



SDL Content Manager Installation Guide

SDL Content Manager 14.0.1

December 2019

Legal notice

Copyright and trademark information relating to this product release.

Copyright © 2003–2019 SDL Group.

SDL Group means SDL PLC. and its subsidiaries and affiliates. All intellectual property rights contained herein are the sole and exclusive rights of SDL Group. All references to SDL or SDL Group shall mean SDL PLC. and its subsidiaries and affiliates details of which can be obtained upon written request.

All rights reserved. Unless explicitly stated otherwise, all intellectual property rights including those in copyright in the content of this website and documentation are owned by or controlled for these purposes by SDL Group. Except as otherwise expressly permitted hereunder or in accordance with copyright legislation, the content of this site, and/or the documentation may not be copied, reproduced, republished, downloaded, posted, broadcast or transmitted in any way without the express written permission of SDL.

SDL Tridion Docs is a registered trademark of SDL Group. All other trademarks are the property of their respective owners. The names of other companies and products mentioned herein may be the trademarks of their respective owners. Unless stated to the contrary, no association with any other company or product is intended or should be inferred.

This product may include open source or similar third-party software, details of which can be found by clicking the following link: "Acknowledgments " on page 2.

Although SDL Group takes all reasonable measures to provide accurate and comprehensive information about the product, this information is provided as-is and all warranties, conditions or other terms concerning the documentation whether express or implied by statute, common law or otherwise (including those relating to satisfactory quality and fitness for purposes) are excluded to the extent permitted by law.

To the maximum extent permitted by law, SDL Group shall not be liable in contract, tort (including negligence or breach of statutory duty) or otherwise for any loss, injury, claim liability or damage of any kind or arising out of, or in connection with, the use or performance of the Software Documentation even if such losses and/or damages were foreseen, foreseeable or known, for: (a) loss of, damage to or corruption of data, (b) economic loss, (c) loss of actual or anticipated profits, (d) loss of business revenue, (e) loss of anticipated savings, (f) loss of business, (g) loss of opportunity, (h) loss of goodwill, or (i) any indirect, special, incidental or consequential loss or damage howsoever caused.

All Third Party Software is licensed "as is." Licensor makes no warranties, express, implied, statutory or otherwise with respect to the Third Party Software, and expressly disclaims all implied warranties of non-infringement, merchantability and fitness for a particular purpose. **In no event will Licensor be liable for any damages, including loss of data, lost profits, cost of cover or other special, incidental, consequential, direct, actual, general or indirect damages arising from the use of the Third Party Software or accompanying materials, however caused and on any theory of liability. This limitation will apply even if Licensor has been advised of the possibility of such damage. The parties acknowledge that this is a reasonable allocation of risk.**

Information in this documentation, including any URL and other Internet website references, is subject to change without notice. Without limiting the rights under copyright, no part of this may be reproduced, stored in or introduced into a retrieval system, or transmitted in any

form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of SDL Group.

Contents

1	Welcome to SDL Content Manager Installation	1
	Acknowledgments	2
	Customer support	16
2	Content Manager requirements	17
	Content Manager hardware requirements	18
	Content Manager software requirements	19
	Installer User Requirements	21
	Platform virtualization	22
	Firewalls and ports	22
3	Installing Content Manager	25
	Install preparation	26
	Enabling https on the IIS website	26
	Defining the bindings in the target web site	27
	Microsoft Windows Server	29
	Establishing a dedicated system user	29
	Changing the Local Group Policy	31
	Microsoft SQL Server database access components	31
	Oracle Data Access Components	32
	Verifying the .NET Framework version	33
	Configuring HTTP Activation for WCF	34
	Configuring IIS and ASP Web services	34
	Configuring application server role	35
	Java	36
	Configuration requirements	36
	Prerequisites for publishing engine	36
	Java Help	36
	HTML Help Workshop	37
	Antenna House XSL Formatter	37
	Configuring IIS applicationHost.Config	37
	Preparation Checklist	39
	Installing and configuring the database server	40
	Microsoft SQL Server	41
	Configuring Microsoft SQL Server	41
	Creating a database	42
	Importing data from the SQL dumpfile	42

Removing the database user and schema	43
Creating a new database user and schema	44
Optionally minimize the database user's roles and permissions	45
Oracle RDBMS	49
Configuring Oracle RDBMS	49
Oracle database configuration requirements	49
Copy template files	50
Activating the Listener service for Oracle	50
Creating the Oracle database with a template	51
Creating the Oracle 12.1 database	51
Creating the Oracle 12.2 database	52
Creating the Oracle 19 database	53
Creating the designated ISOURCE database user	54
Importing the data with Oracle	55
Validating the database	56
Editing the tnsnames.ora database connection file	58
Analyzing the database	57
Installing the Content Manager server	58
Configuring database connection strings	58
Creating and testing Oracle RDBMs	58
Editing the tnsnames.ora database connection file	58
Creating and testing the connection for Oracle RDBMs	59
Creating and testing the connection for Microsoft SQL Server	61
inputparameters.xml	62
Mandatory input parameters	63
Optional input parameters	64
Executing the InstallTool	66
Identifying reverse proxies	67
Post-installation tasks	67
Verifying Microsoft SQL System Administration role permissions	67
Running DBUpgradeTool for maintenance	68
Troubleshooting DBUpgradeTool	69
Completing the installation or upgrade with ISHDeploy	70
Adding the relying party entries for webUI and WCF Services for commercial STS	70
Removing the relying party entries for webUI and WCF Services	72
Configure Security Token Service	72
Content Manager Security Token Service requirements	72
ISHSTS with Windows Authentication	75
Configure application server for Windows Authentication	76

Configure SQL Server database for Windows Authentication	76
The Administrator setup	77
Completing the Administrator setup	78
Validation XML configuration files	79
Checking the TRANSLATORSERVICE role	79
Creating a ServiceUser user	80
Translation management integration configuration	81
Translation services configuration files	81
Application Configuration for TranslationBuilder	81
Application configuration for TranslationOrganizer	82
TranslationOrganizer common parameters	82
TranslationOrganizer WorldServer parameters	83
TranslationOrganizer TMS parameters	85
TranslationOrganizer File System settings	88
Translation Job Workflow	89
Integration requirements for Content Manager and SDL WorldServer	89
Integration requirements for Content Manager and SDL TMS	91
Integration requirements for Content Manager and File System	93
Enabling services	94
Enabling Draft Space	95
Enabling Review Space	95
Configuring the Discovery Service connection	96
Verifying the installation	96
Verifying URLs	97
Verify read access to the database by viewing an inbox	97
Verify read and write access to the database by creating a folder	98
Creating an account and connecting to the Repository	98
Running a client tool	99
Testing publishing	99
Executing the full text search	100
Verifying customer specific components	100
Installing desktop client tools	100
Installing the Authoring Bridge	101
Installing Publication Manager	101
Installing Condition Manager	102
Installing Content Importer	102
Advanced topics for installers	103
InstallTool	103

InstallTool overview	103
The InstallTool	104
Unimplemented features of the InstallTool	104
Background task component	105
Overview of the background task configuration	106
Usage of variables inside the background task configuration	107
Understanding the availability matrix	109
Understanding the isolation level of the handler	110
Server roles	111
Web role	111
Full text indexing role	112
Default background task role	112
Translation role	114
Publish role	115
Best practices for creating a Trisoft InfoShare BackgroundTask service with a specific role	116
How to create a new BackgroundTask service with a role	117
How to adapt the role of an existing BackgroundTask service	118
Firewalls and blocked ports	119
SMTP	120
Microsoft SQL Server ports	120
Oracle RDBMS	122
HTTPS (SSL)	122
4 Troubleshooting Content Manager installation	125
Contacting customer support	126
Diagnosing Problems	126
Providing Information	126
Log Files	127
Using log files	127
Server Logs	128
Desktop Client Logs	130
Logging Configuration	131
Event Log content	133
Using the Event Log	133
Troubleshooting the database installation	134
What to do if Oracle database import fails	134
What to do in case of "ORA-12638" error	134

User is restricted or does not have permissions	135
Login time restriction	135
User account restriction	135
User not granted requested logon type	136
The designated user is running the wrong (date) settings	136
Resolving certificate problems	137
Accepting a certificate using a web browser	137
Importing and accepting a certificate for a user	138
Importing and accepting a certificate for a computer	138
Troubleshooting the install tool	139
Troubleshooting the crawler service	139

1

Welcome to SDL Content Manager Installation

This document presents the complete Content Manager procedure and information.

Acknowledgments

SDL products include open source or similar third-party software.

7zip

Is a file archiver with a high compression ratio. 7-zip is delivered under the GNU LGPL License.

7zip SFX Modified Module

The SFX Modified Module is a plugin for creating self-extracting archives. It is compatible with three compression methods (LZMA, Deflate, PPMd) and provides an extended list of options. Reference website <http://7zsfx.info/>.

Akka

Akka is a toolkit and runtime for building highly concurrent, distributed, and fault tolerant event-driven applications on the JVM.

Amazon Ion Java

Amazon Ion Java is a Java streaming parser/serializer for Ion. It is the reference implementation of the Ion data notation for the Java Platform Standard Edition 8 and above.

Amazon SQS Java Messaging Library

This Amazon SQS Java Messaging Library holds the Java Message Service compatible classes, that are used for communicating with Amazon Simple Queue Service.

Animal Sniffer Annotations

Animal Sniffer Annotations provides Java 1.5+ annotations which allow marking methods which Animal Sniffer should ignore signature violations of.

ANTLR

ANTLR is a powerful parser generator that you can use to read, process, execute, or translate structured text or binary files.

Apache ActiveMQ

Apache ActiveMQ is the most popular and powerful open source messaging and Integration Patterns server.

Apache Ant

Apache Ant is a Java library and command-line tool whose mission is to drive processes described in build files as targets and extension points dependent upon each other. The main known usage of Ant is the build of Java applications. Ant supplies a number of built-in tasks allowing to compile, assemble, test and run Java applications. Ant can also be used effectively to build non Java applications, for instance C or C++ applications. More generally, Ant can be used to pilot any type of process which can be described in terms of targets and tasks.

Apache Commons BeanUtils

The Java language provides *Reflection* and *Introspection* APIs (see the `java.lang.reflect` and `java.beans` packages in the JDK Javadocs). However, these APIs can be quite complex to understand and utilize. The *BeanUtils* component provides easy-to-use wrappers around these capabilities.

[Apache Commons Codec](#)

Apache Commons Codec (TM) software provides implementations of common encoders and decoders such as Base64, Hex, Phonetic and URLs.

[Apache Commons Collections](#)

The Java Collections Framework was a major addition in JDK 1.2. It added many powerful data structures that accelerate development of most significant Java applications. Since that time it has become the recognized standard for collection handling in Java.

[Apache Commons Compress](#)

The Apache Commons Compress library defines an API for working with ar, cpio, Unix dump, tar, zip, gzip, XZ, Pack200, bzip2, 7z, arj, lzma, snappy, DEFLATE, lz4 and Z files.

[Apache Commons Configuration](#)

The Commons Configuration software library provides a generic configuration interface which enables a Java application to read configuration data from a variety of sources. Commons Configuration provides typed access to single, and multi-valued configuration parameters.

[Apache Commons DBCP \(Database Connection Pools\)](#)

Many Apache projects support interaction with a relational database. Creating a new connection for each user can be time consuming (often requiring multiple seconds of clock time), in order to perform a database transaction that might take milliseconds. Opening a connection per user can be unfeasible in a publicly-hosted Internet application where the number of simultaneous users can be very large. Accordingly, developers often wish to share a "pool" of open connections between all of the application's current users. The number of users actually performing a request at any given time is usually a very small percentage of the total number of active users, and during request processing is the only time that a database connection is required. The application itself logs into the DBMS, and handles any user account issues internally. There are several Database Connection Pools already available, both within Apache products and elsewhere. This Commons package provides an opportunity to coordinate the efforts required to create and maintain an efficient, feature-rich package under the ASF license.

[Apache Commons FileUpload](#)

The Commons **FileUpload** package makes it easy to add robust, high-performance, file upload capability to your servlets and web applications.

[Apache Commons HttpClient](#)

HttpClient was started in 2001 as a subproject of the Jakarta Commons, based on code developed by the Jakarta Slide project.

[Apache Commons IO](#)

Commons IO is a library of utilities to assist with developing IO functionality.

[Apache Commons JEXL \(Java EXpression Language\)](#)

JEXL is a library intended to facilitate the implementation of dynamic and scripting features in applications and frameworks written in Java.

JEXL implements an Expression Language based on some extensions to the JSTL Expression Language supporting most of the constructs seen in shell-script or ECMAScript. Its goal is to expose scripting features usable by technical operatives or consultants working with enterprise platforms.

Apache Commons Lang

The standard Java libraries fail to provide enough methods for manipulation of its core classes. Apache Commons Lang provides these extra methods.

Lang provides a host of helper utilities for the java.lang API, notably String manipulation methods, basic numerical methods, object reflection, concurrency, creation and serialization and System properties. Additionally it contains basic enhancements to java.util.Date and a series of utilities dedicated to help with building methods, such as hashCode, toString and equals.

Apache Commons Logging

The Logging package is an ultra-thin bridge between different logging implementations. A library that uses the commons-logging API can be used with any logging implementation at runtime. Commons-logging comes with support for a number of popular logging implementations, and writing adapters for others is a reasonably simple task.

Apache Commons Net

Apache Commons Net™ library implements the client side of many basic Internet protocols. The purpose of the library is to provide fundamental protocol access, not higher-level abstractions.

Apache Commons Pool

Pool provides an Object-pooling API, with three major aspects:

1. A generic object pool interface that clients and implementers can use to provide easily interchangeable pooling implementations.
2. A toolkit for creating modular object pools.
3. Several general purpose pool implementations.

Apache FOP

Apache FOP (Formatting Objects Processor) is a print formatter driven by XSL formatting objects (XSL-FO) and an output independent formatter. It is a Java application that reads a formatting object (FO) tree and renders the resulting pages to a specified output. Output formats currently supported include PDF, PS, PCL, AFP, XML (area tree representation), Print, AWT and PNG, and to a lesser extent, RTF and TXT. The primary output target is PDF.

Apache Geronimo

Apache Geronimo is an open source server runtime that integrates the best open source projects to create Java/OSGi server runtimes that meet the needs of enterprise developers and system administrators.

Apache HttpClient

Although the java.net package provides basic functionality for accessing resources via HTTP, it doesn't provide the full flexibility or functionality needed by many applications. HttpClient seeks to fill this void by providing an efficient, up-to-date, and feature-rich package implementing the client side of the most recent HTTP standards and recommendations.

Designed for extension while providing robust support for the base HTTP protocol, HttpClient may be of interest to anyone building HTTP-aware client applications such as web browsers, web service clients, or systems that leverage or extend the HTTP protocol for distributed communication.

Apache HttpComponents

The Apache HttpComponents™ project is responsible for creating and maintaining a toolset of low level Java components focused on HTTP and associated protocols.

Within the HttpComponents project, [HttpCore](#) is a set of low level HTTP transport components that can be used to build custom client and server side HTTP services with a minimal footprint. HttpCore supports two I/O models: blocking I/O model based on the classic Java I/O and non-blocking, event driven I/O model based on Java NIO

Apache Log4j

Apache Log4j 2 is an upgrade to Log4j that provides significant improvements over its predecessor, Log4j 1.x, and provides many of the improvements available in Logback while fixing some inherent problems in Logback's architecture.

Apache Lucene, SOLR

The Apache Lucene™ project develops open-source search software.

Apache Tomcat, Tomcat Embed

Apache Tomcat is an open source software implementation of the Java Servlet and JavaServer Pages technologies.

Apache XBean :: Spring

XBean :: Spring provides a schema-driven proprietary namespace handler for Spring contexts.

Apache Xerces

The Apache Xerces Project is responsible for software licensed to the Apache Software Foundation intended for the creation and maintenance of:

- XML parsers
- related software components

Apache XML

The Apache XML Project used to be the home for many XML-related subprojects, many of which have moved to top-level project status recently or are currently in migration. The Apache XML Project slowly transforms into an place where you can find pointers to XML-related projects here in The Apache Foundation.

Apache XML Commons External Components

The External Components portion of xml-commons contains interfaces that are defined by external standards organizations.

ASM

ASM is an all purpose Java bytecode manipulation and analysis framework. It can be used to modify existing classes or dynamically generate classes, directly in binary form. Provided common transformations and analysis algorithms allow to easily assemble custom complex transformations and code analysis tools.

AspectJ

AspectJ is a seamless aspect-oriented extension to the Java programming language. It is Java platform compatible easy to learn and use.

AWS SDK for Amazon SQS

The AWS Java SDK for Amazon SQS module holds the client classes that are used for communicating with Amazon Simple Queue Service.

[AWS SDK for Java Core](#)

The AWS SDK for Java - Core module holds the classes that are used by the individual service clients to interact with Amazon Web Services. Users need to depend on aws-java-sdk artifact for accessing individual client classes.

[Byte Buddy](#)

Byte Buddy is a code generation and manipulation library for creating and modifying Java classes during the runtime of a Java application and without the help of a compiler.

[CDI APIs](#)

APIs for CDI (Contexts and Dependency Injection for Java).

[cglib](#)

cglib is a powerful, high performance and quality Code Generation Library, It is used to extend JAVA classes and implements interfaces at runtime.

[Checker Qual](#)

Checker Qual is the set of annotations (qualifiers) and supporting classes used by the Checker Framework to type check Java source code.

[ClassMate](#)

ClassMate is a library for introspecting generic type information of types, member/static methods, fields. Especially useful for POJO/Bean introspection.

[Config \(Typesafe\)](#)

A configuration library for JVM languages.

[DITA-OT](#)

The DITA Open Toolkit is a Java-based implementation of the OASIS DITA Technical Committee's specification for DITA DTDs and schemas. It contains ANT, SAXON,...

[DockPanel Suite](#)

.Net Docking Library for Windows Forms

[dom4j](#)

dom4j is an easy to use, open source library for working with XML, XPath and XSLT on the Java platform using the Java Collections Framework and with full support for DOM, SAX and JAXP.

[dsinfo](#)

The dsinfo library enables you to easily use Scala-side information in implementations of embedded (internal) domain-specific languages. dsinfo is implemented using Scala macros which are an experimental feature of Scala 2.10 and 2.11.

[dsprofile](#)

The dsprofile library provides general facilities to implement domain-specific profiling in Scala and Java programs.

[edtFTPj/Free](#)

Free Java FTP library gives Java developers extensive FTP functionality.

[Ehcache](#)

Ehcache is an open source, standards-based cache for boosting performance, offloading your database, and simplifying scalability. It's the most widely-used Java-based cache because it's robust, proven, and full-featured. Ehcache scales from in-process, with one or more nodes, all the way to mixed in-process/out-of-process configurations with terabyte-sized caches.

Elasticsearch RESTful client

A RESTful client for the Elasticsearch search engine.

Error Prone

Error Prone is a static analysis tool for Java that catches common programming mistakes at compile-time.

Fast Serialization

Fast Serialization reimplements Java Serialization with focus on speed (up to 10 times faster), size and compatibility. This allows the use of FST with minimal code change.

FastInfoSet

Fast Infoset (or FI) is an international standard that specifies a binary encoding format for the XML Information Set (XML Infoset) as an alternative to the XML document format. It aims to provide more efficient serialization than the text-based XML format.

Font Awesome

Font Awesome gives you scalable vector icons that can instantly be customized - size, color, drop shadow, and anything that can be done with the power of CSS.

Fonto Editor

Fonto is an online XML editor designed for people with no knowledge of XML or any other technology that comes with structured content authoring.

GeckoFX

Gecko is a free and open source layout engine used in many applications developed by the Mozilla Foundation and the Mozilla Corporation (notably the Firefox web browser).

globalize

JavaScript globalization and localization. Formats and parses strings, dates and numbers in over 350 cultures.

GNU Aspell

GNU Aspell is a Free and Open Source spell checker designed to eventually replace Ispell. It can either be used as a library or as an independent spell checker. Its main feature is that it does a superior job of suggesting possible replacements for a misspelled word than just about any other spell checker out there for the English language. Unlike Ispell, Aspell can also easily check documents in UTF-8 without having to use a special dictionary. Aspell will also do its best to respect the current locale setting. Other advantages over Ispell include support for using multiple dictionaries at once and intelligently handling personal dictionaries when more than one Aspell process is open at once.

Specifically we are using GNUASpell dictionaries for de-CH, de-DE, en-CA, en-GB, en-US, es-ES, fr-FR, fr-CH, nl-NL.

google-code-prettify

google-code-prettify is a Javascript module and CSS file that allows syntax highlighting in an html page.

google-gson

google-gson is a Java library to convert JSON to Java objects and vice-versa.

Google Guava

The Guava project contains several of Google's core libraries that we rely on in our Java-based projects: collections, caching, primitives support, concurrency libraries, common annotations, string processing, I/O, and so forth.

[Google J2ObjC](#)

J2ObjC is an open-source command-line tool from Google that translates Java source code to Objective-C for the iOS (iPhone/iPad) platform. This tool enables Java source to be part of an iOS application's build, as no editing of the generated files is necessary.

[GraphQL-Java](#)

The Java implementation of GraphQL.

[HdrHistogram](#)

A High Dynamic Range Histogram that supports recording and analyzing sampled data value counts across a configurable integer value range with configurable value precision within the range. Value precision is expressed as the number of significant digits in the value recording, and provides control over value quantization behavior across the value range and the subsequent value resolution at any given level.

[Hibernate](#)

Hibernate is a high-performance Object/Relational persistence and query service. The most flexible and powerful Object/Relational solution on the market, Hibernate takes care of the mapping from Java classes to database tables and from Java data types to SQL data types. It provides data query and retrieval facilities that significantly reduce development time. Hibernate's design goal is to relieve the developer from 95% of common data persistence-related programming tasks by eliminating the need for manual, hand-crafted data processing using SQL and JDBC.

[HK2 Framework](#)

HK2 is a light-weight and dynamic dependency injection framework.

[HSQLDB \(HyperSQL DataBase\)](#)

HSQLDB (HyperSQL DataBase) is the leading SQL relational database engine written in Java. It offers a small, fast multithreaded and transactional database engine with in-memory and disk-based tables and supports embedded and server modes. It includes a powerful command line SQL tool and simple GUI query tools.

[Hunspell](#)

Hunspell is the spell checker of LibreOffice, OpenOffice.org, Mozilla Firefox 3 & Thunderbird, Google Chrome, and it is also used by proprietary software packages, like Mac OS X, InDesign, MemoQ, Opera and SDL Trados Studio.

[InstallAnywhere](#)

InstallAnywhere is the leading multi-platform development solution for application producers who need to deliver a professional and consistent cross installation experience for physical, virtual and cloud environments. From a single project file and build environment, InstallAnywhere creates reliable installations for on-premises platforms - Windows, Linux, Apple OS X, Solaris, AIX, HP-UX, and IBM iSeries - and enables you to take existing and new software products to a virtual and cloud infrastructure.

[Jackson tooling](#)

Inspired by the quality and variety of XML tooling available for the Java platform (StAX, JAXB, etc.), the Jackson is a multi-purpose Java library for processing JSON data format. Jackson aims to be the best possible combination of fast, correct, lightweight, and ergonomic components for developers.

Jakarta Activation API

The JavaBeans Activation Framework API JAR.

Jakarta XML Bind API

Jakarta's XML bind API.

Java API for RESTful web services (javax.ws.rs)

Java API for RESTful Web Services.

JavaBeans Activation Framework

With the JavaBeans Activation Framework standard extension, developers who use Java technology can take advantage of standard services to determine the type of an arbitrary piece of data, encapsulate access to it, discover the operations available on it, and to instantiate the appropriate bean to perform said operation(s).

JavaBeans Validation

Bean Validation (JSR-303) API.

Javassist (*Java Programming Assistant*)

Javassist (*Java Programming Assistant*) makes Java bytecode manipulation simple. It is a class library for editing bytecodes in Java; it enables Java programs to define a new class at runtime and to modify a class file when the JVM loads it. Unlike other similar bytecode editors, Javassist provides two levels of API: source level and bytecode level. If the users use the source-level API, they can edit a class file without knowledge of the specifications of the Java bytecode. The whole API is designed with only the vocabulary of the Java language. You can even specify inserted bytecode in the form of source text; Javassist compiles it on the fly. On the other hand, the bytecode-level API allows the users to directly edit a class file as other editors.

javax.annotation

JSR 250 Common Annotations For The Java Platform.

javax.cache

Caching Java API

javax.Expression Language

Expression Language Java API

javax.inject

Dependency Injection Java API

javax.validation

Bean Validation API

javax.jms

The Java Message Service (JMS) API is a messaging standard that allows application components based on the Java 2 Platform, Enterprise Edition (J2EE) to create, send, receive, and read messages. It enables distributed communication that is loosely coupled, reliable, and asynchronous.

JAXB

The goal of the JAXB project is to develop and evolve the code base for the Reference Implementation (RI) of JAXB, the Java Architecture for XML Binding. The JAXB specification is developed through the Java Community Process following the process described at jcp.org. This process involves an Expert Group with a lead that is responsible for delivering the specification, a reference implementation (RI) and a Technology Compatibility Kit (TCK). The primary goal of an RI is to support the development of the specification and to

validate it. Specific RIs can have additional goals; the JAXB RI is a production-quality implementation that is used directly in a number of products by Oracle and other vendors.

JBoss Java Annotation Indexer (Jandex)

A Java Annotation Indexer for JBoss

JBoss Logging Framework

The JBoss Logging Framework.

jedis

A blazingly small and sane Redis Java client.

Jersey RESTful WS

Developing RESTful Web services that seamlessly support exposing your data in a variety of representation media types and abstract away the low-level details of the client-server communication is not an easy task without a good toolkit. In order to simplify development of RESTful Web services and their clients in Java, a standard and portable JAX-RS API has been designed. Jersey RESTful Web Services framework is open source, production quality, framework for developing RESTful Web Services in Java that provides support for JAX-RS APIs and serves as a JAX-RS (JSR 311 & JSR 339) Reference Implementation.

Jettison

Jettison is a collection of Java APIs (like STaX and DOM) which read and write JSON. This allows nearly transparent enablement of JSON based web services in services frameworks like CXF or XML serialization frameworks like XStream.

Jetty

The Jetty Web Server provides an HTTP server and Servlet container capable of serving static and dynamic content either from a standalone or embedded instantiations. Starting from Jetty version 7, the Jetty webserver and other core components are hosted by the Eclipse Foundation.

JLine

JLine is a Java library for handling console input. It is similar in functionality to BSD editline and GNU readline. People familiar with the readline/editline capabilities for modern shells (such as bash and tcsh) will find most of the command editing features of JLine to be familiar.

JMESPath Java

JMESPath is a query language for JSON. You can extract and transform elements from a JSON document. This is a Java implementation

Joda-Convert

Joda-Convert provides a small set of classes to provide round-trip conversion between Objects and Strings. It does not tackle the wider problem of Object to Object transformation.

Joda-Time

Joda-Time provides a quality replacement for the Java *date* and *time* classes. The design allows for multiple *calendar* systems, while still providing a simple API. The 'default' calendar is the http://www.joda.org/joda-time/cal_iso.html standard which is used by XML. The Gregorian, Julian, Buddhist, Coptic, Ethiopic and Islamic systems are also included, and we welcome further additions. Supporting classes include time zone, duration, format and parsing.

JOL (Java Object Layout)

JOL (Java Object Layout) is the tiny toolbox to analyze object layout schemes in JVMs. These tools are using Unsafe, JVMTI, and Serviceability Agent (SA) heavily to decode the *actual* object layout, footprint, and references.

jQuery

jQuery is a fast, small, and feature-rich JavaScript library. It makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers. With a combination of versatility and extensibility, jQuery has changed the way that millions of people write JavaScript.

jQuery CheckBoxTree

A jQuery based checkbox tree plugin that displays your hierarchical data in a tree structure with checkboxes.

jquery-cookie

jQuery plugin for reading, writing and deleting cookies.

jquery.datatables

DataTables is a plug-in for the jQuery Javascript library. It is a highly flexible tool, based upon the foundations of progressive enhancement, which will add advanced interaction controls to any HTML table.

jquery.dataTables.columnFilter

Adds advanced filter capabilities to the DataTables. JS file.

jQueryFileUpload

File Upload widget with multiple file selection, drag&drop support, progress bar, validation and preview images, audio and video for jQuery.

jquery.TypeScript.DefinitelyTyped

TypeScript Definitions (d.ts) for jquery.

jQuery.Gantt

Draw Gantt charts with the famous jQuery ease of development.

jQuery Highlight

Highlights the search keywords/terms in a preview.

jQuery UI

jQuery UI is a set of user interface interactions, effects, widgets, and themes built on top of the jQuery JavaScript Library.

JSON-js

JSON is a light-weight, language independent, data interchange format. See <http://www.JSON.org> / The files in this collection implement JSON encoders/decoders in JavaScript. JSON became a built-in feature of JavaScript when the ECMAScript Programming Language Standard - Fifth Edition was adopted by the ECMA General Assembly in December 2009. Most of the files in this collection are for applications that are expected to run in obsolete web browsers. For most purposes, json2.js is the best choice.

Json.NET

Json.NET is a popular high-performance JSON framework for .NET.

[jsoup](#)

jsoup is a Java library for working with real-world HTML. It provides a very convenient API for extracting and manipulating data, using the best of DOM, CSS, and jquery-like methods.

[JTA \(Java Transaction API\)](#)

The `javax.transaction` package. It is appropriate for inclusion in a classpath, and may be added to a Java 2 installation.

[Kiama](#)

The Kiama test library contains a collection of examples, tests that use those examples, and useful test support code.

[Knockout JavaScript library](#)

Knockout is a JavaScript library that helps you to create rich, responsive display and editor user interfaces with a clean underlying data model. Any time you have sections of UI that update dynamically (e.g., changing depending on the user's actions or when an external data source changes), KO can help you implement it more simply and maintainably.

[Kryo](#)

Kryo is a fast and efficient binary object graph serialization framework for Java. The goals of the project are high speed, low size, and an easy to use API. The project is useful any time objects need to be persisted, whether to a file, database, or over the network.

Kryo can also perform automatic deep and shallow copying/cloning. This is direct copying from object to object, not object to bytes to object.

[kXML 2](#)

kXML is a small XML pull parser, specially designed for constrained environments such as Applets, Personal Java or MIDP devices. In contrast to kXML 1, kXML 2 is based on the XML pull API.

[LatencyUtils](#)

The LatencyUtils package includes useful utilities for tracking latencies. Especially in common in-process recording scenarios, which can exhibit significant coordinated omission sensitivity without proper handling.

[Logback](#)

Logback is intended as a successor to the popular log4j project, picking up where log4j leaves off.

[MapStruct](#)

MapStruct is a code generator that greatly simplifies the implementation of mappings between Java bean types based on a convention over configuration approach. The generated mapping code uses plain method invocations and thus is fast, type-safe and easy to understand.

[MathJAX](#)

MathJax is an open-source JavaScript display engine for LaTeX, MathML, and AsciiMath notation that works in all modern browsers. It was designed with the goal of consolidating the recent advances in web technologies into a single, definitive, math-on-the-web platform supporting the major browsers and operating systems.

Micrometer

Micrometer provides a simple facade over the instrumentation clients for the most popular monitoring systems, allowing you to instrument your JVM-based application code without vendor lock-in. Think SLF4J, but for metrics.

Microsoft JDBC Driver for SQL Server

Microsoft provides a Java Database Connectivity (JDBC) driver for use with SQL Server, and Azure SQL Database. The driver provides Java database connectivity from any Java application, application server, or Java-enabled applet. This driver is a Type 4 JDBC driver that provides database connectivity through the standard JDBC application program interfaces (APIs).

Minlog

MinLog is a tiny Java logging library.

MVC Web Projects

Auxiliary MVC Web Project libraries.

MXP1

MXP1 is a stable XmlPull parsing engine that is based on ideas from XPP and in particular XPP2 but completely revised and rewritten to take the best advantage of latest JIT JVMs such as Hotspot in JDK 1.4+.

NHunspell

NHunspell brings the spell checking, hyphenation and thesaurus to the Microsoft® .NET Framework. NHunspell is C# library and wraps native libraries for Hunspell, Hyphen and MyThes. One design goal of this library and wrapper is to keep the source code of the included libraries as unmodified as possible. New versions of the base libraries can therefore easily adopted to NHunspell.

The integrated libraries are used in OpenOffice and they work with the dictionaries published on OpenOffice.org.

NLog

NLog is a free logging platform for .NET, Silverlight and Windows Phone with rich log routing and management capabilities. NLog makes it easy to produce and manage high-quality logs for your application regardless of its size or complexity.

Objenesis

Objenesis is a small Java library that serves one purpose: to instantiate a new object of a particular class.

okhttp

An HTTP+HTTP/2 client for Android and Java applications.

okio

A modern I/O API for Java.

Oracle JDBC Drivers

Drivers used for making a JDBC connection from Java to an Oracle database.

Oracle PKI (Public Key Infrastructure)

Oracle public key infrastructure (PKI) is used by Oracle Enterprise Security Manager, LDAP-enabled Oracle Enterprise Manager, Oracle's Secure Socket Layer (SSL) authentication, Oracle Database, and Oracle Application Server.

[**Oracle Security Developer Tools \(OSDT\)**](#)

Oracle Security Developer Tools provide you with the cryptographic building blocks necessary for developing robust security applications, ranging from basic tasks like secure messaging to more complex projects such as securely implementing a service-oriented architecture. The tools build upon the core foundations of cryptography, public key infrastructure, web services security, and federated identity management.

[**PATRICIA Trie in Java**](#)

An implementation of the Practical Algorithm to Retrieve Information Coded in Alphanumeric (PATRICIA).

[**Postal.Mvc5**](#)

Generate emails using ASP.NET MVC views

[**Project Reactor**](#)

Reactor is a fourth-generation Reactive library for building non-blocking applications on the JVM based on the Reactive Streams Specification.

[**PS Cmdlet Help Editor**](#)

PowerShell Cmdlet Help Editor is the tool that helps you to create and edit XML-based help files for your PowerShell modules and PSSnap-Ins.

[**React**](#)

React is a JavaScript library for building user interfaces.

[**Reactive Streams**](#)

A Protocol for Asynchronous Non-Blocking Data Sequence

[**Reactor Core**](#)

Reactor Core is a non-blocking reactive foundation for the JVM.

[**Red Hat Linux**](#)

Red Hat Enterprise Linux OpenStack Platform delivers an integrated foundation to create, deploy, and scale a secure and reliable public or private OpenStack cloud. Red Hat Enterprise Linux OpenStack Platform combines the world's leading enterprise Linux and the fastest-growing cloud infrastructure platform to give you the agility to scale and quickly meet customer demands without compromising on availability, security, or performance.

[**ReflectASM**](#)

ReflectASM is a very small Java library that provides high performance reflection by using code generation. An access class is generated to set/get fields, call methods, or create a new instance. The access class uses bytecode rather than Java's reflection, so it is much faster. It can also access primitive fields via bytecode to avoid boxing.

[**Rx .NET**](#)

Reactive Extensions for .NET library used to validate entered values

[**Scala**](#)

The Scala programming language fuses object-oriented and functional programming in a statically typed programming language. It is aimed at the construction of components and component systems.

[Scallop](#)

Scallop is a command line parser.

[SitemapGen4j](#)

SitemapGen4j is a library to generate XML sitemaps in Java.

[SLF4J](#)

The Simple Logging Facade for Java (SLF4J) serves as a simple facade or abstraction for various logging frameworks (e.g. java.util.logging, logback, log4j) allowing the end user to plug in the desired logging framework at deployment time.

[SnakeYAML](#)

YAML is a data serialization format designed for human readability and interaction with scripting languages. SnakeYAML is a YAML parser and emitter for the Java programming language.

[SNMP4J](#)

SNMP4J is an enterprise class free open source and state-of-the-art SNMP implementation for Java™ 2SE 1.4 or later. SNMP4J supports command generation (managers) as well as command responding (agents). Its clean object oriented design is inspired by SNMP++, which is a well-known SNMPv1/v2c/v3 API for C++.

[SpringFox](#)

Automated JSON API documentation for API's built with Spring.

[Spring Framework](#)

The Spring Framework provides a comprehensive programming and configuration model for modern Java-based enterprise applications - on any kind of deployment platform. A key element of Spring is infrastructural support at the application level: Spring focuses on the "plumbing" of enterprise applications so that teams can focus on application-level business logic, without unnecessary ties to specific deployment environments.

[StAX](#)

StAX is a standard XML processing API that allows you to stream XML data from and to your application. This StAX implementation is the standard pull parser implementation for JSR-173 specification.

[Swagger](#)

Swagger is a simple yet powerful representation of your RESTful API. With the largest ecosystem of API tooling on the planet, thousands of developers are supporting Swagger in almost every modern programming language and deployment environment. With a Swagger-enabled API, you get interactive documentation, client SDK generation and discoverability.

[Swashbuckle.Core](#)

Seamlessly adds a Swagger to WebApi projects.

[Thinkecture IdentityModel](#)

Helpers and client libraries for OpenID Connect, OAuth 2.0 and claims-based Identity.

[Thinkecture IdentityServer](#)

Front-end Secure Token Service to serve SAML tokens.

TwelveMonkeys Common

TwelveMonkeys Common library contains common utility classes relating to languages, I/O and images.

TwelveMonkeys ImageIO

TwelveMonkeys ImageIO is a collection of plugins and extensions for Java's ImageIO. These plugins extend the number of image file formats supported in Java, using the `javax.imageio.*` package. The main purpose of this project is to provide support for formats not covered by the JRE itself.

TXW2

TXW is a library that allows you to write XML documents.

ua-parser

A multi-language port of Browserscope's user agent parser.

WiX

The WiX toolset builds Windows installation packages from XML source code. The tool-set integrates seamlessly into build processes.

Woodstox

Woodstox is a high-performance validating namespace-aware StAX-compliant (JSR-173) Open Source XML-processor written in Java.

Xalan-Java

Xalan-Java is an XSLT processor for transforming XML documents into HTML, text, or other XML document types. It implements XSL Transformations (XSLT) Version 1.0 and XML Path Language (XPath) Version 1.0 and can be used from the command line, in an applet or a servlet, or as a module in other program.

Xerces Java Parser

The Xerces Java Parser 1.4.4 supports the XML 1.0 recommendation and contains advanced parser functionality, such as support for the W3C's XML Schema recommendation version 1.0, DOM Level 2 version 1.0, and SAX Version 2, in addition to supporting the industry-standard DOM Level 1 and SAX version 1 APIs.

XML Pull Parsing

An XML Pull Parsing API.

XStream

XStream is a simple library to serialize objects to XML and back again.

XULRunner

XULRunner is a runtime environment developed by the Mozilla Foundation to provide a common back-end for previewing.

Customer support

To contact Technical Support, connect to the Customer Support Web Portal at <https://gateway.sdl.com> and log a case for your SDL product. You need an account to log a case. If you do not have an account, contact your company's SDL Support Account Administrator.

2

Content Manager requirements

All requirements for the Content Manager application, web, and batch servers are described.

Content Manager hardware requirements

Check the hardware requirements prior to completing the pre-installation tasks.

Hardware

The performance of Content Manager depends primarily on the CPU power and the I/O characteristics of the hardware. High CPU power is needed to allow the system to make calculations on-the-fly, e.g. for publishing. The I/O performance largely influences the system's speed to gather and assemble information from the database to serve user requests. Content Manager imposes no specific requirements for data storage, as it holds generic versions that become specific versions by calculation on a user's request.

The hardware required for a specific Content Manager implementation depends on the specific requirements and settings of the project (for example, the number of concurrent users). The exact definition of the hardware requirements is typically done at the beginning of the project.

Database

The database server may be on any platform supported by the database vendor. Hardware and platform requirements for the database server should be obtained from the database vendor. The specifications supplied by Content Manager should be checked against the specifications supplied by the database vendor for the current hardware on which it is installed.

An example Microsoft Windows server machine could minimally have the following specifications:

- CPU: dual core Xeon® 2.0 GHz
- Internal Memory: 8 GB RAM

Database storage demands must account for the following:

- All XML content and related metadata.
- All images.
- Published output (e.g. PDF, CHM...).

As a rule of thumb, multiply the size of all images by 3 to get an estimate of the starting size for your database. A normal documentation project can use 100 GB for its storage needs for about 2 to 3 years.

Web and Application layer

The server can be on a single system. However, for performance reasons it is advised to scale and have redundancy over multiple servers. The scaling introduction included in Tridion Docs documentation helps you determine the setup. Due to the many setup variations, you may want to contact the support team to discuss your specifics.

Minimum server configuration: A recent quad core system(s) containing 8 GB of RAM or more. Virtualized environments are supported if they are guaranteed to behave like a Windows OS installed on a physical machine. If performance is or becomes an issue, you are advised to use physical servers.

A recommended server configuration should include a quad core Xeon® X5550 2.66 GHz processor system with at least 12 MB Level 3 cache and 8 GB RAM, dual port Gigabit Ethernet, and a smart array RAID controller with 256 MB memory.

Storage demands: The consumers of storage are the actual installed Content Manager software components, the full-text-index collection, exported, and published content. Considering a normal documentation project, with an initial database reservation of 100 GB, the server should have at least 50 GB storage capacity. The typical setup is two servers, one handling the synchronous operations and one server handling the asynchronous/background operations. Initially you can start with one server handling all operations; we then suggest a dual CPU server. A second server can be added quite easily afterwards if load needs to be reduced on the primary server.

Client requirements

Client machines running desktop applications such as Publication Manager should have at least a 2.0 GHz CPU and 4 GB RAM.

Network requirements

Due to its stateless model, Content Manager passes large quantities of data. A 10 Mbit network connection provides a more than acceptable throughput.

Content Manager software requirements

Information about third-party or client software that is packaged, configured and tested for this software version release.

The following overview includes information about:

- Third-party software that is configured or integrated in this server-side component release.
- Third-party software, such as the operating systems, databases, and runtimes that are quality-assurance tested.
- Client hardware and software compatibility.

The relation between the Authoring Bridge and the XML editors is not specified here. Installation packages for Authoring Bridge are not always available for all XML editors. Also third-party software such as authoring tools and databases have their specific requirements. Check out the third-party tools' documentation before installation.

This is a reference list not a task list. It specifies on which items our software relies. Some components might already be installed by other software. Some components may be needed only for certain features or configurations of Content Manager. Refer to the Content Manager installation or upgrade tasks to know which of the specified software you need to install.

Third Party Software supported versions

Note: Names, trademarks, designs, logos, service marks, intellectual property and so on, of the products shown are exclusive property of their respective owners.

Application server

- Microsoft Windows Server 2019 (64-bit)
- Microsoft Windows Server 2016 (64-bit)
- Oracle Data Access Client 19.3.0.0.0
- Microsoft OLE DB Driver for SQL Server
- Oracle Java 11 (18.9 LTS)
- Eclipse Temurin OpenJDK 11 (formerly known as AdoptOpenJDK OpenJDK 11) with Hotspot 11+28 (64-bit)
- Java Help 2.0.05
- Microsoft Server .NET Framework 4.8.0
- Microsoft Server .NET Framework 4.7.2 Revision 461814 (pre-installed with Windows Server 2019)
- Microsoft .NET Framework Visual C++ Redistributable VS2015 (64-bit)
- Microsoft PowerShell 5.1 (pre-installed with Windows Server 2016 and 2019)
- DITA Open Toolkit 2.3

Note: Our standard Tridion Docs installation package holds a DITA Open Toolkit version.

- Microsoft XML Parser 6.0, 32-bit and 64-bit (pre-installed with Windows Server 2012R2 and 2016)
- HTML Help Workshop 1.3
- AntennaHouse XSL Formatter 6.5

Database server

Database systems and versions

- Oracle RDBMs 19.3.0.0.0
- Oracle RDBMs 12.2.0.1.0
- Oracle RDBMs 12.1.0.2.0
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016 SP2
- Microsoft SQL Server 2016 SP1

Client

- Microsoft Windows 10 (64-bit)
- Microsoft Windows 8/8.1 (64-bit)
- Microsoft Edge
- Google Chrome (latest version)
- Mozilla Firefox (latest version)
- JustSystems XMetaL 12.0 / 12.0 (64-bit)
- JustSystems XMetaL 12.0 / 12.0 (Japanese) (64-bit only)

- JustSystems XMetaL 14.0 / 14.0 (64-bit)
- Syncro Soft <oXygen/> XML Author 20.0 (64-bit only)
- Syncro Soft <oXygen/> XML Author 21.1 (64-bit only)
- PTC Arbortext Editor 7.1 (64-bit only)
- Acrolinx 5.0

About XML editors

Only 64-bit mode for the editors is approved and qualified.

Although multiple third-party XML editors are supported, we recommend choosing and using a single third-party editor. SDL is not responsible for third-party editor XML and DITA handling; behavior may differ depending on the XML editor. If you use more than one editor, you may experience cross-compatibility issues related to DITA handling. If you decide to use multiple third-party XML editors and if you experience cross-compatibility issues with DITA handling, contact the XML editor vendor to address these issues.

About web browsers

The browser must be configured to allow the following:

- Cookies
- Pop-up windows for Collective Spaces (that is, Draft Space and Review Space) when the application is called from the Content Manager Web Client.
- A minimum resolution of 1024 x 768 pixels. The optimal resolution is 1280 x 1024 pixels or higher.

Installer User Requirements

The users who can install Content Manager must have permissions and access as required.

An administrator user who has authorized access on the machines to be installed can install the Content Manager software. The user must be able to:

- logon to the machine and have full access to the file system
- alter the registry
- have full access to the Services, Message Queuing, Indexing, Internet Information Services and Component Services

A database administrator must set up the Content Manager database. The user must be able to:

- create a database
- run scripts to set up the database

Platform virtualization

You can deploy Content Manager software in a virtual environment (such as VMWare ESX).

You can deploy Content Manager software in a virtual environment if both of the following conditions are true:

1. Content Manager supports the environment in its non-virtual form.
2. The platform vendor states that it supports the virtual form of this environment.

Note: If you run a software component in a virtual environment, the hardware recommendations listed for that software component in the Product Prerequisites document may not apply. The recommendations listed apply to the software component if it is installed directly on such a hardware profile, and not to the software component installed in a virtual environment that itself runs on the recommended hardware profile.

For specific virtual platform support requests, contact the platform vendor. For specific hardware recommendations, contact your virtual hardware solution vendor to find out how the hardware recommendation for a direct installation translates into a hardware recommendation for a virtual installation.

Firewalls and ports

In specific cases, firewall and ports may require special attention.

Firewalls and ports are an important part of your installation environment. Normally the default settings do not interfere with a basic installation, but there is a variety of possibilities regarding network and firewall configurations. This list provides some of the most common points of attention and is by no means comprehensive.

The user responsible for the network setup knows all the items that should be checked in your environment and has access to the specific technical documentation. Details can be found in the *Advanced topics for installers* section.

SMTP

Simple Mail Transfer Protocol (SMTP) is the standard for e-mail transmissions across the internet.

Microsoft SQL Server

Microsoft SQL Server is the relational database management system (RDBMS) produced by Microsoft.

Oracle RDBMS

Oracle Database, or simply Oracle, is the relational database management system (RDBMS) produced by Oracle Corporation.

HTTPS (SSL)

HTTPS is a URI scheme used to indicate a secure HTTP connection. It refers to the combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL).

3

Installing Content Manager

These steps apply to Content Manager installation specifically.

Install preparation

The pre-installation tasks ensure you do not encounter issues when installing and configuring the necessary Content Manager software components.

Enabling https on the IIS website

Content Manager requires that https is enabled on the IIS website that is used for Content Manager.

Before you begin

Follow this procedure on the main Content Manager server. After installing the certificate, you must bind the website to https (included in the last step below).

About this task

Before you can enable https on the Content Manager website you must first install a SSL certificate on the server. There are several ways to request and install a certificate:

- You can buy a certificate from a commercial certificate authority, for example, Verisign. These commercial CAs have online how-to help pages that guide you through the process of requesting a certificate and installing it.
- When your company has an internal Certificate Authority, you can request certificates yourself, or through your IT staff.
- Use the **Create Domain Certificate** in IIS. To do this follow the procedure below.

Procedure

1. Request and install the certificate.
 - a. In Internet Information Services (IIS) Manager, open: *ComputerName* > **Server Certificates**.
 - b. In the right **Actions** pane, click **Create Domain Certificate**.
A Create Certificate window displays.
 - c. Add the necessary information to the fields in Create Certificate:
 - **Common name:** Enter the complete domain name of the URL to be used for this Content Manager. For example: *techdoccms.sdl.com*
 - **Organization:** enter your company name. For example: *SDL*
 - **Organizational unit:** Enter the name of the department that is requesting the certificate. For example: *SDL IT*
 - **City, State & Country:** Enter the city, state & country where the company is located.
 - d. Click **Next**.
An Online Certificate Authority window displays.

- e. **Specify Online Certificate Authority** that you want to use by clicking **Select** to the right of the field.

Note: If the list for Certificate Authority is empty you cannot continue and you have to ask your IT department for instruction on how to continue.

- f. Enter a **Friendly Name**. The **Friendly Name** is a more user-friendly name for the certificate and is shown in several programs such as IIS.
You should see the requested certificate appearing in the IIS Server Certificates list, and you can now use it.
 - g. Click **Finish**.
2. Bind the website to https:
 - a. Right-click the IIS Website that will be used for Content Manager.
 - b. Select **Edit Bindings**.
 - c. Click **Add**.
 - In the **Type** field, select **https**.
 - In the **SSL certificate** field select the certificate that you requested and installed; select the **Friendly Name** specified in the previous step.
 - If the options **Disable HTTP/2** and **Disable OCSP Stapling** are present (depending on your version of Windows server), leave those box unchecked.
 - d. Click **OK**.

Defining the bindings in the target web site

When using multiple websites IIS, the administrator of IIS should explicitly define the bindings in the target web site to ensure that the installation serves the requests that target it.

When an IIS has multiple websites it is not clear which website should serve the incoming request which can make the Content Manager installation unstable. On a IIS server with multiple websites, there has to be mechanism that guides IIS to the correct website. That mechanism is known as binding configuration. The binding works as a key in a Dictionary of Websites. So simply, IIS analyzes the request, figures out the key and then goes to the dictionary to find the proper website.

Note: Productions systems should always define the bindings on the website even if the website is unique on the IIS. When the bindings are explicitly defined on the website, the website is protected against any other request that was not intended to be served. This is another layer of protection for the website.

Assume the following values for Content Manager's `baseurl` and `localservicehostname`; that is, all requests that have the following host names that must be served by this website:

- `localhostname: example`

- `hostname: example.com`

In addition to the host names, the website must be able to serve the following schemas for both host names:

- `http-hostname`
- `https-hostname`
- `http-localhostname`
- `https-localhostname`

Example of end points that the website (IIS) is to serve:

- `http://example/ISHWS/WCF/API/Application.svc`
- `https://example/ISHWS/WCF/API/Application.svc`
- `http://example.com/ISHWS/WCF/API/Application.svc`
- `https://example.com/ISHWS/WCF/API/Application.svc`
- `https://example.com/ISHCM/`

Based on the above examples, to described the possible schema/hostname combinations for Content Manager, the IIS administrator needs to explicitly define bindings for the following combinations:

- HTTP
Example: `example.com`
- HTTP
Example: `example`
- HTTPS
Example: `example.com`
- HTTPS
Example: `example`

Configuring the HTTP bindings can be done from the user interface.

Configuring the HTTPS bindings must be done by executing a command, such as:

```
%systemroot%\system32\inetsrv\APPCMD set site [WebSiteName]/bindings:https/*:443: [hostname]
```

Where you must replace the references to `[WebSiteName]` and `[hostname]` appropriately for your configuration and site. There are alternatives that are documented in the help of the commands.

The **RequireSSL** on IIS **SSL Settings** forbids any request with the HTTP schema. Based on the above, it is implicitly required that the website cannot have the **RequireSSL** set to `true` in the SSL Settings.

The same requirement for **RequireSSL** on **SSL Settings** is applied for the `infosharewebappname` defined in the input parameters.

For more information about adding a binding to a site, refer to:

- <http://www.iis.net/configreference/system.applicationhost/sites/site/bindings/binding>
- [http://technet.microsoft.com/en-us/library/cc731692\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731692(v=ws.10).aspx)

Microsoft Windows Server

Additional installation and configuration requisites are described for the Content Manager product installation for the current supported versions of Microsoft Windows.

Content Manager must be installed on versions of Microsoft Windows Server referenced in the Content Manager software requirements list.

Note: Content Manager is qualified on an English version of our supported operating systems only. Other languages of these operational systems are not used for quality check purposes.

Establishing a dedicated system user

The Content Manager components need a dedicated OS local administrator per server to host all components, with the right region and language settings.

Before you begin

All Content Manager related components should be run by a designated operating system user (also known as a Service Account, typically named `InfoShare`). This separate user lets you change user settings with little interference with the rest of the system.

About this task

A Windows Domain user is required when using Microsoft ADFS as STS. Ask your Active Directory system administrator to create a service account.

Procedure

1. Create the local or domain `InfoShare` system user:

Note: If you have to configure multiple servers, we advise to create a domain user and make the user a local Administrator on each of the target machines as described here.

- a. Select **Server Manager** in the lower left corner.
- b. Select **Tools > Computer Management**.
- c. Open **Computer Management > System Tools > Local Users and Groups** then select **Users**.
- d. Open the **Action** menu and select **New user**.
- e. Enter `InfoShare` as the **User name**.
- f. Enter a **Full name** and a **Description**.
- g. Enter a **Password**. Enter the password again in the **Confirm password** field.
- h. Clear **User must change password at next logon** then select **User cannot change password** and **Password never expires**.

- i. Select **Create** and **Close**.
- j. Under **Local Users and Groups**, select **Groups**.
- k. Open the local **Administrators** group of the machine and add the `InfoShare` system user.
- l. Select **Apply**.

Note: Microsoft requires some registry keys to be write-enabled for transactions and more. The services, Message Queues, IIS Application Pools and Component Services Server Applications all run within this user's context.

2. Allow the `InfoShare` user to run services, otherwise you may experience service startup failures.
 - a. As an administrator user, open **Server Manager** then Select **Tools > Local Security Policy** on your server.
 - b. Open **Local Policies** then select **User Rights Assignment**.
 - c. Open **Log on as a service** then select **Add User or Group** and add the `InfoShare` user created above.
 - d. Select **OK** to activate the settings.
 - e. Open the **File** menu and select **Exit** to close the window.
3. Set the language and region of the `InfoShare` system user on each application server:
 - a. Login on to your system as the `InfoShare` user to validate the user account.
 - b. Select **Control Panel > Clock, Language and Region**.
 - c. Select **Language**.
 - d. Make sure that `English (United States)` is the language listed.
 - If `English (United States)` is not listed, select **Add a language** then **English** and **Open**. Select **English (United States)**, then click **Add**.
 - If `English (United States)` is among other languages listed and it does not appear first, select it then **Move up** until it appears first.

Note: To allow various code stacks like .NET, VB6, Java, etc to work flawlessly together we strongly advise to pick a Western language entry here.

- e. Still in the **Language** window, select **Change date, time, or number formats** on the left pane
- f. Change format to **English (United States)**.
- g. Change:
 - Short date: **dd/MM/yyyy**
 - Long date: **dddd d MMMM yyyy**
 - Short time: **HH:mm:ss**
 - Long time: **HH:mm:ss**
- h. Select the **Location** tab, for the **Current location** field, select the entry `United States`.

- i. Select the **Administrative** tab and select **Change system locale**.
 - j. Select `English (United States)`.
 - k. Select **OK**.
4. Restart the server.

Changing the Local Group Policy

Set the group policy so that Windows does not forcefully unload the registry.

About this task

A new *User Profile Service* functionality built into the OS by default forces the unload of the user profile on Windows when the user logs off. This results in, for instance, a COM+ application to stop working on Windows Server when the identity user logs off and the COM+ application can no longer read registry keys in the profile of the identity user. The policy setting **Do not forcefully unload the user registry at user logoff** counters the default behavior of Windows. When enabled, Windows does not forcefully unload the registry and waits until no other process is using the user registry before it unloads it.

Procedure

1. As an Administrator user, start the **Windows Powershell** (an icon can usually be found in the taskbar).
2. In the command prompt, type `gpedit.msc`.
A Local Group Policy Editor window displays.
3. In the left pane, open **Local Computer Policy > Computer Configuration > Administrative Templates > System > User Profiles**.
4. In the right pane, open **Do not forcefully unload the user registry at user logoff**.
5. In the resulting window, select the radio button **Enabled**.
6. Select **OK**.

Microsoft SQL Server database access components

If you use a Microsoft SQL Server RDBMs, you need to download and install Microsoft OLE DB Driver 18 for SQL Server (MSOEDBSQL). This driver is no longer included with Microsoft Windows operating systems.

About this task

For information about the OLE DB Driver, refer to <https://docs.microsoft.com/en-us/sql/connect/oledb/oledb-driver-for-sql-server?view=sql-server-ver15>

Procedure

1. Do one of the following:
 - From the webpage at <https://www.microsoft.com/en-us/download/details.aspx?id=56730> , download the 64-bit edition of the installer to your Content Manager server machine.
 - On your installation media, go to the folder `ThirdPartySoftware\SQLServerDrivers\MicrosoftOLEDBDriver\` and copy the installer from that location to your Content Manager server machine.
2. Follow the instructions of the installer to set up the driver.

Oracle Data Access Components

If you use Oracle RDBMs to host your database, you need to install Oracle Data Access Components (ODAC) version 19.3.0.0 32-bit.

Before you begin

The 32-bit Oracle 19 Client requires the installation of the 32-bit Microsoft Visual C++ 2017 Redistributables.

About this task

Oracle Data Access Components (ODAC) is a set of tools to access, manipulate and manage database data stored on Oracle RDBMs. If you host your database using Oracle RDBMs, you need to install the "Oracle Provider for OLE DB" components of Oracle Data Access Components (ODAC) 19.3.0.0 32-bit. To correctly perform the installation, you need to access the target machine as an administrator.

Procedure

1. Go to the Oracle web site, [download section](#) , which should be the page where you can download the 32-bit Oracle Data Access Components product.
2. Go to the section **ODAC XCopy** and download the archive containing the 32-bit ODAC 19.3, named `ODAC193Xcopy_32bit.zip`. Save it locally
3. Unzip the archive to a temporarily location. For instance `C:\Temp\ODAC193Xcopy32bit`
4. Install the "Oracle Provider for OLE DB" components
 - a. Open a 32-bit Command Prompt as administrator
`C:\Windows\SysWOW64\cmd.exe` , right click and choose run as administrator
 - b. Execute the following lines in the 32-bit Command Prompt

```
cd C:\Temp\ODAC193Xcopy32bit
install.bat oledb C:\Oracle\product\19.0.0\ODAC ODAC
```

5. Add the install directory and install directory's bin subdirectory to the system PATH environment variable
 - a. Open **Control Panel > System and Security > System > Advanced system settings > Environment Variables**
 - b. Goto **System variables > Path**

- c. Click **Edit** and add the following paths at the beginning:
 - `C:\Oracle\product\19.0.0\ODAC`
 - `C:\Oracle\product\19.0.0\ODAC\bin`
6. Add a system `TNS_ADMIN` environment variable with the location of the `tnsnames.ora` file
 - a. Open **Control Panel > System and Security > System > Advanced system settings > Environment Variables**
 - b. Goto **System variables**
 - c. Click **New** to add the extra environment variable
 - **Variable name:** `TNS_ADMIN`
 - **Variable value:** The directory holding the `tnsnames.ora` file. For example `C:\Oracle\product\19.0.0\ODAC\network\admin`
7. Reboot the server to ensure that the new system environment variables are available for all processes

Verifying the .NET Framework version

If you use an older Windows server versions (2016 for example), you need to check if the required .NET Framework version is installed.

About this task

The latest version of Windows server automatically installs the version of .NET Framework that is required for Content Manager. If you are using an older Windows server version, you need to check if the required version of .NET Framework is installed, and if not, download and install it.

All the software versions compatible with this Tridion Docs version are listed in the Content Manager software requirements.

Procedure

1. Open a PowerShell session with administrator rights.
2. Type in the following command:

```
Get-ChildItem 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4
\Full\' | Get-ItemPropertyValue -Name Version
```

3. Check the displayed information and make sure the specified version is compatible with the Content Manager software requirements. Also check that the revision number is the one listed in the requirements.

If the version matches the requirements, it will be used for the installation and you don't need to take further action.

4. If you need to install a later .NET Framework version, go to Windows web pages to find it, download it and install it. For example at <https://dotnet.microsoft.com/download/dotnet-framework/>. Be sure to select the *Runtime* install.

Configuring HTTP Activation for WCF

Windows Communication Foundation (WCF) uses the listener adapter interface to communicate activation requests that are received over the non-HTTP protocols supported by WCF. To allow this, configure HTTP Activation.

Procedure

1. In the **Control Panel**, under the **Programs** heading, select **Turn windows features on or off**.
2. Select **Server Selection** in the list on the left.
3. Select the name of the server where the feature needs to be installed, in the center pane.
4. Select **Features** in the list on the left.
5. Open the **.NET Framework 4.X Features (Installed)** tree node then open **WCF services (Installed)**.
6. Select **HTTP Activation**.
7. If a popup window **You cannot install HTTP Activation unless the following role service or features are also installed** opens, then select the **Add Features** button to install the required features.
8. Use **Next** until the **Install** button becomes active.
9. Select **Install**.

Configuring IIS and ASP Web services

It is required that the Web Services (IIS, ASP) be installed.

Before you begin

This is an optional component during a Windows installation, and is not installed by default during operating system setup.

For compatible software versions, check out the Content Manager software requirements.

Procedure

1. In the **Control Panel**, select **Programs and Features** then, on the left side of the window, **Turn windows features on or off**.
2. In the Add roles and features window, select **Next**.
3. Select your server then **Next**.
4. In the Select Server Roles window, expand the **Web Server (IIS)** role.
5. Expand **Web Server**
 - a. Under **Common HTTP features** select:
 - **Default Document**
 - **Directory Browsing**
 - **HTTP Errors**
 - **Static Content**

- b. Under **Application Development** select the following:
 - **ASP .NET 4.x** (depending on your Windows server version)
 - **.NET Extensibility 4.5**
 - **ASP**
 - **ISAPI Extensions**
 - **ISAPI Filters**
- c. To speed up file transfer over the network, we recommend enabling compression: Under **Performance** select **Static Content Compression** and **Dynamic Content Compression**.
- d. Under **Health and Diagnostics** select:
 - **HTTP Logging**
 - **Request Monitor**
6. Under **Management Tools** select:
 - **IIS Management Console**
7. Select **Next** then **Install**.

Configuring application server role

The application server role needs to be installed for Windows Server 2012R2.

Before you begin

This task applies only to Windows server 2012R2. Later versions do not require this.

Procedure

1. Open the **Server Manager**.
2. In the top right menu select **Manage > Add Roles and Features**. This opens the server management Wizard.
3. Select **Server Selection** in the list on the left.
4. Select the name of the server where the roles need to be changed, in the center pane.
5. Select **Next**.
6. Select and expand **Application Server** in the list on the right pane.
7. Under **Distributed Transactions** select:
 - **Incoming Network Transactions**
 - **Outgoing Network Transactions**
8. Select **Next**.
9. Select the checkbox **Restart the destination server** then **Install**.

Note: If the role service is already installed, the **Install** button is greyed out. Select **Cancel**.

Java

The Java tools tested with this version of Content Manager can be retrieved online from Content Manager upon request.

The compatible Java versions are specified in the Content Manager software requirements.

The following Content Manager components use Java:

- DITA Open Toolkit (publishing engine).
- TrisoftSolrLucene (search engine).

Starting from JDK 11, we refer to OpenJDK as the alternative for JDK and JRE.

Note: If you install JDK 64 bit, by default the 64 bit JRE is installed.

Configuration requirements

After installation, some components need to be configured to conform to Content Manager requirements.

It is expected that a designated operating system user will run all Content Manager related components.

Note: A designated operating system user is also known as a Service Account.

It is recommended that you do a system reboot to ensure that all installed components finish their installation.

Prerequisites for publishing engine

These software packages are required on the server that handles Content Manager publishing.

Java Help

Only required if you use the Content Manager Publishing engine to generate Java Help files.

Qualified version(s):

The suggested installation path is `c:\JavaHelp` which results in the availability of the following: `c:\JavaHelp\jh<version>\src.jar` Content Manager

Where `<version>` is the version of Java Help.

InstallTool input parameters allow you to indicate the path before installation using the variable **ps_javahelp_home**.

The javahelp-`<version>`.zip file tested with this release of Content Manager can be retrieved online from SDL upon request.

- extract the contents of the zip file

- create the `c:\JavaHelp\` folder
- copy or move the extracted `jh<version>` folder into the `c:\JavaHelp\` folder

HTML Help Workshop

Only required for the Content Manager Publishing engine.

A `htmlhelp.zip` package can be retrieved online from SDL upon request. That package contains a tested version of HTML Help Workshop.

Extract the executable in `c:\Program Files (x86)\HTML Help Workshop`.

Antenna House XSL Formatter

Required if you use the Content Manager Publishing engine and the Antenna House XSL Formatter software by Antenna House to render your output.

To allow the proper rendering of non-Western language such as Thai or the East Asian languages, you must have the specialized fonts available. Content Manager expects that all available complex script, right-to-left and East Asian language support are available.

Content Manager is tested with the currently supported Antenna House XSL Formatter (specified in the *Software requirements* list) which can be retrieved online from SDL upon request.

Note: You may use a later version of Antenna House XSL Formatter; check with your SDL customer support representative if you have any questions.

Configuring IIS applicationHost.Config

This part describes which actions should be taken to change the `applicationHost.Config` to allow the definition of website specific settings in the `Web.config` file for Content Manager websites and to set the necessary mimetype definitions for compression.

Before you begin

The steps for configuring IIS and ASP Web services must have been executed, especially the static and dynamic compression feature for IIS needs to be installed.

About this task

The `ApplicationHost.config` file can be found in the folder `%WINDIR%\system32\inetsrv\config`. It is the root file of the configuration system when you are using IIS 7 and above. It includes definitions of all sites, applications, virtual directories and application pools, as well as global defaults for the web server settings. It has definitions for locking-down most IIS sections to the global level, so that by default they cannot be overridden by lower-level `Web.config` files in the hierarchy. To make configuration easier, we will unlock some of these global level settings, so we can define these settings in the `Web.config` file for Content Manager websites.

Procedure

1. Make the necessary changes to allow the definition of website specific settings in the Web.config file for the website.
 - a. Start cmd.exe as Administrator
 - b. Execute the following statements in the cmd window

```
%windir%\system32\inetsrv\appcmd unlock config /section:system.webServer/asp /commit:apphost
%windir%\system32\inetsrv\appcmd unlock config /section:system.webServer/serverRuntime /commit:apphost
%windir%\system32\inetsrv\appcmd unlock config /section:system.webServer/defaultDocument /commit:apphost
%windir%\system32\inetsrv\appcmd unlock config /section:system.webServer/staticContent /commit:apphost
%windir%\system32\inetsrv\appcmd unlock config /section:system.webServer/directoryBrowse /commit:apphost
%windir%\system32\inetsrv\appcmd unlock config /section:system.webServer/handlers /commit:apphost
%windir%\system32\inetsrv\appcmd unlock config /section:system.webServer/urlCompression /commit:apphost
```

2. Set the necessary mimetype definitions for static compression
 - a. Start PowerShell as Administrator
 - b. Execute the following statements in the PowerShell window

```
Set-ExecutionPolicy Unrestricted -Force
Import-Module WebAdministration
# Define the mimetypes for IIS that can be statically compressed
$staticcompression = @(
    @{mimeType='text/*'; enabled='True'},
    @{mimeType='message/*'; enabled='True'},
    @{mimeType='application/x-javascript'; enabled='True'},
    @{mimeType='application/atom+xml'; enabled='True'},
    @{mimeType='application/xaml+xml'; enabled='True'},
    @{mimeType='application/octet-stream'; enabled='True'},
    @{mimeType='*/*'; enabled='False'}
)
# Set the specified static mimetypes in the compression settings
# in applicationHost.config
$filter = 'system.webServer/httpCompression/statictypes'
Set-Webconfiguration -Filter $filter -Value $staticcompression
```

3. Set the necessary mimetype definitions for dynamic compression
 - a. Start PowerShell as Administrator
 - b. Execute the following statements in the PowerShell window

```
Set-ExecutionPolicy Unrestricted -Force
Import-Module WebAdministration
# Define the mimetypes for IIS that can be dynamically compressed
$dynamiccompression = @(
    @{mimeType='text/*'; enabled='True'},
    @{mimeType='message/*'; enabled='True'},
    @{mimeType='application/x-javascript'; enabled='True'},
    @{mimeType='application/soap+xml'; enabled='True'},
    @{mimeType='application/xml'; enabled='True'},
    @{mimeType='application/json'; enabled='True'},

```



```
@{mimeType='application/octet-stream'; enabled='True'},
  @{mimeType='*/*'; enabled='False'}
)
# Set the specified dynamic mimetypes in the compression settings
# in applicationHost.config
$filter = 'system.webServer/httpCompression/dynamicTypes'
Set-Webconfiguration -Filter $filter -Value $dynamiccompression
# Note that compression can be set per web.config file
```

c. Close PowerShell

Preparation Checklist

Use this checklist to make sure that all the necessary pre-installation actions have been properly carried out before installing Content Manager.

Refer to the hardware and software requirements list to ensure that the correct versions are installed before you install Content Manager.

Layer	Type	Requirement	Completed?
Database	Hardware	Check hardware requirements for the database server.	
Database	Software	Check that the version of the database system is supported for this release, including the exact service pack.	
Database	Software	Make sure the Microsoft SQL Server installation is AccentSensitive , CaseInsensitive and Unicode-ready .	
Application/Web	Hardware	Check hardware requirements for the application server.	
Application/Web	Environment	The designated database user (<i>isource</i>) has the required system administrator rights.	
Application/Web	Environment	The designated application/web service account for Content Manager (ISHSTS) is a local administrator and is a domain user when using a commercial STS such as ADFS.	
Application/Web	Environment	The designated app/web user (InfoShare) has the correct regional options set (dd/MM/yyyy).	
Application/Web	Environment	Make sure you do not forcefully unload the user registry as user logoff is enabled (Windows application server).	

Layer	Type	Requirement	Completed?
Application/Web	Software	Check that a valid security certificate is available for the web server application (HTTPS enabling).	
Application/Web	Software	Check that the version of the application system is supported for this release, including the exact service pack.	
Application/Web	Software	Check that Web Services IIS/ASP is installed.	
Application/Web	Software	Check that the Application Role is installed (for Windows Server 2012R2).	
Application/Web	Software	Make sure that a supported version of Microsoft Server .NET Framework is installed.	
Application/Web	Software	Check that the version of the RDBM system (Oracle or Microsoft) is supported for this release.	
Application/Web	Software	If Oracle is used as RDBMs, make sure that the Oracle Client Configuration is configured.	
Application/Web	Software	If publishing to JAVA help files is chosen, check that a supported version of Java Help is installed.	
Application/Web	Software	Check that a supported version of Java is installed.	
Application/Web	Software	If publishing to CHM files is chosen, check that a supported version of HTML Help Workshop is installed.	
Application/Web	Software	If publishing to PDF files is chosen, check that a XSL-FO renderer such as Antenna XSL Formatter is installed.	

Installing and configuring the database server

The Content Manager database can reside on an Microsoft SQL Server or Oracle RDBMs database server.

Your database server must be installed with the approved version of database software before beginning with these procedures.

Note: Oracle setup is more complex than an SQL server setup. This is because the SQL Server installation and configuration is explained using a Windows user interface. If you have the choice and are not an Oracle DBA, we advise that you install on an SQL Server platform.

Microsoft SQL Server

Database setup on a Microsoft server requires configuration of the server and creation of the database.

Configuring Microsoft SQL Server

The database setup is done on the Microsoft SQL server.

First read the pre-installation notes for SQL Server provided in this documentation.

The SQL Server installation has to be an **AccentSensitive, CaseInsensitive, Unicode-ready** installation.

- If you are performing a fresh SQL Server installation, make sure that in the **Database engine Collation** settings, **Accent-sensitive** is selected and Case-sensitive is not selected.
- The typical Content Manager collation is **SQL_Latin1_General_CP1_CI_AS** (not the often mistaken collation **Latin1_General_CI_AS**). Depending on the SQL Server version, the collation **SQL_Latin1_General_CP1_CI_AS** is also displayed as **Dictionary order, caseinsensitive, for use with 1252 Character Set**.
- You can check the collation name by issuing a query in **SQL Server Management Studio** connected to your server.
 - Select **New Query** then enter `select ServerProperty('Collation')`.
 - Select **Execute**.
 - Verify that the result shows an Accent-sensitive (AS), Case-insensitive (CI) collation name.
For more information refer to Collations in the SQL Server help files.

We recommend authentication based on named SQL Server login ID and on Windows accounts.

- Check or modify authentication in **SQL Server Management Studio**, right-click **ServerName**, then click **Properties** and select **Security** on the left pane.
- In the **Server authentication** pane on the right, select **SQL Server and Windows Authentication Mode**.

SQL Server Agent is part of the SQL Server software.

- Check that this Windows Service is set to automatically start upon server reboot. In the **Control Panel** select **System and Security** then **Administrative Tools** then open **Services**.
- Verify that **SQL Server Agent** startup type is **Automatic**.

Creating a database

Create a database for the Content Manager data collection.

Procedure

1. Open **SQL Server Management Studio**.
2. Right-click on **Databases** then click **New Database...**
3. Enter a database name (e.g. `ContentManager`).
4. Click **Options** in the left pane.
5. In the **Collation** field, select: **SQL_Latin1_General_CP1_CI_AS**.
6. Select the appropriate **Recovery model**.
 - **Full**: All transactions are logged. The recommended choice for production databases.
 - **Simple**: A portion of the transactions are logged. A choice for some test or development databases.
 - **Bulk-Logged**: temporary setting used for specific large-scale bulk operations.

Note: The recovery model determines the number of transactions logged for later system recovery. Whereas a **Full** model provides the best security with a higher points-in-time for recovery, in some situations a **Full** model may cause logs to grow beyond system's ability to process them. Check your database documentation for more information.

7. In the **Compatibility** level field:
 - If installing on SQL Server 2016 enter: **SQL Server 2016 (130)**
 - If installing on SQL Server 2017 enter: **SQL Server 2017 (140)**
8. Click **OK**.

Importing data from the SQL dumpfile

Import the sample Content Manager database dump to validate the configuration and for training purposes.

About this task

The backup data you import can come from the same version of SQL server or from a previous version.

Procedure

1. In the SQL Server Management Studio window, under **Databases**, right-click on the database you created.
2. Click **Tasks > Restore > Database**.
3. In the **General** tab of the Restore Database window, select that you want to restore from a **Device**.
 - a. Click the ellipsis button next to the **Device** field.
 - b. Click **Add** in the resulting Specify Backup window.

- c. Locate and select the latest available dump provided on the installation CD in:
 - for SQL server 2016: \Database\Dump\SQLServer2016
 - for SQL server 2017: \Database\Dump\SQLServer2017
- d. Click **OK**.
- e. The **Database** field under **Source** is populated with the name of the database in the backup file.
- f. In the **Database** field under **Destination**, select the name of the database you created (e.g. `ContentManager`). This is the database that is to be populated with the data from the backup/dump file.

Note: Make sure to select this after selecting the source otherwise it can default to another database name.

4. In the **Files** tab of the **Restore Database** Window:
 - a. For the **Rows Data** select the data file path of the database you created (e.g. `C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\ContentManager.mdf`).
 - b. For the **Log** select the log file path of the database you created (e.g. `C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\ContentManager_log.ldf`).
5. Under the **Options** tab, select **Overwrite the existing database**.
6. Click **OK**. The database is restored.
7. After restoring the database, use **SQL Server Management Studio** to:
 - a. Open the **Properties** window,
 - b. Go to the **Files** tab,
 - c. Check and adapt (if necessary) the logical name.

File type	Logical Name
Rows Data	Set Logical Name to <dbname> (e.g. <code>ContentManager</code>)
Log	Set Logical Name to <dbname>_Log (e.g. <code>ContentManager_Log</code>)

- d. Check the recovery model and verify that **Full** is selected for the **Recovery model**.

Removing the database user and schema

To ensure successful creation of a new database user and schema, delete the user that was created when importing the sample data, as well as the schema of the same name if one exists.

About this task

A database user in SQL Server exists on two levels, as an account on the SQL Server level and as an account on your database. Depending on the kind of initial database setup dump you received, you could have problems creating your new database user. Therefore, you should delete the Content Manager database designated user (by default named `isource`) and schema if one is present.

Note: The user listed within the created database part is to be removed and not the general SQL Server part listed under Security > Logins.

Procedure

1. In the SQL Server Management Studio window, locate and open the tree under the newly created database.
2. Open **Security > Schemas**.
3. Right-click on **isource** if it appears in the list, then click **Delete**.
A Delete Object window displays.

Note: The **isource** user may not exist under **Schemas**. If it does not exist, skip this and the next step; continue to the step to open **Security > Users**.

4. Click **OK** to confirm the removal.
5. Open **Security > Users**.
6. Right-click on **isource** then click **Delete**.
A Delete Object window displays.
7. Click **OK** to confirm the removal.

Creating a new database user and schema

Add a new user to connect to the newly created database.

Procedure

1. On the database server, open the **SQL Server Management Studio**.
2. In the left pane under the server name open **Security**.
3. Right-click on **Logins** then select **New Login...**
A Login - New window displays.
4. In the **Login name** field, enter an user name (e.g. `isource`).
5. **SQL Server Authentication** should be selected. Enter a **Password** (e.g. `isource`) and **Confirm password** for SQL Server Authentication.

Note: SDL is not able to assist you if you do not know the password so it is advised to store the password in a secure place.

6. Depending on your local password policy, you can enforce password policy and password expiration.

Note: Keep in mind to change the connect string whenever you change the password of the database user!

7. Use the drop down list to select the **Default database**; select your newly created database.
No other changes are required for the General information.
8. Click **Server Roles** in the left pane.
9. Select (check the boxes next to) **public** and **sysadmin** in the right pane.
This allows the Content Manager DBUpgradeTool (DBUT) to fully execute all necessary tasks to update your database with new releases.

Notice: If you want to reduce the server roles for everyday work, read "Optionally minimize the database user's roles and permissions " on page 45.

10. Click **User Mapping** in the left pane.
11. Select (check the boxes next to) the newly created database in the upper right pane.
12. In the upper right pane, in the **Default Schema** field for your database, enter **dbo**.
13. In the bottom pane, select (check the boxes next to) **db_owner** and **public**.

Notice: If you want to reduce the permissions for day to day usage, read "Optionally minimize the database user's roles and permissions " on page 45.

14. In the Login - New window, click **Status** in the left pane.
15. Verify that **Grant** is selected for **Permission to connect to the database engine** and that **Enabled** is selected for **Login**.
16. Click **OK**.
17. Click **File > Exit**.

Optionally minimize the database user's roles and permissions

Describes how to optionally reduce the roles and permissions of the database user for everyday usage.

About this task

Optional execution to minimize the permissions for normal operations outside of the upgrade time frame.

Note: The following steps must be executed by a user who is administrator on the database server.

Procedure

1. On the database server, open **SQL Server Management Studio**.
2. In the left pane under the server name, open **Security > Logins**.
3. Right-click the database user (e.g **isource**) and select **Properties**.
4. Revoke the server role **sysadmin**.

The server role **sysadmin** provides the ability to perform any activity on the server. Content Manager DBUpgradeTool (DBUT) requires this server role to create the standard database job and add extra (error) messages, for example. In order to allow DBUT to fully execute all necessary tasks during an upgrade, we advice to reinstate the **sysadmin** server role for the duration of that task. However, during everyday usage you can revoke **sysadmin** using the following steps:

- a. Select **Server Roles** in the left pane.
- b. Deselect **sysadmin** in the right pane. Make sure that **public** is still selected.
5. Revoke database role **db_owner**.

Note: Revoking the database role **db_owner** should be done only after revoking the server role **sysadmin**.

- a. Select **User Mapping** in the left pane.
- b. Select the correct database in the upper right pane.
- c. In the bottom pane, un-check the box next to **db_owner**. Make sure that **public** is still selected.
6. Select **OK**.
7. After revoking the database role **db_owner**, add the minimal required permissions.

In order for the Content Manager application to work without issues, the database user needs the following permissions:

Name	Description	Usage
SELECT	Retrieve information/ records from the database	Everywhere
INSERT	Insert new records into the database	Everywhere
UPDATE	Update records in the database	Everywhere
DELETE	Delete records from the database	Everywhere

Name	Description	Usage
EXECUTE	Execute a stored procedure in the database	<p>Stored procedures are used everywhere to:</p> <ul style="list-style-type: none"> • Create new objects (maps, topics, publications, users, LOV values...) and get the newly created IDentity back. • Delete objects • Cleanup left-overs during a nightly maintenance job • ...
CREATE TABLE	Create a new table	<p>DBUpgradeTool: during the upgrade of the database from one version to another version, we might introduce new tables.</p> <p>Full-text search: out-of-the-box the tables for the full-text search are created when you start the Crawler for that installation for the first time.</p>
CREATE VIEW	Create a new view	<p>DBUpgradeTool: during the upgrade of the database from one version to another version, we are dropping and recreating views.</p>
CREATE FUNCTION	Create a new function	<p>DBUpgradeTool: during the upgrade of the database from one version to another version, we are dropping and recreating functions.</p>
CREATE PROCEDURE	Create a new stored procedure	<p>DBUpgradeTool: During the upgrade of the database from one version to another version, we are dropping and recreating stored procedures.</p>

Name	Description	Usage
REFERENCES	Create foreign keys between two tables	DBUpgradeTool: During the upgrade of the database from one version to another version, we might introduce new tables and add new foreign keys between those new tables and the existing tables. Full-text search: out-of-the-box the tables for the full-text search are created when you start the Crawler for that installation for the first time, and we are also adding new foreign keys between those new tables and the existing tables.
ALTER ANY SCHEMA	Create, alter and delete objects in any schema	DBUpgradeTool: during the upgrade of the database from one version to another version, we are creating/altering/deleting tables, views, functions, stored procedures... in the schema <code>dbo</code> . Full-text search: we need to create the tables in the schema <code>dbo</code> for the full-text search.

You can grant the necessary permissions to the database user using the following steps:

- In **SQL Server Management Studio** open the file corresponding to your SQL Server version:
 - for SQL server 2016: `c:\InfoShare\App<projectsuffix>\Database\Common\SQLServer2016\Tools\GrantPermissionsToDBUser.sql`
 - for SQL server 2017: `c:\InfoShare\App<projectsuffix>\Database\Common\SQLServer2017\Tools\GrantPermissionsToDBUser.sql`
- If your database user is not `isource`, change `isource` to the correct database user.
- Run the script as an administrator.
- Connect with the database user (e.g. `isource`) and run the following query to check that the database user has the required permissions.

```
SELECT * FROM fn_my_permissions(null, 'DATABASE')
```

Oracle RDBMS

The installation makes use of the Oracle Database Configuration Assistant (DBCA) and command line programs to create and set up the database. This allows for anyone with a mixture of Windows and UNIX knowledge to be able to set up an environment on any Oracle hosting machine.

The configuration instructions refer to a Windows environment when noting system variables and file paths.

These instructions guide a knowledgeable person through the configuration so that no important steps are forgotten. However, it does not provide all explanations, or options pertaining to each step.

Note: The default database name is **ISH**.

Note: In case of issue, be sure to check the troubleshooting section dedicated to the database installation.

Configuring Oracle RDBMS

Configuring tasks are required prior to database creation.

Oracle database configuration requirements

The users who can configure Oracle must have permissions and access as required and be familiar with Oracle and Microsoft environments.

The provided configuration instructions are written for administrators who have knowledge of the Oracle and Microsoft environments.

Make sure that you satisfy the following requirements before you begin:

- Having a DBA role is required for a database migration.
- Reboot after Oracle installation for making sure that all Oracle environment settings are available to you.

Also note:

- All executed actions should be done in the same command window for making sure that shell specific settings, such as `ORACLE_SID` or `ORACLE_HOME`, are available.
- All paths are examples only. Paths are system specific, so make sure that all file paths are valid and contain the correct file(s), and beware of read-only flags on files.
- The default database name is **ISH** and is used in examples in the procedures.

Copy template files

The Content Manager database is created using the Oracle Database Configuration Assistant. When it is installed with the Assistant, Content Manager uses a template with SPFile.

To prepare your environment for the Oracle configuration, you must first copy the template file to your server. The version mentioned below have been quality tested with this version of Content Manager.

Oracle 12.1

From:	\Database\Dump\Oracle\Oracle121.Admin\DBCATemplates\SDL-Trisoft.InfoShare-Database-Template.dbt
To:	C:\Oracle\product\12.1.0\dbhome_1\assistants\dbca\templates on the server

Oracle 12.2

From:	\Database\Dump\Oracle\Oracle122.Admin\DBCATemplates\SDL-Trisoft.InfoShare-Database-Template.dbt
To:	C:\Oracle\product\12.2.0\dbhome_1\assistants\dbca\templates on the server

Oracle 19

From:	\Database\Dump\Oracle\Oracle193.Admin\SDL-Trisoft.InfoShare-Database-Template.dbt
To:	<oracle_home>\assistants\dbca\templates on the server

Activating the Listener service for Oracle

You must start the Oracle listener service so incoming client connection requests are received and sent to the database server.

About this task

There are two possibilities for activating the Listener service for Oracle. Either a general listener is available and you then select this one, or you need to create a specific listener for your database and then you activate that one. Here is the procedure for creating a new listener and activating it.

Procedure

1. Start the Net Configuration Assistant. This Assistant is provided by Oracle.
2. Select the "Listener Configuration" radio button on the opening window, then click "Next".
3. Select the "Add" radio button on the following window, then click "Next".
4. Type in a name for the new listener, then click "Next".
5. Choose "TCP" as selected protocol in the list, then click "Next".
6. Select the "Use the standard port of 1521" radio button on the following window, then click "Next". You may specify another port instead if you know what you're doing.
7. Complete the creation process by clicking "Next" again.

Creating the Oracle database with a template

You must create the Oracle database instance for the Content Manager Repository. This is the place where the data is stored.

Creating the Oracle 12.1 database

The procedure for Oracle 12.1.

Before you begin

This procedure requires that you are part of the local Windows administration group as well as the `ORA_DBA` group.

About this task

The Oracle database is created using the Database Configuration Assistant (DCA). The creation steps are version dependent and can be performed with the help of a template.

Procedure

1. Create the database folder, **C:\oracle\OraData\ISH**.
The directory is required and not created by Oracle. Make sure that all paths exist.
2. Go to `CD_Package\Database\Dump\Oracle\Oracle121.Admin\DBCATemplates` where `CD_Package` is the root folder of the CD package.
3. Open the `ReadMe.txt`, and copy the template `SDL-Trisoft.InfoShare-Database-Template.dbt` to the location specified in the `ReadMe.txt` file.
4. Start the Database Configuration Assistant (DCA). This Assistant is provided by Oracle.
5. On the **Database Operation** page, select **Create Database**, then **Next**.
6. On the **Creation Mode** page, select **Advanced Mode**, then **Next**.
7. On the **Database Template** page, select the `SDL-Trisoft.InfoShare-Database-Template` template, then select **Next**.
8. On the **Database Identification** page, fill in the **Global Database Name** field with the database name, then select **Next**.
9. On the **Management Options** page, select **Configure Enterprise Manager (EM) Database Express**, and specify the port in the field below, then select **Next**.

Note: Make sure that the specified port is unique.

10. On the **Database Credentials** page, fill in the required fields (passwords), then select **Next**.
11. On the **Network Configuration** page, select the Listener that was previously created for this database (refer to the chapter dedicated to the activation of the Listener service), then select **Next**.
12. Leave the **Storage Location** page as is and select **Next**.
13. On the **Database Options** page, leave the **Database Components** page as is and select **Next**.
14. On the **Initialization Parameters** page, make sure that the **Use Automatic Memory**

Management box is checked and select **Next**.

15. On the **Creation Options** page, select **Create the database**, then **Next**.

16. On the **Summary** page, select **Finish**.

Creating the Oracle 12.2 database

The procedure for Oracle 12.2.

Before you begin

This procedure requires that you are part of the local Windows administration group as well as the ORA_DBA group.

About this task

The Oracle database is created using the Database Configuration Assistant (DCA). The creation steps are version dependent and can be performed with the help of a template.

Procedure

1. Go to `CD_Package\Database\Dump\Oracle\Oracle122.Admin\DBCATemplates` where `CD_Package` is the root folder of the CD package.
2. Open the `ReadMe.txt`, and copy the template `SDL-Trisoft.InfoShare-Database-Template.dbt` to the location specified in the `ReadMe.txt` file.
3. Start the Database Configuration Assistant (DCA). This Assistant is provided by Oracle.
4. On the **Database Operation** page, select **Create Database**, then **Next**.
5. On the **Creation Mode** page, select **Advanced Mode**, then **Next**.
6. On the **Database Template** page, select `SDL Trisoft InfoShare Database Template (12.2)`, then **Next**.
7. On the **Database Identification** page, fill in the **Global Database Name** field with the database name, then select **Next**.
8. On the **Storage Option** page:
 - a. Select **Use following for the database storage attributes**.
 - b. In the **Database files storage types** list, select **File System**.
 - c. Fill in the **Database files location** field with the path to the database.
 - d. Then select **Next**.
9. Leave the **Fast Recovery Option** page as is, select **Next**.
10. On the **Network Configuration** page, select the Listener that was previously created for this database (refer to the chapter dedicated to the activation of the Listener service), then select **Next**.
11. Leave the **Data Vault Options** page as is, select **Next**.
12. On the **Configuration Options** page, **Memory** tab, select **Use Automatic Shared Memory Management**. You may want to adapt values to your needs.
13. On the **Configuration Options** page, **Sizing** tab, you may want to increase the processes value, depending on the size of your system. Each current database consumer (end users, services, background tasks...) use a process, so you need to set a sufficient amount of them if you want all the consumers to be able to use the database in parallel.

14. Leave the rest of the **Configuration Options** page as is and select **Next**.
15. Leave the Management Options page as is, select **Next**.

Note: Make sure that the specified port is unique.

16. On the **User Credentials** page, fill in the password fields, then select **Next**.
17. On the **Creation Option** page, select **Create database**, then **Next**.
18. On the **Summary** page, select **Finish**.

Creating the Oracle 19 database

The procedure for Oracle 19.

Before you begin

This procedure requires that you are part of the local Windows administration group as well as the ORA_DBA group.

About this task

The Oracle database is created using the Database Configuration Assistant (DCA). The creation steps are version dependent and can be performed with the help of a template.

Procedure

1. Go to C:\InfoShare\App\Database\Dump\Oracle\Oracle193.Admin.
2. Copy the template `SDL-Trisoft.InfoShare-Database-Template.dbt` to a location of your choosing. For example `<oracle_home>\assistants\dbca\templates`.
3. Start the Database Configuration Assistant (DCA). This Assistant is provided by Oracle.
4. On the **Database Operation** page, select **Create Database**, then **Next**.
5. On the **Creation Mode** page, select **Advanced Mode**, then **Next**.
6. On the **Database Template** page, select `SDL Trisoft InfoShare Database Template (19)`, then **Next**.
7. On the **Database Identification** page, fill in the **Global Database Name** field with the database name, then select **Next**.
8. On the **Storage Option** page:
 - a. Select **Use following for the database storage attributes**.
 - b. In the **Database files storage types** list, select **File System**.
 - c. Fill in the **Database files location** field with the path to the database.
 - d. Then select **Next**.
9. Leave the **Fast Recovery Option** page as is, select **Next**.
10. On the **Network Configuration** page, select the Listener that was previously created for this database (refer to the chapter dedicated to the activation of the Listener service), then select **Next**.
11. Leave the **Data Vault Options** page as is, select **Next**.
12. On the **Configuration Options** page, **Memory** tab, select **Use Automatic Shared**

Memory Management. You may want to adapt values to your needs.

13. On the **Configuration Options** page, **Sizing** tab, you may want to increase the processes value, depending on the size of your system. Each current database consumer (end users, services, background tasks...) use a process, so you need to set a sufficient amount of them if you want all the consumers to be able to use the database in parallel.
14. Leave the rest of the **Configuration Options** page as is and select **Next**.
15. Leave the Management Options page as is, select **Next**.

Note: Make sure that the specified port is unique.

16. On the **User Credentials** page, fill in the password fields, then select **Next**.
17. On the **Creation Option** page, select **Create database**, then **Next**.
18. On the **Summary** page, select **Finish**.

Creating the designated ISOURCE database user

You must create the ISOURCE designated database user for the new database.

Procedure

1. If the folder `c:\oracle\admin\ISH\create` on the server does not exist, create it now.
2. Copy `CD_Package\Database\Common\Oracle\Create\isrcuser.i` (where *CD_Package* is the root folder of the CD package) to the folder `c:\oracle\admin\ISH\create` and make sure the file is writable.

The examples are specific for Windows. Be sure to modify the paths, commands and username/passwords to match your environment.

3. Open `c:\oracle\admin\ISH\create\isrcuser.i` in Notepad and if needed adapt the username and password of the designated user to match your environment.
4. Open a command prompt.
5. Set ORACLE_SID: `ORACLE_SID=ISH`
6. Set ORACLE_HOME:
 - Oracle 12.1: `ORACLE_HOME=c:\oracle\product\12.1.0\dbhome_1`
 - Oracle 12.2: `ORACLE_HOME=c:\oracle\product\12.2.0\dbhome_1`
 - Oracle 19: the location where you copied the application.

Note: All commands must be entered in the same window, ensuring that every environment variable set is available throughout the process. The next steps presume that you use the same shell with these variables set correctly.

7. Start SQLPlus: `sqlplus SYS AS SYSDBA`
8. At a command prompt where the variables for ORACLE_SID and ORACLE_HOME are set, type:

```
SPOOL C:\oracle\admin\ISH\create\dbadmin2.log
```



```
CONNECT SYS/CHANGE_ON_INSTALL AS SYSDBA
@C:\oracle\admin\ISH\create\isrcuser.i
CONNECT ISOURCE/isource
@?/RDBMS/ADMIN/catdbsyn.sql
SPOOL OFF;
```

Note: If the folder `c:\oracle\admin\ISH\create` is missing the error SP2-0606: Cannot create SPOOL file `c:\oracle\admin\ISH\create\dbadmin2.log`, is displayed when issuing the command below.

Importing the data with Oracle

Import the sample data either for validating the configuration or for training purposes. This action follows different paths depending on the Oracle version you are using.

About this task

The use of *Data Pump Import* (`impdp`) is recommended. First you grant the `ISOURCE` user write permissions, then you proceed to the import.

Procedure

1. If the folder `c:\oracle\admin\ISH\dpdump` on the server does not exist, create it now.
2. Copy `CD_Package\Database\Dump\Oracle\impdp\impdp.par` (where `CD_Package` is the root folder of the CD package) to the folder `c:\oracle\admin\ISH\dpdump` and make sure the file is writable.

The examples are specific for Windows. Be sure to modify the paths, commands and username/passwords to match your environment.

3. Open `c:\oracle\admin\ISH\dpdump\impdp.par` in Notepad and adapt the name of the export file (`DUMPFILE` parameter) and, if needed, the designated schema owner (`SCHEMAS` parameter).
4. Open a command prompt.
5. Set `ORACLE_SID: ORACLE_SID=ISH`
6. Set `ORACLE_HOME:`
 - Oracle 12.1: `ORACLE_HOME=c:\oracle\product\12.1.0\dbhome_1`
 - Oracle 12.2: `ORACLE_HOME=c:\oracle\product\12.2.0\dbhome_1`
 - Oracle 19: the location where you copied the application.
7. Start SQLPlus: `sqlplus SYS AS SYSDBA`
8. Make sure the `ISOURCE` user has read and write access to the folder:

```
GRANT read, write ON DIRECTORY data_pump_dir TO isource;
```

9. Make sure the file from the Data Pump Export is copied to the `DATA_PUMP_DIR`:

```
SELECT directory_path FROM dba_directories WHERE directory_name =
'DATA_PUMP_DIR';
```

10. Exit SQLPlus, so you are back at the command prompt.
11. For the import, execute the following command:

```
impdp isource parfile="C:\oracle\admin\ISH\dpdump\impdp.par"
```

Validating the database

The newly imported Oracle database needs some packages, triggers and more to be (re-)compiled for the database to be valid.

Before you begin

ORACLE_SID and ORACLE_HOME variables are set correctly (this is normally done during the ISOURCE user creation).

Procedure

1. Start SQLPLUS /NOLOG from a shell where the ORACLE_SID and ORACLE_HOME variables are set correctly. At the command prompt, type:

```
SQLPLUS /NOLOG
```

2. Enter the following statements to validate the database. Do not use a script file.

```
CONNECT SYS/CHANGE_ON_INSTALL AS SYSDBA  
@?/rdbms/admin/utlrb;
```

All objects in the database should be valid.

Editing the tnsnames.ora database connection file

The Oracle `tnsnames.ora` file must be modified on the Oracle database server and on systems that communicate with the Oracle database server. This file defines the information for a connection to the database server and to the database instance for the Content Manager repository.

About this task

If the Oracle database server and client software was installed on the same system, you must edit the `tnsnames.ora` file under each instance of `oracle_home`.

Procedure

1. Login to the server as an administrator user.
2. Open the `oracle_home\network\admin\tnsnames.ora` file for editing.
If the file does not exist create an empty text document named `tnsnames.ora` in the directory above.
3. Add the following to the file. Make sure that it is left-aligned (that is, no leading whitespace on the first line)

```

net_service_name =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)
      (HOST = hostname)
      (PORT = 1521))
  )
(CONNECT_DATA =
  (SERVICE_NAME = service_name)
)
)

```

where:

- *net_service_name* is an alias that is used for a connect descriptor. For example:

```
ISH.WORLD
```

- *hostname* is the IP address or name of the database server. For example:

```
(HOST = devserver01)
```

or

```
(HOST = 127.0.0.1)
```

- *SERVICE_NAME* is a combination of the *db_name* and *db_domain* values in the `C:\oracle\admin\ISH\pfile\PFILF\initISH.ora` file. For example:

```
SERVICE_NAME = ISH.ORASERVER.DOMAIN.NAME
```

where ISH is the *db_name* value and *ORASERVER.DOMAIN.NAME* is the *db_domain* value in the `initISH.ora` file.

4. Save and close the file.

Analyzing the database

After the import, you need to run a script that will create statistics used by the queries.

Before you begin

ORACLE_SID and ORACLE_HOME variables are set correctly (this is normally done during the ISOURCE user creation).

Procedure

1. At a command prompt where the variables for ORACLE_SID and ORACLE_HOME are set, type:

```

SQLPLUS /NOLOG
CONNECT ISOURCE/isource

```

2. Execute the `FullAnalyze.sql` script located on the CD:

- `CD-Package\Database\Common\Oracle\Tools\FullAnalyze.sql`

Installing the Content Manager server

You must install and configure the application and web server to use the Content Manager application, allowing you to connect to the repository.

Most of the Content Manager server installation process is automated. At the end of the process, some options must be set manually.

Be sure to check the installation requirements before initiating the application server installation.

Configuring database connection strings

Use the Microsoft Universal Data Link tool to create and test a connection string.

An SQL Server oriented environment makes use of **Microsoft OLE DB Driver for SQL Server** (MSOLEDBSQL).

An Oracle oriented environment needs to make use of **Oracle Provider for OLE DB**. The introduction of Unicode requires the use of this provider together with the **Enhanced Oracle Services for Microsoft Transaction Server**.

Creating and testing Oracle RDBMs

To create and test the Oracle RDBM, you must configure the `tnsnames.ora` file so that a connection can be made.

Follow the steps for editing the `tnsnames.ora` file before creating and testing the connection.

Editing the `tnsnames.ora` database connection file

The Oracle `tnsnames.ora` file must be modified on the Oracle database server and on systems that communicate with the Oracle database server. This file defines the information for a connection to the database server and to the database instance for the Content Manager repository.

About this task

If the Oracle database server and client software was installed on the same system, you must edit the `tnsnames.ora` file under each instance of `oracle_home`.

Procedure

1. Login to the server as an administrator user.
2. Open the `oracle_home\network\admin\tnsnames.ora` file for editing.
If the file does not exist create an empty text document named `tnsnames.ora` in the directory above.
3. Add the following to the file. Make sure that it is left-aligned (that is, no leading whitespace on the first line)

```
net_service_name =
(DESCRIPTION =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP)
      (HOST = hostname)
      (PORT = 1521))
  )
(CONNECT_DATA =
  (SERVICE_NAME = service_name)
)
```

where:

- *net_service_name* is an alias that is used for a connect descriptor. For example:

```
ISH.WORLD
```

- *hostname* is the IP address or name of the database server. For example:

```
(HOST = devserver01)
```

or

```
(HOST = 127.0.0.1)
```

- *SERVICE_NAME* is a combination of the *db_name* and *db_domain* values in the `C:\oracle\admin\ISH\pfile\PFIL\initISH.ora` file. For example:

```
SERVICE_NAME = ISH.ORASERVER.DOMAIN.NAME
```

where *ISH* is the *db_name* value and *ORASERVER.DOMAIN.NAME* is the *db_domain* value in the `initISH.ora` file.

4. Save and close the file.

Creating and testing the connection for Oracle RDBMs

An Oracle oriented environment makes use of Oracle Provider for OLE DB.

Before you begin

You must have a valid `tnsnames.ora` file in place to create and test the connection. If this has not been done, refer to the procedure for editing the `tnsnames.ora` database connection file.

Procedure

1. Create a new text document in your installation directory (`C:\InfoShare`) and name it `connection.udl`.

Note:

- Be sure that the file extension is `.udl`. If required, change your Windows Explorer settings to recognize the file extension. You have created a Universal Data Link file, which has a wizard-like program associated to create connection strings.
- Ensure that the filename was not appended with a `.txt` filename extension. If file name extensions are not visible, modify the Windows **Tools > Folder Options > View**, and check that **Hide extensions for known file types** is not selected.

2. Start the associated program by executing the command:

```
%WINDIR%\SysWOW64\cmd.exe /c START C:\InfoShare\connection.udl
```

The command window launched from SysWOW64 ensures that the 32-bit database provider in the wizard screen is found.

3. Click the **Provider** tab, and select **Oracle Provider for OLE DB**.
4. Click **Next**.
5. Under the **Connection** tab, in the first field select or enter the data source. For example: `ISH.WORLD`.
The data source is the `net_service_name` entry in the `oracle_home\network\admin\tnsnames.ora` file.
6. In the second field, select the **Use a specific username and password** checkbox.
 - a. In the **User name** field, enter `isource`.
 - b. In the **Password** field, enter the password for the `isource` user.
The default password is `isource`. If you did not use the default password, be sure to enter the password used when you created the new user. The password was specified for the `isource` user when configuring the Oracle server.
 - c. Select the **Allow saving password** checkbox.
7. Test the connection by clicking **Test Connection**.
If the connection is valid, a message is displayed to notify that the connection is working correctly.
8. Click **OK** to confirm.
This saves the password as plain text in the UDL file. If the connect string does not contain the password variable, no valid connections can be made with this connection string.

Creating and testing the connection for Microsoft SQL Server

An SQL Server oriented environment makes use of the **Microsoft OLE DB Driver for SQL Server**.

Procedure

1. Create a new text document in your installation directory (c:\InfoShare) and name it `connection.udl`.
 Note:
 - Be sure that the file extension is `.udl`. If required, change your Windows Explorer settings to recognize the file extension. You have created a Universal Data Link file, which has a wizard-like program associated to create connection strings.
 - Ensure that the filename was not appended with a `.txt` file extension. If file extensions are not visible, modify the Windows **Tools > Folder Options > View**, and check that **Hide extensions for known file types** is not selected.
2. Start the associated program from Windows Explorer by double-clicking `c:\InfoShare\connection.udl`.
3. Click the **Provider** tab, and select **Microsoft OLE DB Driver for SQL Server**.
4. Click **Next**.
5. Under the **Connection** tab, in the first field select or enter the SQL database server name.
6. In the second field, select the **Use a specific username and password** checkbox.
 - a. In the **User name** field, enter `isource`.
 - b. In the **Password** field, enter the password for the isource user.
 The default password is `isource`. If you did not use the default password, be sure to enter the password used when you created the new user. The password was specified for the isource user when configuring the Microsoft SQL server.
 - c. Select the **Allow saving password** checkbox.
7. In the third field, select the **Select the database on the server** checkbox, and specify the database name.
 This is the name specified when you created the database. The database name was specified when configuring Microsoft SQL server.
8. Test the connection by clicking **Test Connection**.
 If the connection is valid, a message is displayed to notify that the connection is working correctly.
9. Click **OK** to confirm.
 This saves the password as plain text in the UDL file. If the connect string does not contain the password variable, no valid connections can be made with this connection string.

Results

When using this connection string in `inputparameter.xml`, remove the last two keywords: Initial File Name and Server SPN.

inputparameters.xml

The `inputparameters.xml` file stores key parameters that are used by the Content Manager installer. This file must accurately reflect your environment for the install tool to work correctly. Only the mandatory parameters need to be considered in the vast majority of installations. The optional parameters cover rare and advanced cases.

Overview

Note: Before modifying the `inputparameters.xml` file, you need to

- Obtain and install the certificate.
- Configure HTTPS bindings.

Each parameter in this configuration file has the following syntax:

```
<param name="parameter">
  <currentvalue>value</currentvalue>
  <defaultvalue>example_value</defaultvalue>
  <description>description_of_how_used</description>
  <validate>if_validated</validate>
</param>
```

The XML elements perform the following functions:

<currentvalue>

Contains the value that is used by the Content Manager installer.

<defaultvalue>

Contains a predefined value as an example. Do not use the predefined value as a default value; its only purpose is to serve as an example.

<description>

Contains details describing how the current value of the parameter is used.

<validate>

Defines whether the value of the parameter is validated or not. If the element is empty, no validation is performed. The `<validate>` values are provided, and they should not be modified.

Mandatory input parameters

This section lists and describes the main input parameters contained in the `inputparameters.xml` file, the ones you need to set for any installation. Some of these input parameters are mandatory: you need to set them for the installation to work correctly.

osuser

The user name for the designated operating system account.

ospassword

The password for the designated operating system account. Set the password so that it never expires.

connectstring

The connection string for the instance of the database application.

Note: To obtain the required `connectstring` parameter:

- In a text editor, for example Notepad, open the `connection.udl` file you created in the installation directory (typically, `c:\InfoShare`).
- Browse to the line beginning with `Provider=`.
For Oracle:

```
Provider=OraOLEDB.Oracle.1;Password=isource-password;Persist Security
Info=True;User ID=isource;Data Source=data_source_name
```

For MSSQL:

```
Provider=SQLOLEDB.1;Password=isource-password;Persist Security
Info=True;User ID=isource;Initial Catalog=database;Data Source=
server-name
```

- Copy the line and paste it in the `inputparameters.xml` file to specify the `connectstring` parameter.
-

apppath

The root directory for the Content Manager installation.

By default, this is set to `c:\InfoShare`.

ps_java_home

The path to the `JAVA HOME` directory.

serviceusername

Specify the user name for the Content Manager services.

servicepassword

Specify the password matching `serviceusername`'s value.

Optional input parameters

This section lists and describes the optional input parameters contained in the `inputparameters.xml` file. The value of several optional parameters are calculated by Content Manager, others have a default value. These parameters should be changed only by an expert of Content Manager.

Optional parameters

Note: When you provide a value to a parameter that is calculated by default, the parameter is set to your value and is no longer calculated.

Name	Description	Remarks
projectsuffix	A suffix that specifies the particular instance of Content Manager, if you are installing multiple Content Manager instances on a server.	By default: no value
webpath	The root directory for the Web site.	By default: <apppath value> (calculated)
datapath	The directory containing the data directory. This directory stores all data exported from Content Manager	By default: <apppath value> (calculated)
workspacepath	The temporary directory where installation files are stored before installation.	By default: <apppath value>_workspace (calculated)
infoshareauthorwebappname	The name of the web client application.	By default: ISHCM + <projectsuffix value>
infosharewswebappname	The name of the web services application.	By default: ISHWS + <projectsuffix value>
infosharestswebappname	The name of the website with the Content Manager Secure Token Service (STS).	By default: ISHSTS + <projectsuffix value>
websitename	The name of the web site where all virtual directories are created.	By default: Default Web Site
baseurl	The base URL that is used to access the Content Manager web client.	By default: extracted from the Common Name of the certificate specified for HTTPS binding on IIS (calculated).
localservicehostname	The hostname for the local address: The host name with which communication within the Content Manager box takes place.	By default: the NetBIOS name of this local computer (calculated)

Name	Description	Remarks
ps_fo_processor	The fully qualified file name of the XSL-FO processor, for example <code>C:\Program Files\AntennaHouse\AHFormatterV6\AHFCmd.exe</code> .	By default: the highest installed version from <code>%ProgramFiles%</code> (calculated).
ps_htmlhelp_processor	The fully qualified file name of the HTML Help processor.	By default: <code>C:\Program Files (x86)\HTML Help Workshop\hhc.exe</code> Note: Do not use environment variables or quotation marks.
ps_java_jvmdll	The full path to <code>jvm.dll</code> inside the <code>openJDK JAVA_HOME</code> folder, used by the TrisoftSolrLucene service.	By default: <code><ps_java_home value>\bin\server\jvm.dll</code> Note: do not use environment variables or quotation marks.
ps_javaahelp_home	The full path to a <code>JavaHelp JHHOME</code> folder, used when you want to publish with the JavaHelp output type.	By default: <code>C:\javaahelp\jh2.0</code> Note: do not use environment variables or quotation marks.
ps_webworks_automap_application	The fully qualified path and filename of WebWorks .	By default: No value Note: do not use environment variables or quotation marks.
solrlucene_service_port	The port the SolrLucene service uses. This port must be unique for each Content Manager instance installed on a server.	By default: 8078
solrlucene_stop_port	The port that is used to stop the SolrLucene service. This port must be unique for each Content Manager instance installed on a server.	By default: 8077
basehostname	The hostname part of the base URL, calculated using <i>baseurl</i> as input stripping the protocol HTTP/HTTPS (e.g. <code>TRIDT06.tribe.trisoft.be</code>)	By default: from <i>baseurl</i> (calculated)

Name	Description	Remarks
infosharestswindowsauthenticationenabled	Whether or not the infosharests web site enables IIS windows authentication.	By default: False
servicecertificatethumbprint	The thumbprint of the service certificate (can be a re-purposed SSL certificate). All the linked web/app servers in a farm must offer the same trusted certificate.	By default: from HTTPS binding of <code>websitename</code>
servicecertificatevalidationmode	The validation mode of the service certificate (<code>servicecertificatethumbprint</code>).	By default: ChainTrust
servicecertificatesubjectname	The subject name of an already installed certificate for unique service identification (can be a re-purposed SSL certificate). All the linked web/app servers in a farm must offer the same trusted certificate.	By default: from HTTPS binding of <code>websitename</code>
fontoreview_service_port	The port used by the FontoReview service. This port must be unique for each Content Manager instance installed on a server.	By default: 8001

Executing the InstallTool

Use the Content Manager InstallTool to install and merge all standard and customer specific project files.

Before you begin

In the context of a Content Manager install or uninstall operation, before you run InstallTool you need to make sure the Microsoft Distributed Transaction Coordinator MSDTC service is running.

Procedure

1. Login to your Windows system as a Content Manager user with the Administrator user role.
2. In Windows Explorer, go to
`C:\IShCD\yyyyymmdd.CD.InfoShare<version_num>\ProjectName.IT__InstallTool`
3. Locate and double-click on **InstallTool.exe**.
4. Select the **Install** option by entering the number **2**.
5. Hit enter to respond to all questions; the default options should be sufficient.

All standard and customer specific project files are merged and installed. All required services are up and running (the Crawler, SolrLucene, IISAdmin, W3SVC).

Identifying reverse proxies

Various reverse proxy servers can be used in combination with Content Manager. Using reverse proxy servers may result in connection problems to the Content Manager repository. You can check the BASEURL to verify that it is not causing a problem in Internet Explorer.

When you identify reverse proxy servers, verify that the following URLs do not cause any problems in Internet Explorer:

- BASEURL/ISHWS/Application.asmx?wsdl
- BASEURL/ISHWS/Application.asmx?disco

The BASEURL is specified in the `inputparameters.xml` file used by the Content Manager installer.

The BASEURL must use the `https` schema. It must also reference a hostname that is valid for the SSL certificate.

For example if the server has a SSL certificate configured with `CN=example.com` then the BASEURL must be `https://example.com`.

Example:

```
<param name="baseurl">
<currentvalue>https://example.com</currentvalue>
<defaultvalue>https://example.com</defaultvalue>
<validate/>
</param>
```

Make sure that the URLs are accessible by your users.

Post-installation tasks

After you complete the installation of your Content Manager server, you should perform a number of post-upgrade tasks. The post-installation tasks help you verify the installation and configure the components that you have just installed.

Verifying Microsoft SQL System Administration role permissions

To ensure that the database upgrade tool (DBUpgradeTool or DBUT) works properly, the `isource` user must have system administrator permissions.

About this task

To allow DBUT to fully execute all necessary tasks to update your MS SQL database now and for each new release, follow the procedure below to ensure the database user has the necessary permissions.

Note: This procedure applies only if you are using SQLServer. This procedure does not apply to Oracle.

Procedure

1. Access the **SQL Server Management Studio**.

Windows 2012: To access the **SQL Server Management Studio** if not readily accessible, use the **Windows Powershell** icon on the bottom toolbar then at the prompt type: **Ssms.exe**.

Note: If prompted and required, connect to the server.

2. Under the folder for the MSSQL server in the left pane, open **Security > Logins**.
3. Right-click on the **isource** user and select **Properties**.
A Login Properties - isource window displays.
4. In the left pane of the Login Properties - isource window select **Server Roles**.
5. In the right pane for Server Roles select **public** and **sysadmin**.
6. Click **OK**.
7. Click **File > Exit** to exit and close the Microsoft Server Management window.

Running DBUpgradeTool for maintenance

DBUpgradeTool (DBUT), for all supported database engines, performs an overall verification of the database and updates database objects such as views, indexes, packages and stored procedures and modifies metadata structures.

Before you begin

- System Administrator rights for the **isource** database user.
- Available, complete and correctly installed Content Manager server and Content Manager database (up and running).
The installation ensures that the upgrade files and connections are in place to allow a successful upgrade.
- Exclusive access to the Content Manager database for DBUT.
Be sure to stop all components and services, such as InfoShare Crawler, on all servers.

Procedure

1. Login to the server as a Windows user with the Administrator user role.
2. In Windows Explorer, in the Content Manager installation directory, open: \ App\ Setup\ DBUpgradeTool\
3. Locate and double-click on DBUpgradeTool.exe
4. Optional, for ADFS only:
Use DBUT to configure the FishExternalID of the administrator user with a value such as *domain\ username*, for the user who has to log in the system as administrator.
 - Run DBUpgradeTool, select option 1: **Maintenance**.
 - Select option 5: **Append** an user's externalid for initial STS logon.
 - Choose the installation and then fill in the appropriate value for the Content Manager admin user.
5. Select the **DatabaseUpgrade** option.
6. Hit the **Enter** key to respond to all questions; the default options are sufficient for the following questions:
 - Select your recently installed project (thereby selecting the database location and user, upgrade script paths, version and so on).
 - Default for the application.

The result is an upgrade from an older or same version to the installed version when applicable. The application pool needs to be restarted after a DBUT run.

Troubleshooting DBUpgradeTool

You may encounter issues during DBUT execution for database upgrade purposes.

Execution is interrupted

If the DBUT suddenly dies, it results in a hanging database upgrade logged in to the database. All other attempts to upgrade will fail since only one upgrade process is permitted to run at a time.

To force an undo of a hanging update, execute DBUT then select **Maintenance > Terminate** and your current project.

Current user isource warnings

The following warnings can occur in DBUT:

- WARNING: The current user "isource" does not have permission to disable the standard database job for InfoShare.
- WARNING: The current user "isource" does not have permission to install the standard database job for InfoShare. Ask a System Administrator to manually execute ISH_CreateStandardInfoShareJob.sql and ISH_EnableStandardInfoShareJob.Sql to create and enable the standard InfoShare job!
- WARNING: The current user "isource" does not have permission to enable the standard database job for InfoShare.

These warnings are returned when the user executing DBUT has not enough rights to access/create database jobs.

- Creating a database job requires a database administrator to execute `CD-Package\Database\Common\<SQLServerVersion>\Create\ISH_CreateStandardInfoShareJob.sql`
- Enabling a database job requires a database administrator to execute `CD-Package\Database\Common\<SQLServerVersion>\Create\ISH_EnableStandardInfoShareJob.Sql`

Requesting assistance

In case you need to request assistance, you need to provide the following information:

- A screenshot of the failed execution of DBUpgradeTool.
- The log file: `\App\Setup\DBUpgradeTool\DBUpgradeTool.log`

Completing the installation or upgrade with ISHDeploy

Most post-install/upgrade tasks can be carried out with ISHDeploy.

Always configure Windows Authentication with ISHDeploy.

You can also replace most of the manual configuration tasks described in the installation and upgrade sections of this documentation by the use of commandlets.

The presentation and documentation for ISHDeploy can be found [here](#).

Adding the relying party entries for webUI and WCF Services for commercial STS

After the Content Manager installation you have to create the Relying Party Trust for the website and the WCF services on the STS Server if you are not using ISHSTS. This is required to allow logins to Content Manager.

About this task

These post-installation steps have to be done when you are using a commercial STS such as ADFS (ADFS is used as example here). If you are using ISHSTS as STS, do not follow these steps.

Doing this manually can be error prone, therefore SDL provides you a PowerShell script that creates the Relying Party Trust and does the configuration. To execute the script do the following:

Procedure

1. The ADFS server needs the service certificate that is used by the Content Manager WCF Services.
This is the same value as the certificate whose thumbprint is used in the inputparameters parameter `servicecertificatethumbprint`. With the typical Content Manager setup, this WCF Service certificate is the same as the IIS Website Certificate for SSL.
 - a. Open **Internet Information Services (IIS) Manager *Servername***.
 - b. Double-click **Server Certificates** in the right pane.
 - c. Right-click on the certificate of the IIS website that is going to be used for Content Manager then click **View**.
 - d. Click on the **Details** tab then click **Copy to File** and export the certificate to the file system (only export the public key) e.g. *SDL.ISH.cer*.
2. Copy the PowerShell scripts which are created in the directory `\InfoShare\App\Setup\STS\ADFS\scripts\scripts` to a temporary directory on the ADFS server e.g. `c:\SDL.ISH`. Copy also the certificate `c:\SDL.ISH` from the previous step.
3. Login into the ADFS Server and open a administrative PowerShell command line; right-click on the PowerShell shortcut and choose **Run as administrator**.
4. Set the PowerShell execution policy to `Unrestricted`.

Note: The scripts provided are not signed because they are generated during the Content Manager installation. To execute unsigned scripts in PowerShell you must set the execution policy to `Unrestricted`.

- To check if PowerShell's execution policy is already set to `unrestricted`, execute the command:

```
Get-ExecutionPolicy
```

- If the output of this command shows something other than `Unrestricted`, execute the command:

```
Set-ExecutionPolicy Unrestricted
```

5. Change the working directory of the command prompt by executing the command:

```
cd c:\SDL.ISH
```

6. Before running the script, load the `ADFS` PowerShell module by issuing the command:

```
Import-Module ADFS
```

7. Execute the command:

```
.\SDL.ISH-ADFSv3.0-RP-Install.ps1 "C:\SDL.ISH\SDL.ISH.cer"
```

Now if you open **AD FS Management** you should see two new Relying Party entries with the base URLs you use for the Content Manager instance.

Removing the relying party entries for webUI and WCF Services

If you want to remove the Relying Party entries, for instance because Content Manager is moved to another server or the URL has changed, follow the steps below.

Procedure

1. Check if the Uninstall script for the Relying Party entries is on the ADFS server. If not, copy it from the Content Manager application server directory `\InfoShare\ App\ Setup\ STS\ADFS\Scripts\`.
2. Login into the ADFS Server and open a administrative PowerShell command line; right-click on the PowerShell shortcut and choose **Run as administrator**.
3. Before running the script, load the `ADFS` PowerShell module by issuing the command:

```
Import-Module ADFS
```

4. Execute the command:

```
.\SDL.ISH-ADFSv3.0-RP-UnInstall.ps1
```

Now if you open **AD FS Management** you should see that the two Relying Party entries are removed.

Configure Security Token Service

Client installations can be used only if you properly configure a Security Token Service (STS). The default system that manages user identity for Tridion Docs is ISHSTS.

Using ISHDeploy is an alternative to the manual tasks described in this chapter.

Content Manager Security Token Service requirements

Required identifiers and certificates for a Security Token Service configuration applicable to Content Manager.

Profiles

Content Manager relies on both the *Passive profile* and the *Active profile* to do *Federated Authentication*.

Content Manager service name	Profile	Remarks
ISHCM	Passive profile	Refers to web applications. Token encryption is optional.
ISHWS	Active profile	Refers to SOAP-based web services implementing the WS Trust protocol. Token encryption is mandatory.

Identifiers and encryption certificates

For each service Content Manager expects the following combination of identifiers and encryption certificate to be configured on a Security Token Service.

Service: ISHCM

No encryption certificate.

Identifier: <https://example.com/ISHCM/>

Service: ISHWS

The encryption certificate is the public key of the certificate referenced through the `servicecertificatethumbprint` input parameter

Identifiers:

- <https://example.com/ISHWS/>
- <https://example.com/ISHWS/Wcf/API25/Application.svc>
- <https://example.com/ISHWS/Wcf/API25/Baseline.svc>
- <https://example.com/ISHWS/Wcf/API25/DocumentObj.svc>
- <https://example.com/ISHWS/Wcf/API25/EDT.svc>
- <https://example.com/ISHWS/Wcf/API25/EventMonitor.svc>
- <https://example.com/ISHWS/Wcf/API25/Folder.svc>
- <https://example.com/ISHWS/Wcf/API25/ListOfValues.svc>
- <https://example.com/ISHWS/Wcf/API25/MetadataBinding.svc>
- <https://example.com/ISHWS/Wcf/API25/OutputFormat.svc>
- <https://example.com/ISHWS/Wcf/API25/PublicationOutput.svc>
- <https://example.com/ISHWS/Wcf/API25/Search.svc>
- <https://example.com/ISHWS/Wcf/API25/Settings.svc>
- <https://example.com/ISHWS/Wcf/API25/TranslationJob.svc>
- <https://example.com/ISHWS/Wcf/API25/TranslationTemplate.svc>
- <https://example.com/ISHWS/Wcf/API25/User.svc>

- <https://example.com/ISHWS/Wcf/API25/UserGroup.svc>
- <https://example.com/ISHWS/Wcf/API25/UserRole.svc>
- <https://example.com/ISHWS/Wcf/API20/Application.svc>
- <https://example.com/ISHWS/Wcf/API20/DocumentObj.svc>
- <https://example.com/ISHWS/Wcf/API20/EDT.svc>
- <https://example.com/ISHWS/Wcf/API20/EventMonitor.svc>
- <https://example.com/ISHWS/Wcf/API20/Folder.svc>
- <https://example.com/ISHWS/Wcf/API20/MetaDataAssist.svc>
- <https://example.com/ISHWS/Wcf/API20/OutputFormat.svc>
- <https://example.com/ISHWS/Wcf/API20/Publication.svc>
- <https://example.com/ISHWS/Wcf/API20/PublicationOutput.svc>
- <https://example.com/ISHWS/Wcf/API20/Reports.svc>
- <https://example.com/ISHWS/Wcf/API20/Search.svc>
- <https://example.com/ISHWS/Wcf/API20/Settings.svc>
- <https://example.com/ISHWS/Wcf/API20/Workflow.svc>
- <https://example.com/ISHWS/Wcf/API/Application.svc>
- <https://example.com/ISHWS/Wcf/API/ConditionManagement.svc>

Claims in the token

Content Manager maps an incoming token to a user in the users repository by the external identifier.

The mapping is done through the token's attribute matching the claim type

<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name>.

For a token to be useful for Content Manager, the token's subject name should match a user in the Content Manager users repository.

Token claims example

For a user that can be identified as `user@company.com`, the External ID in the users repository is expected to be `user@company.com`.

A valid incoming token must have at least the following attributes defined in it:

```
<saml:AttributeStatement>
  <saml:Attribute AttributeName="name" AttributeNamespace="http://schemas.xmlsoap.org/ws/2005/05/identity/claims">
    <saml:AttributeValue>user@company.com</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
```

ISHSTS with Windows Authentication

You need to perform several settings before ISHSTS can provide Windows Authentication. Both server and SQL server database must be properly configured. You can either make these settings manually or use the scripts provided with the package.

ISHSTS is automatically configured through the installation.

InstallTool creates an application pool such as `TrisoftAppPoolISHSTS` based on the input parameter `infosharestswebappname`. The application pool is assigned an identity based on the input parameter `osuser`. This user is responsible for hosting the endpoints provided by ISHSTS

For Windows Authentication endpoints to work, the following changes based on the requirements of `Service Principal Names` defined in the Active Directory must be made, either manually or through a script.

Note: The following needs to be applied per installation server and are valid only for deployments that do not include network balanced front end servers

Application pool identity

A change of the application pool identity in order to use the integrated `ApplicationPoolIdentity`. This changes the user who hosts the endpoints to an account that the correct `Service Principal Names` is assigned to. The expected `Service Principal Names` are

- `http/baseurl`
- `host/baseurl`

Note: The new user is identified locally as `IIS AppPool\infosharestswebappname` and it requires certain permissions to access resources. When this user accesses network resources it is identified as the computer account `Domain\ Computer$` where the `Domain` and `Computer` are netbios based. e.g. `TESTDOMAIN\SERVER01$`

Read permissions

Read permissions to the token signing certificate's private key are assigned to the `IIS AppPool\infosharestswebappname`. The token signing certificate in ISHSTS is configured through the InstallTool parameter `issuercertificatethumbprint`

Read/write permissions to the three target installation paths defined in the input parameters are assigned to the `IIS AppPool\infosharestswebappname`:

- `webpath`
- `datapath`
- `apppath`

Integrated authentication

If the database is SQL Server and the connection string utilizes integrated authentication then we grant the computer account permissions to the database.

The only permission required is `SELECT`

Configure application server for Windows Authentication

Here is how you execute the script that configures the server for ISHSTS with Windows Authentication.

Before you begin

This task requires a PowerShell session that with `Execution Policy` set to `Unrestricted`. If it is not set, you need to set it permanently by executing the following:

```
Set-ExecutionPolicy Unrestricted
```

The task requires administrator privileges.

Note: InstallTool has already transformed the script based on the input parameters.

Procedure

1. Locate the PowerShell script `SDL.ISH-ISHSTS-Configure for Windows Authentication.ps1` in the folder `\InfoShare\App\Setup\STS\ISHSTS\Scripts`
2. Open PowerShell with elevated administrator privileges. `Run As Administrator`. If the PowerShell session is not running with administrator privileges, the script will launch a new session and administrator privileges will be requested to the user.
3. Navigate to the script folder `\InfoShare\App\Setup\STS\ISHSTS\Scripts`
 - a. `cd \InfoShare\App\Setup\STS\ISHSTS\Scripts`
4. Execute script `SDL.ISH-ISHSTS-Configure for Windows Authentication.ps1`
 - a. `.\SDL.ISH-ISHSTS-Configure for Windows Authentication.ps1`

PowerShell session

```
cd \InfoShare\App\Setup\STS\ISHSTS\Scripts  
& '.\SDL.ISH-ISHSTS-Configure for Windows Authentication.ps1'
```

Configure SQL Server database for Windows Authentication

Here is how you execute the script that allows the server's computer account to access a SQL Server database.

Before you begin

The task applies for SQL Server database when the connection string used integrated authentication.

The task requires sysadmin rights on the SQL Server.

Note: InstallTool has already transformed the script based on the input parameters.

Procedure

1. Locate the script `GrantComputerAccountPermissions.sql` in the `\InfoShare\App\Database\Common\` folder. Depending on your version of SQL Serve:
 - For SQL Server 2016 the script path is `\InfoShare\App<Projectsuffix>\Database\Common\SQLServer2016\Tools\GrantComputerAccountPermissions.sql`
 - For SQL Server 2017 the script path is `\InfoShare\App<Projectsuffix>\Database\Common\SQLServer2017\Tools\GrantComputerAccountPermissions.sql`
2. Execute the script on the target SQL server instance

SQL Server script that grants necessary permissions

If the target database is INFOSHAREDB and the computer account is TESTDOMAIN\SERVER01\$ then the script looks like this:

```
USE [master]
GO
CREATE LOGIN [TESTDOMAIN\SERVER01$] FROM WINDOWS WITH DEFAULT_DATABASE=
[INFOSHAREDB]
GO
USE [INFOSHAREDB]
GO
CREATE USER [GLOBAL\MEDEVASARAFIA01$] FOR LOGIN [TESTDOMAIN\SERVER01$]
GO
USE [INFOSHAREDB]
GO
GRANT SELECT TO [TESTDOMAIN\SERVER01$]
GO
```

The Administrator setup

Needs to be done only if you did not receive a fully prepared database dump-backup file, otherwise this is done and configured.

Note:

- This is the responsibility of a functional administrator not of a technical administrator.
 - The configurations handled in this section are all managed through the Author website Settings tab.
 - The delivered configuration files are available in `web\Author\EnterViaUI` or, for your customer specific files, in `\CustomerSpecificFiles\Websites\Author\EnterViaUI`.
-

Completing the Administrator setup

Needs to be done only if you did not receive a fully prepared database dump-backup file, otherwise this is done and configured.

About this task

Procedure

1. Login to the Content Manager web client as an administrator user.
2. In the web Content Manager, select the **Settings** tab.
3. To configure each of the following:
 - a. Under the **Settings** tab, go to the place as noted in the **To configure, go to** column in the table below.
 - b. Delete the contents of the textbox.
 - c. Copy the contents of the file indicated in the **Copy from** column to the textbox. When you copy, ensure that there are no leading empty lines.

The files are located on the server in the Content Manager_home directory in \ web\ Author\EnterViaUI

To configure, go to:	Copy the contents from:	On the top menu bar, click:
XML Inbox Settings	Admin.XMLInboxConfiguration.xml	Save
XML Write Plug-In Settings	Admin.XMLWriteObjPluginConfiguration.xml	Save
XML Publish Plug-In Settings	Admin.XMLPublishPluginConfiguration.xml	Save
XML Status Settings	Admin.XMLStatusConfiguration.xml	Save
XML Translation Settings	Admin.XMLTranslationconfiguration.xml	Save
XML ChangeTracker Settings	Admin.XMLChangeTrackerConfiguration.xml	Save
XML Background Task Settings	Admin.XMLBackgroundTaskConfiguration.xml	Save
XML Extension Settings	Admin.XMLElementExtensionConfiguration.xml	Save
XML Collective Spaces Settings	Admin.XMLCollectiveSpacesConfiguration.xml	Save

Validation XML configuration files

As part of the introduction of the Settings API 2.5, a schema was made for all configuration XML files.

- Configuration files received a version number

```
<InfoShareStates version="1.0">
...
</InfoShareStates>
```

- Configuration files are validated against this schema when they are submitted through the user interface (UI). The rest of the application assumes that the configuration files in the database are valid.

Resubmit the legacy configuration XML files using the Web Client, **Settings** tab. The configuration file is validated and some corrections are made. For example, a @version attribute with the value, 1.0 is added. If there are validation errors when resubmitting the configuration files, remove all statuses in the status definitions with value "Not found as LOV Value".

```
<Status Elm="..." value="Not found as LOV Value"/>
```

Checking the TRANSLATORSERVICE role

An active TRANSLATORSERVICE role is necessary for translation services (TranslationOrganizer, TranslationBuilder) to operate. This role is part of the out-of-the-box settings for Content Manager 10.0.0 and later. Older versions require that you create it manually along with a list of status transitions.

Procedure

1. In the web client, click the **Settings** tab.
2. Click **User Roles** in the left pane.
 - If *TRANSLATORSERVICE* is part of the list, select it and click the **Properties** button. Make sure that the **Active** checkbox is ticked.
 - If *TRANSLATORSERVICE* is not part of the list, create it by clicking the **New** button and specifying *TRANSLATORSERVICE* in the **Name** field.
3. Click **Status Transitions** in the left pane.
4. Check that the following status transitions are part of the list:

From Status	To Status	User Role
To be translated	In translation	TRANSLATORSERVICE
In translation	Translation in review	TRANSLATORSERVICE
In translation	Translation approved	TRANSLATORSERVICE
Translation in review	Translation approved	TRANSLATORSERVICE

From Status	To Status	User Role
Translation in review	Translation rejected	TRANSLATORSERVICE
Translation rejected	In translation	TRANSLATORSERVICE

- If all these transitions are part of the list, no other action is required.
- If any of these transitions are not part of the list, create them by clicking the **Add** button and filling in the fields with the information from the table above. You can skip the **Condition** fields.

Creating a ServiceUser user

Creating a user ServiceUser user is a mandatory action for translation services, and for the interaction between Content Manager and a delivery platform.

About this task

The ServiceUser user must be available with all user groups because it needs to be used by important services. User roles must also be added (e.g. the TRANSLATORSERVICE role is necessary for using the translation services).

Procedure

1. In the web client, click the Settings tab.
2. Click **Users** in the left pane.
3. Click **New** in the toolbar in the right pane to display the User Properties window.
4. In the User Properties window:
 - As **User name**, enter `ServiceUser`.
 - As **Password**, enter a password that is specified in `inputparameters.xml`.
 - As **Roles**, select all roles that this ServiceUser needs. A basic set would be `TRANSLATORSERVICE`, `Translator`, and `Administrator`.
 - As **Groups**, select all available groups.
 - As **User type**, enter `Internal`.
 - As **External ID**, enter `Domain\ ServiceUser`.

Note: This *ServiceUser* needs to be a user which is created within the domain and has permission to run the TranslationOrganizer service. It can be any name on the domain, *ServiceUser* is only an example.

- Click **OK**.

Translation management integration configuration

The configuration of the Translation management integration with WorldServer, TMS and File System is described.

Translation services configuration files

The configuration files for translation management are described. You can modify the files to configure or customize translation management for your needs.

Application Configuration for TranslationBuilder

Modify the `translationbuilder.exe.config` file parameters noted below to configure or customize TranslationBuilder.

The file is located on the Content Manager server: `\InfoShare\App\TranslationBuilder\Bin\translationbuilder.exe.config`

All the parameters are configured in the `<settings>` element in the `trisoft.infoShare.translationBuilder` section.

Name	Description
<code>maxObjectsInOnePushTranslation</code>	Maximum number of objects in a single push translation. The default value is 1000.
<code>maxTranslationJobItemsCreatedInOneCall</code>	Maximum number of items created in a single transaction. The default value is 10000
<code>maxTranslationJobItemsUpdatedInOneCall</code>	Maximum number of items updated in a single transaction. Default value is 100. Maximum allowed value is 999.
<code>completedJobLifeSpan</code>	The time after which the completed/ cancelled job is deleted. Default value is 90.00:00:00.000
<code>jobProcessingTimeout</code>	The time that a job can be processed by a single step without updating the job lease before it is considered dead. Default value is 01:00:00.000.
<code>userName</code>	The name of the user to access Content Manager. This value is initialized from install parameters.
<code>password</code>	The password of the user to access Content Manager. This value is initialized from install parameters.
<code>jobPollingInterval</code>	Interval at which jobs are polled for processing. Default value is 00:05:00.000.

Name	Description
pendingJobPollingInterval	Interval at which jobs that are pending the push translations are polled for processing. Default value is 00:15:00.000.
updateLeasedByPerNumberOfItems	Number of items that have to be updated before the translation job is updated. Default value is 100.

Application configuration for TranslationOrganizer

Modify the `TranslationOrganizer.exe.config` file parameters noted below to configure or customize `TranslationOrganizer`.

The file is located on the Content Manager server: `\InfoShare\App\TranslationOrganizer\Bin\TranslationOrganizer.exe.config`.

The parameters within the section **trisoft.infoShare.translationOrganizer** are grouped as follows:

- The `Settings` element contains the common parameters. They are all related to the working of the `TranslationOrganizer` service or with the update of the Content Manager Repository.
- The `worldServer/instances/add` element contains the parameters specific to SDL WorldServer.
- The `tms/instances/add` element contains the parameters specific to SDL TMS.
- The `fileSystem/instances/add` element contains the parameters specific to the File System.

TranslationOrganizer common parameters

TranslationOrganizer common parameters are grouped in the `Settings` element of the `trisoft.infoShare.translationOrganizer` section of the `\InfoShare\App\TranslationOrganizer\Bin\TranslationOrganizer.exe.config` file.

dumpFolder

The folder where the temporary files are created. This value is initialized from install parameters.

maxTranslationJobItemsUpdatedInOneCall

Maximum number of items updated in a single transaction. Default value is 100.

jobPollingInterval

Interval at which jobs are polled for processing. Default value is 00:05:00.000.

pendingJobPollingInterval

Interval at which jobs pending translation are polled for processing. Default value is 00:15:00.000.

systemTaskInterval

The minimal interval that system tasks (for example, template synchronisation) are run. Default value is 00:10:00.000.

attemptsBeforeFailOnRetrieval

Number of attempts the update of single content object fails before the job is moved to failed status. The default value is 3.

updateLeasedByPerNumberOfItems

Number of items that have to be updated before the translation job is updated. Default value is 100.

synchronizeTemplates

Specifies whether service should synchronize templates.

retriesOnTimeout

Number of times the single server call can fail and be retried before the job is moved to failed status. Default value is 3.

TranslationOrganizer WorldServer parameters

TranslationOrganizer WorldServer parameters are grouped in the `worldServer/instances/` add element of the `trisoft.infoShare.translationOrganizer` section of the `\InfoShare\App\TranslationOrganizer\Bin\TranslationOrganizer.exe.config` file.

alias

An unique display name for the SDL WorldServer installation (e.g. wsDemo, prod, dev,...).

uri

The base URI for SDL WorldServer (e.g. `http://worldserver.example.com:8080/ws-legacy/services` when using legacy web services or `http://worldserver.example.com:8080/ws-api` when using the new REST API). This value has to be set manually.

userName

The user name to access SDL WorldServer. This value has to be set manually.

password

The password to access SDL WorldServer. This value has to be set manually.

externalJobMaxTotalUncompressedSizeBytes

Maximum total size of the single translation job. Default value is 5242880 bytes.

retriesOnTimeout

Number of times the single external call can fail and be retried before the job is moved to failed status. Default value is 3.

apiProtocol

The protocol that is used to connect to SDL WorldServer. Use `SOAP` to connect using the legacy web services. Use `REST` to connect using the latest REST API. Default value is `REST`.

httpTimeout

The timeout used when doing the WorldServer call using REST API. Default value is 00:02:00.000.

The language mapping

The configuration must also contain a mapping of the language from Content Manager to the locale of SDL WorldServer.

```
<mappings>
<add trisoftLanguage="en" worldServerLocaleId="1145" />
<add trisoftLanguage="nl" worldServerLocaleId="1147" />
<add trisoftLanguage="fr" worldServerLocaleId="1146" />
```

```
</mappings>
```

Note: No more than one SDL WorldServer installation instance is supported in this release. If you are not configuring for use with SDL WorldServer, do not configure any instances for SDL WorldServer.

TranslationOrganizer TMS parameters

TranslationOrganizer TMS parameters are grouped in the `tms/instances/add` element of the `trisoft.infoShare.translationOrganizer` section of the `\InfoShare\App\TranslationOrganizer\Bin\TranslationOrganizer.exe.config` file.

alias

A unique display name for the SDL TMS installation (e.g. demo, prod, dev,...).

uri

The base URI for SDL TMS (e.g. `http://tms.example.com/`). A value is mandatory.

Authentication parameters

Depends on the `authenticationMode` setting: the type of authentication used for signing in SDL TMS from Content Manager. Possible values: `ApiSecret` (the SDL TMS legacy authentication mode), `UserCredentials` (the current SDL TMS authentication mode). The default value is `ApiSecret`.

ApiSecret: legacy authentication mode (SDL TMS 12 and earlier)

- **apiKey:** the API key that is associated with a user (is used only by REST API). It can be obtained from TMS (**Setup > Users & Groups > Users > "<user name>" > TMS API key**). A value is mandatory.
- **secret:** API key encrypted using the user password (is used only by REST API). You can obtain the secret by contacting your SDL TMS contacts or contact SDL Support and providing them the API key as well as the username and password of the user performing the integration. A value is mandatory.

UserCredentials: current SSO authentication (SDL TMS 12.1 and later)

- **Username:** the `username` of the user who is signing in.
- **Password:** the password of the user who is signing in.

externalJobMaxTotalUncompressedSizeBytes

Maximum total size of the single translation job. Default value is 5242880 bytes.

retriesOnTimeout

Number of times the single external call can fail and be retried before the job is moved to failed status. Default value is 3.

httpTimeout

The timeout used when doing the SDL TMS call using REST API. Default value is 00:02:00.000.

destinationPortNumber

Gets or sets a value indicating the TCP Port number over which communications should be conducted.

isapiFilterLocation

Gets or sets a value indicating the path of the CTAISAPI component in SDL TMS that will receive communication requests.

useCompression

Gets or sets a value indicating whether communications should be compressed (is used only by CTAISAPI).

useSsl

Gets or sets a value indicating whether communications should be conducted over a secure channel (is used only by CTAISAPI). If the URI is `https`, this parameter must be set to `true`.

useDefaultProxyCredentials

Gets or sets a value indicating whether to use default credentials when communicating with a Proxy server.

proxyServer

Gets or sets a value indicating the URI of the Proxy server to use.

proxyPort

Gets or sets a value indicating the TCP port to use when communicating with the proxy.

The language mapping

The configuration must also contain a mapping of the language from Content Manager to the language of SDL TMS:

```
<mappings>
  <add trisoftLanguage="en" tmsLanguage="EN" />
  <add trisoftLanguage="fr" tmsLanguage="FR" />
  <add trisoftLanguage="de" tmsLanguage="DE" />
  <add trisoftLanguage="nl" tmsLanguage="NL" />
</mappings>
```

The SDL TMS configurations that specify the workflow and the language pairs. Each configuration that you want to use within Content Manager must be configured within a `<template>` element:

```
<templates>
  <add templateId="81143C38-0C96-4A8C-9BBB-87C1CF464FE3"
    templateName="My template" />
  <add templateId="70407FBC-86FA-4A9D-8E6D-35E1AE85DB73" templateName="
    Trisoft template" />
</templates>
```

Note: After selecting a `template`, only the target languages that are configured for that SDL TMS configuration can be used as possible target language within Content Manager.

Metadata settings

The configuration can contain:

- The metadata that will be extracted and passed to SDL TMS.

```
<requestedMetadata>
  <ishfields>
    <ishfield name="FAUTHOR" level="lng" ishvaluetype="value" />
    <ishfield name="DOC-LANGUAGE" level="lng" ishvaluetype="value" />
  </ishfields>
</requestedMetadata>
```

- The metadata that will be used for grouping items in SDL TMS.

```
<groupingMetadata>
<ishfields>
<ishfield name="FAUTHOR" level="lng" ishvaluetype="value" />
<ishfield name="DOC-LANGUAGE" level="lng" ishvaluetype="value" />
</ishfields>
</groupingMetadata>
```

This metadata will be passed to SDL TMS together with the metadata specified in the `requestedMetadata` section.

Note: No more than one SDL TMS installation instance is supported in this release. If you are not configuring for use with SDL TMS, do not configure any instances for SDL TMS.

TranslationOrganizer File System settings

TranslationOrganizer file system parameters are grouped in the `fileSystem/instances/add` element of the `trisoft.infoShare.translationOrganizer` section of the `\InfoShare\App\TranslationOrganizer\Bin\TranslationOrganizer.exe.config` file.

alias

An unique display name for the configured File System (e.g. demo, prod, dev,...).

externalJobMaxTotalUncompressedSizeBytes

Maximum total size of the single translation job. Default value is 5242880 bytes.

exportFolder

Export folder wherer the exported zip archives will be stored. This value is initialized from install parameters.

Metadata settings

The configuration can contain the metadata that will be extracted and exported as `.met` files next to the actual files.

```
<requestedMetadata>
<ishfields>
<ishfield name="FAUTHOR" level="lng" ishvaluetype="value" />
<ishfield name="DOC-LANGUAGE" level="lng" ishvaluetype="value" />
</ishfields>
</requestedMetadata>
```

Note: No more than one File System instance is supported in this release. If you are not configuring for use with File System, do not configure any instances for File System.

Translation Job Workflow

The life cycle of the translation job.



The main workflow of the translation job.



Failing steps of the translation job workflow.

- TranslationBuilder is responsible for unlocking outdated leases of TranslationJobs so they are part of the workflow again.
- Manual actions can only be executed on TranslationJobs which are not having a status controlled by the two services. This includes Definition, Completed, Cancelled and all Failed statuses.

Integration requirements for Content Manager and SDL WorldServer

The following will help you better understand the integration of Content Manager and SDL WorldServer and considerations when configuring translation and workflow.

Content Manager

Required for Content Manager integration:

- Languages are defined as described for source and pivot languages (see related topic). For example:
The following example defines a source language of English with target languages for German, Spanish, French, Italian and Chinese. The last group indicates that Chinese can be used as source language (pivot) for translating to Japanese and Korean.

```
<languagepaths>
<languagepath from="nl" to="fr"/>
<languagepath from="en" to="de"/>
<languagepath from="en" to="es"/>
<languagepath from="en" to="fr"/>
<languagepath from="en" to="it"/>
<languagepath from="en" to="zh"/>
<languagepath from="zh" to="ja"/>
<languagepath from="zh" to="ko"/>
</languagepaths>
```

- Translation templates come from SDL WorldServer and are automatically pushed to Content Manager by TranslationOrganizer.
- Content Manager uses UTF-16 for the content.
- The dedicated user (typically *ServiceUser*) having the role TRANSLATORSERVICE.
- Statuses and status transitions, configured for the TRANSLATORSERVICE role and for user roles, that defines a workflow for the integration:
 - There is an initial status to indicate that the object is ready for translation: **To be translated**.
This status is used by TranslationBuilder to create new target language objects and by TranslationOrganizer to identify and include objects to send.

- With the status transition from the initial status, there is a status to indicate that the object is no longer under control of the CMS: **In translation**.
Status transition: **To be translated** to **In translation**.
TranslationJob option `Include 'In translation' items` forces the re-sending of objects in this status.
- With the status transition from the status above, there is a status to indicate that the object is back in CMS control: **Translation in review**.
Status transition: **In translation** to **Translation in review**.
- With a status transition from the **Translation in review**, there is a status indicating that a user approved the translation: **Translation approved**.
Status transition: **Translation in review** to **Translation approved**.
- With a status transition from the **Translation in review**, there is a status indicating that a user rejected the translation and the object needs to be re-translated: **Translation rejected**.
Status transition: **Translation in review** to **Translation rejected**.
- Status transitions allow for objects to be re-translated from several positions in the flow, thus making the process cancelled or rolled back to the status **To be translated**.
Status transitions:
 - **In translation** to **To be translated**.
 - **Translation in review** to **To be translated**.
 - **Translation rejected** to **To be translated**.

The TRANSLATORSERVICE role and the status transitions are configured accordingly out-of-the-box.

SDL WorldServer

Required for SDL WorldServer integration:

Note: Refer to the SDL WorldServer manuals for the further details about how to configure the workflow in SDL WorldServer, and related settings.

- A dedicated user in SDL WorldServer.
This is the user that is used by Translation Organizer to logon to SDL WorldServer. This is the parameter `userName` within the `worldServer` section in the configuration file.
- Content Manager mount configured to use UTF-16.
- Locales, Workflow, Project Types, whatever is required by WorldServer to go through the translation process.
- A first step named *Translate*.
- After the *Translate* step there should be an automatic *Save* step.
- After the *Save* step there should be *Translated Content Retrieval* step which is used by Content Manager to start getting the translation.
- After the *Translated Content Retrieval* step, a transition named **Ready for review** leads to the *Translated Content In Review* step.
- After the *Translated Content In Review* step, there must be two possible transitions:

- The **Approved** transition that leads to the end of the flow.
- The **Rejected** transition that leads back to the *Translate* step.
- The *Asset path normalizer*. This optional custom component can be implemented separately and installed in SDL WorldServer to force SDL WorldServer TM to consider the file name when doing the match.

Compatibility

- For backward compatibility, it is still possible to configure a simplified flow made of *Translated Content Retrieval* immediately followed by a transition called **Retrieved**.
- The translation review flow with the possibility to approve or reject the translation, introduced in Content Manager 13.0.0, is incompatible with the SOAP API protocol. Therefore when WorldServer uses that protocol, only the legacy flow can be used (*Translated Content Retrieval* immediately followed by **Retrieved**).
- Any given job must be using only one type of flow: Either the current flow with an approval step, or the legacy flow. The system can not manage mixed flows.

Integration requirements for Content Manager and SDL TMS

The following will help you better understand the integration of Content Manager and SDL TMS and how to configure translation and workflow.

Content Manager

Required for Content Manager integration:

- Languages are defined as described for source and pivot languages (see related topic). For example:
The following example defines a source language of English with target languages for German, Spanish, French, Italian and Chinese. The last group indicates that Chinese can be used as source language (pivot) for translating to Japanese and Korean.

```
<languagepaths>
<languagepath from="nl" to="fr"/>
<languagepath from="en" to="de"/>
<languagepath from="en" to="es"/>
<languagepath from="en" to="fr"/>
<languagepath from="en" to="it"/>
<languagepath from="en" to="zh"/>
<languagepath from="zh" to="ja"/>
<languagepath from="zh" to="ko"/>
</languagepaths>
```

- Translation templates come from SDL TMS and are automatically pushed to Content Manager by TranslationOrganizer.
- Content Manager uses UTF-16 for the content.
- The dedicated user (typically *ServiceUser*) must have the role TRANSLATORSERVICE.
- Statuses and status transitions, configured for the TRANSLATORSERVICE role and for user roles, define a workflow for the integration:
 - There is an initial status to indicate that the object is ready for translation: **To be translated**.

This status is used by TranslationBuilder to create new target language objects and by TranslationOrganizer to identify and include objects to send.

- With the status transition from the initial status, there is a status to indicate that the object is no longer under control of the CMS: **In translation**.

Status transition: **To be translated** to **In translation**.

TranslationJob option `Include 'In translation' items` forces the re-sending of objects in this status.

- With the status transition from the status above, there is a status to indicate that the object is back in CMS control: **Translation in review**.

Status transition: **In translation** to **Translation in review**.

- With a status transition from the **Translation in review**, there is a status indicating that a user approved the translation: **Translation approved**.

Status transition: **Translation in review** to **Translation approved**.

- With a status transition from the **Translation in review**, there is a status indicating that a user rejected the translation and the object needs to be re-translated: **Translation rejected**.

Status transition: **Translation in review** to **Translation rejected**.

- Status transitions allow for objects to be re-translated from several positions in the flow, thus making the process cancelled or rolled back to the status **To be translated**.

Status transitions:

- **In translation** to **To be translated**.
- **Translation in review** to **To be translated**.
- **Translation rejected** to **To be translated**.

The TRANSLATORSERVICE role and the status transitions are configured accordingly out-of-the-box.

SDL TMS

Required for SDL TMS integration:

- Configurations specifying the workflow and all necessary language pairs.

Remember: When a configuration is selected, only the target languages (and workflow) that are configured for the source language can be used.

- The workflow should contain minimally the following steps in TMS:
 - The *Translation* step. In TMS by default.
 - The *Translated Content retrieval* step which is used by Content Manager to start getting the translation. In TMS by default.
 - The *Translated Content In Review* step. You need to add this step manually, as a human step (it is not performed by the system).
- Every step between *Translation* (not included) and *Translated Content In Review* (included) must have the user performing the integration assigned as default user. If it is not, then the integration user must be included in every group the steps are assigned to.

- Refer to the SDL TMS manuals for the further details about how to configure the workflow in SDL TMS.

Compatibility

- The oldest required SDL TMS version allowing the use of **Translation rejected** along with all the cancellation options is SDL TMS 11.2.1.
- Any given job must be using only one type of flow: Either the current flow with an approval step, or the legacy flow. The system can not manage mixed flows.

Integration requirements for Content Manager and File System

The following are items that will help you better understand the integration of Content Manager and File System and considerations when configuring translation and workflow.

Content Manager

Required for Content Manager integration:

- Languages are defined as described for source and pivot languages (see related topic). For example:
The following example defines a source language of English with target languages for German, Spanish, French, Italian and Chinese. The last group indicates that Chinese can be used as source language (pivot) for translating to Japanese and Korean.

```
<languagepaths>
  <languagepath from="nl" to="fr"/>
  <languagepath from="en" to="de"/>
  <languagepath from="en" to="es"/>
  <languagepath from="en" to="fr"/>
  <languagepath from="en" to="it"/>
  <languagepath from="en" to="zh"/>
  <languagepath from="zh" to="ja"/>
  <languagepath from="zh" to="ko"/>
</languagepaths>
```

- Translation templates are based on configured source and pivot languages, and are automatically pushed to Content Manager by TranslationOrganizer.
- Content Manager uses UTF-16 for the content.
- The dedicated user (typically *ServiceUser*) having the role TRANSLATORSERVICE.
- Statuses and status transitions, configured for the TRANSLATORSERVICE role, that defines a workflow for the integration:
 - There is an initial status to indicate that the object is ready for translation: **To be translated**.
This status is used by TranslationBuilder to create new target language objects and by TranslationOrganizer to identify and include objects to send.
 - With the status transition from the initial status, there is a status to indicate that the object is no longer under control of the CMS: **In translation**.
Status transition: **To be translated** to **In translation**.

TranslationJob option `Include 'In translation' items` forces the re-sending of objects in this status.

- With the status transition from the status above, there is a status to indicate that the object is back in CMS control: **Translation in review**.

Status transition: **In translation** to **Translation in review**.

- With a status transition from the **Translation in review**, there is a status indicating that a user approved the translation: **Translation approved**.

Status transition: **Translation in review** to **Translation approved**.

- With a status transition from the **Translation in review**, there is a status indicating that a user rejected the translation and the object needs to be re-translated: **Translation rejected**.

Status transition: **Translation in review** to **Translation rejected**.

- Status transitions allow for objects to be re-translated from several positions in the flow, thus making the process cancelled or rolled back to the status **To be translated**.

Status transitions:

- **In translation** to **To be translated**.
- **Translation in review** to **To be translated**.
- **Translation rejected** to **To be translated**.

The TRANSLATORSERVICE role and the status transitions are configured accordingly out-of-the-box.

File System

Required for File System integration:

- The dedicated user (see above) configured for the integration has an access to the folder where the zip files should be created.

Enabling services

After the install is complete, services will not start automatically, since the database is not guaranteed to be in the right state until you run DBUT tool. Also, you might decide not to start some services on the specific installation depending on the server role. To enable typical services you can locate and run the `Enable-DefaultServices.ps1` script.

Before you begin

- DBUT completed successfully.
- The Administrator setup completed successfully.
- The TRANSLATORSERVICE role is created and the translation status transitions have been assigned to it.
- System Administrator rights.

Procedure

1. Run the script `\App\Setup\Manage\Enable-DefaultServices.ps1`
Typical services (Trisoft InfoShare Crawler One, Trisoft InfoShare SolrLucene, Trisoft InfoShare BackgroundTask One, Trisoft InfoShare TranslationBuilder One etc.) are started, startup type is set to "Automatic (Delayed Start)".

Enabling Draft Space

We recommend you enable Draft Space with ISHDeploy.

Before you begin

Check how to access to and use ISHDeploy in the documentation located [here](#).

About this task

Draft Space is one of two tools that are grouped under the name Collective Spaces.

Procedure

1. Enter the following command:

```
Enable-ISHUICollectiveSpaces -DraftSpace -ISHDeployment ISHDEPLOYMENT
```

where *ISHDEPLOYMENT* is the deployment you want to use. (If you have only one deployment, you can omit the `-ISHDeployment` parameter and its value.)

Results

You now have access to Draft Space for web browser-based content authoring.

Enabling Review Space

We recommend you enable Review Space with ISHDeploy.

Before you begin

Check how to access to and use ISHDeploy in the documentation located [here](#).

About this task

Review Space is one of two tools that are grouped under the name Collective Spaces.

Procedure

1. On your Content Manager server machine, go to `c:\InfoShare\App\Utilities\FontoReview`.
2. Open the application configuration file `appsettings.json` for editing.
3. Set the value of the `ApiBaseUrl` property to the URL of the Tridion Docs website that is used to retrieve the revision information and content. The URL has the format `https://HOSTNAME/ISHCSORA19/api/TrustedSubsystem/Fonto/`, where *HOSTNAME* is the name of the host server on which the website runs.
4. Set the value of the `Url` property to the URL of the Fonto Review service, the ASP.NET

service used by Review Space. The URL has the format `https://localhost:PORT`, where *PORT* is the specific port on which the Fonto Review service is listening. If you did not specify a custom port number as a value for the `fontoreview_service_port` parameter in the file `inputparameters.xml` when you installed the Content Manager server, the service runs on the default port, which is 8001.

5. Enter the following command:

```
Enable-ISHUICollectiveSpaces -ReviewSpace -ISHDeployment ISHDEPLOYMENT
```

where *ISHDEPLOYMENT* is the deployment you want to use. (If you have only one deployment, you can omit the `-ISHDeployment` parameter and its value.)

Results

You now have access to Review Space for web browser-based content reviewing.

Configuring the Discovery Service connection

To enable UGC, configure the Discovery Service URL and credentials in the Web Client.

Procedure

1. Access the Content Manager Web Client.
2. In the slide-out navigation, select **Content Manager**.
The Content Manager user interface opens.
3. At the top of the screen, select **Settings**.
The **Settings** screen opens.
4. At the left hand side of the screen, select **Default Settings**.
A list of default settings appears in the content area.
5. Find the **SDL Tridion Docs Dynamic Delivery - UGC** setting and set it to the Discovery Service URL for Dynamic Delivery. This URL defaults to `http://SERVER:8082/discovery.svc`, where *SERVER* is the host name of the server on which the Discovery Service is installed.
6. Set the **Client ID** setting to the client ID of an account that can access the Discovery Service.
7. Set the **Client Secret** setting to the secret of that account.
8. Select **Save** to commit your changes.

Verifying the installation

Conduct some testing to verify critical parts of your installation.

Verifying URLs

If your environment includes reverse proxy servers, after you install Content Manager, you need to check that certain URLs are accessible.

Procedure

1. Using Windows Internet Explorer, ensure that you can reach the following URLs:
 - *BaseURL/ISHWS/Application.asmx?wsdl*
 - *BaseURL/ISHWS/Application.asmx?disco* where *BaseURL* is the value specified for the *baseurl* parameter, and *ISHWSWS* is the value specified for the *infosharewebswebappname* parameter. These parameters are set in the *inputparameter.xml* file that is used by the Content Manager installer.
2. If you cannot access the URLs, verify that the reverse proxy servers are correctly configured. See the documentation for the reverse proxy servers.

Verify read access to the database by viewing an inbox

To verify read access to the database, request to view an inbox in the web client.

Procedure

1. Open Internet Explorer and enter the address for the Content Manager web client.

Note: The web client address is a combination of the value in the parameters in the *inputparameters.xml* file:

```
baseurl/infoshareauthorcmwebappname/
```

For example, if:

```
<param name="baseurl">
<currentvalue>https://example.corp</currentvalue>
```

and

```
<param name="infoshareauthorwebappname">
<currentvalue>ISHCM</currentvalue>
```

then the URL is:

```
https://example.corp/ISHCM/
```

Enter a Content Manager username and password. If you are not sure about the login/password and you imported the default database you can use **admin/admin** to login.

2. Access the SDL product menu by clicking on the icon in the upper left of the window and select **Content Explorer**.
3. If not selected, select the **Inbox** tab at the top of the window.
4. In the left pane, select one of the inboxes, for instance, select **Reviewer**.
If no objects are in the inbox, an empty inbox is displayed; **No objects in inbox** is reported in the right pane.

If there are objects in the inbox, a list of objects is displayed in the right pane.

Verify read and write access to the database by creating a folder

Create, modify, and delete actions are handled through transactions and verifies read and write access to the database.

Procedure

1. Login to the Content Manager web client as an existing user. For example as the admin user.
2. Select the **Repository** tab at the top of the window.
3. Click the **New Folder** icon in the upper left of the Repository pane.
A New Folder window displays.
4. Enter a name in the **Folder Name** field. For example enter the folder name, **Test**.
5. Click **OK**.
The folder is created and displayed in the left pane.

What to do next

You can remove the test folder by selecting it in the left pane then clicking the **Delete Folder** icon (red X) in the upper left pane. You are asked to confirm the delete action, click **Yes** to confirm and delete the folder.

Creating an account and connecting to the Repository

Before you can use Content Importer, you need to set up your user account. If you installed Content Importer on a system where Publication Manager is already installed, the user account settings are recognized.

Before you begin

You must create the user account and configure the connection to the Repository to allow a user to connect and access data in the Content Manager Repository. Use this procedure to create a new user account for testing purposes.

To create the account and connect to the Repository, you need the URL of the Content Manager web services.

Procedure

1. In Content Importer, select **Create an account**.
The account window is displayed.
2. Enter an **Account Name** and the URL of the Content Manager **Web Service**.
3. Select **Next**.
4. If necessary, select the **Authentication Method**.
5. Enter the username and password.
Check **Remember password** if you do not want to enter the information each time you use the application.

6. Select **Next**.

Content Manager validates the account and synchronizes files.

Running a client tool

When started, the client tools verify availability of the synchronization website and web services.

Before you begin

- A desktop client workstation must be installed with the client tools. If not done, refer to the section for installing desktop clients.
- The client tool must be configured with a user login and account.
- To fully test the client, the database should contain data.

Procedure

1. If necessary, create an account and connection to the repository.
2. Start a client tool such as Publication Manager, Condition Manager or Authoring Bridge from the **Start** menu or desktop shortcut.

If you can view and access the repository through the client tool, and can view or preview a topic in the repository then web services, synchronization, and network availability have been successfully verified.

Testing publishing

You can test the publish functionality if your database contains topics, maps and publications, and it is configured to render an output type.

Before you begin

If your database is not configured to render an output, refer to the [Content Manager Information Portal](#) documentation for information about adding output formats.

Procedure

1. Login to the Content Manager web client as an existing user. For example as the admin user.
2. Select the **Repository** tab at the top of the window.
3. Select a publication in the left pane.
4. Select a version in the upper right pane by clicking on the publication name.
The available versions of the publication are listed in the lower right pane.
5. Select a version and language for the publication in the bottom right pane.
This is done in the right and left check boxes next to the output format.
6. Click the **Publish** button in the menu on the bottom right.
A confirmation dialog displays.
7. Click **OK** to confirm and begin the publish process.

8. To display progress, click **Refresh**.
Verification is complete when the Event Description is **Publish Process ended** and the status says **SUCCESS**.
9. Click **Close**.

Executing the full text search

You can test the search functionality if the database contains content.

Procedure

1. Login to the Content Manager web client as an existing user. For example as the admin user.
2. Select the **Search** tab at the top of the window.
3. Enter a word in the **Search Term** field then click **Search**.

If there is no search result, verify if a rebuild of the full-text-index collection is required. Note that the full-text-index collection is not immediately available after installation since it takes some time to build.

Verifying customer specific components

If you requested customizations of the out-of-the-box Content Manager software, a check that they were delivered is recommended at this time.

About this task

Customizations of the delivered software may be, for example, PDF stylesheets, extra metadata, or extra development to integrate with other systems such as SDL-TMS, PLMs, SingleSignOns.

If you contracted for additional customizations, check that they were delivered and functioning as required.

Installing desktop client tools

You can choose to install desktop client tools (Authoring Bridge, Publication Manager, Condition Manager and Content Importer) based on the role and responsibilities of the user. The versions of the desktop clients tools must match the version of Content Manager installed on the server.

Installing the Authoring Bridge

The Authoring Bridge is used to access the repository using an authoring tool.

About this task

Choose the Authoring Bridge installer for the XML editor software that you are using (XMetaL, oXygen, ...). The type and version of the editor you are using must be qualified with the installed version of Content Manager.

If an incompatible version of the .NET runtime framework is installed, the installer will install a correct one after your validation.

The install package's names match the following format, one for each compatible XML Editor:

- `<date>.AuthoringBridge.<version>-XMetaL-Connector.msi`
- `<date>.AuthoringBridge.<version>-oXygen-Connector.msi`
- `<date>.AuthoringBridge.<version>-ArbortextEditor-Connector.msi`

The development kit's executable name matches the following format:

- `<date>.AuthoringBridgeSDK.<version>.exe`

Procedure

1. Double-click the Authoring Bridge install package, or **Setup Wizard**, and follow the proposed list of steps. After you hit the **Finish** button, the installation is complete and the SDL Tridion Docs menu is now available in your authoring tool's menu bar.

Results

When you first try to access the Repository from your authoring tool, you will be requested to specify a user account in order to establish the connection.

For uninstall, be aware of the following:

- If you are using XMetaL on Windows, you must uninstall the Authoring Bridge before uninstalling XMetaL.
- If the Authoring Bridge is uninstalled, the SDL Tridion Docs menu will remain in the menu bar, with all menu options greyed out. You must start XMetaL while pressing the **CTRL** key in order to have XMetaL clean up the menu bar and remove the SDL Tridion Docs menu.

Installing Publication Manager

The publication manager is used to create, modify, check the status of, and produce publications in various formats.

About this task

If an incompatible version of the .NET runtime framework is installed, the installer will install a correct one after your validation.

The install package's name matches the following format: <date>.PublicationManager.<version>.msi

Procedure

1. Double-click the Publication Manager install package, or **Setup Wizard**, and follow the proposed list of steps. After you hit the **Finish** button, the installation is complete and Publication Manager is now available for you to use.

Installing Condition Manager

The Condition Manager is used to create and manage conditions for your publications.

About this task

If an incompatible version of the .NET runtime framework is installed, the installer will install a correct one after your validation.

The install package's name matches the following format: <date>.ConditionManager.<version>.msi

Procedure

1. Double-click the Condition Manager install package, or **Setup Wizard**, and follow the proposed list of steps.
2. Select the **Enable Synchronization** option when proposed (on the tab where you specify the installation folder). Content Manager can synchronize the set of conditions with definitions from another system. Synchronization needs to be configured separately, **Enable Synchronization** only makes the menu items available in the application.
3. After you hit the **Finish** button, the installation is complete and Condition Manager is now available for you to use.

Installing Content Importer

Content Importer helps you import content through the Content Manager Web Client commands.

About this task

If an incompatible version of the .NET runtime framework is installed, the installer will install a correct one after your validation.

The install package's name matches the following format: <date>.ContentImporter.<version>.msi

Procedure

1. Double-click the Publication Manager install package, or **Setup Wizard**, and follow the proposed list of steps. After you hit the **Finish** button, the installation is complete and Content Importer had added functionality to the Content Manager Web Client.

Advanced topics for installers

The following can be referenced for additional information when installing or upgrading your systems.

InstallTool

InstallTool is a command line driven application which allows you to install Content Manager, including customer-specific files and components.

InstallTool overview

InstallTool logs all installation actions and keeps an installation history which allows you to rollback.

InstallTool was developed to:

- reduce the time needed to install Tridion Docs
- eliminate the most common mistakes when installing Tridion Docs
- provide reproducible installations over DEV, QA and PROD
- provide a framework for system integrators to deploy a customer-specific Content Manager application
- make it easier to have multiple Content Manager applications on one server

Training is available on how to build and maintain the InstallTool package. Note that the Generate InstallPlan option cannot take into account all variations of all possible setups or all possible options. Manual actions on the InstallPlan may be required to describe your installation. InstallTool is only available to generate the initial file.

Executing the program consists of starting InstallTool and following the instructions. The Content Manager Database should be up and all Microsoft components and Third Party Software should be installed.

The InstallTool

The InstallTool package contains three parts.

The InstallTool package contains:

The root of your CD location

It is a folder on your file system that uses the Content Manager official structure containing the raw data.

InstallPlan.xml

The InstallPlan is generated by Content Manager or an integrator. It describes the installation. That is, it describes every install action such as the source and target folder for every file, COM+ Applications and their content, Virtual Directories, Registry structures, Services and so on.

An install plan is built from two types of building blocks:

- file elements (from-to copy statements)
- webapp/commapp/registry/serviceapp (system change statements)

These building blocks are in the following three groups:

- Core (can only be installed once).
- Standard (the out-of-the-box components for the project/environment).
- Customer Specific (your customized/project files overwriting the Standard/DITA files).

Note that if you add files to the CD, you must regenerate the install plan, otherwise it does not contain extra file elements.

InputParameters.xml

This file contains a list of variables that require a value assignment from the system administrator. The main goal is to centrally define global settings such as `AppPath`, `WebPath`, `DataPath`, `ProjectName`, `Designated OSUser`, `database ConnectString`, and so on.

The file contains the prompts displayed in a graphical user interface of an install program. All these values are inserted in the necessary places during the installation.

The `InputParameters` file needs to assign a value for ALL variables used somewhere in the `InstallPlan.xml` or in files which use variables on the CD.

Unimplemented features of the InstallTool

InstallTool must know about all Content Manager options, features, and environment changes that are impossible however, some operations are not automated.

For reasons of security and complexity, the following operations are not automated:

- Installing SQL Server or Oracle.
- Running scripts on an existing database.
- Creating the designated operating system user.
- Changing the transaction timeout settings.

- Delta upgrading of environments (only full (un)install).
- Checking the availability of correct Microsoft components.

There are some additional, manual configurations or edits that need to be done included in the procedure for installing or upgrading.

Background task component

Background task is an application logic that is triggered on certain events, does not require user interaction and runs in a background by a background task service. Typical example is publishing process: it has to be triggered by user, but after it is triggered, it does not require user input neither does it require user to wait. Instead, the publishing process runs in a background, and user can know that it is finished by periodically checking the status of a publication.

Starting background tasks

Typically tasks are created by plugins. For example, it is possible to register a plugin that will run when user changes the status of the topic and create the background task. Typically, background task does not start executing immediately after it is created. Instead it is added to the queue from where it can be later picked up by a background task service which executes the task. This allows better distribution of load since the task can be picked up by the service (or server, because background task services can run on different servers) which is less busy.

Executing background tasks

There is only one background tasks queue which is available to every background task service. Under the hood, it is implemented as a database table, which means that once added, task will not get lost. Practically it means that task will survive the server reboot, and even if the task execution fails in the middle, task remains in the queue and can be re-started.

Every background task has an event type it is created for. For example, when you trigger the publish, there will be a background task created with event type `EXPORTFORPUBLICATION`. Task can be picked up by one of installed background task services. You can limit event types that service is allowed to pick and amount of background tasks with the same event type that can be executed in parallel.

When task fails for one reason or another, it is automatically re-tried later. You can adjust this behavior by changing the limit of retry attempts.

Monitoring background tasks

Typically, background tasks update the status of the execution by writing to the event log. For example, background task that executes publishing will update the corresponding Publish event.



There is only one queue for background tasks. There can be any number of background task services picking up tasks.

Overview of the background task configuration

The background task configuration contains all information for running the background task services and handling the background tasks.

Introduction

The configuration is stored inside the Content Manager database and is accessible via the Content Manager web client using **Settings > XML Background Task Settings**.

Tip: For detailed information, check the `Admin.XMLBackgroundTaskConfiguration.xml` file.

Configuration for the background task services

The configuration can contain different types of services. Every background service runs with a specific *role*. For every role the configuration describes the behavior:

- Should the service execute background tasks?
- How often should it poll for a new background task?
- Should the service recover failed background tasks?

If the service is configured to execute background tasks, the configuration specifies for which groups of event types the service is responsible. The configuration defines for every group how many background tasks are allowed to run in parallel.

Out-of-the-box, the services are installed with the 'Default' role and will pick up all possible background tasks. However, it is possible to configure for instance a service with the role 'Publish' picking up only the background tasks with event type *EXPORTFORPUBLICATION*

Configuration for the handlers

The configuration contains a list with handlers. Each handler is handling one *eventType* and can be executed synchronously or asynchronously. The handler is responsible for (1) starting the activator which will execute the background task and (2) handling any exception which occurs.

Per type of activator, the configuration not only contains the necessary information to create and run the activator, but it also contains the configuration with parameters that are used during the execution of the background task.

Note: These parameters can contain (environment) variables that are resolved by the background task service configuration.

The configuration also specifies if the background task must be executed within the same process (of the service) or within a new process, and for how long the background task is allowed to execute. Each background task is executed within the security context of the user that submitted the background task. How the security context is created depends on the authorization type.

When the execution of the background fails, the configuration indicates for each error number if the background task must be retried and how many times the background task can be scheduled to re-execute.

Usage of variables inside the background task configuration

Referencing environment variables inside the background task configuration is useful when exact configuration value varies from server to server and therefore cannot be single-sourced. Environment variables are resolved at the moment background task service is being initialized with the actual values set on that specific server.

Normally background task gets its parameters from the background task configuration. This way the background task parameters are defined in a single place and can be easily accessed by the task regardless of which server or service executes it.

However, sometimes it is not easy (or even possible) to provide a value that would work on every server. The typical case is the file path, which may differ from one server to another. For example, PUBLICATIONEXPORT event type needs to know the export location, which can be a different folder depending which server picks up the task.

To solve this problem, background task configuration allows referencing environment variables. Environment variable can be provided as a value of any element or attribute.

PUBLICATIONEXPORT references %ISHPROJECTDATAPATH% in the value of exportlocation and exportspeclocation parameters.

```
<handler eventType="PUBLICATIONEXPORT">
  <scheduler executeSynchronously="false" />
  <authorization type="authenticationContext" />
  <execution timeout="01:00:00" recoveryGracePeriod="00:10:00"
    isolationLevel="Process" useSingleThreadApartment="true" />
  <activator>
  <comIEventHandler projectName="IshPluginsIso" className="cout">
  <configuration>
  <parameters>
  <parameter name="exportlocation" type="value">%ISHPROJECTDATAPATH%
    \ExportService\Data\DataExports</parameter>
  <parameter name="exportspeclocation" type="value">%ISHPROJECTDATAPATH%
    \ExportService\Data\WatchFolder</parameter>
  <parameter name="separatelng" type="value">yes</parameter>
  <parameter name="requestedmetadata" type="ishfields">
  <ishfields>
  <ishfield name="FSTATUS" level="lng" />
  </ishfields>
  </parameter>
  <parameter name="raiseevent" type="value">ZIPFILES</parameter>
  <parameter name="filenameprefix" type="ishfields">
  <ishfields>
```

```
<ishfield name="FTITLE" level="logical" />
</ishfields>
</parameter>
</parameters>
</configuration>
</comIEventHandler>
</activator>
<errorHandler maximumRetries="0" />
</handler>
```

When the background task service is being initialized, every environment variable is replaced with the actual value.

Remember: It is your responsibility to make sure that every environment variable referenced in the background task configuration is set!

Remember: Setting environment variable to empty string deletes the environment variable!

The easy way to set the environment variables for the lifetime of the background task service is to add them to the background task service configuration file. The file is located on the Content Manager server: `\InfoShare\App\BackgroundTask\Bin\BackgroundTask.exe.config`

Variables are configured in the **variables** element within the section **trisoft.infoShare.backgroundTask**. Background task service will read these values during initialization and use them to set the actual environment variables.

Providing the environment variable values for PUBLICATIONEXPORT in the background task service configuration file.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
<configSections>
<section name="trisoft.infoShare.backgroundTask" type="Trisoft.
InfoShare.BackgroundTask.BackgroundTaskConfigurationSection, Trisoft.
InfoShare.BackgroundTask, Version=11.0.0.0, Culture=neutral,
PublicKeyToken=555d9fcb450e0935"/>
<!-- Other <section> and <sectionGroup> elements. -->
</configSections>
<startup>
<supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
</startup>
<trisoft.infoShare.backgroundTask>
<variables>
<!-- Value cannot be an empty string! -->
<add key="ISHPROJECTAPPPATH" value="C:\InfoShare\App" />
<add key="ISHPROJECTDATAPATH" value="C:\InfoShare\Data" />
</variables>
</trisoft.infoShare.backgroundTask>
</configuration>
```

Understanding the availability matrix

The availability matrix defines which event types and how many of their instances is the background task service allowed to execute in parallel.

Executing background tasks consumes system resources, most importantly CPU time and system memory. Deciding which kind of tasks and how many instances of them are allowed to run in parallel on the same server is important because this will affect stability, throughput and overall system performance. This decision is a compromise: increasing the task parallelism can increase the throughput (more tasks are executed within the same amount of time), but it puts the system under pressure and may even result in situations when your process on the server runs out of memory.

The availability matrix is configured in the background task configuration, per server role, under matrix element. The default background task configuration is located in `\Websites\Author\EnterViaUI\Admin.XMLBackgroundTaskConfiguration.xml`, which is delivered on every CD, and contains the latest suggested out of box values for the matrix.

```
<matrix>
  <group name="Translations" maxExecutions="2">
    <handlers>
      <add ref="CREATETRANSLATIONFROMREPORT" />
      <add ref="CREATETRANSLATIONFROMLIST" />
      <add ref="CREATETRANSLATION" />
      <add ref="RELEASETRANSLATIONS" />
    </handlers>
  </group>
  <group name="Export" maxExecutions="2">
    <handlers>
      <add ref="EXPORTFORPUBLICATION" />
      <add ref="INBOXEXPORT" />
      <add ref="REPORTEXPOR" />
      <add ref="SEARCHEXPORT" />
      <add ref="PUBLICATIONEXPORT" />
    </handlers>
  </group>
  <group name="SynchronizeToLiveContent" maxExecutions="1">
    <handlers>
      <add ref="SYNCHRONIZETOLIVECONTENT" />
    </handlers>
  </group>
  <group name="Others" maxExecutions="2">
    <handlers>
      <add ref="THUMBNAILSUBMIT" />
      <add ref="ISHBATCHIMPORT" />
    </handlers>
  </group>
</matrix>
```

Matrix defines groups of handlers with common features or requirements or functionality. For every group, maxExecutions attribute specifies how many instances of the specified background task handler can be executed concurrently. The availability matrix works proactively by controlling what the background task service will poll each time. Only tasks that are valid for the current state of execution and the availability matrix are allowed to begin executing.

Here is an example flow to better understand what happens when the service begins to execute.

Looking at the first group Translations, the service will try to execute any background task with the configured handler for example `CREATETRANSLATIONFROMREPORT`. While a `CREATETRANSLATIONFROMREPORT` instance is executing the service is allowed to pick one more item from the queue matching the configured handlers of this specific group including `CREATETRANSLATIONFROMREPORT`, for example `RELEASETRANSLATIONS`. As long as both background tasks are executing the service is not allowed to execute any more from this group because the limit 2, defined in `maxExecutions` attribute, is reached. Once one of the tasks finishes then the service is allowed once again to execute background tasks from the this group. The above reasoning is applied to every configured group and the service will always try to execute a background task from any group that still hasn't reached its `maxExecutions` limit.

Important: You can only put one event type in one group. If you configure the same event type in 2 different groups, you will get an error when trying to submit this configuration.

Default background task configuration comes with 2 background task service roles. The Console background task service role is optimized for testing through the console mode. This role will restrict the process to execute a maximum of 1 background task at any given time.

Understanding the isolation level of the handler

Explains the significance of isolation level configuration value for a background task handler.

Every handler configuration in the Background task XML settings defines an `isolationLevel` within the `execution` element .

The isolation level is allowed to have one of the following values

- None
- Process

When the value is `None` then all background tasks of this handler will execute within the process of the background task service.

Every operating system process has a limited amount of resources that it can access. With the background task service, we are interested in the memory limitation. The process's maximum memory must be shared between the requirements of the service's components but also the running background tasks.

There is also the potential of memory leaks than can be caused by a background task. Although the background task service is optimized against memory leaks it can run out of memory because a background task had misused the memory.

Different combinations can result to an unstable background task service process or handler that runs out of memory. To protect the background task service but also provide an isolated memory space to a specific background task, the `Process` value was introduced for the `isolationLevel`. When this configuration is enabled for a handler, the background task service will spawn a new process with the sole goal to execute this specific background task instance. This way the execution is isolated within the memory space of a specific process that is dedicated fully for the background task. Also any memory leak caused by the handler's execution is limited to the lifetime of this process and has no effect to the background task service process. There is an overhead though. A new process means that everything has to be

loaded resulting to slower startup times of the actual execution. The total overhead depends on the load on the server.

This way the handler receives maximum memory space and also the background task service is protected against memory leaks. The only tradeoff is a potential overhead in the total execution time.

Based on the above, here are some suggestions to help you get to the correct value for `isolationLevel` of a handler:

- If the handler of the background task requires a lot of memory then it must be isolated.
- If the handler has the potential to execute for long then it should be isolated.
- Choosing `Process` for the `isolationLevel` should take into account the overhead of the startup time compared to the average actual execution time of the handler

Out of the box configuration has all handlers configured to execute with `isolationLevel` set to `None`. Only for `EXPORTFORPUBLICATION` is configured to execute with `isolationLevel` set to `Process` because it is very memory intensive. Because it has the potential to execute for long the extra overhead in startup time is small relative to the average expected execution time.

Server roles

An overview of the different server roles which can be recognized within a Content Manager installation

In a standard Content Manager installation some functionality relies on the combination of some components and configurations. The combination of components and configurations which provide a specific functionality are referenced as a "server role".

Web role

The web role provides all web endpoints like the web site, the web services and the internal security token service

The web role provides the following web endpoints

- `ISHCM` which is the Content Manager Web Client
- `ISHWS` which hosts all web services
- `ISHSTS` which is the internal Security Token Service

Since the `Web role` is required on every Content Manager installation, an out-of-the-box Content Manager installation will enable all web endpoints.

The `Web role` is used to serve external clients, but it is also used to serve the internal roles like the Translation role and the Default background task role. When it is used for external web endpoints, the `Web role` can be scaled out via Network Load Balancing (NLB).

Full text indexing role

This role groups everything for the full text search functionality by SolrLucene

The full text indexing role contains all components for the full text search functionality.

- The **Trisoft InfoShare SolrLucene** windows service that hosts and controls **SolrLucene**.
- The **Trisoft InfoShare Crawler** windows service that is responsible for gathering all data that needs to be indexed by **SolrLucene**.

How to enable the full text indexing role?

Execute the following steps in the described order to enable the full text indexing role:

- Goto **Start > Administrative Tools > Services**
- Goto the **Trisoft InfoShare SolrLucene** windows service
 - Open the **Properties**
 - Set the **Startup type** to *Automatic (Delayed Start)*
 - Click OK
 - Start the service
- Goto the **Trisoft InfoShare Crawler One** windows service
 - Open the **Properties**
 - Set the **Startup type** to *Automatic (Delayed Start)*
 - Click OK
 - Start the service
- If the server can handle more load, you can also start the **Trisoft InfoShare Crawler Two** windows service.

Remarks

We strongly advise you to allow only one deployment of this role per database. Typically this role is installed next to one of the Web roles, but it can also be a dedicated server.

Default background task role

This role provides everything which is necessary to execute all possible background tasks

The *default background task role* runs the **Trisoft InfoShare BackgroundTask** service configured with a role that contains all possible `eventTypes`.

Prerequisites

Out-of-the-box the **Trisoft InfoShare BackgroundTask One** service is configured with the **Default** role which contains all possible `eventTypes`. In this case, starting the **Trisoft InfoShare BackgroundTask One** service is enough to enable the default background task role.

However, using the following steps you can double check the configuration:

- Find the role which is used by the **Trisoft InfoShare BackgroundTask One** service
 - Goto **Start > Administrative Tools > Services**
 - Goto **Trisoft InfoShare BackgroundTask One** service
 - Click **Properties**
 - Check the value for **Path to executable**. The value should contain something like:

```
C:\InfoShare\App\BackgroundTask\Bin\BackgroundTask.exe --service
"Trisoft InfoShare BackgroundTask One" Default
```

The last parameter in the command line is the name of the service role. Out-of-the-box the role will be "Default".

- Check that the role contains all possible `eventTypes`.
 - Login to Content Manager Web Client as an administrator user.
 - Click **Settings > XML Background Task Settings**.
 - Find all `eventTypes` using `handlers/ handler/ @eventType`.
 - Goto the server definition with the role used by the service (e.g. "Default") and check that all `eventTypes` from the previous step are referenced in one of the groups. If necessary, add the missing `eventTypes`.

Note: If you had to change the configuration, you need to restart all **Trisoft InfoShare BackgroundTask** services on all servers.

Make sure that all required third-party software is installed and configured properly on this server, because if one of the dependencies is not present the background tasks will fail.

How to enable the default background task role?

Execute the following steps to enable the default background task role:

- Goto **Start > Administrative Tools > Services**
- Goto **Trisoft InfoShare BackgroundTask One** service
- Start the service

How to scale out?

There are 2 possibilities to scale out on the **Trisoft InfoShare BackgroundTask** service:

- Adding extra services with the same role
- Introducing specialized roles with a limited set of `eventTypes`.

Translation role

This role provides everything for the translation related functionality

The `Translation` role groups all components which are required for the translation related functionality:

- The **Trisoft InfoShare BackgroundTask One** service running with a role that minimally includes the following `eventTypes`:
 - `CREATETRANSLATIONFROMREPORT`
 - `CREATETRANSLATIONFROMLIST`
 - `CREATETRANSLATION`
 - `RELEASETRANSLATIONS`

These background tasks will create the necessary target language objects which can be used by the `TranslationBuilder` to be sent for translation

- The **Trisoft InfoShare TranslationBuilder One** service will group all language objects which needs to be translated for a specified translation job
- Finally, the **Trisoft InfoShare TranslationOrganizer One** service will
 - send the files to the configured translation service (SDL TMS, SDL WorldServer, ...)
 - retrieve the translated files back from the translation service (SDL TMS, SDL WorldServer, ...)
 - submit the translations back into the Content Manager repository

How to enable the translation role?

There are 2 possible scenario's for the translation role:

- Use the translation role on a dedicated translation server
- Use the translation role in combination with "Default background task role " on page 112

In the first scenario, you need to configure a new service role in **XML Background Task Settings**

1. Login to Content Manager Web Client as an administrator user
2. Click **Settings > XML Background Task Settings**.
3. Add an extra service definition with role `Translation`

```
<service role="Translation">
  <matrix>
    <group name="Translations" maxExecutions="2">
      <handlers>
        <add ref="CREATETRANSLATIONFROMREPORT" />
      </handlers>
    </group>
  </matrix>
</service>
```

```

    <add ref="CREATETRANSLATIONFROMLIST" />
    <add ref="CREATETRANSLATION" />
    <add ref="RELEASETRANSLATIONS" />
  </handlers>
</group>
</matrix>
<leaseRecovery isEnabled="true" interval="00:05:00" />
<poller isEnabled="true" interval="00:00:10" />
<aggregationRecovery isEnabled="true" gracePeriod="00:10:00" interval="
00:10:00" maximumRetries="3" />
</service>

```

4. Adapt **Trisoft InfoShare BackgroundTask One** service to use the role `Translation`.

For both scenario's you can now continue with the following steps:

1. Configure the **TranslationBuilder** and the **TranslationOrganizer**.
2. Start all services
 - Goto **Start > Administrative Tools > Services**
 - Start the **Trisoft InfoShare TranslationBuilder One** service
 - Start the **Trisoft InfoShare TranslationOrganizer One** service
 - Start the **Trisoft InfoShare BackgroundTask One** service (if it is not running already)

Publish role

This role is the sub set of the default background task role that is responsible for exporting and publishing.

The *publish role* runs the **Trisoft InfoShare BackgroundTask** service configured with a role that contains the following `eventTypes`

- PUBLISH
- PUBLISHDITADELIVERY
- PUBLISHCONTENTDELIVERY
- INBOXEXPORT
- REPORTEXPORT
- SEARCHEXPORT
- PUBLICATIONEXPORT

Prerequisites

Make sure that all required third-party software is installed and configured properly on this server, because if one of the dependencies is not present the background tasks will fail.

How to enable the publish role?

- Configure the role in **XML Background Task Settings**:
 1. Login to Content Manager Web Client as an administrator user.
 2. Click **Settings > XML Background Task Settings**.
 3. Add an extra service definition with role `Publish`:

```
<service role="Publish">
  <matrix>
    <group name="Export" maxExecutions="2">
      <handlers>
        <add ref="INBOXEXPORT" />
        <add ref="REPORTEEXPORT" />
        <add ref="SEARCHEXPORT" />
        <add ref="PUBLICATIONEXPORT" />
        <!-- New publish -->
        <add ref="PUBLISH" />
        <add ref="PUBLISHDITADELIVERY" />
        <add ref="PUBLISHCONTENTDELIVERY" />
        <!-- Legacy publish -->
        <add ref="EXPORTFORPUBLICATION" />
      </handlers>
    </group>
  </matrix>
  <leaseRecovery isEnabled="true" interval="00:05:00" />
  <poller isEnabled="true" interval="00:00:10" />
  <aggregationRecovery isEnabled="false" gracePeriod="00:10:00"
    interval="00:10:00" maximumRetries="3" />
</service>
```

- Create a **Trisoft InfoShare BackgroundTask** service with the role `Publish`.
- Start the service.

Best practices for creating a Trisoft InfoShare BackgroundTask service with a specific role

The topic described how to create a Trisoft InfoShare BackgroundTask service with a specific role

Of course, there are multiple ways to make a **Trisoft InfoShare BackgroundTask** service run with a specific role.

However, if possible try to create the **Trisoft InfoShare BackgroundTask** service immediately with the correct role configured by adapting the install plan.

If you want to adapt the role of an existing background task service after the installation, refer to the corresponding section in the documentation.

How to create a new BackgroundTask service with a role

This topic explains how to adapt the install plan to create a Trisoft InfoShare BackgroundTask service with the specified service role.

Before you begin

- There is no Content Manager installation yet.
- Check the name of the service role via **Settings > XML Background Task Settings**. If the name is `newServiceRole`, there should be a XML fragment like the following:

```
<service role="newServiceRole">
  <matrix>
    ...
  </matrix>
  <leaseRecovery isEnabled="true" interval="00:05:00" />
  <poller isEnabled="false" interval="00:00:10" />
  <aggregationRecovery isEnabled="false" gracePeriod="00:10:00" interval="00:10:00" maximumRetries="3" />
</service>
```

About this task

The following procedure describes how to adapt the out-of-the-box configuration of the Trisoft InfoShare BackgroundTask One windows service before installing. Of course, you can also add extra services by adapting the install plan.

Procedure

1. Open the install plan (`_InstallTool\installplan.xml`) from a Content Manager CD
2. Goto to the service definition for `Trisoft-InfoShare-BackgroundTask`

```
<serviceapp name="Trisoft-InfoShare-BackgroundTask">
  <servicename>Trisoft InfoShare##installtool:PROJECTSUFFIX##
  BackgroundTask One</servicename>
  <filepath>##installtool:APPPATH##\App##installtool:PROJECTSUFFIX##
  \BackgroundTask\Bin\BackgroundTask.exe --service "Trisoft
  InfoShare##installtool:PROJECTSUFFIX## BackgroundTask One" Default</
  filepath>
  ...
</serviceapp>
```

3. Replace the `Default` role with `newServiceRole`

```
<serviceapp name="Trisoft-InfoShare-BackgroundTask">
  <servicename>Trisoft InfoShare##installtool:PROJECTSUFFIX##
  BackgroundTask One</servicename>
  <filepath>##installtool:APPPATH##\App##installtool:PROJECTSUFFIX##
  \BackgroundTask\Bin\BackgroundTask.exe --service "Trisoft
  InfoShare##installtool:PROJECTSUFFIX## BackgroundTask One"
  newServiceRole</filepath>
  ...
</serviceapp>
```

4. Save the modified install plan

Results

An install plan that will install a Trisoft InfoShare BackgroundTask One windows service with the specified service role

How to adapt the role of an existing BackgroundTask service

This topic explains how to adapt the role of an existing Trisoft InfoShare BackgroundTask service.

Before you begin

Check the name of the service role via **Settings > XML Background Task Settings**.

If the name is `newServiceRole`, there should be a XML fragment like the following:

```
<service role="newServiceRole">
  <matrix>
    ...
  </matrix>
  <leaseRecovery isEnabled="true" interval="00:05:00" />
  <poller isEnabled="false" interval="00:00:10" />
  <aggregationRecovery isEnabled="false" gracePeriod="00:10:00" interval="00:10:00" maximumRetries="3" />
</service>
```

Warning: Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system.

Procedure

1. Modify the `Default` service role configured for the Trisoft InfoShare BackgroundTask One windows service.
 - a. Open the Registry Editor with Administrator rights.
 - b. Open the key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Trisoft InfoShare BackgroundTask One`.
 - c. Open the value with name `ImagePath`.
The current data looks like.

```
D:\InfoShare\App\BackgroundTask\Bin\BackgroundTask.exe --service
"Trisoft InfoShare BackgroundTask One" Default
```

where `Default` is the default service role name configured out-of-the-box and present in the XML Background Task Settings.

- d. Edit the data and change `Default` to the new service role name `newServiceRole`
The data should now look like.

```
D:\InfoShare\App\BackgroundTask\Bin\BackgroundTask.exe --service
"Trisoft InfoShare BackgroundTask One" newServiceRole
```

- e. Save the data.

At this point we have configured the Trisoft InfoShare BackgroundTask One windows

service to run with the `newServiceRole`.

2. Start the `Trisoft InfoShare BackgroundTask One` windows service

Firewalls and blocked ports

There is a variety of possibilities regarding network and firewall configurations. Only some of typical firewall configurations are described. A user knowledgeable about networking can infer the required ports and protocol settings needed for more complex configurations.

Note: The following description is intended to guide you in your network and firewall configuration. Its intention is not to be a complete how-to guide for setting up firewalls. Several settings are subject to change in newer software versions. Be certain to refer to the latest reference materials.

Network configuration using a single firewall

The first firewall is located between the Internet and the internal network

This is the first line of protection from the world wide web. All information passed through the Content Manager web sites or web services are based on the HTTPS protocol.

The techniques described in the section for HTTPS (SSL) could be required depending on the task of the Content Manager server.

Network configuration using two firewalls

The first firewall is located between the Internet and the DMZ as described above and the second is located between the DMZ and the intranet

The second line of protection protects servers which are open to the general public from the more critical company intranet servers. The zone between the first and second line of protection is also called the DMZ (DeMilitarized Zone).

The following techniques could be required depending on the task of the Content Manager server

- SMTP - when SMTP communication is required
- Database engines
 - Microsoft SQL Server access is required
 - Oracle RDBMs access is required
- HTTP(S)

SMTP

Ports and protocols used by the Simple Mail Transfer Protocol (SMTP).

Simple Mail Transfer Protocol (SMTP) is the standard for e-mail transmissions across the internet. Formally SMTP is defined in RFC 821 (STD 10) as amended by RFC 1123 (STD 3) chapter 5. The protocol used today is also known as ESMTP, and it is defined in RFC 2821.

Used by:

- Content Manager Publishing components
- Content Manager Author components

Settings:

What	Protocol	Port	Direction
SMTP	TCP	25	IN/OUT

For more information, refer to:

- <http://msdn2.microsoft.com/en-us/library/ms942998.aspx>
- <http://en.wikipedia.org/wiki/SMTP>

Microsoft SQL Server ports

Ports and protocols used by Microsoft SQL Server database engine (SQLServer).

About this task

Microsoft SQL Server is a relational database management system (RDBMS) produced by Microsoft. Its primary query language is Transact-SQL, an implementation of the ANSI/ISO standard Structured Query Language (SQL) which is used by Microsoft. You need to allow distant users to connect to the SQL server so they can address it their queries.

SQL Server is used by:

- Content Manager End User components;
- Content Manager Author components;
- Content Manager Database.

Note: The first step of this procedure is sufficient in most cases. Go through the other steps if you encounter any issue.

Procedure

1. Enable remote connections to your SQL Server.
 - a. Open **SQL Server Management Studio**.
 - b. Right-click your server's name and select **Properties**.
 - c. Tick the checkbox **Allow remote connections to this server**.
 - d. Select **OK**.

Microsoft SQL Server by default uses TCP 1433 but this can be changed using **SQL Server Enterprise Manager** or the database **Management Studio**.

2. Enable TCP/IP.
 - a. Open the **SQL Server Configuration Manager**.
 - b. In **SQL Server Network Configuration** select **Protocols for [yourServerInstance]**.
 - c. In the right-hand pane, make sure that **TCP/IP** is **Enabled**.
3. Open the 1433 port in your firewall.
 - a. In the **SQL Server Configuration Manager**, right-click **TCP/IP** and select **Properties**.
 - b. Select the **IP Addresses** tab and make sure the **TCP Port** for **IP1** is **1433**.
4. If you are using a named instance, create an extra rule in your firewall with the port 1434.

Note: For a named SQL Server instance (e.g. [yourServerInstance] \ SQL2012SP2), the firewall needs an extra rule on the UDP protocol with the specific port 1434. Without this rule the system will return the exception error: 26 - Error Locating Server/Instance Specified.

- a. Display the firewall advanced settings by navigating to **Control Panel > System and Security > Windows Firewall > Advanced settings**.
- b. Select **Inbound Rules** in the left-hand pane, then click **New Rule** in the right-hand pane.
- c. In the **New Inbound Rule Wizard, Rule Type step**, select **Port**.
- d. **Protocols and Ports** step, select **UDP** and set **Specific local ports** to **1434**.
- e. **Action** step, select **Allow the connection**.
- f. **Profile** step, tick the **Domain** checkbox.
- g. **Name** step, enter a name for this rule, e.g. **Named instance port 1434**.
- h. Select **Finish**.

What to do next

For more information, refer to:

- <http://support.microsoft.com/kb/287932>
- <http://msdn.microsoft.com/en-us/library/ms942998.aspx>

Oracle RDBMS

Ports and protocols used by the Oracle RDBMS.

Oracle Database, Oracle RDBMS, or simply Oracle is a relational database management system (RDBMS) software product released by Oracle Corporation that has become a major feature of database computing.

Used by:

- Content Manager End User components
- Content Manager Author components
- Content Manager Database

The Oracle database server communicates with the Content Manager application server using a port, so make sure this port is opened IN/OUT in your firewall. The port by default is 1521.

What	Protocol	Port	Direction
Listener (runs on the database server)	TCP	1521 (default)	IN/OUT

HTTPS (SSL)

Ports and protocols used by Microsoft Internet Information Server (IIS).

HTTPS is a URI scheme used to indicate a secure HTTP connection. It is syntactically identical to the `http://` scheme normally used for accessing resources using HTTP. The `https:` URL indicates that HTTP is to be used but with a different default TCP port (443) and an additional encryption/authentication layer between the HTTP and TCP.

HTTPS is not a separate protocol, but refers to the combination of a normal HTTP interaction over an encrypted Secure Sockets Layer (SSL). An `https:` URL may specify a TCP port. If it does not, the connection uses port 443.

Used by:

- Content Manager End User Website
- Content Manager Author Website
- Content Manager WebServices

Settings:

What	Protocol	Port	Direction
HTTPS	TCP	443	IN/OUT

For more information, refer to:

- <http://msdn2.microsoft.com/en-us/library/ms942998.aspx>

- <http://en.wikipedia.org/wiki/Https>

4

Troubleshooting Content Manager installation

Should you run into an installation issue, here are recommendations on how to deal with it.

Contacting customer support

This section contains information about where to go for additional information about the Content Manager product, what to do if you experience a problem with your system, and whom to call for service when necessary.

Diagnosing Problems

There are a number of ways you can help the Content Manager support team resolve your issue solved in an efficient way.

Introduction

- Make sure the defect isn't caused by an external cause: problems might be caused by reasons external to the application, for example, disk space not sufficient, controller error, network down, etc. Software issues can also be caused by incompatibilities among programs.
- Make sure the problem isn't caused by data issues: verify that the problem occurs for all sets of data, not just one specific data set.

Use Windows Event Viewer to discover External Failures

You can use the **Event Viewer** in Windows. **Event Viewer** maintains logs about program, security, and system events on your computer. You can use **Event Viewer** to view and manage the event logs, gather information about hardware and software problems, and monitor Windows security events.

To open **Event Viewer**, click **Start > Settings > Control Panel > Administrative Tools > Event Viewer**.

Providing Information

When entering issues, please describe the steps needed to reproduce the problem and provide other pertinent information.

When contacting support for Content Manager, please provide information about:

- The user interface in which the problem occurs
- The frequency with which the problem occurs
- The menus or dialog boxes you are using
- The specific elements or attributes that are causing problems
- Any error messages you are receiving
- Any screenshot that may help the support representative understand the problem

- A copy of the log file generated by your authoring tool, if you feel it is pertinent
- The GUID of the repository object that is causing problems,
- Whether the problem is preventing you from releasing crucial documentation
- Any other information which can help our support team replicate your problem

Log Files

Information in the log files is valuable to you and the Content Manager support team when investigating and troubleshooting issues.

Using log files

To use a log file most effectively, it is important that the log file only contains the information or steps necessary to reproduce the problem.

Procedure

1. Navigate to the folder that contains the log file.
2. Rename the most recent log file.
3. Repeat the steps needed to reproduce the problem. Since all actions from all users are logged in the same log file, this needs to be done as quickly as possible.
A new log file is generated which contains logging for steps needed to reproduce the problem.
4. Move the file to a subfolder or rename it by adding a bug tracker number or a short description of what you reproduced.

Results

Tip: If the system is used quite intensively by multiple users, try to do this during a time when activity is low (for instance, lunch or in the evening).

Note: Before repeating the steps, make sure that the log file will contain all necessary information by checking that the following registry settings contain the value `ALL`:

- HKLM\SOFTWARE\Wow6432Node\Trisoft\TriDK\TriDKApp\InfoShareAuthor\LogLevel
 - HKLM\SOFTWARE\Wow6432Node\Trisoft\TriDK\TriDKApp\InfoShareAuthor\LogLayer
-

Server Logs

Content Manager relies on third party software products such as Microsoft Server, Microsoft SQLServer, Oracle RDBMs, Java Runtime Environment, DITA-OpenToolkit, AntennaHouse XSLFormatter, and so on, which generate log files that are stored on the server.

Microsoft Windows logs

Applications and operating system components often make use of the **Event Viewer**. Event viewer is centralized log service to report events that have taken place such as a failure to start a component or complete an action.

To open Event Viewer: **Settings > Control Panel > Administrative Tools > Event Viewer**

Note: Although Content Manager has its own logging mechanism, it uses Event Viewer when there is limited or no free database space.

Content Manager COM+ logs

Typically, all components write to the log file specified in registry entry `FileName` or `LogFile` of the given application/TriDKApp name. When no application/TriDKApp name was provided for example, because the application is not yet initialized, the Core entry is used.

Log files are named using the following format: `InfoShareAuthor_yyyy_mm_dd.log` (for example, `InfoShareAuthor_2008_01_26.log`).

New log files are generated daily. When a log file exceeds 10MB, a new log file is generated and a time stamp is added to the original log file: e.g. `InfoShareAuthor_2008_01_26_20_52_25.log`.

Note: The Can Clean column specifies whether logging can be cleaned without locked-file problems.

Used by	Initialized	Location defined in	Can clean	Typical location
COM+ 'Trisoft-InfoShare-Author' (dllhost.exe)				
	No	HKLM\SOFTWARE\Wow6432Node\Trisoft\TriDK\FileName	Yes	C:\InfoShare\DataCore\Logs\TriDK.log
	Yes	HKLM\SOFTWARE\Wow6432Node\Trisoft\TriDK\TriDKApp\InfoShareAuthor\LogFile	Yes	C:\InfoShare\Data\Logs\InfoShareAuthor.log
cscript.exe C:\InfoShare\App\Utilities\PublishingService\Tools\Publish.wsf				
	N/A	Console	N/A	

Note: To reduce the logging on a production system, you can change the following registry settings:

- RegistrysettingHKLM\SOFTWARE\Wow6432Node\Trisoft\TriDK\TriDKApp\InfoShareAuthor\LogLevel from ALL to ERR, WRN, MES
- RegistrysettingHKLM\SOFTWARE\Wow6432Node\Trisoft\TriDK\TriDKApp\InfoShareAuthor\LogLayer from ALL to PUBL, PRES, APP

Content Manager .NET component logging

The following .NET components are driven through the NLog logging library and are configured with the NLog.config file located next the to hosting process.

Extra record with Application= "FontoXml.Apps.Review.exe", Is Nlog= "yes", Typical Configuration Path = "C:\InfoShare\App\Utilities\FontoReview\NLog.config", Initialized= NA, Typical Log File Path = "C:\InfoShare\Data\Logs\

FontoReviewORA19_pid4648_20191127.log"

Application	Is NLog	Typical Configuration Path relative to C:\InfoShare\	Initial	Typical Log File Path relative to C:\InfoShare\
Crawler.exe	Yes	App\Crawler\Bin\NLog.config	N/A	Data\Logs\InfoShareBuilders_pid2944_20130607.log
TrisoftSolrLucene	Yes	App\TrisoftSolrLucene\Bin\NLog.config	N/A	Data\Logs\TrisoftSolrLucene_pid7884.log
BackgroundTask	Yes	App\BackgroundTask\Bin\NLog.config	N/A	Data\Logs\BackgroundTask_pid14164_20190109.log Note: Contains entries from the BackgroundTask service components Data\Logs\BackgroundTask_pid14164_Execution_20190109.log Note: Contains entries from the executing handlers components
BackgroundTaskIso	Yes	App\BackgroundTask\Bin\NLog.config	N/A	Data\Logs\ BackgroundTaskIso_pid14165_Execution_20190109.log Note: Contains the logging of the background tasks using isolationLevel="Process". In the out-of-the-box configuration, it is only used for publishing actions.
Trisoft.InfoShare.Web	Yes	Web\Author\Asp\NLog.config	N/A	Data\Logs\Trisoft.InfoShare.Web_2013_06_17.log

Application	Is NLog	Typical Configuration Path relative to <i>C:\InfoShare\</i>	Initial Typical Log File Path relative to <i>C:\InfoShare\</i>
ISHWS	Yes	Web\InfoShareWS\NLog.config	N/A
PublishResult	Yes	App\Utilities\PublishResult\NLog.config	N/A
ISHSTS	Yes	Web\InfoShareSTS\NLog.config	N/A
TranslationBuilder	Yes	App\TranslationBuilder\Bin\NLog.config	N/A
TranslationOrganizer	Yes	App\TranslationOrganizer\Bin\NLog.config	N/A
SynchronizeToLiveContent	Yes	App\Utilities\SynchronizeToLiveContent\NLog.config	N/A
PublishService	Yes	App\Utilities\PublishingService\Tools\NLog.config	N/A
ISHCM	Yes	AppCore\Common\Configuration\NLog.config	No
			Yes
FontoXml.Apps.Review.exe	Yes	App\Utilities\FontoReview\NLog.config	N/A
InstallTool.exe	No	DefaultInstallToolLog in InstallTool.exe.config	N/A
DBUpgradeTool.exe	No	DefaultDBUpgradeToolLog in App\Setup\DBUpgradeTool\DBUpgradeTool.exe.config	N/A

Note: Modifications to the NLog configuration are immediately applied without the need to restart the hosting process.

Desktop Client Logs

Logs are produced for the Publication Manager, Condition Manager, Authoring Bridge, and Launcher and are stored in a log directory on the local client system.

Used by	Default location
Authoring Bridge	C:\Users\<user name>\AppData\Local\SDL\InfoShare Client\<version>\Log\Arbortext Editor Connector.log
	C:\Users\<user name>\AppData\Local\SDL\InfoShare Client\<version>\Log\Oxygen Connector.log
	C:\Users\<user name>\AppData\Local\SDL\InfoShare Client\<version>\Log\XMetaL Connector.log
Condition Manager	C:\Users\<user name>\AppData\Local\SDL\InfoShare Client\<version>\Log\Condition Manager.log
Content Importer	C:\Users\<user name>\AppData\Local\SDL\InfoShare Client\<version>\Log\Content Importer.log
Content Importer conversion	C:\Users\<user name>\AppData\Local\SDL\InfoShare Client\<version>\Log\Content Importer - Import Report.log
Launcher	C:\Users\<user name>\AppData\Local\SDL\InfoShare Client\<version>\Log\InfoShare Launcher.log
Publication Manager	C:\Users\<user name>\AppData\Local\SDL\InfoShare Client\<version>\Log\Publication Manager.log

The following example paths are part of the Client Tool installation:

1. The Authoring Bridge logging is located in the user directory: C:\Users\<user name>\AppData\Local\SDL\InfoShare Client\<version number>\Log.
For example: C:\Users\kcat\AppData\Local\SDL\InfoShare Client\12.0\Log
2. The synchronized application configuration (DTDs, Preview, Metadata,...) files are located in the user directory: C:\Users\<user name>\AppData\Local\SDL\InfoShare Client\<num>\Config.
For example: C:\Users\kcat\AppData\Local\SDL\InfoShare Client\0015454899\Config
3. The user data, such as temporary stored images or checked out objects, are stored in the user directory: C:\Users\<user name>\My Documents\SDL\InfoShare\<num>\Admin
For example: C:\Users\kcat\My Documents\SDL\InfoShare\0015454899\Admin

Note: In the examples above, <num> is 0015454899 which is a hashed version of the repository location, web services virtual directory name, and the application name. This was done to avoid file path issues since a Windows file path is limited to 260 characters. There is an informational folder created inside the cryptic number folder which indicates to which repository the stored information is related, for example: example.com_ISHWS_ISHCM

Logging Configuration

Default location:

The logging configuration file 'NLog.config' is, by default, located in the application's directory, for example: C:\Program Files\SDL\Publication Manager\14.0)

Log Level:

Available log levels are :

- Trace
- Debug
- Info
- Warn
- Error
- Fatal

By default, only `Fatal`, `Error`, and `Warning` messages are logged.

Change the log level to increase or change logging. For example, when you set the minimum level to `Trace`, all messages are logged.

Sample configuration file:

All messages, from any class in the application whose level is `Warn` or higher, that is, `Warn`, `Error`, and `Fatal`, are written to the file `C:\Users\Local Settings\Application Data\SDL\InfoShare Client\12.0\Log\Publication Manager.log`.

```
<nlog xmlns="http://www.nlog-project.org/schemas/NLog.xsd"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <include file="NLog.Include.ClientApplications.config"/>
  <targets>
    <target name="File"
      xsi:type="File"
      layout="${fileLayout}"
      fileName="${specialfolder:folder=LocalApplicationData}\SDL\InfoShare
Client\12.0\Log\Publication Manager.log"
      archiveAboveSize="2000000"
      maxArchiveFiles="3"
      archiveNumbering="Rolling"
      keepFileOpen="false"
    />
  </targets>
  <rules>
    <logger name="*" minLevel="Warn" writeTo="File"/>
  </rules>
</nlog>
```

To enable maximum logging, set the minimum level to `Trace`.

```
...
<logger name="*" minLevel="Trace" writeTo="File"/>
...
```

For more information about configuring logging, refer to the [NLog Configuration file](#).

Event Log content

The **Event Log** contains detailed information about all background processes. For example, it contains information about each step of the output generation, and contains warning and error information that can help you troubleshoot output generation failures.

Administrator users have access to event logs for warnings, failures, are in progress, or recently occurred. The event logs include information about:

- Translation Management
- Translation Jobs
- Lower-level Element Reuse
- Export
- Publish
- Synchronize with the delivery platform
- Thumbnails
- All Events

Information in the log files is valuable to your support team when investigating and troubleshooting issues. Copy the information and forward it with your issue report to your customer support representative when requesting assistance or reporting an issue.

Using the Event Log

Information in the event log helps you and SDL customer support, troubleshoot problems when encountered. Access information is provided to users with Administrator privileges.

Before you begin

Click the event log you want to view then, for more details on a particular event, click the **Event Type** in the right pane. The log is displayed in the bottom right pane. For additional information on a specific action in the log, click on the action in the bottom right pane.

Procedure

1. Login to the web client as a user with administrator privileges.
2. Click the **Event Log** tab.
3. Click the event or log file you want to display, from the left pane.
4. Click an option on the top right toolbar to:
 - **Show Recent** activities for the event; shows activities in the last 24 hours.
 - **Show Failed** logging messages for the event.
 - **Show Busy** events or events that are currently running.
 - **Show Warning** messages only for the event.
 - **Show All** activities for the event.
5. Click the **Event Type** for the event which you want to display additional information. To help find the event type, you can sort in descending or ascending order on any of the

fields by clicking on the field name. Additional information about the event type is displayed in the bottom right pane. In this pane you can:

- Click the toggle button for **Show Verbose - Hide Verbose** to show or hide verbose logging messages.
 - Click on the **CreationDate** of an **Action** to display additional information about the action. An Event Monitor Details window is displayed with additional information.
6. If the status was **Warning**, in the Event Monitor Details window you can:
- Click the toggle button for **List - Detail** in the bottom pane of the window to display or suppress additional messages.
 - **Download** the event details. You are prompted to **Save**, **Open**, or **Cancel**.
 - In list view, display the **Next** or **Previous** message.

Troubleshooting the database installation

When the database returns errors after creation or import, check the available corrective actions.

What to do if Oracle database import fails

If the import fails, you may want to remove the designated ISOURCE database user and all the objects it owns before you can try again.

Procedure

1. Start SQLPLUS /NOLOG from a shell where the ORACLE_SID and ORACLE_HOME variables are set correctly; at a command prompt type:

```
CONNECT SYS/CHANGE_ON_INSTALL AS SYSDBA
DROP USER ISOURCE CASCADE;
```

2. Recreate the ISOURCE user.

What to do in case of "ORA-12638" error

A freshly installed Oracle database sometimes results in ORA-12638 errors. If you are running a dedicated Content Manager Oracle server, you can resolve problems by altering the SQLNET.AUTHENTICATION_SERVICES setting.

Note: If you are not running a dedicated Content Manager Oracle server, contact your Oracle DBA.

1. Open Oracle file `\network\admin\sqlnet.ora`
2. Change the value of parameter **SQLNET.AUTHENTICATION_SERVICES** to **(none)**. This setting is instead of (NTS).

User is restricted or does not have permissions

Login errors can occur if a user restriction is set or the user does not have proper permissions.

Login time restriction

Login fails because there is a logon time restriction.

Problem

The user sees the following DCOM error:

```
Logon failure: account logon time restriction violation
```

Explanation

The **Logon hours** restriction is selected.

Resolution

Remove the **Logon hours** restriction.

User account restriction

Login fails with a user account restriction error.

Problem

The user sees the following error:

```
Logon failure: user account restriction
```

Explanation

The password has expired, or one of the following is selected:

- **Logon hours** restriction
- **Logon to** restriction
- **Account disabled**

Resolution

To resolve, depending on the cause (see explanation above):

- Change the password. Refer to information about the password or user name locations.
- Remove the **Logon hours** restriction.
- Remove the **Logon to** restriction.
- Re-enable the account.

User not granted requested logon type

Login fails because the user does not have requested login type.

Problem

The user sees the following DCOM error:

```
Logon failure: the user has not been granted the requested logon type at this computer
```

Explanation

The account has no **log on as service** permissions, or no **log on as batch job** on the computer.

Resolution

Provide the permissions.

The designated user is running the wrong (date) settings

The designated account is used to set some environment variables or settings. Most common is the Regional Options short date setting. A Windows operating system has two levels of environment variables: the system level and the user level. Know that user settings can override system settings.

System and user settings

An example of environment variables that may be set for both the system and user is the TEMP variable. TEMP may be set to `c:\TEMP\system` for the system, however, when the user SophieC logs in, it may be set to `c:\TEMP\SophieC`.

Other user specific settings such as the Regional Options, are stored in the registry. When a computer starts, the system defaults are loaded. The user level is only loaded upon request, for example, a login to a command prompt login.

The following contains information about user settings that may be helpful:

- The Microsoft knowledge base article **KB257757** describes server-side automation of Office
- The Microsoft knowledge base article **KB288367** describes how to run COM components under a specific user account.

Note: To access Microsoft knowledge base articles, go to the Microsoft support website and search for the article number(s): <http://search.microsoft.com/en-us/search.aspx>

Resolving certificate problems

Content Manager does not use certificates on a regular basis. It does however, test secure connections for regular web sites and web services.

Content Manager has an internal Certificate Authority (ADS01). It uses the certificates of this server to publish web sites to the world wide web. You must confirm that ADS01 is a trusted authority to use the certificate.

Accepting a certificate using a web browser

When browsing within one session of your browser, it is sufficient to accept the certificate provided from our internal certificate server (normally ADS01).

Problem

The user may see the following **Security Alert**:

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate. The security certification was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
Do you want to proceed?

Explanation

As noted, the security certification was issued by a company you have not chosen to trust.

Resolution Click **Yes** to continue with secure communication enabled.

Importing and accepting a certificate for a user

If a user imports the certificate, the user can trust the certificate and be able to connect to the publishing services.

Procedure

1. Double-click on the certificate file.
A Certificate Information window displays.
2. Click **Install Certificate**.
A Certificate Store window displays.
3. Select **Place all certificates in the following store**.
4. Confirm or if necessary, select by clicking the **Browse** button, the Certificate store: **Trusted Root Certificate Authorities**
5. Click **Next**.
A Security Warning window displays.
6. Click **Yes** to install the certificate.

Importing and accepting a certificate for a computer

If a certificate is imported for a computer system, the system can trust the certificate and be able to connect to the publishing services.

Procedure

1. Start the Microsoft Management Console by entering **mmc.exe** at a command prompt.
A Console Root window is displayed.
2. Click **File > Add/Remove Snap-in**
The Add/Remove Snap-in window displays with the Standalone tab selected.
3. Click **Add**.
An Add Standalone Snap-in window displays.
4. Select **Certificates** from the list of available standalone snap-ins, then click **Add**.
A Certificate snap-in window displays.
5. Select **Computer account** to be able to manage all computer account certificates.
6. Click **Next**.
7. Accept the default **Local Computer** and click **Finish**.

8. Click **Close** then **OK** to close the Add/Remove Snap-in window.
The Console Root window is again visible.
9. Under **Certificates (Local computer)**, right-click **Trusted Root Certification Authorities**
10. Click **All Tasks > Import**.
The Certificate Import Wizard window displays.
11. Click **Next**.
12. **Browse** to, and select the certificate (file) to install.
13. Click **Next**.
A Certificate Store window displays.
14. Select **Place all certificates in the following store**.
15. Confirm or if necessary, select by clicking the **Browse** button, the Certificate store: **Trusted Root Certificate Authorities**
16. Click **Next**.
17. Click **Yes** to install the certificate.

Troubleshooting the install tool

Error when running the install tool: RegAsm.exe - .NET Framework Initialization Error

If the Microsoft Server .Net 4.0 is not installed you get errors from InstallTool such as:

```
RegAsm.exe - .NET Framework Initialization Error
```

The NETFramework2010_4.0.30319_(dotNetF40_Full_x86_x64).exe tested with this version of Content Manager can be retrieved online from SDL upon request.

Troubleshooting the crawler service

If the crawler service does not run after the installation, you can unregister and register the crawler service to fix this issue.

Procedure

1. Login into the server as an Administrator user.
2. Run the following bat scripts:

```
<INFOSHARE>\App\Crawler\Configuration\UnregisterAllCrawlers.bat
```

```
<INFOSHARE>\App\Crawler\Configuration\RegisterThisCrawler.bat
```

