute holds the SAP ArchiveLink document type of the d
\$SAPObjectID\$	Text		This attribute holds the SAP Object ID

Figure 13-2 Example Entries in Attribute Container

Some predefined attributes are always present in the Attribute Container (Table 13-2).

Table 13-2 Predefined Attributes in Attribute Containers

Attribute	Description
\$SAPObjectID\$	SAP object ID of the business object whose attributes are being extracted. Note: Not all attribute bindings involve an SAP field. Such bindings leave the SapFieldName blank.
\$SAPClient\$	SAP Client ID (MANDT) of the SAP application server.
\$ArchiveID\$	ArchiveLink archive ID.
\$DocumentID\$	ArchiveLink document ID.

\$SAPDocument- Class\$	SAP ArchiveLink document class of the document being processed.
\$SAPDocument- Type\$	SAP ArchiveLink document type of the document being processed.

2. To populate the Attribute Container with the attributes that you want, use the **Add Attribute**, **Edit Attribute**, and **Delete Attribute** buttons. [Table 13-3](#) describes all the fields.

Table 13-3 Fields to Add Attribute

Name	Description
Attribute Name	Name of the attribute as the column in SAP displays.

Table 13-3 Fields to Add Attribute

Name	Description
Attribute Type	SharePoint attribute type. Only attributes of the following types are support in the attribute container. <ul style="list-style-type: none"> • Text • Currency • Date Time • Integer
ABAP Type	ABAP attribute type: <ul style="list-style-type: none"> • C: character data • N: numerical character data • P: packed numeric data • D: date • I: 32-bit integer
Description	A description of this attribute.

13.3 Configuring Read Fields from SharePoint

The **Read Fields from Sharepoint** pane maps fields from the Sharepoint site configured in the index action to attributes in the Attribute Container. The response bindings of this mapping are used in the Index Actions that you configure ([13.4 \(Optional\) Configuring Scan.link to Perform Validation Using Indexed Metadata](#)).

To configure the fields to read from SharePoint, follow these steps.

1. Click **Read Fields from SharePoint** under the Document Service Module instance that you want to configure.
2. Modify the list by using the **Add Binding**, **Edit Binding**, and **Delete Binding** tabs. [Table 13-4](#) describes the fields.

Table 13-4 Fields to Add Attribute

Binding	Description
SharePoint Field Title	Title of SharePoint field to map to attribute name. This is the column in the SharePoint document library that you want to map to an Attribute Name. Note: The SharePoint Field Title uses SharePoint's display names.
Attribute Name	Attribute name used as input parameter to SAP business object type. Populated from Attribute Container.

Table 13-4 Fields to Add Attribute

Binding	Description
Comment	Comment to describe the attribute mapping.

13.4 (Optional) Configuring Scan.link to Perform Validation Using Indexed Metadata

If you need validation, Scan.link can use the Indexer function to validate the SAP object IDs for documents in the iNet.DM library. The Scan.link event listener queries the SAP application server to determine whether an SAP object with the supplied SAP object ID truly exists before proceeding with archival. If no object with the supplied SAP object ID can be found, Scan.link stops processing the scanned document and indicates a validation failure in one of the document properties. User intervention can resolve validation failures, or Scan.link continues periodically to query the SAP server until the SAP object ID does exist. Then Scan.link continues with its configured tasks on the document.

The validation support will catch errors where the operator has entered nonexistent SAP object IDs. However, Scan.link validation cannot prevent the operator from errors such as entering an incorrect SAP object ID 4512 instead of 4511 when both object IDs are valid. Advanced validation scenarios are handled by implementing a validation workflow before the Scan.link operation.

To implement validation, follow these steps.

1. Configure indexing to confirm if a particular field in the document's SharePoint record has been indexed by Auto.index; for example, determine if the SAP object ID is present.
2. In the main Scan.link configuration pane (see [Figure 13-1](#) and [Table 13-1](#)), set the **Validation** fields as follows:

- a. **InvalidText:** Enter the text here that you want to appear in the SharePoint column **ValidationStatusFieldTitle** if the validation is invalid; that is, if the SAP business object does not exist yet.
- b. **PerformValidation:** Set this field to *True*.
 - i. If the status is *False*, Scan.link does nothing with the document. It remains in the iNet.DM library.
 - i. If the status is *True*, Scan.link performs whatever actions that you configured it to perform on the document.
- c. **ValidationStatusFieldTitle:** Enter the name of the SharePoint column that you want the validation status written to.
- d. **ValidText:** Enter the text here that you want to appear in the SharePoint column **ValidationStatusFieldTitle** if the validation is valid; that is, if the SAP business object does exist.

13.5 Mapping SharePoint Content Types and File Extensions to SAP Document Types and Classes

Before Scan.link can archive a document, it must obtain an SAP Document Type for the document. SAP Document Types are *required* when linking documents to business objects. You can configure Scan.link with rules that assign a document a particular Document Type depending on the SharePoint content type of the document, the file extension of the document, or a combination of both. Scan.link can also apply a default Document Type and a default Document Class to *all* documents arriving in the monitored document library, if no other rules apply.

You can configure it to do this by creating rules in the **SAP Document Type Mappings** pane. Each rule consists of a SharePoint content type, file extension, SAP document type, and an SAP document class. If the archived document's SharePoint content type and file extension match a rule, then the document is assigned the corresponding SAP document type and class.

To map the SharePoint content types to the SAP document types, follow these steps.

1. Click **SAP Document Type Mappings** under the Scan.link instance in the left pane.

Scan.link processes the rules from top to bottom as they appear in the **SAP Document Type Mappings** pane. Specifying an asterisk (*) or an empty string in either the SharePoint **Content Type** or **File Ext** fields is equivalent to *match anything* and specifies a default rule after all previous rules have been tried. If at runtime, no rule matches, no SAP document type and/or class is assigned to the document and a warning is issued in the Event log.

SAP Document Type Mappings			
Content Type	File E...	SAP Document ...	SAP Document ...
*	DOC	Z_B1_DOC	DOC
*	PDF	Z_B1_PDF	PDF
*	DOCX	Z_B1_DOCX	DOCX
*	JPG	Z_B1_JPG	JPG
*	TXT	Z_B1_TXT	TXT

Figure 13-3 Example of Mapping the SharePoint Content Types and File Extensions to the SAP Document Types and SAP Document Classes

2. Click **Add Mapping**, **Edit Mapping**, or **Delete Mapping** as necessary to create the list of mapping that you want. [Table 13-5](#) describes the fields.

Table 13-5 Fields in SAP Document Type Mapping Pane

Binding	Description
(SharePoint) Content Type	Sharepoint Content Type to be mapped to SAP Document Type and SAP Document Class
(SharePoint) File Extension	File extension of the SharePoint archived document
SAP Document Type	SAP document type
SAP Document Class	SAP document class

13.6 Using Linkers

Scan.link can link to SAP in several different ways.

- The default linker is **ArchiveLink linker**, which uses the standard ArchiveLink function module in SAP
- Documents with bar codes can be managed and linked to corresponding bar codes in SAP with the **Barcode linker**.
- The RFC linker uses a custom function module in SAP to connect with ArchiveLink.
- Workflow starter invokes a workflow in SAP.

13.6.1 Configuring ArchiveLink Linker to Link Document to SAP Business Object

After the document is successfully archived, Scan.link can use ArchiveLink linker to link the document to an SAP business object instance specified by the identifier computed by the KeyExpression. This automatic attachment is only carried out if Scan.link has been configured to calculate the SAP object ID from one or more of the properties on the archived SharePoint document. To perform this calculation, Scan.link evaluates the **KeyExpression** to yield an SAP object ID. The **KeyExpression** is expected to be a syntactically correct expression. Identifiers in the expression are interpreted as the titles of SharePoint fields on the document.

Example:

The SharePoint field **PO Number** is used to store a user-entered purchase order number "1052". To indicate that this field should be used verbatim, the following expression is used:

```
[PO Number]
```

When evaluated, this returns *1052*, the same value as was stored in the field "PO Number". To ensure that the **PO Number** consists of 10 digits, the following expression can be used:

```
Pad([PO Number],10,"0","R")
```

This expression pads the **PO Number** in a 10-digit, right-justified field with zeros, yielding the value *0000001052*.

After the KeyExpression is evaluated, the resulting value is used as the SAP Object ID and passed to SAP ArchiveLink, which in turn establishes a link between the SAP Object ID and the archived document.

If all these stages complete successfully, the original document in the monitoring document library is deleted. This deletion normally happens within a second of the document arriving in the monitoring document library. This timing implies that during normal operation, the Scan.link monitoring document library should be empty. If the monitoring document library is not empty after a few seconds, an error has occurred. Troubleshooting errors by consulting the Windows Application log and referring to [17 Troubleshooting](#) in this guide.

To configure Scan.link for this task, follow these steps:

1. Click **Linker** in the left pane under the instance of Scan.link that you are configuring.
2. Select *ArchiveLink linker* as the **Linker Type**.

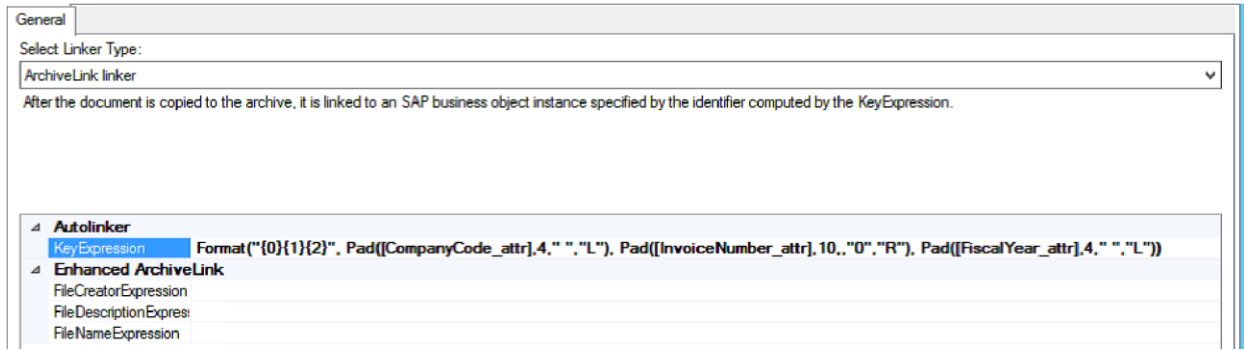


Figure 13-4 ArchiveLink linker Pane 3.

Complete the fields. [Table 13-6](#) describes all the fields. [Table 13-6 ArchiveLink linker Pane Settings](#)

Field Title	Description
KeyExpression	Expression which when evaluated yields the unique SAP object identifier used for linking. Enter the KeyExpression in a formatting string. The example in Figure 13-4 pads input as necessary to fit SAP’s requirements. This KeyExpression consists of the Response Bindings requested in Read Fields from SharePoint . See also Configuring RFC linker to Call Custom SAP Function Module .

Table 13-6 ArchiveLink linker Pane Settings

Field Title	Description
FileCreatorExpression	Specifies an expression which, when evaluated, is used as the enhanced ArchiveLink file creator name. Note: Do not use this field unless you have applied the enhancement described in SAP note 1451769.
FileDescriptorExpression	Specifies an expression which, when evaluated, is used as the enhanced ArchiveLink description. Note: Do not use this field unless you have applied the enhancement described in SAP note 1451769.

<p>FileNameExpression</p>	<p>Specifies an expression that, when evaluated, is used as the enhanced ArchiveLink file name.</p> <hr/> <p>Note:</p> <p>Do not use this field unless you have applied the enhancement described in SAP note 1451769.</p> <hr/>
---------------------------	---

13.6.2 Configuring Barcode Linker to Associate Document with Barcode

You can configure Scan.link to assume that image files in the SharePoint iNet.DM library configured for Scan.link are documents with a Barcode present in one of the properties. Scanning software might add bar codes automatically to documents before the documents are placed in the SharePoint iNet.DM library, or the scan operator might enter them manually.

Scan.link archives the document in the iNet.DM content repository and then requests the SAP application server to establish a link between the archived document and the bar code. If the bar code exists in SAP (*late archival*), the bar code is resolved immediately. If the bar code has not yet been introduced to SAP (*early archival*), the bar code and the ID of the document it is associated with is stored in the table BDS_BAR_EX.

When Scan.link is configured to perform linking between archived documents and bar codes, no other linking is done with SAP business objects.

To configure Scan.link to associate an archived document with a bar code in SAP, follow these steps:

1. Click **Linker** in the left pane under the instance of Scan.link that you are configuring.
2. Select *Barcode linker* as the **Linker Type** in the right pane.

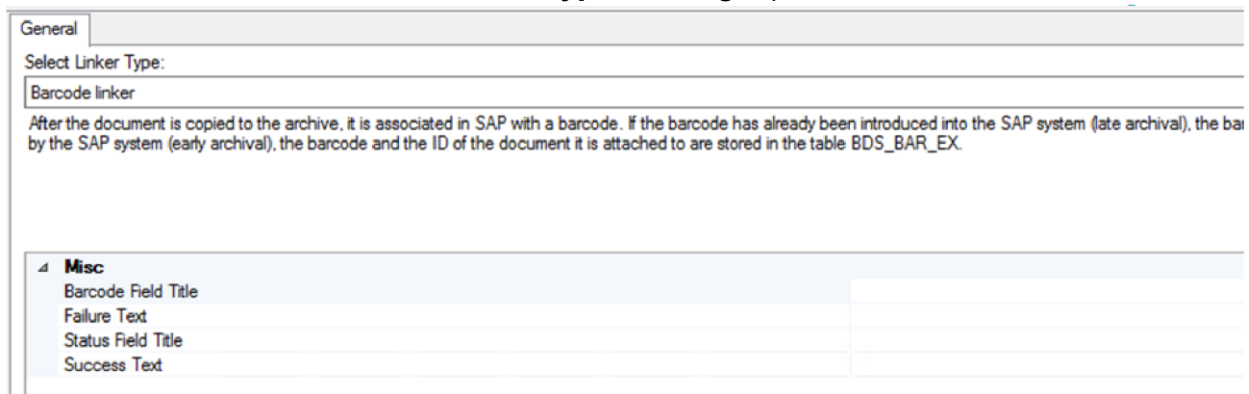


Figure 13-5 Setting up Linker for Invoices 3.

Complete the fields. [Table 13-7](#) describes all the fields.

Table 13-7 Barcode linker Pane Settings

Field Title	Description
Barcode Field Title	The title of the field that contains the bar code
Failure Text	The value that is displayed in the StatusFieldTitle field
Status Field Title	Title of the field containing the status of the bar code operation.
Success Text	The text to display in the BarcodeFieldTitle if bar code operation succeeds.

13.6.3 Configuring Workflow Starter to Trigger a Workflow in SAP

After the document is copied to the archive, an SAP workflow can be started with the specified user name. These workflows are custom workflows defined by the customer SAP developers and administrator.

A Workflow Starter linker could, for example, be configured to link a document to a SAP business object to implement other processes such as approvals or calls to other processes in SAP or external systems.

Scan.link can also add an arbitrary number of workflow container element bindings. The SAP workflow is responsible for making sure that the document is linked to an SAP business object at some later point in time.

To configure Scan.link to launch an SAP workflow, follow these steps.

1. Click **Linker** in the left pane under the instance of Scan.link that you are configuring.
2. Select *Workflow starter* as the **Linker Type** in the right pane.

General | SAP Workflow Container

Select Linker Type:

Workflow starter

After the document is copied to the archive, an SAP workflow is started. The workflow will be initiated with the specified user name. An administrator is responsible for making sure the document is linked to an SAP business object at some later point in time.

Misc

Username	
Workflow Id	

Figure 13-6 Setting up Linker for Invoices 3.

Complete the fields. [Table 13-8](#) describes all the fields.

Table 13-8 Workflow starter Pane Settings

Field Title	Description
Username	SAP user ID used when starting the workflow. Obtained from the SAP administrator.
Workflow ID	SAP workflow ID to be started after the document is archived. Obtained from the SAP administrator.

4. Click the **SAP Workflow Container** tab.

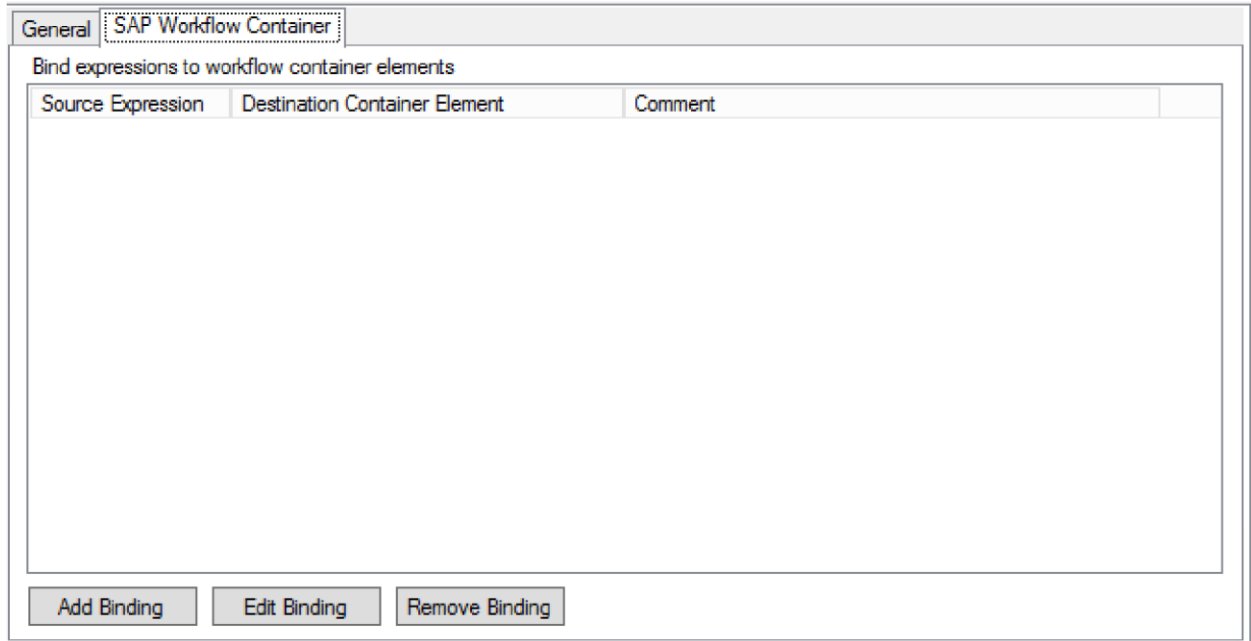


Figure 13-7 Example Entries in SAP Workflow Container Tab for Workflow Linker

5. Populate the **SAP Workflow Container** using the **Add Binding**, **Edit Binding**, and **Remove Binding** buttons. [Table 13-9](#) describes all the fields.

Table 13-9 SAP Workflow Container Settings

Field Title	Description
Source Expression	Expression from the Attribute Container to map to the SAP workflow attribute
Destination Container Element	SAP workflow attribute that the Source Expression is mapped to
Comment	A descriptive comment for the mapping

13.6.4 Configuring RFC linker to Call Custom SAP Function Module

Scan.link can be configured to use the RFC linker to call an SAP function module. Such a custom function module can link the document in the iNet.DM library to a SAP business object by calling ArchiveLink, and it can also perform other custom actions, including calls to SAP or external systems.

The configuration depends on the following.

- You must use a remote-enabled SAP function module.
- Scan.link passes parameters from the SharePoint columns and a uniquely generated document ID to the SAP function module.
- The SAP function module is responsible for appropriate SAP side actions; for example, creating link entries in SAP based on the Scan.link-passed Document ID.
- Upon successful execution of the SAP function module, Scan.link archives the document to the archive location.

To configure the parameter values to send to the function module based on the values of the attribute container, follow these steps.

1. Click **Linker** under the Scan.link instance you want to configure to call the SAP function module.
2. In the right pane, select **Linker Type RFC linker**.

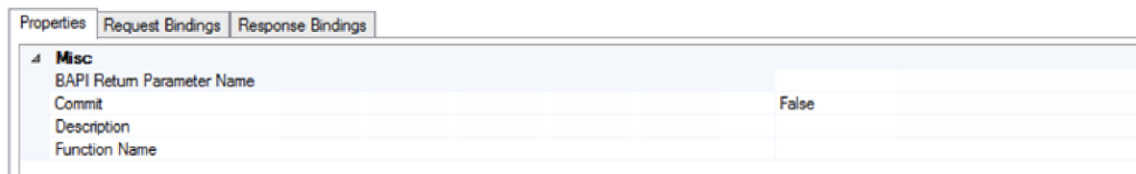
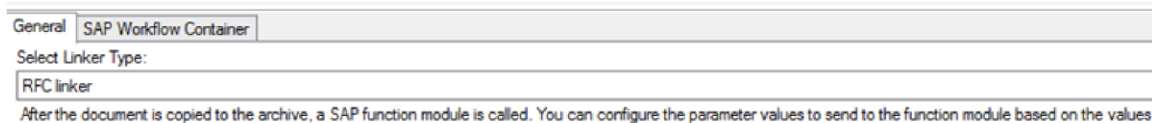


Figure 13-8 RFC linker Calling Custom SAP Function Module

3. Complete the fields. [Table 13-10](#) describes the fields.

Table 13-10 RFC linker Settings

Field Title	Description
Bapi Return Parameter Name	Return parameter name of the SAP business object (BAPI)

Commit	Boolean indicating if the SAP business object is committed
Description	Optional descriptive text of the SAP business object
FunctionName	Name of the SAP business object

- Click the **Request Bindings** tab.
- Populate the list using the **Add Binding**, **Edit Binding**, and **Delete Binding** buttons. [Table 13-11](#) describes all the fields.

Table 13-11 RFC linker Request Bindings Tab

Field Title	Description
Source Expression	An expression incorporating attributes forming a value to be used when invoking the RFC call
SAP Input Parameter Name	The SAP input parameter name to be used to supply the value from the source expression when invoking the RFC call
Required	Specifies whether the RFC call expects a non-empty value to make a valid call
Comment	A descriptive comment

- Click the **Response Bindings** tab.
- Populate the list using the **Add Binding**, **Edit Binding**, and **Delete Binding** buttons. [Table 13-12](#) describes all the fields.

Table 13-12 RFC linker Request Bindings Tab

Field Title	Description
SAP Output Parameter Name	The name of the SAP output parameter to hold the value to be used.
Attribute Name	The attribute from the Attribute Container to hold the returned value.
Comment	A descriptive comment.

13.7 Testing Scan.link Configuration

To verify that Scan.link is working properly, follow this step:

- Upload a document manually into the iNet.DM folder configured for Scan.link.
- The uploaded document remains in the monitoring library until the SharePoint item properties specified as *Required* have non-empty values. Property values can be entered using the **Edit properties** button in SharePoint.

3. Check to see if the document was properly processed. Once all the properties have been entered, Scan.link copies the document along with the properties to the iNet.DM content repository. Then, it deletes the original document from the monitoring library. Verify that a new document has appeared in the iNet.DM content repository and that the monitoring folder is empty.

An item that remains in the monitoring folder after the values have been entered indicates a problem. Ensure that all fields specified as *Required* have non-empty values; then consult the Windows event log for diagnostic messages.

Note:

Scan.link does not perform any validation of these property values. The default configuration assumes that the operator is entering valid information in the required fields. Typically, one of the SharePoint properties specified as *Required* is the `keyFieldTitle`, which stores a business object identifier (such as a purchase order number or a vendor ID). Scan.link evaluates the `keyExpression` field in its default configuration to provide the object ID for the linking operation. If `keyExpression` evaluates to an incorrect object ID, it could cause documents to be linked to the wrong SAP business object.

Scan.link provides simple validation support. Custom scenarios that extend Scan.link can implement a validation workflow that ensures that value obtained by evaluating the `keyExpression` field is indeed a valid object number before performing the linking operation. Please contact Gimmel for more information about implementing a custom extension of Scan.link.

14 Configuring Auto.index Update Connection

You must configure the shared configuration for Web Service Security and the SAP Parameters for the Auto.index Update Connection.

14.1 Configuring the Shared Configuration for Web Service Security

Follow these steps to configure Web Service Security for the Shared Configuration.

1. Log onto the Gimmel Link Admin Console.
2. Select **Web Service Security** in the left pane. The Web Service Security information displays on the right.

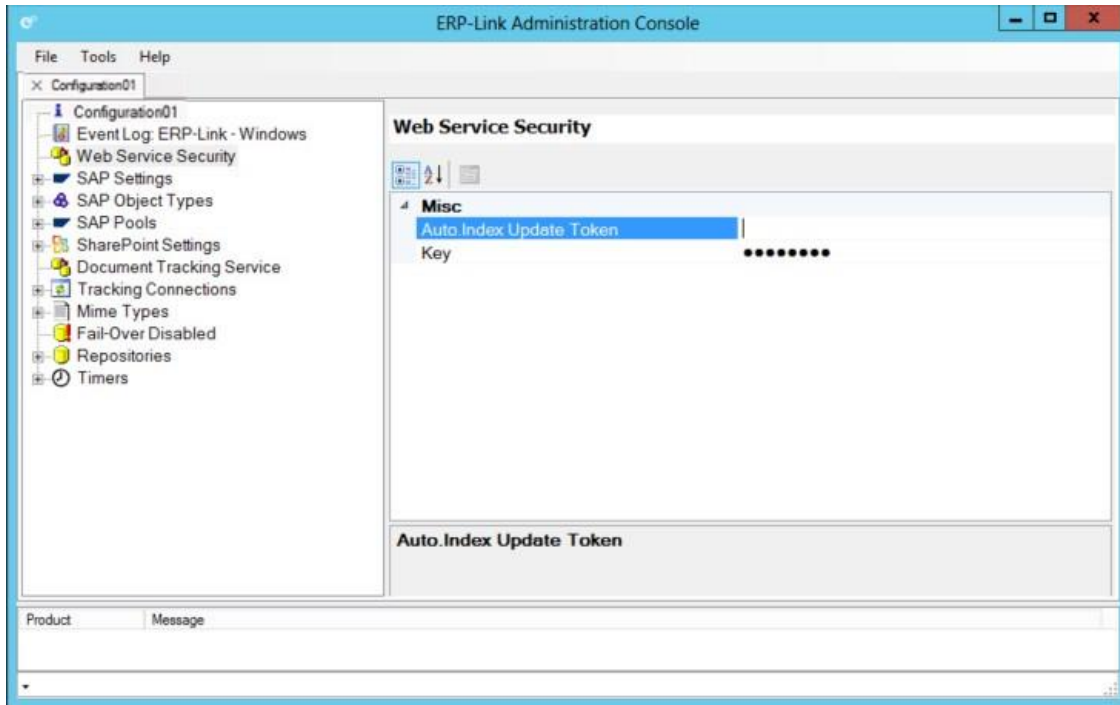


Figure 14-1 Selecting Web Service Security from the Gimmel Link Administration Console

3. Enter the **Auto.Index Update Token**.

Note:

You also enter this same token when configuring the SAP parameters in the next section.

4. The **Key** field populates by default, which can be any value, but is a required field.
5. Click **Save**.

14.2 Configuring SAP Parameters for Auto.index Update

Follow these steps to configure the parameters necessary for SAP to connect to Auto.index Update:

1. Log on to SAP.
2. Import all distributed transports for Auto.index Update.
3. Type `/n/ERPLKGM/ AIUPD` in the transaction field and press **Enter**. See [Deploying Custom SAP Transports](#) for more information.
4. Click **Auto.index Update** on the top menu to see the transaction menu.

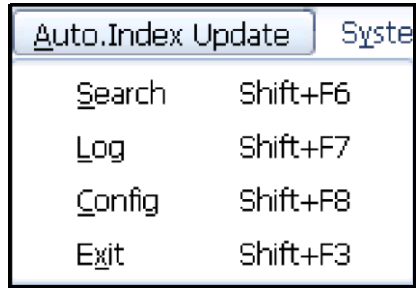


Figure 14-2 Transaction Menu

5. From the transaction menu, choose **Config**.

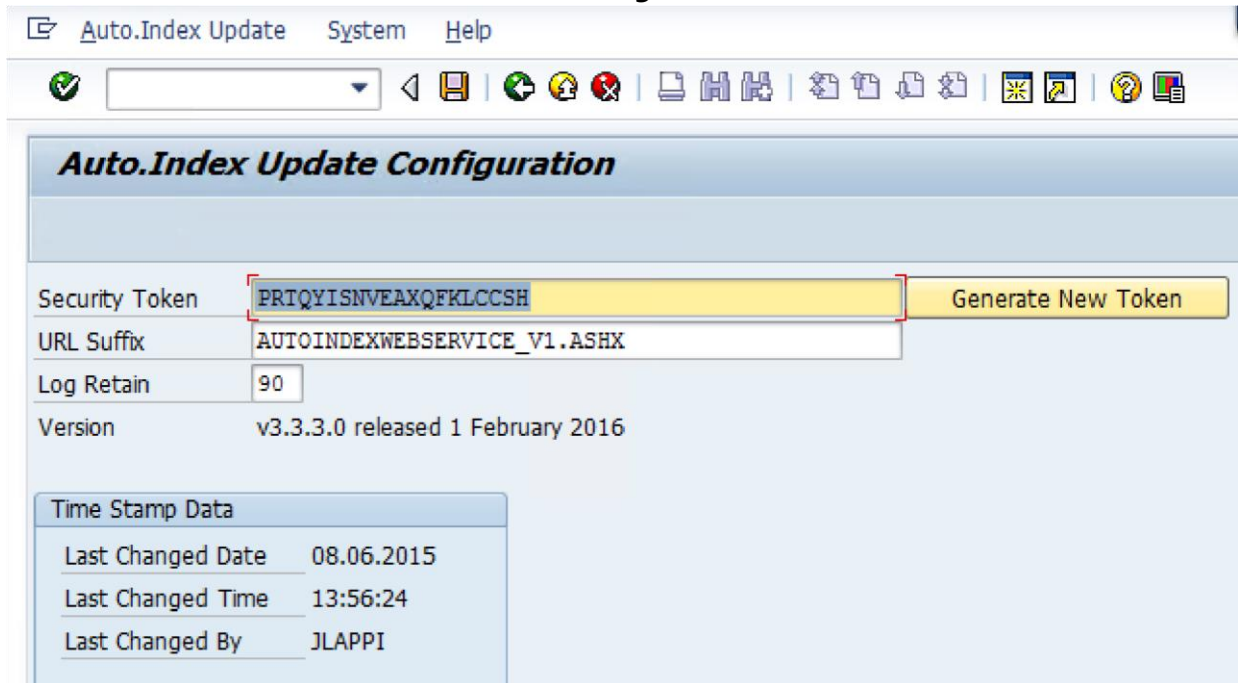


Figure 14-3 Auto.Index Update Configuration Dialog Box

6. If this is the first configuration of Auto.index Update or if you want to change a previous token, click **Generate New Token**. The new token displays in the **Security Token** field.

Note:

The Security Token must be synchronized in the ERPLinkConfig.xml file for Auto.Index Update to work.

7. In the **URL Suffix** field, enter the name of the Auto.index Update Web service that Auto.index Update sends the notification to and which then relays the information to Auto.index.
-

Note:

Change this parameter ONLY upon instructions from your Gimmel implementation consultant.

8. In the **Log Retain** field, enter the number of days to retain log entries. You can also manually trim the log.
9. Click **Save**.

15 Changing Auto.index Update Notifications

You can configure different types of Auto.index Update notifications:

- Manually Invoking a One-Time Update
- Configuring SAP to Notify Auto.index of Changes

Note:

See [Configuring Auto.index Update Notifications Outside SAP Workflow](#) for information on configuring notifications outside of the SAP workflow.

15.1 Manually Invoking a One-Time Update

You can create a transaction to manually invoke SAP to compile a list of documents that match the search criteria and notify Auto.index via Auto.index Update. Auto.index then indexes all the metadata that it is configured to index for these documents stored in SharePoint, whether the metadata changed since the initial indexing or not.

Follow these steps to manually invoke a one-time notification to Auto.index. You must have configured SAP to connect to Auto.index Update (See [Configuring Auto.index Update Connection](#)).

1. Log on to SAP.
2. Type `/n/ERPLKGML/AIUPD` into the transaction field and press **Enter**.
3. Click **Auto.index Update** on the top menu and select **Search**.

Auto.Index Update Object Search			
Execute			
Enter Selection Parameters			
Object Type	BUS2012	to	<input type="text"/>
SAP object ID	<input type="text"/>	to	<input type="text"/>
Archive ID	<input type="text"/>	to	<input type="text"/>
Document ID	<input type="text"/>	to	<input type="text"/>
Storage date	<input type="text"/>	to	<input type="text"/>

Figure 15-1 Search Dialog Box

4. Enter the selection parameters to identify the SAP business object to be monitored. You can enter ranges of parameters to search on. You do not have to enter all these parameters. You can, for example, enter a range of Object Types, OR a range of SAP object IDs. Use this dialog to make the search as broad or as specific as you want it.

- a. **Object Type:** Enter the SAP object type for the given object to update; for example, BUS2012 or BKPF.
- b. **SAP object ID:** Enter the unique object identifier.
- c. **Content Rep. ID:** Enter the two-letter content repository ID corresponding to the iNet.DM repository.
- d. **Document ID:** Enter a range of document IDs to monitor.
- e. **Storage date:** Enter a range of storage dates to include.

5. Click **Execute** to start the search.

The query returns a list of document IDs and the associated metadata that meet the specified search criteria.

Client	ObjectType	Object ID	Cont. Rep.	Document ID	Doc. type
800	BUS2012	4500004871	C1	02CC3E4BE923...	Z_C1_PDF
800	BUS2012	4500004871	C1	51782E3A553C...	Z_C1_PDF
800	BUS2012	4500004871	C1	64E8FE4269964...	Z_C1_PDF
800	BUS2012	4500004871	C1	8E241F6B7A0D...	Z_C1_PDF

Figure 15-2 Search Results

6. Click **Execute** on the **Search Results** pane. The list of IDs is passed to the Auto.index Update Web service, which passes the list to Auto.index. Auto.index reindexes all fields that it is configured to index for all the document IDs in the iNet.DM repository in SharePoint.

If you want another search, you must configure another search and execute it. If you want ongoing notification whenever something changes, refer to the next section [Configuring SAP to Notify Auto.index of Changes](#).

Sometimes there is no SAP event that corresponds to an object modification. If you have a custom program, then you might need to manually trigger Auto.index Update for attached documents.

15.2 Configuring SAP to Notify Auto.index of Changes

You can configure tasks for event linkages to specify changes that you want SAP to notify Auto.index of as they occur. After notification, Auto.index retrieves the new metadata and updates the documents stored in SharePoint. You can create and configure as many tasks as you need to.

Follow these steps to create a new task. You must have configured SAP to connect to Auto.index Update (see Chapter 14 [Configuring the Shared Configuration for Web Service Security](#)).

1. Log into SAP and locate the transaction field.



Figure 15-3 Transaction Field in SAP 2.

Type *PFTC* in the transaction field and press **Enter**.

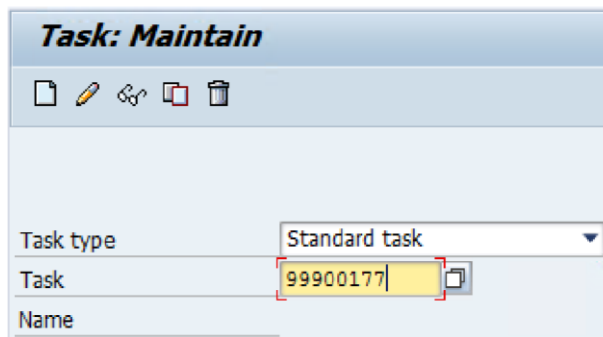


Figure 15-4 Task: Maintain Pane for Transaction PFTC

3. In the **Task: Maintain** pane:
 - a. Select **Task type** Standard task.
 - b. Type *99900177* for the **Task**.
 - c. Click the **Create** button in the tool bar.

Standard Task: Create

Standard task: 99900177
 Name: TestingAIUpdate
 Package: _____ Applicatn Component: _____

Basic data | Description | Container | Triggering events | Terminating

Name
 Abbr.: 99900177
 Name: TestingAIUpdate
 Release status: Released

Work Item Text
 Work item text: &IV_OBJECT_ID&& &_WI_OBJECT_ID.&

Object method
 Object Category: ABAP Class
 Object Type: /ERPLKGML/CL_AUTOINDEX_UPDATER ERP-Link Auto.index
 Method: SEND_HTTP_NOTIFICATIONS
 Synchronous object method

Execution
 Background processing Executable with SAPforms
 Confirm end of processing

Figure 15-5 Standard Task: Create Pane with Example Entries

4. Complete the following values in the **Standard Task: Create** pane:
 - a. **Abbr:** Enter an identifying abbreviation for the task.
 - b. **Name:** Enter a name for the task.
 - c. **Release status:** Select a status. Select Released if you want the task to start when you complete all the steps to configuring the task.
 - d. **Work item text:** This is a free-form text entry that will appear in the log. You can type whatever you want, or click in the field and then click the Insert Variables button to select a meaningful description.
 - e. **Object Category:** Select ABAP Class.
 - f. **Object Type:** Type /ERPLKGML/CL_AUTOINDEX_UPDATER.
 - g. **Method:** Type SEND_HTTP_NOTIFICATIONS for updates to be sent to all content repositories.
 - h. **Synchronous object method:** Select this option.
 - i. **Background processing:** Select this option.

5. Click the **Binding Object Method** button in the **Object Method** section (see [Figure 15-5 Standard Task: Create Pane with Example Entries](#)).

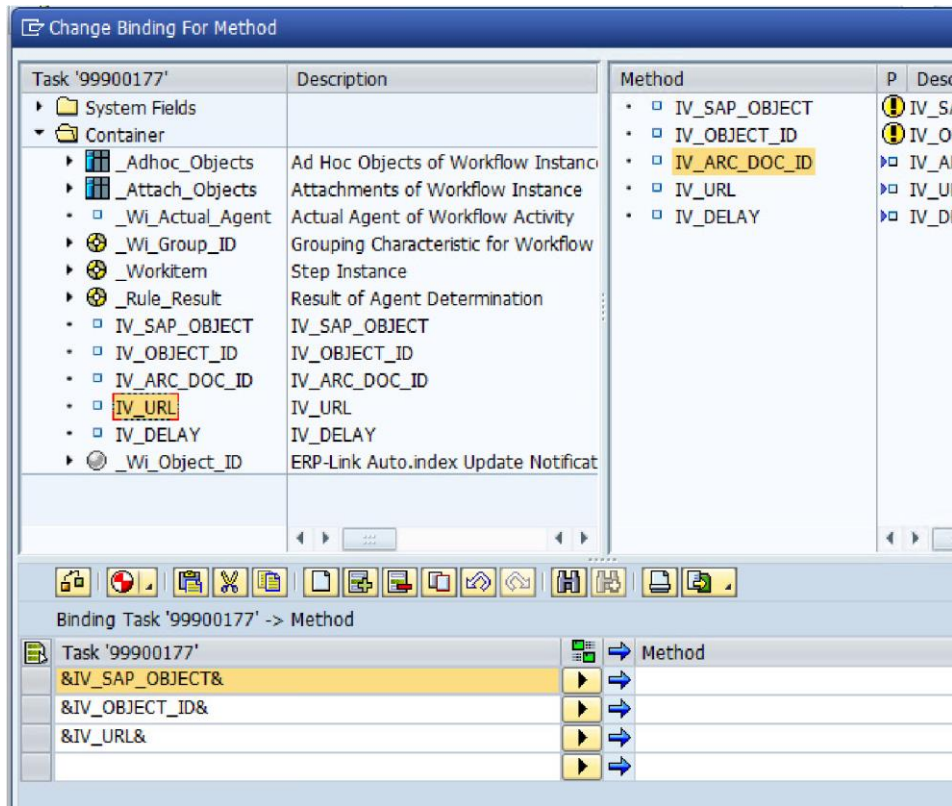


Figure 15-6 Change Binding Tasks in Method Dialog Box

6. Drag and drop the following items from the **Task** field at the top left of the dialog box to the **Binding Task** field at the bottom left of the dialog box.
 - IV_SAP_OBJECT
 - IV_OBJECT_ID
 - IV_URL (Optional, this field is used for advanced configuration options)
7. Look at the right side of the same pane.

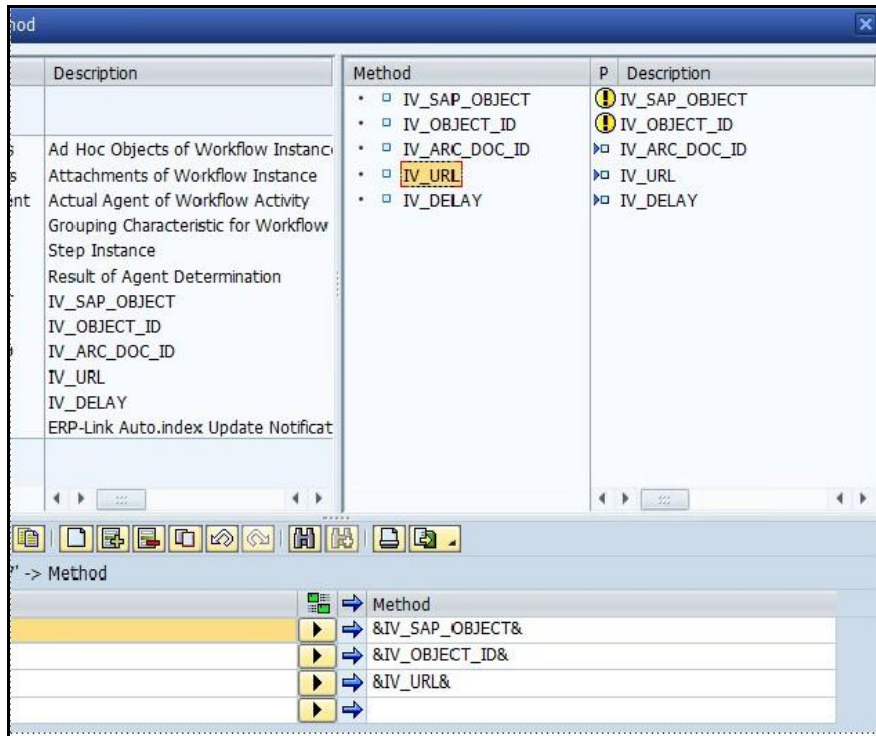


Figure 15-7 Change Method in Method Dialog Box

8. Drag and drop the following Tasks from the Method field in the top right to the Method field at the right side of the grid at the bottom
 - IV_SAP_OBJECT
 - IV_OBJECT_ID
 - IV_URL (Optional: this field is used for advanced configuration options)

9. Click the **Exit Binding Editor** button at the bottom of the dialog box to return to the previous dialog box.

10. On the **Standard Task: Create** pane, click the **Triggering events** tab.

For this example, this task executes when the **Changed** event is initiated for a purchase order with object type BUS2012.

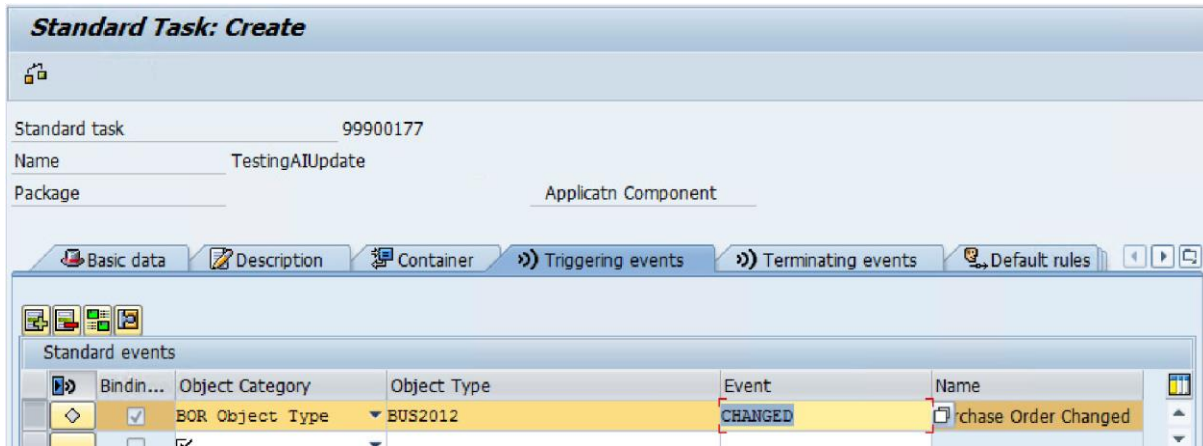


Figure 15-8 Triggering an Event

11. Select a configured row by clicking the gray box to the left of it; then click the **Call Binding Editor** button in the grid command bar.
12. Configure the event parameters by dragging and dropping the following fields into the grids for **Event Changed** and **Task**.

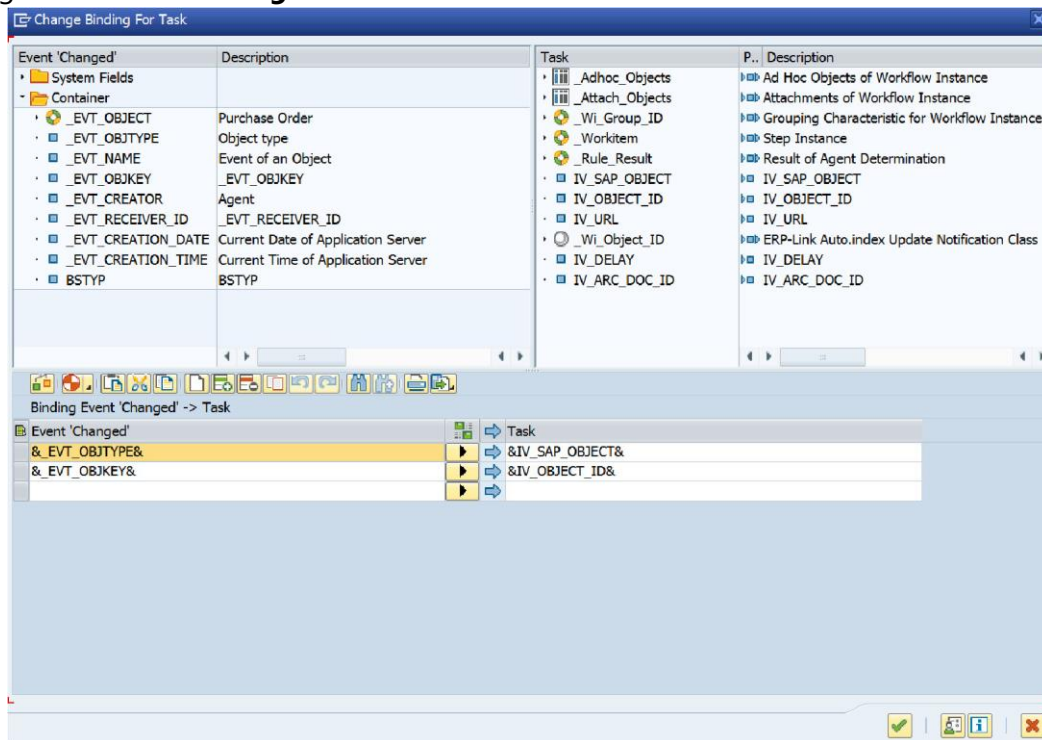


Figure 15-9 Configuring Event Parameters

13. Click the **Exit** button to return to the **Triggering Events** tab.
14. Click the activation button for the selected row to enable the task to call the Auto.index Update Document Service Module.

If the activation is successful, a green square will appear on the button to the left of the Binding column. If it does not successfully activate, you can click this button to see a message explaining why the activation was not successful.

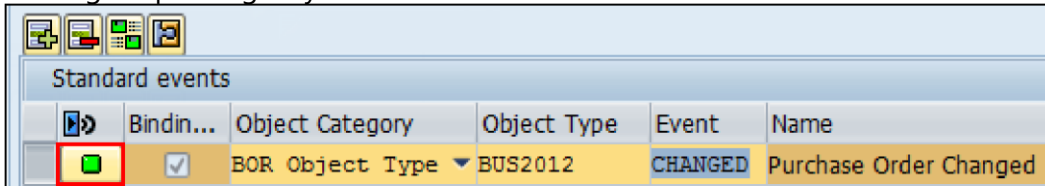


Figure 15-10 Activating the Task

15. If you selected **Released** as the Release status on the Basic Data tab, then the task activates immediately.

You can configure additional events as needed.

16 Configuring the Gimmel Link Timer Service

The Gimmel Link Timer Service performs the following tasks:

- Executes Scan.link instances (See “Timer Task” in [Table 13-1 Scan.link Configuration Pane Settings](#))
- Moves files from one file system location to another file system location ([16.3 Adding a File Mover Task](#))
- Uploads files from a file system location into SharePoint ([16.4 Adding a File Uploader Task](#))

The File Mover and File Uploader tasks are described later in this chapter.

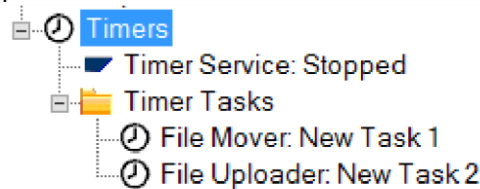


Figure 16-1 Timer Configuration Node in the Gimmel Link Configuration File

16.1 Enabling the Timer Service for a Configuration

The Gimmel Link Timer Service supports processing of the current configuration file.

For a timer task to be processed, the following conditions must be met:

- The Timer Service should be enabled for the configuration.
- The Timer Task must be configured on the "Current Configuration".
- The individual timer task needs to be enabled.

You can edit an Gimmel Link configuration service’s description and indicate whether it is Timer Service Enabled.

Follow these steps to enable the Timer Service on a configuration:

1. Launch the Gimmel Link Administration Console.
2. Open a configuration from the Configuration Service.



Figure 16-2 Configuration Information

3. Click the Configuration Title in the left pane to display the Configuration Information.
4. Change "Timer Service Enabled" to **True**.

Note

The **Description** field is the Title of the Configuration.

The **Timer Service Enabled** field indicates whether the Timer Service processes the configuration during its operation.

The **Uniqueld** field is the primary key in the database for the configuration and is readonly.

5. Click **File > Save** to save the modifications to this configuration.

16.2 Stopping or Starting Timer Service

To stop or start the Timer Service global configuration, follow these steps.

1. Launch the Gimmel Link Administration Console.
2. Open the current configuration.
3. Expand the **Timers** node.
4. Click the **Timer Service: Stopped/Started** node to display the timer service control pane.

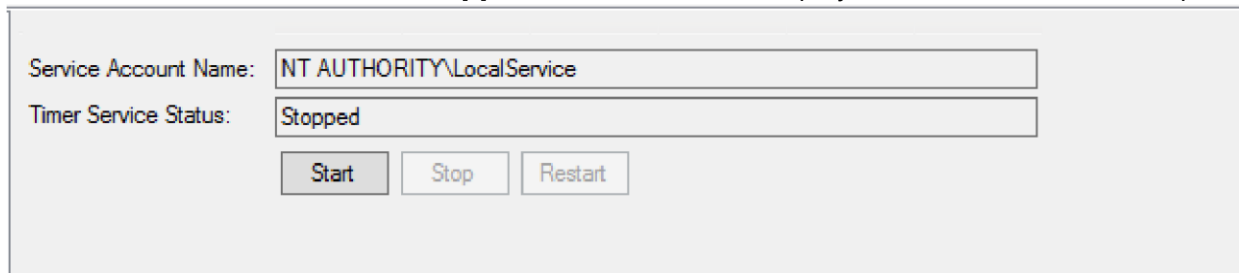


Figure 16-3 The Timer Service Control Pane

Table 16-1 describes the fields in the control pane.

Table 16-1 Timer Service Control Pane Fields

Field	Description
Service Account Name	The Windows user that the service runs under. This user can be changed in the services snap-in of the Microsoft Management Console (MMC).
Timer Service Status	The current status of the timer service.
Start, Stop, and Restart Buttons	The Start and Stop buttons toggle between themselves. The Timer Service Status tells you whether the service is stopped or started; click the Start or Stop button to change the status to the desired value. The Restart button stops and then restarts the Timer Service.

16.3 Adding a File Mover Task

Add a new File Mover task by following these steps.

1. Launch the Gimmel Link Administration Console.
1. Open the current configuration.
2. Right-click the **Timers** node and select **Add File Mover Task**.
3. Click the **File Mover: New Task X** in the tree. The right pane displays the configuration parameters.

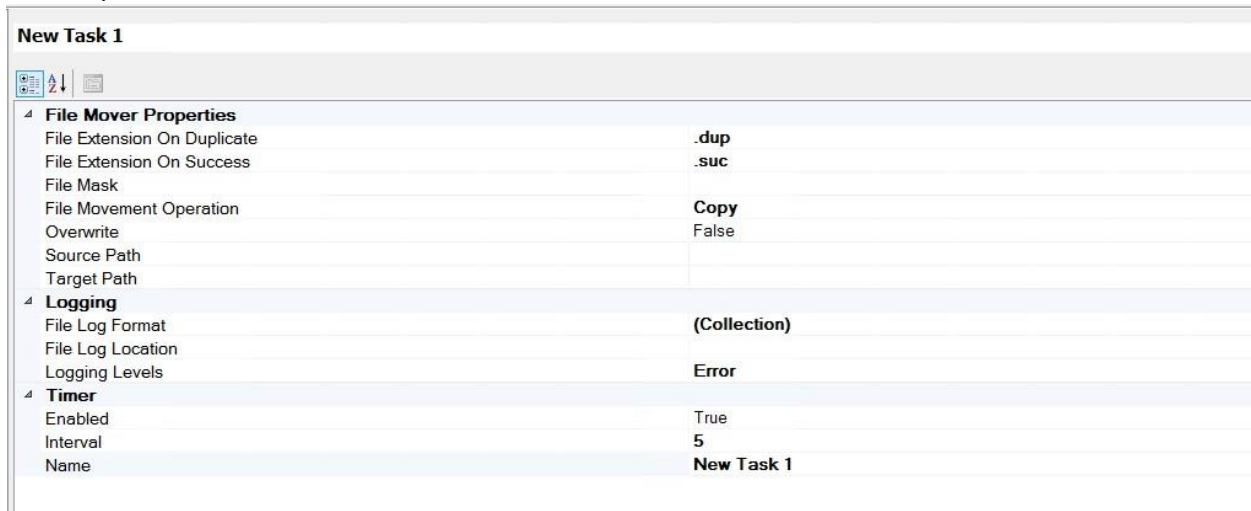


Figure 16-4 File Mover Task Configuration Pane

4. Complete the fields in the right pane. Table 16-2 describes the fields.

Table 16-2 File Mover Task Configuration Fields

Field	Description
File Mover Properties	
File Extension On Duplicate	Append file extension upon duplicate file detection.
File Extension on Success	Append file extension upon successful processing.
File Mask	File mask of items to move. Must be in format .pdf,.docx, etc.

Table 16-2 File Mover Task Configuration Fields

Field	Description
File Movement Operation	<p>Indicates what file processing mode the timer is operating in (Copy, Move, Rename).</p> <p>Copy: Files are copied to the destination location. The original file is left in place.</p> <p>Move: File are moved to the destination location. The original file is removed.</p> <p>Rename: Files are copied to the destination location. Original files are renamed in accordance with the File Extension on Duplicate and File Extension on Success properties.</p> <hr/> <p>Note:</p> <p>When using the file mover or file uploader in Rename mode, a file mask must be used to prevent a cascading processing of duplicate files. In the Rename operation, files are processed and then appended with either the success file extension or the duplicate file extension (configured in the admin console). If the file mask is not used, each file will continue to be processed again and again. Setting the file extension property prevents this behavior.</p> <hr/>
Overwrite	The mover will overwrite a duplicate file if True, or register an error if a duplicate file is detected if False.
Source Path	Source path of the location that the File Mover task monitors.
Target Path	Target path to the location where the task places processed files.

Field	Description
Logging	

Table 16-2 File Mover Task Configuration Fields

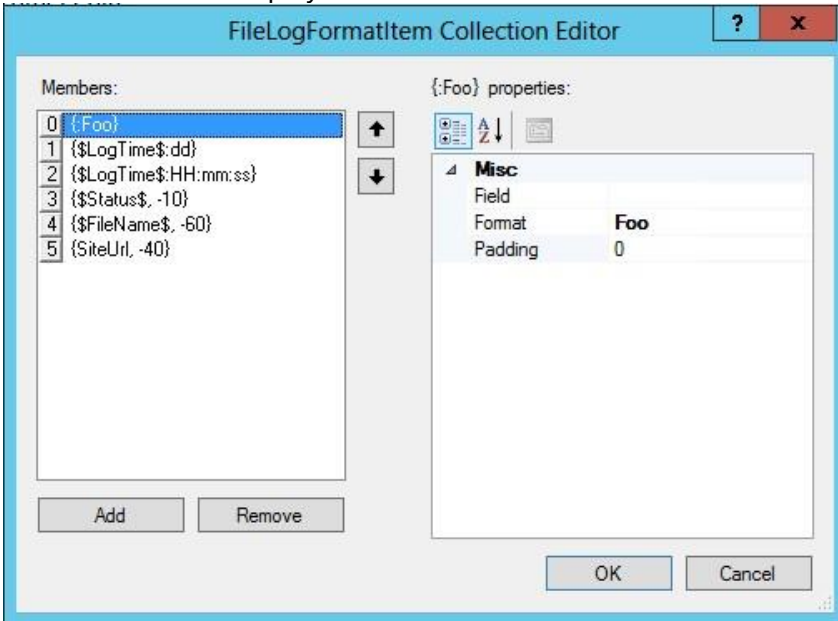
<p>File Log Format</p>	<p>Click this field to display the Collection Editor.</p>  <p>This example contains the following entries:</p> <ul style="list-style-type: none"> • Foo: Literal text • \$LogTime\$ with format <i>dd</i>: Output current UTC log time day • \$LogTime\$ with format <i>HH:mm:ss</i>: Output current UTC log time in format <i>HH:mm:ss</i> (24 hour time), for example,16:51:42 • \$Status\$ with padding 10: Output processing status with padding trailing spaces up to max length of 10 characters • \$FileName\$ with padding 60: Output file name with padding trailing spaces up to max length of 60 characters • SiteUrl with padding 40: Output SiteUrl from configuration with padding trailing spaces up to max length of 40 characters
<p>File Log Location</p>	<p>Location for file logging.</p>
<p>Logging Levels</p>	<p>Logging level of messages sent to event log (Information, Warning, or Error).</p>
<p>Timer</p>	
<p>Enabled</p>	<p>Enables or disables the File Move task.</p>

Table 16-2 File Mover Task Configuration Fields

16.4 Adding a File Uploader Task

To add a File Uploader task, follow these steps.

1. Launch the Gimmel Link Administration Console.
2. Open the current configuration.

Field	Description
File Mover Properties	
File Extension On Duplicate	Append file extension upon duplicate file detection.

Table 16-2 File Mover Task Configuration Fields

File Extension on Success	Append file extension upon successful processing.
Field	Description
Interval	Interval in seconds between timer execution.
Name	Name of the timer. Useful for diagnostics in event logging.

3. Right-click the **Timers** node and select **Add a File Uploader**. The configuration parameters display in the right pane.

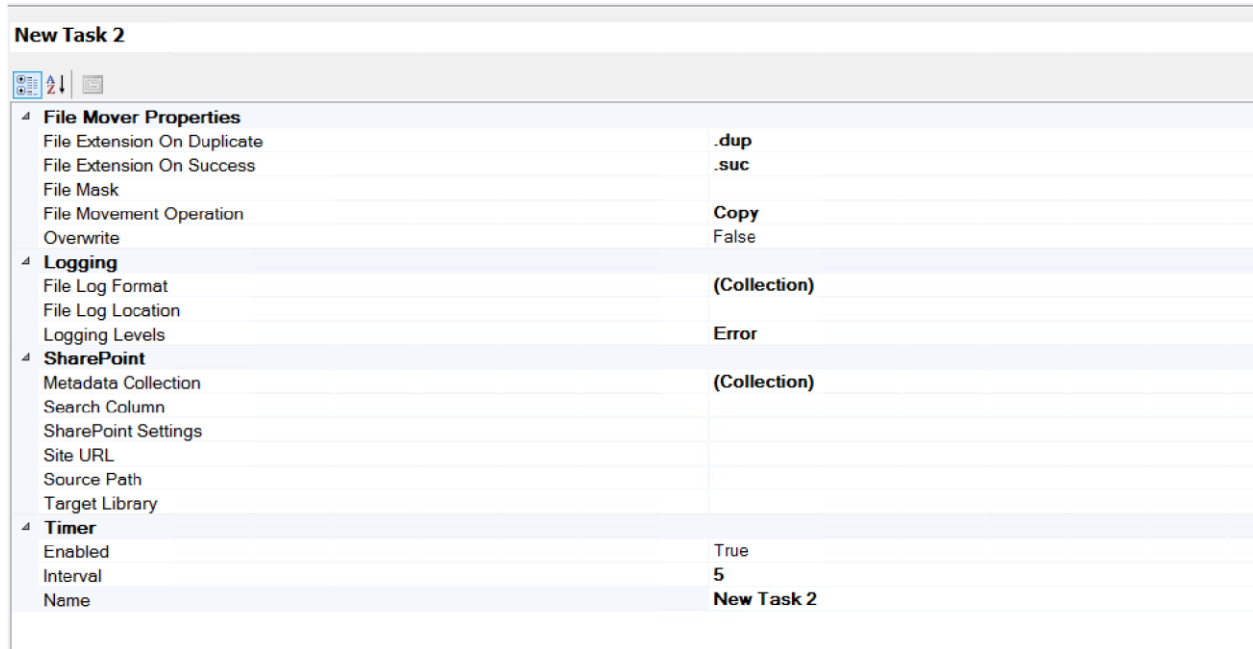


Figure 16-5 New File Uploader Task Pane 4.

Complete the fields. Table 16-3 describes the options.

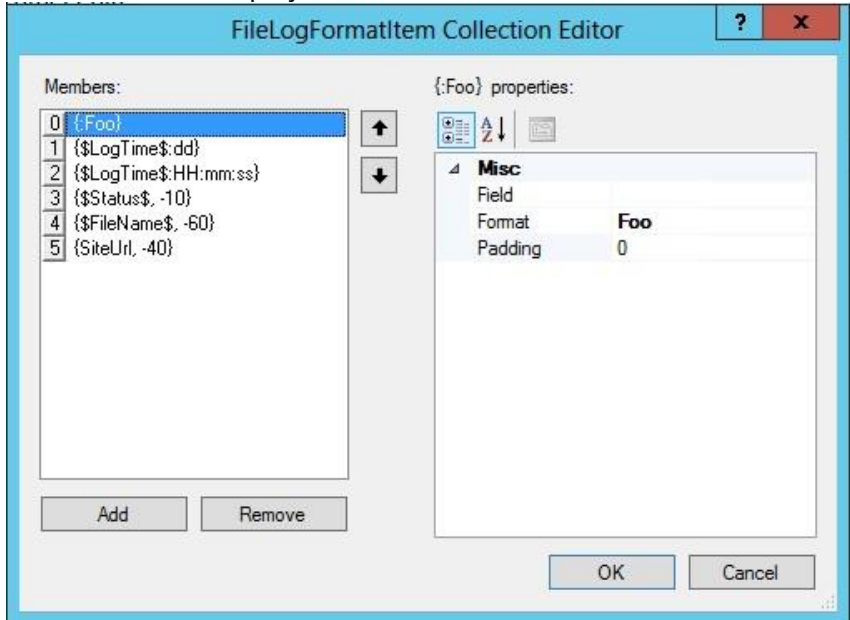
Table 16-3 Options in File Mover Task Control Pane

Table 16-3 Options in File Mover Task Control Pane

Field	Description
File Mask	File mask of items to move. Must be in format: .pdf,.docx, etc...
File Movement Operation	<p>Indicates what file processing mode the timer is operating in (Copy, Move, Rename).</p> <p>Copy: Files are copied to the destination location. The original file is left in place.</p> <p>Move: File are moved to the destination location. The original file is removed.</p> <p>Rename: Files are copied to the destination location. Original files are renamed in accordance with the File Extension on Duplicate and File Extension on Success properties.</p> <hr/> <p>Note:</p> <p>When using the file mover or file uploader in Rename mode, a file mask must be used to prevent a cascading processing of duplicate files. In the Rename operation, files are processed and then appended with either the success file extension or the duplicate file extension (configured in the admin console). If the file mask is not used, each file will continue to be processed again and again. Setting the file extension property prevents this behavior.</p> <hr/>
Overwrite	The mover will overwrite a duplicate file if True, or register an error if a duplicate file is detected if False.
Source Path	
Target Path	Target path to the location where the task places processed files.

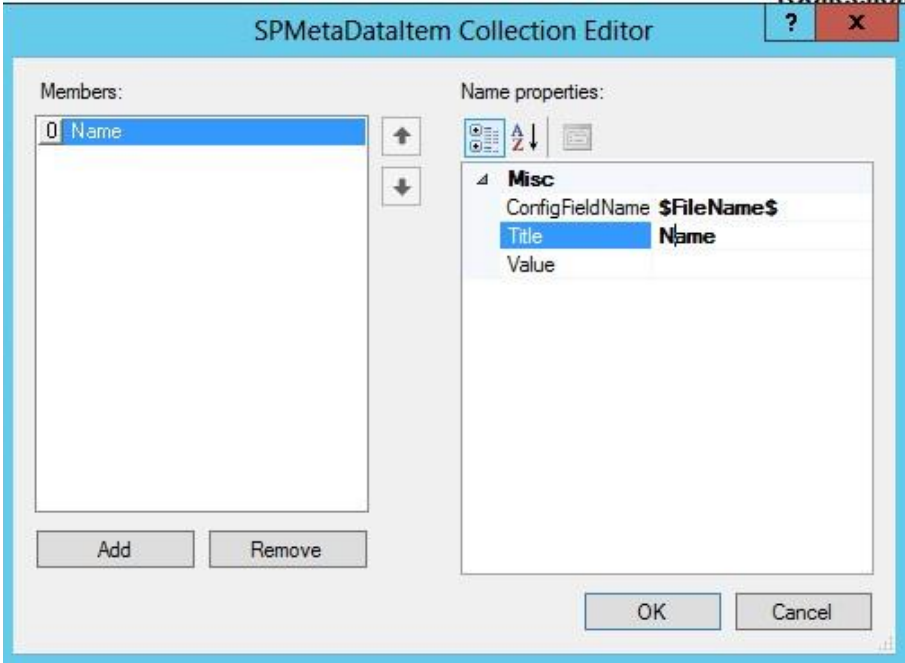
Field	Description
Logging	

Table 16-3 Options in File Mover Task Control Pane

File Log Format	<p>Click this field to display the Collection Editor.</p>  <p>This example contains the following entries:</p> <ul style="list-style-type: none"> • Foo: Literal text • \$LogTime\$ with format <i>dd</i>: Output current UTC log time day • \$LogTime\$ with format <i>HH:mm:ss</i>: Output current UTC log time in format <i>HH:mm:ss</i> (24 hour time), for example,16:51:42 • \$Status\$ with padding 10: Output processing status with padding trailing spaces up to max length of 10 characters • \$FileName\$ with padding 60: Output file name with padding trailing spaces up to max length of 60 characters • SiteUrl with padding 40: Output SiteUrl from configuration with padding trailing spaces up to max length of 40 characters
-----------------	---

Field	Description
SharePoint	

Table 16-3 Options in File Mover Task Control Pane

<p>Metadata Collection</p>	<p>Click the button to display the SPMetaDataltem Collection Editor. Used to apply metadata to uploaded files. The source value comes from one of two values: Config Field Name: Several configuration value options are available. The field Name is selected below. Value: Predefined value determined by the administrator.</p>  <p>In this example, the ConfigFieldName value <code>\$FileName\$</code> (determined at runtime) will be written to the Name column in SharePoint.</p>
<p>Search Column</p>	<p>Used to search for unique identifiers, typically the Name column.</p>
<p>SharePoint Settings</p>	<p>Predefined connection to use to connect to SharePoint.</p>
<p>Site URL</p>	<p>URL of the SharePoint instance.</p>
<p>Source Path</p>	<p>File system location from which files are uploaded.</p>
<p>Target Library</p>	<p>Destination SharePoint library where files are uploaded.</p>
<p>Timer</p>	
<p>Enabled</p>	<p>Enables or disables the File Upload task.</p>
<p>Interval</p>	<p>Interval in seconds between timer execution.</p>
<p>Name</p>	<p>Name of the timer. Useful for diagnostics in event logging.</p>

17 Troubleshooting

Issue: The required properties of a scanned document have been entered in the Scan.link monitoring folder, but saving the properties yields no results.

Action: First, make sure all RequiredFields have non-blank values. Then, consult the Windows Event Log. If you only see access denied errors being reported from SharePoint, the identity running SharePoint (typically the farm account) has not been granted permissions to write to the event log defined in the <Logging> element.

Open regedit, navigate to
HKLM\System\CurrentControlSet\Services\EventLog\Application\`<source name>`, where source name is the one given in the <Logging> element. Assign full permissions to the SharePoint application pool identity.

Issue: The document has been marked with a DocStatus of "Failed"

Action: Consult the Windows Event Log. Failures are typically caused by network connectivity to the SAP application server being interrupted, or misconfiguration.

Issue: Administration tool fails to open SharePoint site, with the error message "Website not found."

Action: Double-check that the URL to the SharePoint site has been entered correctly in the Administration tool.

Make sure that the currently logged in user is in the
WSS_CONTENT_APPLICATION_POOLS role on Configuration and Admin databases of the SQL database running the SharePoint configuration database.

Issue: Windows Event Log messages indicate that iNet.CS is denying access.

Action: Make sure that the iNet.CS connection pool used by the Document Service Modules has been configured to allow access to the SharePoint Service Account identity. Use the "Access Ctrl" button in the iNet.CS Administration Console to set this access privilege.

18 FAQs

This section contains frequently asked questions (FAQs) about Gimmel Link.

[How do I determine the installed version of Gimmel Link DM?.....210](#)

[How do I configure an SAP content repository for HTTPS?.....211](#)

*How do I configure unauthorized access safeguards for Gimmel Link Document Manager?
.212 Is there support for hybrid content repositories; for example, on-premise and O365
Share-*

Point Online?.....214

*How do I configure document movements (or routing) that occurs outside the knowledge
of
the Gimmel Link Suite (e.g. SharePoint Content
Organizer)?.....214*

How do I determine the installed version of Gimmel Link DM?

Follow these steps to determine the installed version:

1. Launch IIS Admin on the Gimmel Link Document Manager server and browser to the iNet.DM virtual directory.
2. Right-click the bin folder and select **Explore** from the context menu.
3. Right-click the **ERPLink.iNetDM.DLL** and select the **Properties** option.
4. Right-click the *ERPLink.dll* or *ERPLink.iNetDM.dll* file and select **Properties** from the context menu.

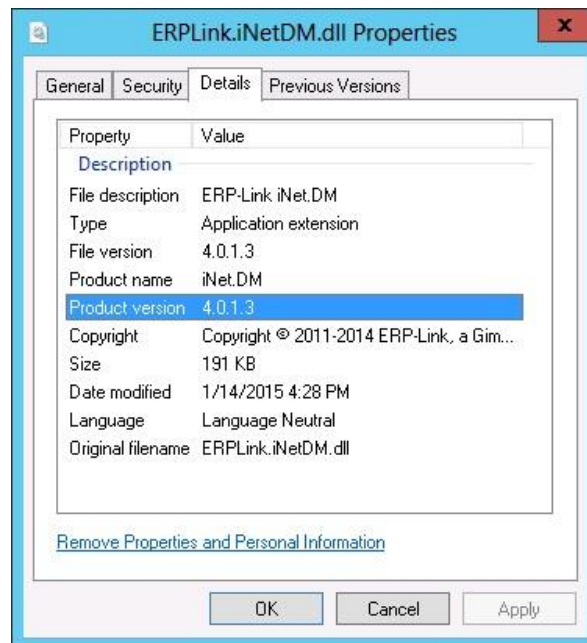


Figure 18-1 Determining the Installed Version

5. Click the **Details** tab to view the version property.

How do I configure an SAP content repository for HTTPS?

Follow these steps to configure an SAP content repository to use the HTTPS protocol to communicate to an HTTP content server, such as Gimmel Link Document Manager.

1. Launch SAP.
2. In the ribbon, enter `/nOACO` to display the **Display Content Repositories: Detail** page.

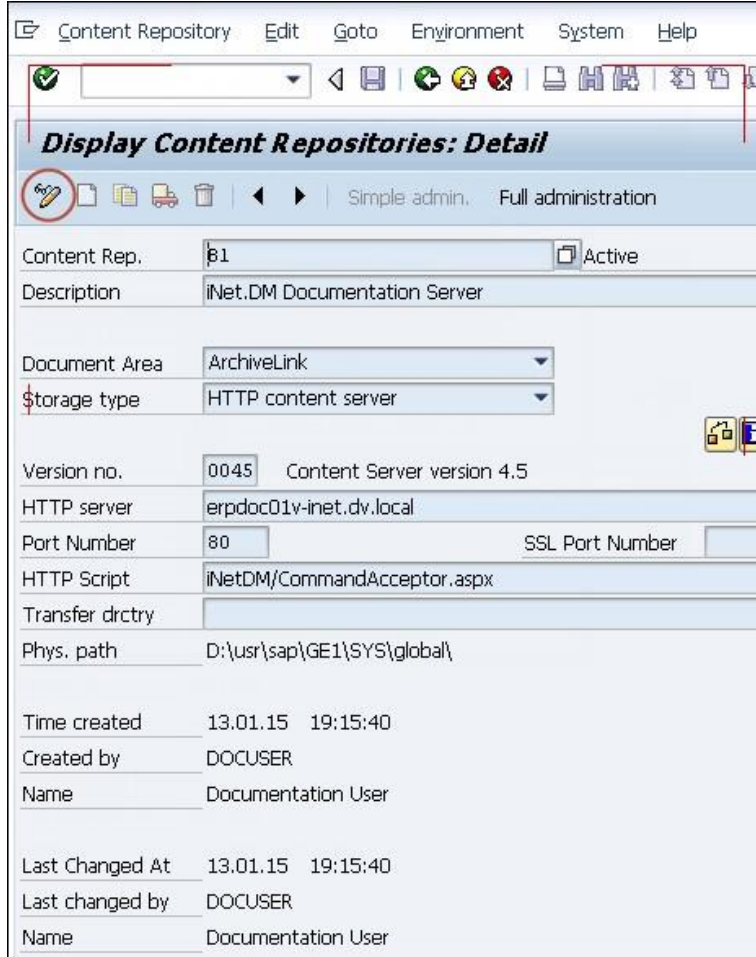


Figure 18-2 Display Content Repositories: Detail Page

3. Select the content repository and click **Display/Change**.

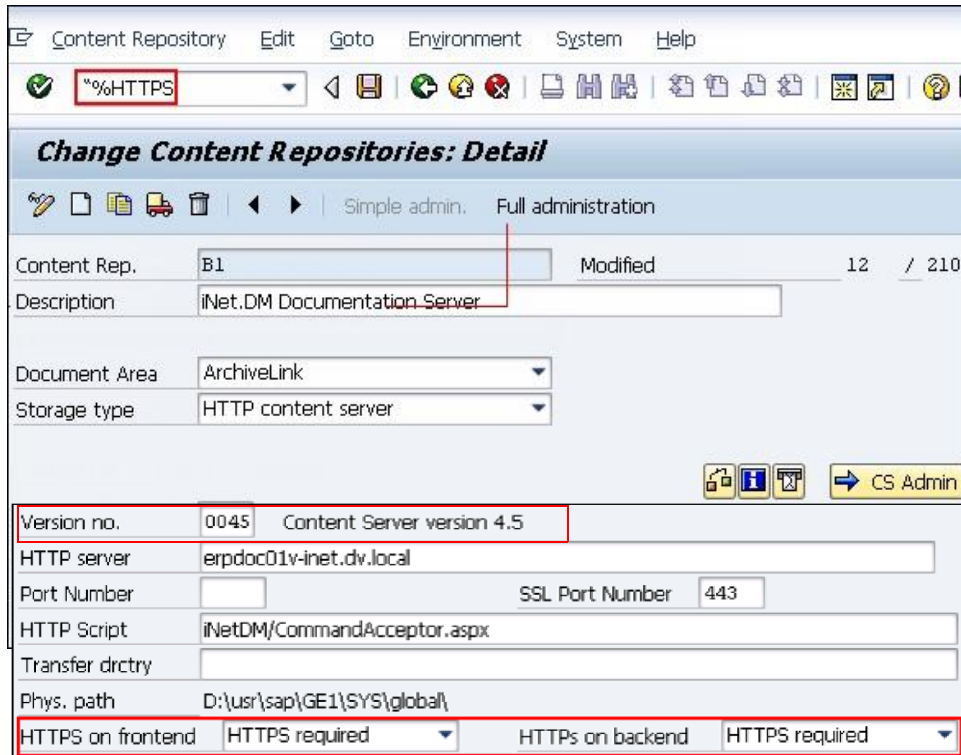


Figure 18-3 Change Content Repositories: Detail Page

4. Activate the HTTPS options by entering %HTTPS in the transaction field.
5. Clear the HTTP port value and enter the appropriate SSL Port Number value.
6. (Required) Switch backend and frontend HTTPS modes to HTTPS.
7. Save the settings.

How do I configure unauthorized access safeguards for Gimmel Link Document Manager?

Follow these steps to configure Gimmel Link Document Manager's SAP security integration with an SAPSECU encryption certificate.

1. Create the certificate folder called SAPCert.
2. Right-click the **SAPCert** folder and select **Properties** from the context menu.

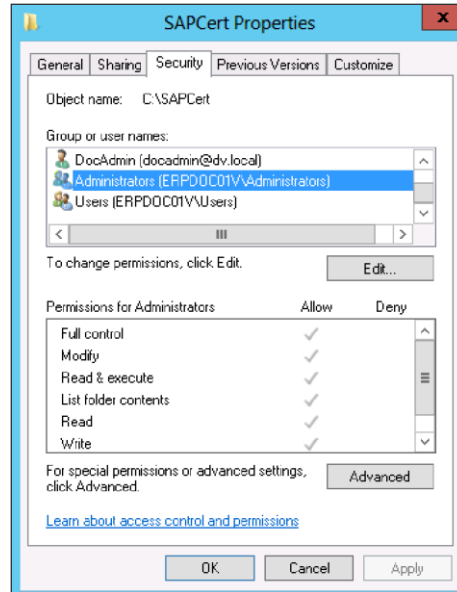


Figure 18-4 Viewing Folder Properties

3. Click the **Security** tab and set permissions on this folder.
4. Click **OK**.
5. From the Gimmel Link Administration Console, open the configuration file.
6. Scroll the right scroll bar down to see these parameters.

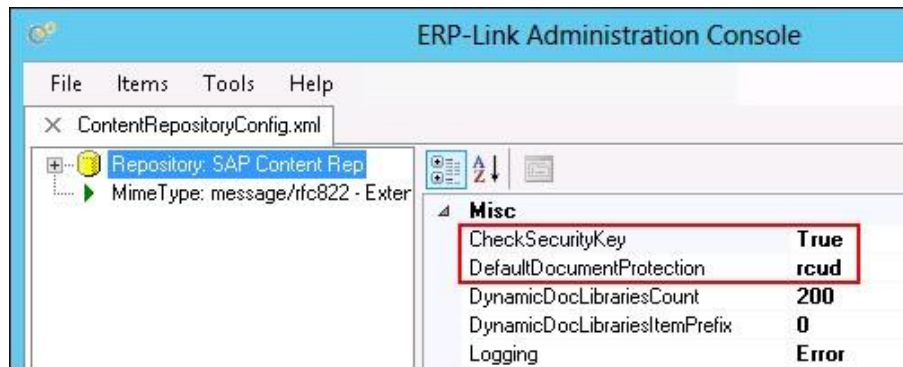


Figure 18-5 Misc Pane

7. Set **CheckSecurityKey** to *True* and **DefaultDocumentProtection** to *rcud*.
8. Launch SAP.
9. In the ribbon, enter */nOACO*.
10. Select the content repository and click the **Display/Change** button.

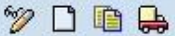




Change Content Repositories: Detail			
 Simple admin. Full administration			
Content Rep.	B1	Active	1 / 1
Description	iNet.DM Documentation Server		
Document Area	ArchiveLink		
Storage type	HTTP content server		
			   
Version no.	0045	Content Server version 4.5	
HTTP server	erpdoc01v-inet.dv.local		
Port Number		SSL Port Number	443
HTTP Script	iNetDM/CommandAcceptor.aspx		
Transfer drctry			
Phys. path	D:\usr\sap\GE1\SYS\global\		
HTTPS on frontend	HTTPS required	HTTPS on backend	HTTPS required

Figure 18-6 Change Content Repositories: Detail Page

11. Click the **Send the certificate button**.
12. Test the archival and retrieval as described in [9 Validating Gimmel Link Document Manager Functionality](#).

Is there support for hybrid content repositories; for example, on-premise and O365 SharePoint Online?

Answer: Yes, however, for version v5.0.0, each configured SAP content repository in the Gimmel Link configuration files supports only **one** SharePoint connection mode (SSOM or one of the CSOMs); for example, on-premise SharePoint server or O365 SP Online. The Gimmel Link Suite supports hybrid in that one SAP content repository can be configured to store documents on-premise and another SAP Content Repository can be configured to store documents on O365 SP Online.

How do I configure document movements (or routing) that occurs outside the knowledge of the Gimmel Link Suite (e.g. SharePoint Content Organizer)?

Answer: Parallel queries leveraging indexed site columns can be configured to search various document library locations for a document. Parallel queries are enabled in the Gimmel Link Document Manager configuration.

Appendix A Additional Information

This appendix contains additional technical information to explain the functions of Gimmel Link.

A.1 Data Flow Diagrams

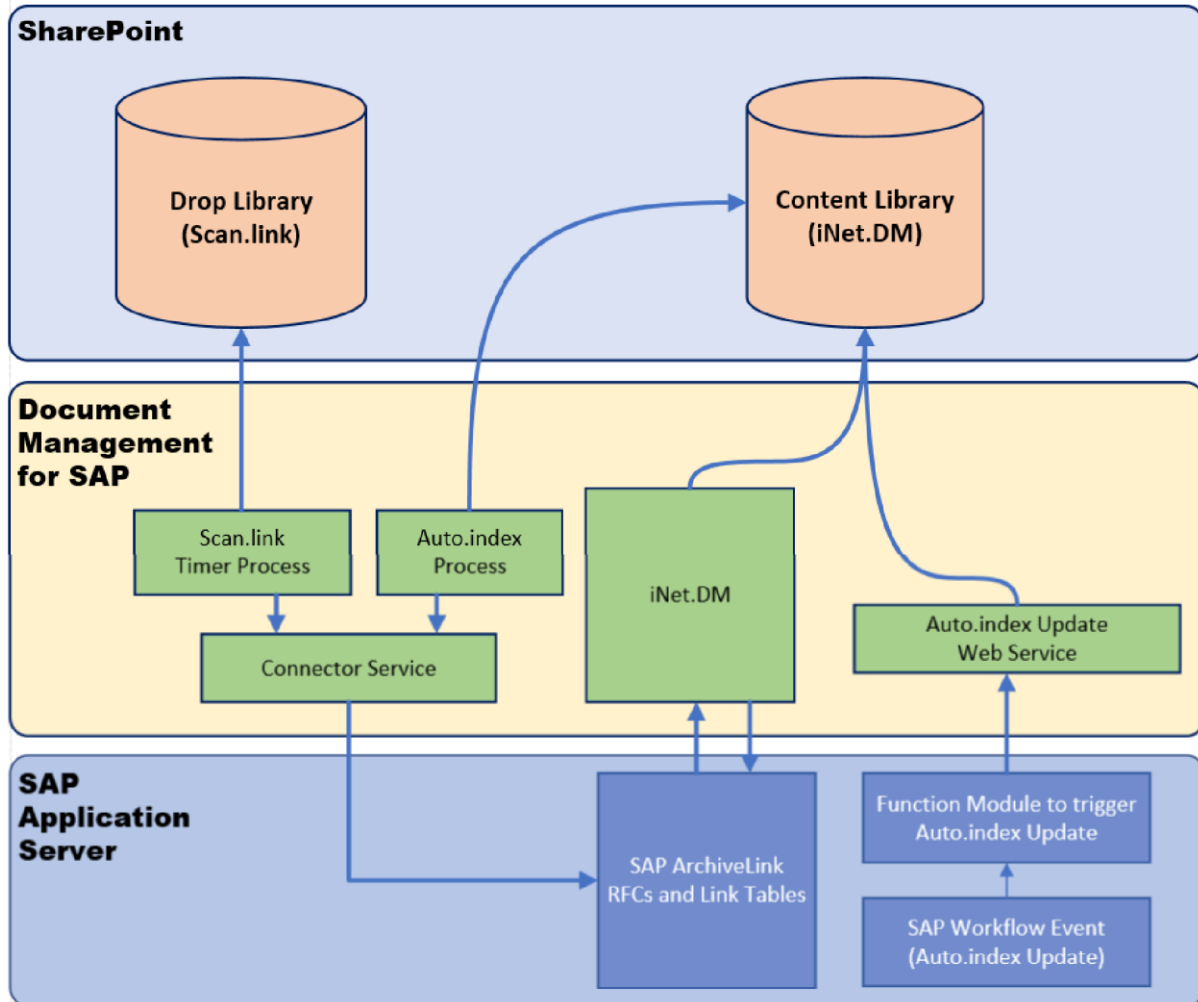


Figure A-1 Document Service Module Concept

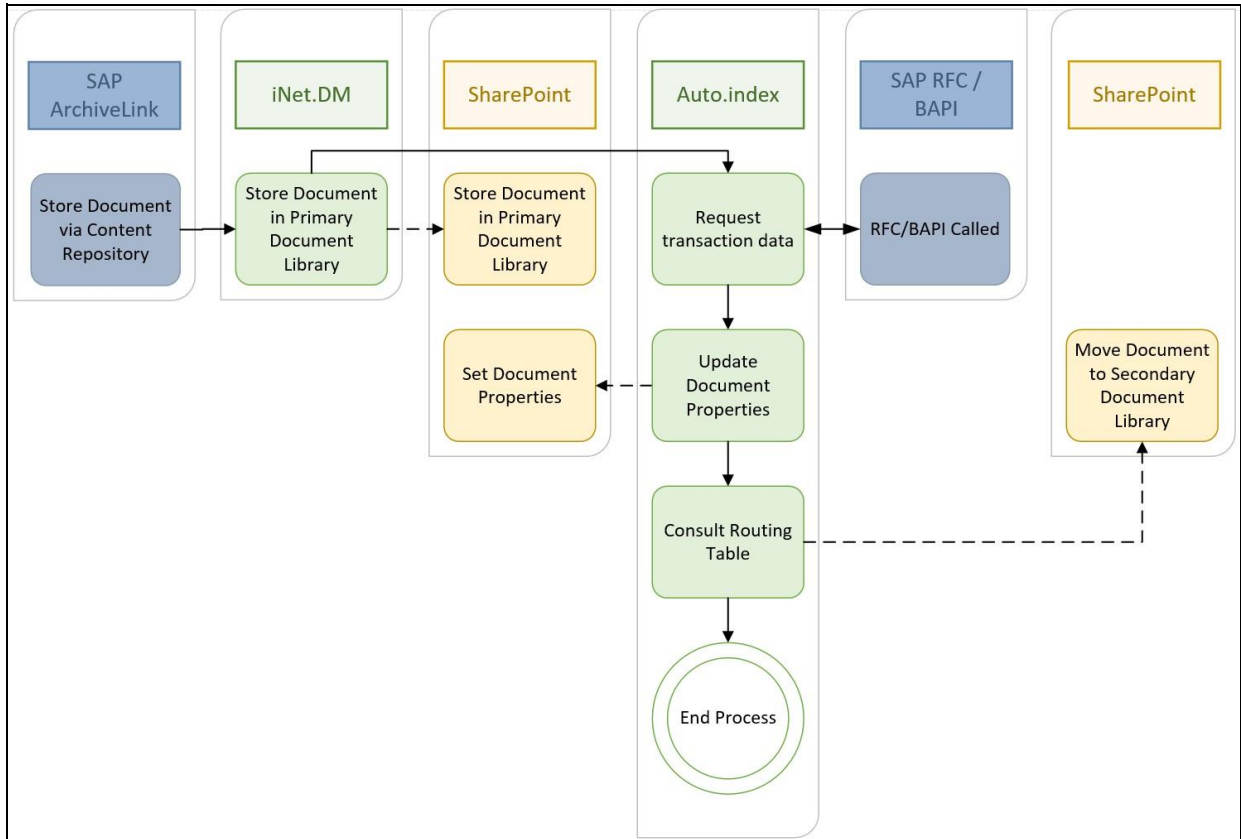


Figure A-2 Document Routing Sequence

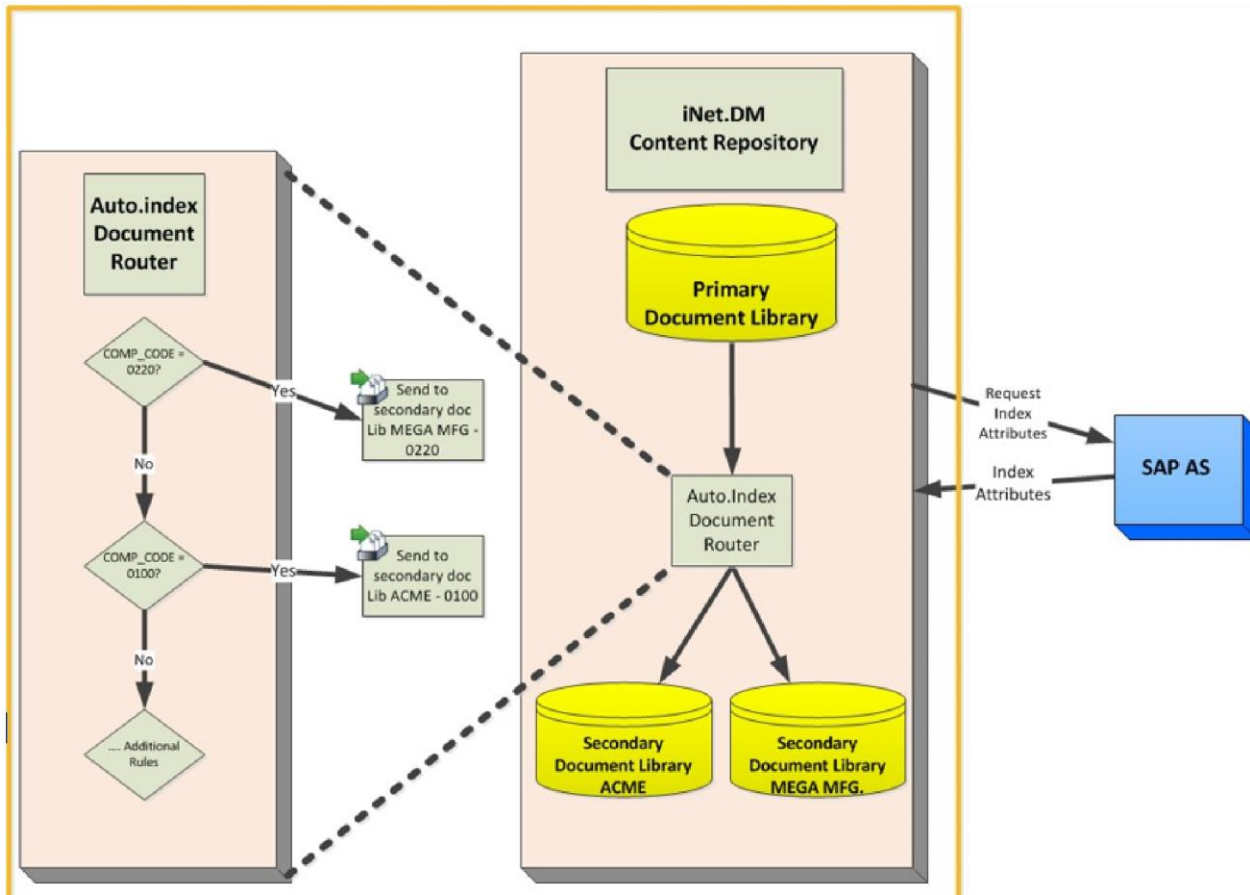


Figure A-3 Document Routing

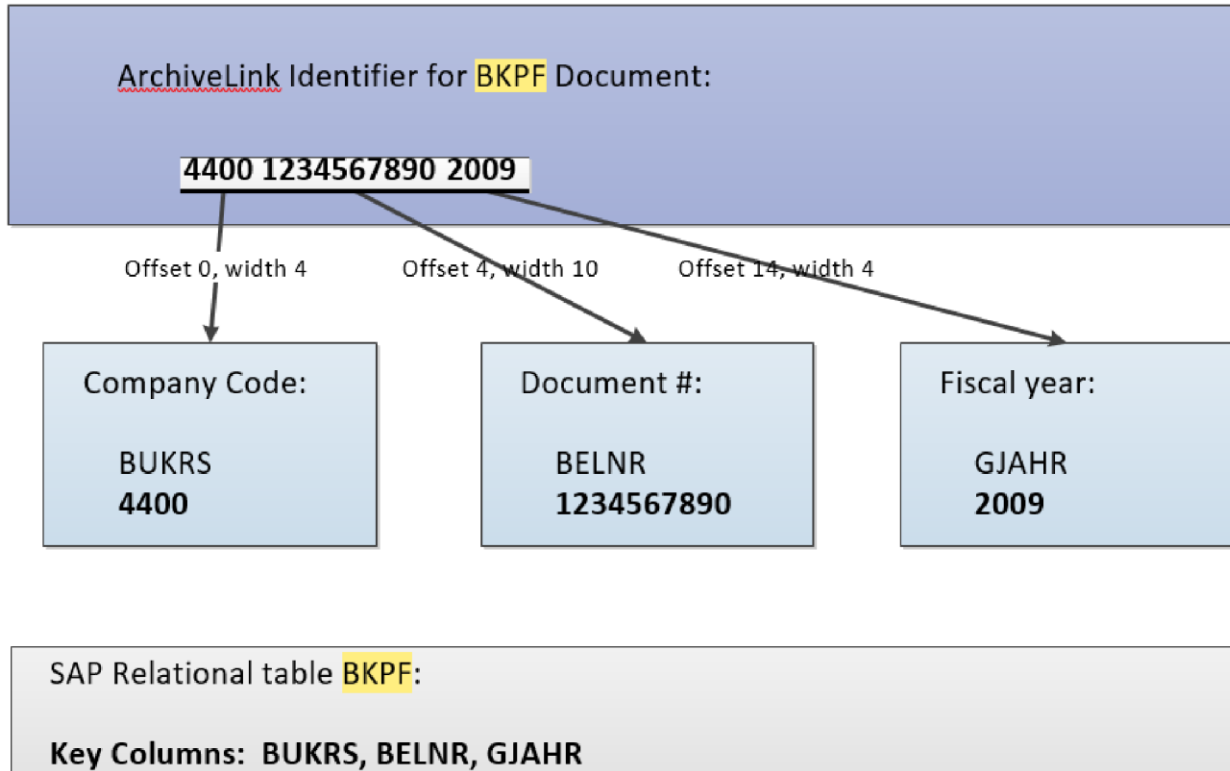


Figure A-4 BKPF Table

A.2 Writing Expressions

Expressions are provided to enable simple string trimming and formatting tasks that sometimes become necessary when processing values during the execution of a Document Service Module. An example is the composition of the separate parts of the **BKPF** composite ID (described above) into a single string identifier, as expected by ArchiveLink.

Expressions obey the following syntax:

expr ::= string-constant expr ::= numeric-constant

expr ::= identifier expr ::= function-call string-

constant ::= " <0..n characters> ", Where \

(backslash) escapes the following character. numeric-

constant ::= <base-10 integer>

identifier ::= <letter><0..n letters or digits> identifier ::=

[<letters, spaces, digits>] (bracketed identifier as seen in Transact-

SQL) function-call ::= <identifier>(<expr0>, <expr1>,...<exprn>)

where <identifier> specifies one of the built-in functions detailed below.

White space acts as a token separator as customary, except inside strings or bracketed identifiers. The built-in functions are shown in the following table.

Table A-1 Built-in Functions

Function Name	Description
Pad(<expr>, <width>, <pad-char>, <justification>)	Converts the expression <expr> into a string, then pads it into a string field of width <width>. If the string is too short, it is padded with <pad-char>s. Justification can be either 'R' or 'L' (left or right).
Format(<format-string>, <arg0> ... <argn>)	A variadic function that works like the standard .NET system.String.Format() method, converting the <arg0>-<argn> parameters to a string using the <format-string>.

Examples:

Some valid strings:

"Hello world"

"She said \"Hello world\" to me"

Some valid identifiers:

A

variableName1

[Purchase Order Number]

To format a BKPF multipart composite object key into a format suitable for use with ArchiveLink, use the following expression as the **KeyExpression** (broken into separate lines for clarity):

```
Format(“{0}{1}{2}”, Pad(CompCode,4,' ','L'),  
      Pad(DocNumber,10,'0','R'), Pad(FiscalYear,4,'0','R')) where CompCode,  
DocNumber, and FiscalYear are component key values that correspond to the fields BUKRS, BELNR,  
and GJAHR of the SAP BKPF table.
```

Note:

The expressions used in the Document Service Modules are intentionally restricted in their expressive power, and are not intended for general purpose programming.

A.3 Formatting Concatenated Strings

For some SAP tables, such as EKPO (purchase order headers), the specification of a key is simple because the SAP object ID in the ArchiveLink linking table has the same format as the purchase order key, which is a 10-digit number. In this case, a single binding is required, from SAPObjectID to EBELN (the key field of the EKPO table).

For others, such as BKPF, The bindings are more complex. The SAP object ID, stored by ArchiveLink, is a **composite key**, and needs to be broken apart into three components corresponding to the three key columns of the BKPF table:

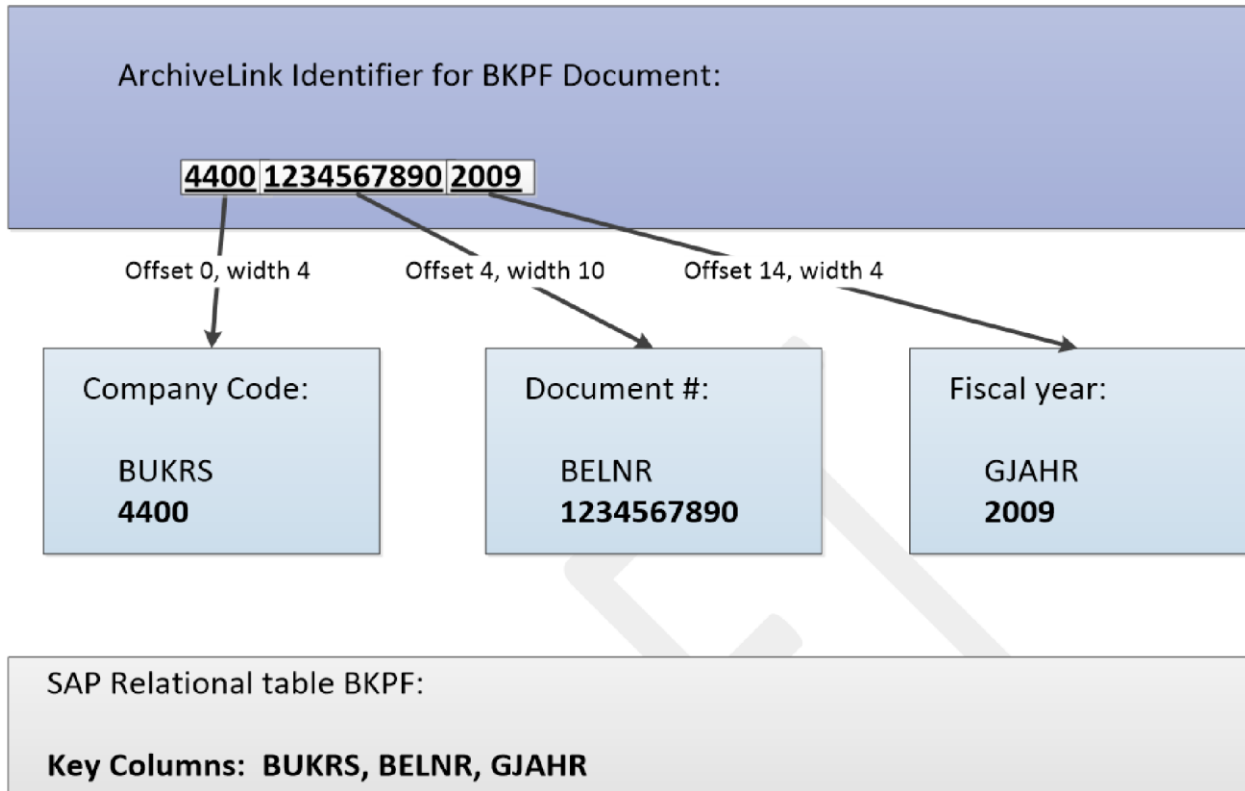


Figure A-5 Putting together a Composite Key for Indexing by SAP Table

To create the three necessary fragments of the key, use the **Edit Binding** button to define one binding for each fragment. Each binding specifies a

- **SourceName**, which is the name of the attribute from which the value is fetched
- The **offset** within that attribute at which to start the fragment
- The **width** of the fragment, in characters

The resulting substring is copied to the **SAP Table Column**.

```
Format("{0}{1}{2}", Pad([CompanyCode], 4, " ", "L"), Pad([DocumentNo], 10, "0", "R"), Pad([FiscalYear], 4, "0", "R"))
```

A.3.1 Examples

Function Name: *Format*

Purpose: Concatenate multiple strings (attributes and/or literals)

Syntax: `Format("{0}{1}{..}", <attribute/literal string 1>, <attribute/literal string 2>, ...)` **Special**

Considerations:

- Attribute's name should be enclosed in square brackets
- String literals should be enclosed in double quotes

Examples:

1. `Format("{0}{1}", [Invoice Number], [Fiscal Year])` creates a string consisting of Invoice Number and Fiscal year (if value of Invoice Number is 123, and Fiscal Year is 2005, The function will construct a string *1232005*).
2. `Format("{0}{1}(2)(3)", "Invoice Number = ", [Invoice Number], " and Fiscal Year = ", [Fiscal Year])`

Result: If value of **Invoice Number** is *123*, and **Fiscal Year** is *2005*, the function will construct a string *Invoice Number = 123 and Fiscal Year = 2005*

Function Name: *Pad*

Purpose: Padding of a string to make it specific length string

Syntax: `Pad(<attribute/literal string>, int DesiredLength, String PadChar, String Justification)`

Special Considerations:

- Attributes name should be enclosed in square brackets.
 - String literals should be enclosed in double quotes **Example:**
1. `Pad([Invoice Number], 10, "0", "R")`
Result: If **Invoice Number** is 123, the function will construct a string *0000000123*
 2. `Pad([Invoice Number], 10, " ", "L")`
Result: If **Invoice Number** is 123, the function will construct a string *123*; that is, *123* followed by seven spaces.

Function Name: *Substr*

Purpose: Extracts part of a string

Syntax: `Substr(<attribute/literal string>, int startindex, int NoOfChars)` **Special**

Considerations:

- Attributes name should be enclosed in square brackets.
- String literals should be enclosed in double quotes
- Start Index is (CharPosition – 1), so to start from 1

November 12, 2021

- st char, StartIndex should be set to 0

Example:

1. Substr("Example", 0, 3)

Result: Output string will be "Exa"

2. Substr("Example", 2, 5) **Result:** Output will be "ample"

A.4 Function Modules Used by Document Service Modules

The following standard function modules are used by Document Service Modules to accomplish their task. In no particular order:

Table A-2 Standard Function Modules

Standard Function Module	Task	Component
RFC_READ_TABLE	Used by TableIndexers to read data. Used by the configuration tool to generate SharePoint content types based on SAP table schemas.	Auto.index Administration console
SO_FOLDER_ROOT_ID_GET SO_OBJECT_INSERT BINARY_RELATION_CREATE_COMMIT	Used when creating URL attachments.	Auto.index
ARCHIV_GET_CONNECTIONS	Used to determine what SAP business objects are linked to a particular archived document.	Auto.index
ARCHIV_CONNECTION_INSERT	Used to establish a connection between an early archived document and its SAP business object.	Scan.link
SO_OBJECT_READ BAPI_REL_GETRELATIONS	Used to avoid duplicate attached URLs.	Auto.index
SAPI_WAPI_CREATE_EVENT	Used to create SAP inbox work items.	Scan.link
RFC_GET_FUNCTION_INTERFACE RFC_GET_NAMETAB	Used by the configuration tool to generate SharePoint content types based on SAP functions.	Administration console

B Gimmel Connection Service

The Gimmel Connection Service v5.1 provides a REST-based service for connecting to enterprise services such as SAP. Applications, such as Gimmel Link 5.1, read and write data from providers implemented in the Connection Service. Gimmel Link 5.1 uses the SAP RFC provider for the Connection Service 5.1. The SAP RFC provider provides RESTful endpoints for the SAP .NET Connector 3.0, which is installed separately.

B.1 Service Architecture to Support On-Premise and AzureHosted Deployment

The Connection Service architecture supports varying deployment models to support on-premise or Azure-hosted deployment. The following are supported in Gimmel Link Connection Service 5.1:

- On-premise DM and SharePoint 2013/2016
- On-premise DM and Office365
- Azure hosted DM and SharePoint 2013/2016
- Azure hosted DM and Office365

B.2 Relationship to SAP .NET Connector 3.0

The SAP RFC provider implemented in the Connection Service 5.1 leverages the SAP .NET Connector 3.0 developed and supported by SAP and Microsoft. The SAP .NET Connector enables the following features.

- Security enhancements to inhibit security attacks including the following:
 - Unauthorized access to SAP logon credentials
 - Replacement of SAP logon credentials in connection sessions
 - Interception of SAP logon credentials in connection sessions
- Configurable caching of logon credentials
- No dependency on the generation of code or proxy classes
- Implements a singleIRfcFunction class, whose Invoke() method dynamically executes every given ABAP function module
- Implements a generic IRfcStructure class representing all possible structures, and analogously one generic IRfcTable class for all tables
- Remote Function Module Parameter Discovery

B.3 Authentication

Authentication to the connection service is secured through token-based claims. The Connection Service requires that clients include a Gimmel token and SharePoint context token as claims to verify the client source and unique tenant.

B.4 Secure Sockets Layer

Gimmel requires that all client communications to the Connection Service are secured through Secure Sockets layer (SSL) to encrypt all communications. The Connection Service web application is created as an HTTP web application during installation, and SSL should be configured for the Connection Service web application after installation.

B.5 Secure Network Communications

RFC connections from the Connection Service to SAP may be secured with Secure Network Communications to encrypt the RFC channel. Refer to the *Secure Network Communications for ERPLink v5.2 Configuration Guide* for more details.

C Gimmel Document Tracking Service

The Gimmel Document Tracking Service 5.1 provides a RESTful service for managing the location of a document through the document lifecycle. This service will be leveraged by applications where document routing may be implemented through applications such as Gimmel Link 5.1, or through varying business processes or metadata based routing rules, such as SharePoint Content Organizer, SendTo, Explorer View, or third party applications.

The Document Tracking Service 5.1 replaces the Gimmel Link Document Tracking Database with a scalable enterprise RESTful service for managing the location of a document through the document lifecycle. In Gimmel Link 5.1, the Document tracking Service is the primary method for scalable document retrieval.

C.1 Document Tracking Service Technical Details

The following are technical details about the tracking service. Please refer to [5.7 Configuring the Document Tracking Service](#) for information on how to configure this service in Gimmel Link.

C.1.1 Service Architecture

The Document Tracking Service architecture supports various deployment models:

- On-premise DM and SharePoint 2013/2016
- On-premise DM and Office365
- Azure-hosted DM and SharePoint 2013/2016
- Azure-hosted DM and Office365

C.1.2 Provider Model for Document Tracking Data Storage

The data storage for the Document Tracking Service leverages a provider model, with providers implemented for specific storage architectures to manage document tracking data. The Document Tracking storage manages the metadata and location of the document, and documents are managed in the application repository, such as SharePoint. The Document Tracking Service 5.1 supports a SQL Server provider to store the metadata and location of the document.

C.1.3 RESTful Endpoints

The Connection Service is implemented with the ASP.NET WebAPI2 framework as a RESTful service. Web service tracking is secured by HTTPS as well as a common encryption key used by Gimmel software. If this key is absent from RESTful web service calls, they will be rejected.

D Information Architecture

Information Architecture

- __ Name of the IIS Web site that iNet.DM will be installed in: _____
- __ Name of the IIS Web site that the Connector Service v5.1 will be installed in:

- __ Name of the IIS Web site that the Connection Service v5.1 will be installed in:

- __ Determine the SharePoint Web application that will host Gimmel Link:

Note:

You can use an existing SharePoint library or create a new one.

- __ Determine the SharePoint content types:_____
- __ Determine the SharePoint site(s) that will store the documents:

- __ Determine the number of SharePoint document libraries per SharePoint site:

- __ Create the SharePoint Web applications, sites, and libraries that will host the Gimmel Link repository:

Business Metadata for Auto.index

- __ Identify the SAP object types:_____
- __ Identify the SAP RFC-capable function modules or SAP tables to retrieve the metadata from the SAP object types:_____
- __ Identify and create the SharePoint content types and site columns that will contain metadata from the SAP object types._____
- __ Create the content types and site columns in a SharePoint Content Type hub and publish content types to subscribing sites:_____

Library for Scan.link

- __ Identify the SAP object type that will be used to attach incoming SharePoint documents with the associated SAP transaction/application document:_____
 - __ Identify the primary key fields on the SAP object type to uniquely identify incoming SharePoint documents with the associated SAP transaction/application document:
-

E Configuring Auto.index Update Notifications Outside SAP Workflow

You can write code to send notifications to SharePoint outside the SAP workflow and the SAP event framework. The following is sample code to perform this task.

```
CALL METHOD /erplkgml/cl_autoindex_updater=>send_http_notifications
EXPORTING
  iv_sap_object = '{SOME BUSINESS OBJECT}'
  iv_object_id = '{SOME OBJECT ID}'.
```