



Informatica® Test Data Management  
10.2.0 HotFix 2

# Installation Guide

© Copyright Informatica LLC 2003, 2019

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

Informatica, the Informatica logo, and PowerCenter are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at <https://www.informatica.com/trademarks.html>. Other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties, including without limitation: Copyright DataDirect Technologies. All rights reserved. Copyright © Sun Microsystems. All rights reserved. Copyright © RSA Security Inc. All Rights Reserved. Copyright © Ordinal Technology Corp. All rights reserved. Copyright © Aandacht c.v. All rights reserved. Copyright Genivia, Inc. All rights reserved. Copyright Isomorphic Software. All rights reserved. Copyright © Meta Integration Technology, Inc. All rights reserved. Copyright © Intalio. All rights reserved. Copyright © Oracle. All rights reserved. Copyright © Adobe Systems Incorporated. All rights reserved. Copyright © DataArt, Inc. All rights reserved. Copyright © ComponentSource. All rights reserved. Copyright © Microsoft Corporation. All rights reserved. Copyright © Rogue Wave Software, Inc. All rights reserved. Copyright © Teradata Corporation. All rights reserved. Copyright © Yahoo! Inc. All rights reserved. Copyright © Glyph & Cog, LLC. All rights reserved. Copyright © Thinkmap, Inc. All rights reserved. Copyright © Clearpace Software Limited. All rights reserved. Copyright © Information Builders, Inc. All rights reserved. Copyright © OSS Nokalva, Inc. All rights reserved. Copyright Edifecs, Inc. All rights reserved. Copyright Cleo Communications, Inc. All rights reserved. Copyright © International Organization for Standardization 1986. All rights reserved. Copyright © ej-technologies GmbH. All rights reserved. Copyright © Jaspersoft Corporation. All rights reserved. Copyright © International Business Machines Corporation. All rights reserved. Copyright © yWorks GmbH. All rights reserved. Copyright © Lucent Technologies. All rights reserved. Copyright © University of Toronto. All rights reserved. Copyright © Daniel Veillard. All rights reserved. Copyright © Unicode, Inc. Copyright IBM Corp. All rights reserved. Copyright © MicroQuill Software Publishing, Inc. All rights reserved. Copyright © PassMark Software Pty Ltd. All rights reserved. Copyright © LogiXML, Inc. All rights reserved. Copyright © 2003-2010 Lorenzi Davide, All rights reserved. Copyright © Red Hat, Inc. All rights reserved. Copyright © The Board of Trustees of the Leland Stanford Junior University. All rights reserved. Copyright © EMC Corporation. All rights reserved. Copyright © Flexera Software. All rights reserved. Copyright © Jinfonet Software. All rights reserved. Copyright © Apple Inc. All rights reserved. Copyright © Telerik Inc. All rights reserved. Copyright © BEA Systems. All rights reserved. Copyright © PDFlib GmbH. All rights reserved. Copyright © Orientation in Objects GmbH. All rights reserved. Copyright © Tanuki Software, Ltd. All rights reserved. Copyright © Ricebridge. All rights reserved. Copyright © Sencha, Inc. All rights reserved. Copyright © Scalable Systems, Inc. All rights reserved. Copyright © jQWidgets. All rights reserved. Copyright © Tableau Software, Inc. All rights reserved. Copyright © MaxMind, Inc. All Rights Reserved. Copyright © TMate Software s.r.o. All rights reserved. Copyright © MapR Technologies Inc. All rights reserved. Copyright © Amazon Corporate LLC. All rights reserved. Copyright © Highsoft. All rights reserved. Copyright © Python Software Foundation. All rights reserved. Copyright © BeOpen.com. All rights reserved. Copyright © CNRI. All rights reserved.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>), and/or other software which is licensed under various versions of the Apache License (the "License"). You may obtain a copy of these Licenses at <http://www.apache.org/licenses/>. Unless required by applicable law or agreed to in writing, software distributed under these Licenses is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the Licenses for the specific language governing permissions and limitations under the Licenses.

This product includes software which was developed by Mozilla (<http://www.mozilla.org/>), software copyright The JBoss Group, LLC, all rights reserved; software copyright © 1999-2006 by Bruno Lowagie and Paulo Soares and other software which is licensed under various versions of the GNU Lesser General Public License Agreement, which may be found at <http://www.gnu.org/licenses/lgpl.html>. The materials are provided free of charge by Informatica, "as-is", without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

The product includes ACE(TM) and TAO(TM) software copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (©) 1993-2006, all rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (copyright The OpenSSL Project. All Rights Reserved) and redistribution of this software is subject to terms available at <http://www.openssl.org> and <http://www.openssl.org/source/license.html>.

This product includes Curl software which is Copyright 1996-2013, Daniel Stenberg, <[daniel@haxx.se](mailto:daniel@haxx.se)>. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://curl.haxx.se/docs/copyright.html>. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

The product includes software copyright 2001-2005 (©) MetaStuff, Ltd. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://www.dom4j.org/license.html>.

This product includes software copyright © 1996-2006 Per Bothner. All rights reserved. Your right to use such materials is set forth in the license which may be found at <http://www.gnu.org/software/kawa/Software-License.html>.

This product includes OSSP UUID software which is Copyright © 2002 Ralf S. Engelschall, Copyright © 2002 The OSSP Project Copyright © 2002 Cable & Wireless Deutschland. Permissions and limitations regarding this software are subject to terms available at <http://www.opensource.org/licenses/mit-license.php>.

This product includes software developed by Boost (<http://www.boost.org/>) or under the Boost software license. Permissions and limitations regarding this software are subject to terms available at [http://www.boost.org/LICENSE\\_1\\_0.txt](http://www.boost.org/LICENSE_1_0.txt).

This product includes software copyright © 1997-2007 University of Cambridge. Permissions and limitations regarding this software are subject to terms available at <http://www.pcre.org/license.txt>.

This product includes software copyright © 2007 The Eclipse Foundation. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at <http://www.eclipse.org/org/documents/epl-v10.php> and at <http://www.eclipse.org/org/documents/edl-v10.php>.

This product includes software licensed under the terms at <http://www.tcl.tk/software/tcltk/license.html>, <http://www.bosrup.com/web/overlib/?License>, <http://www.stlport.org/doc/license.html>, <http://asm.ow2.org/license.html>, <http://www.cryptix.org/LICENSE.TXT>, <http://hsqldb.org/web/hsqldbLicense.html>, <http://httpunit.sourceforge.net/doc/license.html>, <http://jung.sourceforge.net/license.txt>, [http://www.gzip.org/zlib/zlib\\_license.html](http://www.gzip.org/zlib/zlib_license.html), <http://www.openldap.org/software/release/license.html>, <http://www.libssh2.org>, <http://slf4j.org/license.html>, <http://www.sente.ch/software/OpenSourceLicense.html>, <http://fusesource.com/downloads/license-agreements/fuse-message-broker-v-5-3-license-agreement>, <http://antlr.org/license.html>, <http://aopalliance.sourceforge.net/>, <http://www.bouncycastle.org/license.html>, <http://www.jgraph.com/jgraphdownload.html>, <http://www.jcraft.com/jsch/LICENSE.txt>, [http://jotm.objectweb.org/bsd\\_license.html](http://jotm.objectweb.org/bsd_license.html), <http://www.w3.org/Consortium/Legal/2002/copyright-software-20021231>, <http://www.slf4j.org/license.html>, <http://nanoxml.sourceforge.net/org/copyright.html>, <http://www.json.org/license.html>, <http://forge.ow2.org/projects/javaservice/>, <http://www.postgresql.org/about/license.html>, <http://www.sqlite.org/copyright.html>, <http://www.tcl.tk/software/tcltk/license.html>, <http://www.jaxen.org/faq.html>, <http://www.jdom.org/docs/faq.html>, <http://www.slf4j.org/license.html>, <http://www.iodbc.org/dataspace/iodbc/wiki/IODBC/License>, <http://www.keplerproject.org/md5/license.html>, <http://www.toedter.com/en/jcalendar/license.html>, <http://www.edankert.com/bounce/index.html>, <http://www.net-snmp.org/about/license.html>, <http://www.openmdx.org/#FAQ>, [http://www.php.net/license/3\\_01.txt](http://www.php.net/license/3_01.txt), <http://www.srp.stanford.edu/license.txt>, <http://www.schneider.com/blowfish.html>, <http://www.jmock.org/license.html>, <http://xsom.java.net>, <http://benalman.com/about/license/>, <https://github.com/CreateJS/EaselJS/blob/master/src/easeljs/display/Bitmap.js>, <http://www.h2database.com/html/license.html#summary>, <http://jsoncpp.sourceforge.net/LICENSE>, <http://jdbc.postgresql.org/license.html>, <http://protobuf.googlecode.com/svn/trunk/src/google/protobuf/descriptor.proto>, <https://github.com/rantav/hector/blob/master/LICENSE>, <http://web.mit.edu/Kerberos/krb5-current/doc/mitK5license.html>, <http://jibx.sourceforge.net/jibx-license.html>, <https://github.com/lyokato/libgeohash/blob/master/LICENSE>, <https://github.com/hjiang/jsonxx/blob/master/LICENSE>, <https://code.google.com/p/lz4/>, <https://github.com/jedisct1/libsodium/blob/master/>

LICENSE; <http://one-jar.sourceforge.net/index.php?page=documents&file=license>; <https://github.com/EsotericSoftware/kryo/blob/master/license.txt>; <http://www.scala-lang.org/license.html>; <https://github.com/tinkerpop/blueprints/blob/master/LICENSE.txt>; <http://gee.cs.oswego.edu/dl/classes/EDU/oswego/cs/dl/util/concurrent/intro.html>; <https://aws.amazon.com/asl/>; <https://github.com/twbs/bootstrap/blob/master/LICENSE>; <https://sourceforge.net/p/xmlunit/code/HEAD/tree/trunk/LICENSE.txt>; <https://github.com/documentcloud/underscore-contrib/blob/master/LICENSE>, and <https://github.com/apache/hbase/blob/master/LICENSE.txt>.

This product includes software licensed under the Academic Free License (<http://www.opensource.org/licenses/afl-3.0.php>), the Common Development and Distribution License (<http://www.opensource.org/licenses/cddl1.php>), the Common Public License (<http://www.opensource.org/licenses/cpl1.0.php>), the Sun Binary Code License Agreement Supplemental License Terms, the BSD License (<http://www.opensource.org/licenses/bsd-license.php>), the new BSD License (<http://opensource.org/licenses/BSD-3-Clause>), the MIT License (<http://www.opensource.org/licenses/mit-license.php>), the Artistic License (<http://www.opensource.org/licenses/artistic-license-1.0>) and the Initial Developer's Public License Version 1.0 (<http://www.firebirdsql.org/en/initial-developer-s-public-license-version-1-0/>).

This product includes software copyright © 2003-2006 Joe Walnes, 2006-2007 XStream Committers. All rights reserved. Permissions and limitations regarding this software are subject to terms available at <http://xstream.codehaus.org/license.html>. This product includes software developed by the Indiana University Extreme! Lab. For further information please visit <http://www.extreme.indiana.edu/>.

This product includes software Copyright (c) 2013 Frank Balluffi and Markus Moeller. All rights reserved. Permissions and limitations regarding this software are subject to terms of the MIT license.

See patents at <https://www.informatica.com/legal/patents.html>.

DISCLAIMER: Informatica LLC provides this documentation "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of noninfringement, merchantability, or use for a particular purpose. Informatica LLC does not warrant that this software or documentation is error free. The information provided in this software or documentation may include technical inaccuracies or typographical errors. The information in this software and documentation is subject to change at any time without notice.

#### NOTICES

This Informatica product (the "Software") includes certain drivers (the "DataDirect Drivers") from DataDirect Technologies, an operating company of Progress Software Corporation ("DataDirect") which are subject to the following terms and conditions:

1. THE DATADIRECT DRIVERS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at [info\\_documentation@informatica.com](mailto:info_documentation@informatica.com).

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2019-05-14

# Table of Contents

<b>Preface .....</b>	<b>8</b>
Informatica Resources. ....	8
Informatica Network. ....	8
Informatica Knowledge Base. ....	8
Informatica Documentation. ....	8
Informatica Product Availability Matrices. ....	9
Informatica Velocity. ....	9
Informatica Marketplace. ....	9
Informatica Global Customer Support. ....	9
 <b>Chapter 1: Test Data Management Installation Overview.....</b>	<b>10</b>
Installation Overview. ....	10
Test Data Management Installation. ....	10
Rules and Guidelines for Multinode Installations. ....	11
 <b>Chapter 2: Before You Install TDM.....</b>	<b>13</b>
Before You Install TDM on UNIX. ....	13
Read the Release Notes. ....	13
Verify the License Key. ....	14
Verify the Minimum System Requirements. ....	14
Verify the Status of the Informatica Domain. ....	15
Set the Environment Variables. ....	15
Determine Port Availability . ....	16
Set Up a Keystore File. ....	16
Set Up the X Window Server. ....	18
Extract the Installer Files on UNIX. ....	18
Before You Install TDM on Windows. ....	19
Read the Release Notes. ....	19
Verify the License Key. ....	19
Verify the Minimum System Requirements. ....	19
Verify the Status of the Informatica Domain. ....	20
Set the Environment Variables. ....	21
Determine Port Availability . ....	21
Set Up a Keystore File. ....	21
Extracting the Installer Files on Windows. ....	23
Repository Database Requirements. ....	23
Verify the Database Requirements for the TDM Repository. ....	24
Set Up the TDM Repository Database. ....	24
Verify the Database Requirements for the Test Data Warehouse. ....	27
Set up the Test Data Warehouse. ....	27

<b>Chapter 3: Create the Application Services.....</b>	<b>31</b>
Create the Application Services Overview. . . . .	31
Prepare Databases for the Informatica Domain. . . . .	32
Model Repository Database Requirements. . . . .	32
PowerCenter Repository Database Requirements. . . . .	34
Profiling Warehouse Requirements. . . . .	36
Create and Configure the PowerCenter Repository Service. . . . .	37
Create the PowerCenter Repository Service. . . . .	37
After You Create the PowerCenter Repository Service. . . . .	39
Create and Configure the PowerCenter Integration Service. . . . .	40
Create the PowerCenter Integration Service. . . . .	41
Create and Configure the Model Repository Service. . . . .	42
Create the Model Repository Service. . . . .	42
Create and Configure the Data Integration Service. . . . .	45
Create the Data Integration Service. . . . .	45
Create and Configure the Analyst Service. . . . .	48
Create the Analyst Service. . . . .	48
Install the Informatica Client. . . . .	51
Verify Installation Requirements. . . . .	51
PowerCenter Client Requirements. . . . .	51
Installing in Graphical Mode. . . . .	52
Installing in Silent Mode. . . . .	53
Starting the PowerCenter Client. . . . .	54
 <b>Chapter 4: TDM Installation.....</b>	 <b>55</b>
TDM Installation Overview. . . . .	55
Installing in Graphical Mode. . . . .	55
Installing in Console Mode. . . . .	56
Installing in Silent Mode. . . . .	57
Creating the Properties File. . . . .	57
Running the Silent Installer. . . . .	58
 <b>Chapter 5: After You Install TDM.....</b>	 <b>59</b>
After You Install TDM Overview. . . . .	59
Verify File Permissions. . . . .	60
Verify the Services and Objects in the Informatica Domain. . . . .	60
Create and Configure the Test Data Warehouse Service. . . . .	61
Test Data Warehouse Service Dependencies. . . . .	62
Creating the Test Data Warehouse Service. . . . .	62
Create and Configure the Test Data Manager Service. . . . .	65
Test Data Manager Service Dependencies. . . . .	65
Creating the Test Data Manager Service. . . . .	66

Editing the Test Data Manager Service. . . . .	69
Test Data Manager Service Logs. . . . .	70
Configure the Informatica Services Machine for Kerberos-Enabled Hadoop HDFS Connections. . . .	71
Configure the Test Data Management Machine for Format Preserving Encryption Masking. . . . .	72
Third-Party JAR Files. . . . .	72
Storage Tables for Repeatable Masking. . . . .	73
Creating the Storage Tables. . . . .	74
<b>Chapter 6: Infacmd. . . . .</b>	<b>75</b>
infacmd Overview. . . . .	75
infacmd tdm Command Reference. . . . .	75
CreateService. . . . .	75
CreateContents. . . . .	82
EnableService. . . . .	83
DisableService. . . . .	84
removeService. . . . .	85
infacmd tdw Command Reference. . . . .	86
CreateService. . . . .	87
CreateContents. . . . .	92
infacmd isp Commands for the Test Data Warehouse Service. . . . .	93
EnableService. . . . .	93
DisableService. . . . .	95
RemoveService. . . . .	96
<b>Chapter 7: Starting and Stopping Informatica and TDM. . . . .</b>	<b>99</b>
Starting and Stopping Informatica and TDM Overview. . . . .	99
Starting and Stopping Informatica. . . . .	100
Starting and Stopping Informatica on UNIX. . . . .	100
Starting and Stopping Informatica on Windows. . . . .	100
Configuring the Informatica Windows Service. . . . .	101
Log In to Informatica Administrator. . . . .	102
Starting and Stopping the TDM Server. . . . .	102
Logging in to Test Data Manager. . . . .	102
<b>Chapter 8: Uninstallation. . . . .</b>	<b>104</b>
Uninstallation Overview. . . . .	104
Rules and Guidelines for Uninstallation. . . . .	104
Before You Uninstall. . . . .	104
Uninstalling TDM. . . . .	104
<b>Appendix A: Updating the DynamicSections Parameter of a DB2 Database. . . . .</b>	<b>106</b>
DynamicSections Parameter Overview. . . . .	106
Setting the DynamicSections Parameter. . . . .	106

Downloading and Installing the DDconnect JDBC Utility . . . . .	106
Running the Test for JDBC Tool . . . . .	107
<b>Index. . . . .</b>	<b>108</b>

# Preface

The Informatica *Test Data Management Installation Guide* is written for the system administrator who is responsible for installing Test Data Management. This guide assumes that you have knowledge of relational database concepts and are familiar with the relational database systems and other file systems in your environment. This guide also assumes that you are familiar with the operating systems in your environment.

## Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

### Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit <https://network.informatica.com>.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

### Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit <https://search.informatica.com>. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at [KB\\_Feedback@informatica.com](mailto:KB_Feedback@informatica.com).

### Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit <https://docs.informatica.com>.



Informatica maintains documentation for many products on the Informatica Knowledge Base in addition to the Documentation Portal. If you cannot find documentation for your product or product version on the Documentation Portal, search the Knowledge Base at <https://search.informatica.com>.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at [infa\\_documentation@informatica.com](mailto:infa_documentation@informatica.com).

## Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at <https://network.informatica.com/community/informatica-network/product-availability-matrices>.

## Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at <http://velocity.informatica.com>. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at [ips@informatica.com](mailto:ips@informatica.com).

## Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at <https://marketplace.informatica.com>.

## Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:

<https://www.informatica.com/services-and-training/customer-success-services/contact-us.html>.

To find online support resources on the Informatica Network, visit <https://network.informatica.com> and select the eSupport option.

# CHAPTER 1

## Test Data Management Installation Overview

This chapter includes the following topics:

- [Installation Overview, 10](#)
- [Test Data Management Installation, 10](#)
- [Rules and Guidelines for Multinode Installations, 11](#)

### Installation Overview

Use the TDM installer to install Test Data Management.

You must have installed Informatica before you install Test Data Management. Run the installer to install Test Data Management on an existing Informatica domain and node. When you run the Test Data Management installer, you can choose to install in graphical or console mode.

### Test Data Management Installation

You can install Test Data Management on a machine that hosts an Informatica node.

Test Data Management runs on the node within the Informatica domain.

The Informatica domain must have Informatica services that you can use to run Test Data Management processes.

**Note:** If no instance of Informatica exists, you must install Informatica before you install Test Data Management. See the Informatica *Installation and Configuration Guide* for information.

#### RELATED TOPICS:

- [“Before You Install TDM” on page 13](#)
- [“TDM Installation” on page 55](#)
- [“After You Install TDM” on page 59](#)

# Rules and Guidelines for Multinode Installations

You can install TDM on more than one machine in an Informatica domain that has a master gateway node and nodes.

Read the following rules and guidelines and understand the limitations before you install TDM in a multinode setup:

## General

- The Test Data Manager Service connects to a PowerCenter® Integration Service in the domain. The nodes on which you create the Test Data Manager Service and the PowerCenter Integration Service must be on the same operating system. Create both nodes on the same operating system to link the paths to run workflows.
- If multiple nodes connect to a single PowerCenter Repository Service, use different folder names as work areas for each node.
- If you use parameters to enter the connection information in a plan, the parameter file must be present on the node on which the Test Data Manager Service runs. The file must be in the same directory path on both nodes.
- You can create a TDM multinode setup in a Kerberos environment.

## Installation and Upgrade

- Install TDM on the master gateway node first.
- You must install TDM on the master node even if you do not create a Test Data Manager Service on the master node. You cannot install TDM and create the Test Data Manager Service on other nodes without installing TDM on the master node.
- When you create a Test Data Manager Service on a node that is not a master node, it is recommended to retain the default Test Data Manager Server Configuration settings and the Advanced Properties.
- You must install TDM on each node on which you create a Test Data Manager Service.
- You must install a single TDM version on all nodes in the domain.
- After you create the Test Data Manager Service, log in to Test Data Manager and verify the default staging connection on each node. You must use different connection names on each node. Use the default TDM\_CONNECTION only on one node.
- The PowerCenter Integration Service creates temporary cache files on the node where you run a TDM workflow. The cache files must be available to the PowerCenter Integration Service for the workflow to run. If you configure the Test Data Manager Service and the PowerCenter Integration Service on different nodes, you must configure the TDM cache directory inside an `infa_shared` directory. The `infa_shared` directory must be accessible to all nodes that the Test Data Manager Service and the PowerCenter Integration Service use. Configure the TDM cache directory from the **Workflow Generation** tab in the **Administrator | Preferences** view in Test Data Manager.
- Configure a different cache directory within the `infa_shared` directory for each node on which you create a Test Data Manager Service. TDM generates temporary folders with the plan name in the cache directory. The plan names might conflict with plans created on other nodes.
- It is recommended that you install TDM in the same directory structure on all nodes if you configure the Test Data Manager Service and PowerCenter Integration Service on different nodes. This is because TDM workflows that you run from a specific node use the scripts in the `<Informatica installation directory>\TDM\utilities` directory with the absolute path as set in TDM.

- If you install Informatica services in a different directory structure on each node on Windows, create a soft link on the node with the PowerCenter Integration Service. The soft link must allow the node with the PowerCenter Integration Service to access the cache folder on the node that generates the workflow.
- If you install Informatica services in a different directory structure on each node on Linux, you must mount the directories. Users must have read, write, and execute permission on the mounted directories.

### Connection Sharing

Multiple nodes can connect to a single Model Repository Service, but the connections are not shared across the nodes. Changes to connections on one node do not impact other nodes.

### Restrictions

- The Test Data Manager Service cannot connect to a PowerCenter Integration Service or a Data Integration Service that runs on a grid.
- Failover and recovery are not available with the Test Data Manager Service.
- You can install TDM in HTTPS mode only on a master node.

## CHAPTER 2

# Before You Install TDM

This chapter includes the following topics:

- [Before You Install TDM on UNIX, 13](#)
- [Before You Install TDM on Windows, 19](#)
- [Repository Database Requirements, 23](#)

## Before You Install TDM on UNIX

You can install TDM on UNIX.

Before you start the installation, set up the machine to meet the requirements to install and run TDM. If the machine where you install TDM is not configured correctly, the installation can fail.

Before you install on UNIX, complete the following tasks:

- Read the Release Notes.
- Verify the license key.
- Verify the system requirements.
- Set up the required environment variables.
- Verify the status of the Informatica Domain.
- Determine the availability of ports for TDM.
- Optionally, set up a keystore file for a secure connection.
- Set up the X Window server.
- Extract the installer files.

### Read the Release Notes

Before you install or upgrade, read the product Release Notes. The Release Notes contain important information about the product installation and upgrade process. The Release Notes also contain information about known and fixed limitations.

## Verify the License Key

The TDM installation requires a license key.

Before you install TDM to work with an existing instance of Informatica, verify that you have a license key for TDM available. The license key allows you to create the Test Data Manager Service to run the TDM Server and Test Data Manager and create repositories within an Informatica domain.

You can get the license key in one of the following ways:

- Installation DVD. If you receive the Informatica installation files in a DVD, the license key file is included in the Informatica License Key CD.
- FTP download. If you download the Informatica installation files from the Informatica Electronic Software Download (ESD) site, the license key is in an email message from Informatica. Copy the license key file to a directory accessible to the user account that installs the product.

Contact Informatica Global Customer Support if you do not have the required license key.

## Verify the Minimum System Requirements

TDM works with Informatica services and repositories in the Informatica domain. The machine where you install TDM must contain an Informatica node and must meet minimum system requirements.

For more information about product requirements and supported platforms, see the Product Availability Matrix on Informatica Network:

<https://network.informatica.com/community/informatica-network/product-availability-matrices>

### Minimum System Requirements for TDM

You install TDM on a machine that hosts an Informatica node. The machine must meet the memory and disk space requirements for TDM.

The following table lists the minimum requirements for TDM:

Component	RAM	Disk Space
TDM Server	4 GB	7 GB

### Temporary Disk Space Requirements for Installation

The installer writes temporary files to the hard disk. Verify that you have enough available disk space on the machine to support the installation. When the installation completes, the installer deletes the temporary files and releases the disk space.

The following table lists the temporary disk space requirements during installation:

Product	Disk Space
Installer	1 GB
Test Data Management	2 GB

## Verify the Status of the Informatica Domain

When you install TDM, you must join an Informatica domain. TDM uses the services, databases, and connections that you configure in the Informatica domain. The domain must have the required application services and repositories to support TDM.

Verify the status of the Informatica domain and the application services in the domain that you plan to join.

Before you start the TDM installation, perform the following tasks:

- Verify the Informatica version installed on the machine where you plan to install TDM. The TDM version that you install must work with the Informatica version installed. For information about installing Informatica, see the Informatica *Installation and Configuration Guide*.
- Install required domain patches and libraries. For information about the required domain patches and libraries, see the *Informatica Release Notes*.
- Verify that the Informatica domain has the following application services:
  - PowerCenter Repository Service.
  - PowerCenter Integration Service.
  - Model Repository Service.
  - Data Integration Service. If you want to perform data discovery, verify that the Data Integration Service is configured to connect to a profiling warehouse.
  - Analyst Service. Required if you want to link TDM global objects with terms in the Business Glossary.

## Set the Environment Variables

Set the required environment variables to work with the TDM installation.

The following table describes the environment variables to review or set on UNIX:

Variable	Description
IATEMPDIR	Location of the temporary files created during installation. Configure the environment variable if you do not want to create temporary files in the /tmp directory.
JAVA_HOME	Set the JAVA_HOME environment variable to the root of the JDK directory.
INFA_HOME	Set the INFA_HOME environment variable to the root of the Informatica installation directory.
INFA_JDK_HOME	Location of the directory that contains the supported Java Development Kit (JDK). Set the INFA_JDK_HOME environment variable if you are installing on AIX, HP-UX, or z/Linux.  In the configuration file for your shell, for example the .bashrc file, set the INFA_JDK_HOME environment variable to the directory that contains the JDK. Verify that the login shell can access the INFA_JDK_HOME environment variable.
LANG and LC_ALL	Change the locale to set the appropriate character encoding for the terminal session. For example, set the encoding to <code>Latin1</code> or <code>ISO-8859-1</code> for French, <code>EUC-JP</code> or <code>Shift JIS</code> for Japanese, or <code>UTF-8</code> for Chinese or Korean. The character encoding determines the types of characters that appear in the UNIX terminal.

## Determine Port Availability

The installer sets up the ports for the TDM connections.

You can specify the port numbers to use or you can use the default port numbers assigned by the installer. Verify that the port numbers are available on the machine where you install TDM.

The following table describes the ports that are used by TDM:

Port Type	Description
Startup port	Port number that controls the server startup for TDM. The TDM Server listens for startup commands on this port. Default is 6605.
Shutdown port	Port number that controls the server shutdown for TDM. The TDM Server listens for shutdown commands on this port. Default is 6607.
JMX port	Port number for the JMX/RMI connections to TDM. Default is 6675.
HTTPS port	Port number to use when secure connection is enabled for TDM. Default is 6643.

## Set Up a Keystore File

You can optionally set up a secure connection to the TDM Server.

You can also choose to set up a secure connection to the test data warehouse.

When you configure the Test Data Manager Service, you can configure secure communication between Test Data Manager and the TDM Server. Set up a keystore file and provide the location of the file when you create the Test Data Manager Service to create a secure connection.

When you configure the Test Data Warehouse Service, you can configure secure communication between Test Data Manager and the test data warehouse. Set up a keystore file and provide the location of the file when you create the Test Data Warehouse Service to create a secure connection.

To create the required files, you can use the following programs:

### **keytool**

You can use keytool to create an SSL certificate or a Certificate Signing Request (CSR) as well as keystores and truststores in JKS format.

For more information about using keytool, see the documentation on the following web site:  
<http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>.

### **OpenSSL**

You can use OpenSSL to create an SSL certificate or CSR as well as convert a keystore in JKS format to PEM format.

For more information about OpenSSL, see the documentation on the following website:  
<https://www.openssl.org/docs/>

For a higher level of security, send your CSR to a Certificate Authority (CA) to get a signed certificate.

The software available for download at the referenced links belongs to a third party or third parties, not Informatica LLC. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.



## Secure Communication Within the Informatica Domain

Before you enable secure communication within the Informatica domain, verify that the following requirements are met:

**You created a certificate signing request (CSR) and private key.**

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

**You have a signed SSL certificate.**

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

**You imported the certificate into keystores.**

You must have a keystore in PEM format named `infa_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

The keystore files must contain the root and intermediate SSL certificates.

**Note:** The password for the keystore in JKS format must be the same as the private key pass phrase used to generate the SSL certificate.

**You imported the certificate into truststores.**

You must have a truststore in PEM format named `infa_truststore.pem` and a truststore in JKS format named `infa_truststore.jks`.

The truststore files must contain the root, intermediate, and end user SSL certificates.

**The keystores and truststores are in the correct directory.**

The keystore and truststore must be in a directory that is accessible to the installer.

For more information about how to create a custom keystore and truststore, see the Informatica How-To Library article "How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain": <https://kb.informatica.com/h2l/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf>

## Secure Connection to Test Data Manager

Before you secure the connection to Test Data Manager, verify that the following requirements are met:

**You created a certificate signing request (CSR) and private key.**

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

**You have a signed SSL certificate.**

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

**You imported the certificate into a keystore in JKS format.**

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

**The keystore is in the correct directory.**

The keystore must be in a directory that is accessible to the installer.

## Set Up the X Window Server

To run the installer in graphical mode, use a graphics display server. If you are logged in remotely to a UNIX machine, you can use an X Window server to redirect the graphics display to your local host.

If you do not have a display device installed on the machine where you want to install the product, you can run the installer by using an X Window server installed on another machine. Use the DISPLAY variable to redirect output of the X Window to another machine that has X Window and xterm installed.

The following table lists the commands to set the DISPLAY environment variable:

Shell	Command
C	setenv DISPLAY <host name>:0
Bash/Korn	export DISPLAY=<host name>:0
Bourne	DISPLAY=<host name>:0 export display

If you do not know the host name of the machine that has the X Window server that you want to use, ask your network administrator. You can also use the IP address of the machine. For more information about redirecting the DISPLAY variable, see the documentation from the UNIX or X Window vendor.

If the X Window server does not support the font that the installer uses, the installer displays the labels on the buttons incorrectly.

## Extract the Installer Files on UNIX

Before you perform the installation, extract the installer files on the UNIX machine. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on install.sh.

The installer files are compressed and distributed as a tar file. Use a native tar or GNU tar utility to extract the installer files to a directory on the UNIX machine. For example,

```
tar -xvf <filename.tar>
```

You can extract the installer files in the following ways:

- Installation DVD. Download the Informatica tar file from the installation DVD to a directory on your machine and then extract the installer files, or extract the installer files directly from the DVD to a directory on your machine.
- FTP download. Download the Informatica installation tar file from the Informatica Electronic Software Download site to a directory on your machine and then extract the installer files.

**Note:** If you extract the tar file on Windows and then copy the installer files to UNIX, the installation can fail.

# Before You Install TDM on Windows

You can install TDM on Windows. Before you install TDM, set up the machine to meet the requirements to install and run TDM.

If the machine where you install the TDM is not configured correctly, the installation can fail.

Before you install TDM on Windows, complete the following tasks:

- Read the Release Notes.
- Verify the license key.
- Verify the system requirements.
- Verify the status of the Informatica domain.
- Set up the required environment variables.
- Determine the availability of ports for TDM.
- Optionally, set up a keystore file for a secure connection.
- Extract the installer files.

## Read the Release Notes

Before you install or upgrade, read the product Release Notes. The Release Notes contain important information about the product installation and upgrade process. The Release Notes also contain information about known and fixed limitations.

## Verify the License Key

The TDM installation requires a license key.

Before you install TDM to work with an existing instance of Informatica, verify that you have a license key for TDM available. The license key allows you to create the Test Data Manager Service to run the TDM Server and Test Data Manager and create repositories within an Informatica domain.

You can get the license key in one of the following ways:

- Installation DVD. If you receive the Informatica installation files in a DVD, the license key file is included in the Informatica License Key CD.
- FTP download. If you download the Informatica installation files from the Informatica Electronic Software Download (ESD) site, the license key is in an email message from Informatica. Copy the license key file to a directory accessible to the user account that installs the product.

Contact Informatica Global Customer Support if you do not have the required license key.

## Verify the Minimum System Requirements

TDM works with Informatica services and repositories in the Informatica domain. The machine where you install TDM must contain an Informatica node and must meet minimum system requirements.

For more information about product requirements and supported platforms, see the Product Availability Matrix on Informatica Network:

<https://network.informatica.com/community/informatica-network/product-availability-matrices>

## Minimum System Requirements for TDM

You install TDM on a machine that hosts an Informatica node. The machine must meet the memory and disk space requirements for TDM.

The following table lists the minimum requirements for TDM:

Component	RAM	Disk Space
TDM Server	4 GB	7 GB

## Temporary Disk Space Requirements for Installation

The installer writes temporary files to the hard disk. Verify that you have enough available disk space on the machine to support the installation. When the installation completes, the installer deletes the temporary files and releases the disk space.

The following table lists the temporary disk space requirements during installation:

Product	Disk Space
Installer	1 GB
Test Data Management	2 GB

## Verify the Status of the Informatica Domain

When you install TDM, you must join an Informatica domain. TDM uses the services, databases, and connections that you configure in the Informatica domain. The domain must have the required application services and repositories to support TDM.

Verify the status of the Informatica domain and the application services in the domain that you plan to join.

Before you start the TDM installation, perform the following tasks:

- Verify the Informatica version installed on the machine where you plan to install TDM. The TDM version that you install must work with the Informatica version installed. For information about installing Informatica, see the Informatica *Installation and Configuration Guide*.
- Install required domain patches and libraries. For information about the required domain patches and libraries, see the *Informatica Release Notes*.
- Verify that the Informatica domain has the following application services:
  - PowerCenter Repository Service.
  - PowerCenter Integration Service.
  - Model Repository Service.
  - Data Integration Service. If you want to perform data discovery, verify that the Data Integration Service is configured to connect to a profiling warehouse.
  - Analyst Service. Required if you want to link TDM global objects with terms in the Business Glossary.

## Set the Environment Variables

Set environment variables to work with the TDM installation.

The following table describes the environment variables to review or set on Windows:

Variable	Description
IATEMPDIR	Location of the temporary files created during installation. Configure the environment variable if you do not want to create temporary files in the /tmp directory.
JAVA_HOME	Set the JAVA_HOME environment variable to the root of the JDK directory.
INFA_HOME	Set the INFA_HOME environment variable to the root of the Informatica installation directory.

## Determine Port Availability

The installer sets up the ports for the TDM connections.

You can specify the port numbers to use or you can use the default port numbers assigned by the installer. Verify that the port numbers are available on the machine where you install TDM.

The following table describes the ports that are used by TDM:

Port Type	Description
Startup port	Port number that controls the server startup for TDM. The TDM Server listens for startup commands on this port. Default is 6605.
Shutdown port	Port number that controls the server shutdown for TDM. The TDM Server listens for shutdown commands on this port. Default is 6607.
JMX port	Port number for the JMX/RMI connections to TDM. Default is 6675.
HTTPS port	Port number to use when secure connection is enabled for TDM. Default is 6643.

## Set Up a Keystore File

You can optionally set up a secure connection to the TDM Server.

You can also choose to set up a secure connection to the test data warehouse.

When you configure the Test Data Manager Service, you can configure secure communication between Test Data Manager and the TDM Server. Set up a keystore file and provide the location of the file when you create the Test Data Manager Service to create a secure connection.

When you configure the Test Data Warehouse Service, you can configure secure communication between Test Data Manager and the test data warehouse. Set up a keystore file and provide the location of the file when you create the Test Data Warehouse Service to create a secure connection.

To create the required files, you can use the following programs:

## keytool

You can use keytool to create an SSL certificate or a Certificate Signing Request (CSR) as well as keystores and truststores in JKS format.

For more information about using keytool, see the documentation on the following web site:  
<http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html>.

## OpenSSL

You can use OpenSSL to create an SSL certificate or CSR as well as convert a keystore in JKS format to PEM format.

For more information about OpenSSL, see the documentation on the following website:  
<https://www.openssl.org/docs/>

For a higher level of security, send your CSR to a Certificate Authority (CA) to get a signed certificate.

The software available for download at the referenced links belongs to a third party or third parties, not Informatica LLC. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.

## Secure Communication Within the Informatica Domain

Before you enable secure communication within the Informatica domain, verify that the following requirements are met:

### You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.  
If you use RSA encryption, you must use more than 512 bits.

### You have a signed SSL certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

### You imported the certificate into keystores.

You must have a keystore in PEM format named `infa_keystore.pem` and a keystore in JKS format named `infa_keystore.jks`.

The keystore files must contain the root and intermediate SSL certificates.

**Note:** The password for the keystore in JKS format must be the same as the private key pass phrase used to generate the SSL certificate.

### You imported the certificate into truststores.

You must have a truststore in PEM format named `infa_truststore.pem` and a truststore in JKS format named `infa_truststore.jks`.

The truststore files must contain the root, intermediate, and end user SSL certificates.

### The keystores and truststores are in the correct directory.

The keystore and truststore must be in a directory that is accessible to the installer.

For more information about how to create a custom keystore and truststore, see the Informatica How-To Library article "How to Create Keystore and Truststore Files for Secure Communication in the Informatica Domain": <https://kb.informatica.com/h2l/HowTo%20Library/1/0700-CreateKeystoresAndTruststores-H2L.pdf>

## Secure Connection to Test Data Manager

Before you secure the connection to Test Data Manager, verify that the following requirements are met:

**You created a certificate signing request (CSR) and private key.**

You can use keytool or OpenSSL to create the CSR and private key.

If you use RSA encryption, you must use more than 512 bits.

**You have a signed SSL certificate.**

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

**You imported the certificate into a keystore in JKS format.**

A keystore must contain only one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

If you use the installer-generated SSL certificate for the Administrator tool, you do not need to import the certificate into a keystore in JKS format.

**The keystore is in the correct directory.**

The keystore must be in a directory that is accessible to the installer.

## Extracting the Installer Files on Windows

The installer files are compressed and distributed as a zip file. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on install.bat.

You can extract the installer files in the following ways:

- Installation DVD. Download the Informatica zip file from the installation DVD to a directory on your machine and then extract the installer files, or extract the installer files directly from the DVD to a directory on your machine. If you download the zip file to a directory on your machine, verify the length of the entire installation directory path, including the zip file name, is 60 characters or less.
- FTP download. Download the Informatica installation zip file from the Informatica Electronic Software Download (ESD) site to a directory on your machine and then extract the installer files.

## Repository Database Requirements

The TDM Server stores configuration and process information in the TDM repository. You must set up the database for the TDM repository before installation. You specify the database connection when you create the Test Data Manager Service.

Before you install TDM, complete the following database setup tasks:

- Verify the database requirements.
- Set up the database.

## Verify the Database Requirements for the TDM Repository

Before you start the installation process, verify that the database server has adequate disk space for the TDM repository.

The following table describes the database requirement for the TDM repository:

Informatica Component	Database Type	Disk Space	Comments
TDM repository	IBM DB2 UDB Microsoft SQL Server Oracle <b>Note:</b> On a Microsoft SQL Server database, you must set the collation to case insensitive on the database.	35 MB	Set up the database before you create the Test Data Manager Service. Allocate more space based on the number of objects you plan to store.

After you install TDM, verify that the Informatica domain contains the repositories required to use TDM. If the domain does not contain a PowerCenter repository, you must create the repository in the Informatica domain. You must set up the database for the repository before you create the PowerCenter Repository Service.

If you have the Data Discovery option, you must create a Model repository and profiling warehouse in the Informatica domain. You must set up the databases before you create the Model Repository Service and Data Integration Service.

The following table describes the requirements for the repository databases:

Informatica Component	Database Type	Disk Space	Comments
PowerCenter repository	IBM DB2 UDB Microsoft SQL Server Oracle Sybase ASE	35 MB	Set up the database before you create the PowerCenter Repository Service. Allocate more space based on the number of repository objects you plan to store.
Model repository	IBM DB2 UDB Microsoft SQL Server Oracle	200 MB	Set up the database before you create the Model Repository Service. Allocate more space based on the number of repository objects you plan to store.
Profiling warehouse	IBM DB2 UDB Microsoft SQL Server Oracle	35 MB	Set up the database before you create the Data Integration Service.

## Set Up the TDM Repository Database

Before you start the installation process, set up a database and user account for the TDM repository.

When you create the Test Data Manager Service, you provide the database and user account information to create the TDM repository. The service uses JDBC to connect to the database and create the repository.

You can create the TDM repository in one of the following databases:

- Oracle



- IBM DB2
- Microsoft SQL Server

Use the following rules and guidelines when you set up the database and user account for the TDM repository:

- The database must be accessible to the gateway nodes in the Informatica domain.
- To prevent database errors from affecting other repositories, create the TDM repository in a separate database schema and with a separate database user account.

See the required Database Requirements sections for information on specific database requirements. For more information about configuring the database, see the documentation for your database system.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:

CREATE SESSION

CREATE TABLE

CREATE VIEW

- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Set the system temporary tablespace to 32k bytes.
- If the repository is in an IBM DB2 database, verify that IBM DB2 Version 10.5 is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
  - DB2\_SKIPINSERTED
  - DB2\_EVALUNCOMMITTED
  - DB2\_SKIPDELETED
  - AUTO\_RUNSTATS
- On the database, set the configuration parameters.

The following table lists the configuration parameters that you must set:

Parameter	Value
logfilsiz	8000
maxlocks	98

Parameter	Value
locklist	50000
auto_stmt_stats	ON

Parameter	Value
applheapsz	8192
appl_ctl_heap_sz	8192
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.

In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

In a multi-partition database, specify a tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.

- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.

The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

For more information about updating the DynamicSections parameter, see [Appendix A, "Updating the DynamicSections Parameter of a DB2 Database" on page 106](#).

## Microsoft SQL Server Database Requirements (TDM)

You must set the collation to *case insensitive* on the database.

Use the following guidelines when you set up the repository:

- Set the allow snapshot isolation and read committed isolation level to ALLOW\_SNAPSHOT\_ISOLATION and READ\_COMMITTED\_SNAPSHOT to minimize locking contention.

To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

## Verify the Database Requirements for the Test Data Warehouse

If you create and store data sets in the test data warehouse, you must create a test data warehouse repository and a test data warehouse in Test Data Manager.

Set up the databases before you create the Test Data Warehouse Service.

The following table describes the requirements for the databases:

Component	Database Type	Disk Space	Comments
Test data warehouse repository	IBM DB2 Microsoft SQL Server Oracle	35 MB	Set up the database before you create the Test Data Warehouse Service. Allocate more space based on the number of objects you plan to store.
Test data warehouse	Oracle PostgreSQL <b>Note:</b> The TDM installer includes a PostgreSQL installer that you can use to create the database. The installer is available in the following location in the TDM installer files: <TDM installer directory>\Postgres_installer\ 	35 MB	Set up the database before you create the Test Data Warehouse Service. Allocate more space based on the number of objects you plan to store.

## Set up the Test Data Warehouse

Before you create a test data warehouse, you must configure relational databases for the test data warehouse repository and the test data warehouse.

The test data warehouse repository is a relational database that stores the source table metadata and the TDM metadata that you create when you create a data set.

You can create a test data warehouse repository in the following databases:

- IBM DB2 UDB
- Microsoft SQL Server

- Oracle

The test data warehouse is a relational database that stores the source data that you include in a data set.

You can create a test data warehouse in the following databases:

- Oracle
- PostgreSQL

For more information about configuring the database, see the documentation for your database system.

## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Set the system temporary tablespace to 32k bytes.
- If the repository is in an IBM DB2 database, verify that IBM DB2 Version 10.5 is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
  - DB2\_SKIPINSERTED
  - DB2\_EVALUNCOMMITTED
  - DB2\_SKIPDELETED
  - AUTO\_RUNSTATS
- On the database, set the configuration parameters.

The following table lists the configuration parameters that you must set:

Parameter	Value
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

Parameter	Value
applheapsz	8192
appl_ctl_heap_sz	8192
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.

In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

In a multi-partition database, specify a tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.

- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.

The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

For more information about updating the DynamicSections parameter, see [Appendix A, "Updating the DynamicSections Parameter of a DB2 Database" on page 106](#).

## Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- Specify the database schema name when you use Microsoft SQL Server as the Model Repository database.
- Set the allow snapshot isolation and read committed isolation level to ALLOW\_SNAPSHOT\_ISOLATION and READ\_COMMITTED\_SNAPSHOT to minimize locking contention.  
To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:

```
CREATE SESSION
```

```
CREATE TABLE
```

```
CREATE VIEW
```

- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

## PostgreSQL Database for Test Data Warehouse

You can create a test data warehouse on a PostgreSQL database.

Read the following rules and guidelines before you create a test data warehouse on a PostgreSQL database:

- The PostgreSQL database installer is bundled with the TDM installer. Use the installer available with the TDM installer to create the database.
- You must use the same PostgreSQL database and user to create two connections in Test Data Manager.
  - Use the PostgreSQL database to create an ODBC connection.
  - Use the same PostgreSQL database and database user to create a JDBC connection.
- You use the connections when you create the Test Data Warehouse Service in Informatica Administrator. Enter the following properties in the Step 3 - Test Data Warehouse Properties dialog box:
  - Enter a name and description.
  - Select ODBC from the **Connection Type** list.
  - Choose the ODBC connection that you created as the **Target Connection**.
  - Choose PostgreSQL from the **Connection Database Type** list.
  - In the **JDBC Connection for ODBC** field, select the JDBC connection that you created. TDM uses the connection in workflows with tasks that require a JDBC connection string.

For information about configuring the database, see the documentation for the database system.

## CHAPTER 3

# Create the Application Services

This chapter includes the following topics:

- [Create the Application Services Overview, 31](#)
- [Prepare Databases for the Informatica Domain, 32](#)
- [Create and Configure the PowerCenter Repository Service, 37](#)
- [Create and Configure the PowerCenter Integration Service, 40](#)
- [Create and Configure the Model Repository Service, 42](#)
- [Create and Configure the Data Integration Service, 45](#)
- [Create and Configure the Analyst Service, 48](#)
- [Install the Informatica Client, 51](#)

## Create the Application Services Overview

Use the Administrator tool to create the application services in the required order.

Before you create the application services, you must prepare the following databases:

- Model repository database
- PowerCenter repository database
- Profiling warehouse

You must create the following application services:

- PowerCenter Repository Service
- PowerCenter Integration Service
- Model Repository Service
- Data Integration Service
- Analyst Service

# Prepare Databases for the Informatica Domain

Informatica stores data and metadata in repositories in the domain. Before you create the application services, set up the databases and database user accounts for the repositories.

Set up a database and user account for the following repositories:

- Model repository
- PowerCenter repository
- Profiling warehouse

To prepare the databases, verify the database requirements and set up the database. The database requirements depend on the application services that you create in the domain and the number of data integration objects that you build and store in the repositories.

## Model Repository Database Requirements

Informatica services and clients store data and metadata in the Model repository. Configure a separate Model repository to store monitoring statistics. Before you create the Model Repository Service, set up a database and database user account for the Model repository.

The Model repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle

Allow 3 GB of disk space for DB2. Allow 200 MB of disk space for all other database types.

For more information about configuring the database, see the documentation for your database system.

## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- Specify the tablespace name when you use IBM DB2 as the Model Repository database.
- If the repository is in an IBM DB2 database, verify that IBM DB2 Version 10.5 is installed.
- On the IBM DB2 instance where you create the database, set the following parameters to ON:
  - DB2\_SKIPINSERTED
  - DB2\_EVALUNCOMMITTED
  - DB2\_SKIPDELETED
  - AUTO\_RUNSTATS
- On the database, set the configuration parameters.



The following table lists the configuration parameters that you must set:

Parameter	Value
logfilsiz	8000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Set the tablespace pageSize parameter to 32768 bytes.

In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

In a multi-partition database, specify a tablespace that meets the pageSize requirements. Define the tablespace in the catalog partition of the database.

- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.
- Verify that the database user has CREATETAB, CONNECT, and BINDADD privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- In the DataDirect Connect for JDBC utility, update the DynamicSections parameter to 3000.

The default value for DynamicSections is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000. If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica services.

For more information about updating the DynamicSections parameter, see [Appendix A, "Updating the DynamicSections Parameter of a DB2 Database" on page 106](#).

## Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- Set the allow snapshot isolation and read committed isolation level to ALLOW\_SNAPSHOT\_ISOLATION and READ\_COMMITTED\_SNAPSHOT to minimize locking contention.

To set the isolation level for the database, run the following commands:

```
ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
```

```
ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
```

To verify that the isolation level for the database is correct, run the following commands:

```
SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
```

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
```

- The database user account must have the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Set the OPEN\_CURSORS parameter to 4000 or higher.  
Verify that the database user has the following privileges:
  - CREATE SEQUENCE
  - CREATE SESSION
  - CREATE SYNONYM
  - CREATE TABLE
  - CREATE VIEW
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

## PowerCenter Repository Database Requirements

A PowerCenter repository is a collection of database tables containing metadata. A PowerCenter Repository Service manages the repository and performs all metadata transactions between the repository database and repository clients.

The PowerCenter repository supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle
- Sybase ASE

Allow 35 MB of disk space for the database.

**Note:** Ensure that you install the database client on the machine on which you want to run the PowerCenter Repository Service.

For more information about configuring the database, see the documentation for your database system.

## IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- To optimize repository performance, set up the database with the tablespace on a single node. When the tablespace is on one node, PowerCenter Client and PowerCenter Integration Service access the repository faster than if the repository tables exist on different database nodes.  
Specify the single-node tablespace name when you create, copy, or restore a repository. If you do not specify the tablespace name, DB2 uses the default tablespace.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.

## Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.

- Verify that the database user account has the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Set the storage size for the tablespace to a small number to prevent the repository from using an excessive amount of space. Also verify that the default tablespace for the user that owns the repository tables is set to a small size.

The following example shows how to set the recommended storage parameter for a tablespace named REPOSITORY:

```
ALTER TABLESPACE "REPOSITORY" DEFAULT STORAGE ( INITIAL 10K NEXT 10K MAXEXTENTS
UNLIMITED PCTINCREASE 50 );
```

Verify or change the storage parameter for a tablespace before you create the repository.

- Verify that the database user has the following privileges:

```
CREATE SEQUENCE
CREATE SESSION
CREATE SYNONYM
CREATE TABLE
CREATE VIEW
```

- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

## Sybase ASE Database Requirements

Use the following guidelines when you set up the repository on Sybase ASE:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.
- Set the Sybase database option "ddl in tran" to TRUE.
- Set "allow nulls by default" to TRUE.
- Verify the database user has CREATE TABLE and CREATE VIEW privileges.
- Set the database memory configuration requirements.

The following table lists the memory configuration requirements and the recommended baseline values:

Database Configuration	Sybase System Procedure	Value
Number of open objects	sp_configure "number of open objects"	5000
Number of open indexes	sp_configure "number of open indexes"	5000
Number of open partitions	sp_configure "number of open partitions"	8000
Number of locks	sp_configure "number of locks"	100000

## Profiling Warehouse Requirements

The profiling warehouse database stores profiling and scorecard results. You specify the profiling warehouse connection when you create the Data Integration Service.

The profiling warehouse supports the following database types:

- IBM DB2 UDB
- Microsoft SQL Server
- Microsoft Azure SQL Database
- Oracle

Allow 10 GB of disk space for the database.

**Note:** Ensure that you install the database client on the machine on which you want to run the Data Integration Service. You can specify a JDBC connection or Hive connection as a profiling warehouse connection for IBM DB2 UDB, Microsoft SQL Server, and Oracle database types.

For more information about configuring the database, see the documentation for your database system.

### IBM DB2 Database Requirements

Use the following guidelines when you set up the repository on IBM DB2:

- The database user account must have the CREATETAB, CONNECT, CREATE VIEW, and CREATE FUNCTION privileges.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.
- Set the tablespace pageSize parameter to 32768 bytes.
- Set the NPAGES parameter to at least 5000. The NPAGES parameter determines the number of pages in the tablespace.

**Note:** Informatica does not support the partitioned database environment for IBM DB2 databases when you use a JDBC connection as the profiling warehouse connection.

### Microsoft SQL Server Database Requirements

Use the following guidelines when you set up the repository:

- The database user account must have the CONNECT, CREATE TABLE, CREATE VIEW, and CREATE FUNCTION privileges.

## Oracle Database Requirements

Use the following guidelines when you set up the repository on Oracle:

- Verify that the database user has the following privileges:
  - ALTER TABLE
  - CREATE ANY INDEX
  - CREATE PROCEDURE
  - CREATE SESSION
  - CREATE TABLE
  - CREATE VIEW
  - DROP TABLE
  - UPDATE TABLE
- Informatica does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.
- Set the tablespace parameter.
- Set the following parameters to the Informatica recommended values:

Parameter	Recommended Value
open_cursors	3000
Sessions	1000
Processes	1000

## Create and Configure the PowerCenter Repository Service

The PowerCenter Repository Service is an application service that manages the PowerCenter repository. The PowerCenter repository stores metadata created by the PowerCenter Client and application services in a relational database.

When you access a PowerCenter repository object from the PowerCenter Client or the PowerCenter Integration Service, the client or service sends a request to the PowerCenter Repository Service. The PowerCenter Repository Service process fetches, inserts, and updates metadata in the PowerCenter repository database tables.

### Create the PowerCenter Repository Service

Use the service creation wizard in the Administrator tool to create the service.

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > PowerCenter Repository Service**.  
The **New PowerCenter Repository Service** dialog box appears.

- On the **New PowerCenter Repository Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
Primary Node	If your license includes high availability, node on which the service runs by default. Required if you select a license that includes high availability.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.

- Click **Next**.  
The **New PowerCenter Repository Service - Step 2 of 2** page appears.
- Enter the following properties for the PowerCenter repository database:

Property	Description
Database Type	The type of the repository database.
Username	The database user name for the repository.
Password	Password for the PowerCenter repository database user. Must be in 7-bit ASCII.
Connection String	Native connection string the PowerCenter Repository Service uses to access the repository database. Use the following native connect string syntax for each supported database: - servername@databasename for Microsoft SQL Server and Sybase. - databasename.world for Oracle. - databasename for IBM DB2.
Code Page	Repository database code page. The PowerCenter Repository Service uses the character set encoded in the database code page to write data. You cannot change the code page in the PowerCenter Repository Service properties after you create the PowerCenter Repository Service.
Tablespace Name	Name of the tablespace in which to create all the repository database tables. You cannot use spaces in the tablespace name. Available for IBM DB2 and Sybase databases. To improve repository performance on IBM DB2 EEE repositories, specify a tablespace name with one node.

- Select **No content exists under specified connection string. Create new content**.

7. Optionally, choose to create a global repository.  
After you create the service, you can promote a local repository to a global repository, but you cannot change a global repository to a local repository.
8. If your license has the team-based development option, you can optionally enable version control of the repository.  
After you create the service, you can convert a non-versioned repository to a versioned repository, but you cannot convert a versioned repository to a non-versioned repository.
9. Click **Finish**.  
The domain creates the PowerCenter Repository Service, starts the service, and creates content for the PowerCenter repository.

After you create the service through the wizard, you can edit the properties or configure other properties.

## After You Create the PowerCenter Repository Service

After you create the PowerCenter Repository Service, perform the following tasks:

- Configure the PowerCenter Repository Service to run in the Normal mode.
- Create the PowerCenter repository user if the domain does not use Kerberos authentication.
- Create other application services.

### Run the PowerCenter Repository Service in Normal Mode

After you create the PowerCenter Repository Service, it starts in exclusive mode and access is restricted to the administrator. Edit the service properties to run the service in normal operating mode to provide access to other users.

1. In the Administrator tool, click the **Manage** tab.
2. In the Navigator, select the PowerCenter Repository Service.
3. Click **Properties**.
4. Click **Edit Repository Properties**.
5. In the **Operating Mode** field, select Normal.
6. Click **OK**.  
You must recycle the PowerCenter Repository Service for the changes to take effect.
7. Select **Actions > Recycle Service**.

### Create the PowerCenter Repository User

If the domain does not use Kerberos authentication, the domain uses a user account to authenticate other application services that make requests to the PowerCenter Repository Service. You must create a user account and assign the user the Administrator role for the PowerCenter Repository Service.

When you create an application service that depends on the PowerCenter Repository Service, you provide the name of the PowerCenter Repository Service and of this PowerCenter repository user.

1. In the Administrator tool, click the **Security** tab.
2. On the Security Actions menu, click **Create User** to create a native user account.  
**Note:** If you set up LDAP authentication in the domain, you can use an LDAP user account for the PowerCenter repository user.

3. Enter the following properties for the user:

Property	Description
Login Name	Login name for the user account. The login name for a user account must be unique within the security domain to which it belongs.  The name is not case sensitive and cannot exceed 128 characters. It cannot include a tab, newline character, or the following special characters: , + " \ < > ; / * % ? &  The name can include an ASCII space character except for the first and last character. All other space characters are not allowed.
Password	Password for the user account. The password can be from 1 through 80 characters long.
Confirm Password	Enter the password again to confirm. You must retype the password. Do not copy and paste the password.
Full Name	Full name for the user account. The full name cannot include the following special characters: < > "
Description	Description of the user account. The description cannot exceed 765 characters or include the following special characters: < > "

4. Click **OK**.  
The user properties appear.
5. Click the **Privileges** tab.
6. Click **Edit**.  
The **Edit Roles and Privileges** dialog box appears.
7. On the **Roles** tab, expand the PowerCenter Repository Service.
8. Under **System Defined Roles**, select Administrator and click **OK**.

## Create and Configure the PowerCenter Integration Service

The PowerCenter Integration Service is an application service that runs workflows and sessions for the PowerCenter Client.

When you run a workflow in the PowerCenter Client, the client sends the requests to the PowerCenter Integration Service. The PowerCenter Integration Service connects to the PowerCenter Repository Service to fetch metadata from the PowerCenter repository, and then runs and monitors the sessions and workflows.



## Create the PowerCenter Integration Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the PowerCenter Integration Service, verify that you created and enabled the PowerCenter Repository Service. If the domain does not use Kerberos authentication, verify that you created a PowerCenter repository user that the PowerCenter Integration Service can use to access the PowerCenter Repository Service.

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > PowerCenter Integration Service**.

The **New PowerCenter Integration Service** dialog box appears.

3. On the **New PowerCenter Integration Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
Assign	Select <b>Node</b> to configure the service to run on a node. If your license includes grid, you can create a grid and assign the service to run on the grid after you create the service.
Primary Node	If your license includes high availability, node on which the service runs by default. Required if you select a license that includes high availability.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.

4. Click **Next**.
5. On the **New PowerCenter Integration Service - Step 2 of 2** page, enter the following properties:

Property	Description
PowerCenter Repository Service	PowerCenter Repository Service you want to associate with the service.
Username	User name that the service uses to access the PowerCenter Repository Service. Enter the PowerCenter repository user that you created. Required when you associate a PowerCenter Repository Service with the service. Not available for a domain with Kerberos authentication.

Property	Description
Password	Password associated with the PowerCenter repository user. Not available for a domain with Kerberos authentication.
Security Domain	LDAP security domain for the PowerCenter repository user. The <b>Security Domain</b> field appears when the Informatica domain contains an LDAP security domain. Required when you associate a PowerCenter Repository Service with the service. Not available for a domain with Kerberos authentication.

6. Select the data movement mode that determines how the PowerCenter Integration Service handles character data. Choose ASCII or Unicode. Default is ASCII.  
  
In ASCII mode, the PowerCenter Integration Service recognizes 7-bit ASCII and EBCDIC characters and stores each character in a single byte. In Unicode mode, the PowerCenter Integration Service recognizes multibyte character sets as defined by the supported code pages. Use Unicode mode when the sources or targets use 8-bit or multibyte character sets and contain character data.
7. Click **Finish**.
8. On the **Specify Code Pages** dialog box, assign a code page for the PowerCenter Integration Service.  
  
The code page for the PowerCenter Integration Service must be compatible with the code page of the associated repository.
9. Click **OK**.  
  
The domain creates the PowerCenter Integration Service. The domain does not enable the PowerCenter Integration Service during the service creation process.
10. To enable the PowerCenter Integration Service, select the service in the Navigator, and click **Actions > Enable Service**. The PowerCenter Repository Service must be running to enable the PowerCenter Integration Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

## Create and Configure the Model Repository Service

The Model Repository Service is an application service that manages the Model repository. The Model repository stores metadata created by Informatica clients and application services in a relational database to enable collaboration among the clients and services.

When you access a Model repository object from the Developer tool, the Analyst tool, the Administrator tool, or the Data Integration Service, the client or service sends a request to the Model Repository Service. The Model Repository Service process fetches, inserts, and updates the metadata in the Model repository database tables.

### Create the Model Repository Service

Use the service creation wizard in the Administrator tool to create the service.

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > Model Repository Service**.  
  
The **New Model Repository Service** dialog box appears.

3. On the **New Model Repository Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) ] [
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.

4. Click **Next**.  
The **New Model Repository Service - Step 2 of 2** page appears.
5. Enter the following properties for the Model repository database:

Property	Description
Database Type	The type of the repository database.
Username	The database user name for the repository.
Password	Repository database password for the database user.
Database Schema	Available for Microsoft SQL Server. Name of the schema that will contain Model repository tables.
Database Tablespace	Available for IBM DB2. Name of the tablespace in which to create the tables. For a multi-partition IBM DB2 database, the tablespace must span a single node and a single partition.

6. Enter the JDBC connection string that the service uses to connect to the Model repository database.

Use the following syntax for the connection string for the selected database type:

Database Type	Connection String Syntax
IBM DB2	<code>jdbc:informatica:db2:// &lt;host_name&gt;:&lt;port_number&gt;;DatabaseName=&lt;database_name&gt;;BatchPerformanceWorkaround=true;DynamicSections=3000</code>
Microsoft SQL Server	<ul style="list-style-type: none"> <li>- Microsoft SQL Server that uses the default instance <code>jdbc:informatica:sqlserver:// &lt;host_name&gt;:&lt;port_number&gt;;DatabaseName=&lt;database_name&gt;;SnapshotSerializable=true</code></li> <li>- Microsoft SQL Server that uses a named instance <code>jdbc:informatica:sqlserver://&lt;host_name&gt; \&lt;named_instance_name&gt;;DatabaseName=&lt;database_name&gt;;SnapshotSerializable=true</code></li> </ul>
Oracle	<code>jdbc:informatica:oracle:// &lt;host_name&gt;:&lt;port_number&gt;;SID=&lt;database_name&gt;;MaxPooledStatements=20;CatalogOptions=0;BatchPerformanceWorkaround=true</code>

7. If the Model repository database is secured with the SSL protocol, you must enter the secure database parameters in the **Secure JDBC Parameters** field.

Enter the parameters as `name=value` pairs separated by semicolon characters (;). For example:

```
param1=value1;param2=value2
```

Enter the following secure database parameters:

Secure Database Parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. This parameter must be set to <code>SSL</code> .
ValidateServerCertificate	<p>Optional. Indicates whether Informatica validates the certificate that the database server sends.</p> <p>If this parameter is set to <code>True</code>, Informatica validates the certificate that the database server sends. If you specify the <code>HostNameInCertificate</code> parameter, Informatica also validates the host name in the certificate.</p> <p>If this parameter is set to <code>False</code>, Informatica does not validate the certificate that the database server sends. Informatica ignores any truststore information that you specify.</p>
HostNameInCertificate	Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the SSL certificate.
cryptoProtocolVersion	Required. Specifies the cryptographic protocol to use to connect to a secure database. You can set the parameter to <code>cryptoProtocolVersion=TLSv1.1</code> or <code>cryptoProtocolVersion=TLSv1.2</code> based on the cryptographic protocol used by the database server.

Secure Database Parameter	Description
TrustStore	Required. Path and file name of the truststore file that contains the SSL certificate for the database.  If you do not include the path for the truststore file, Informatica looks for the file in the following default directory: <Informatica installation directory>/tomcat/bin
TrustStorePassword	Required. Password for the truststore file for the secure database.

**Note:** Informatica appends the secure JDBC parameters to the JDBC connection string. If you include the secure JDBC parameters directly in the connection string, do not enter any parameter in the **Secure JDBC Parameters** field.

8. Click **Test Connection** to verify that you can connect to the database.
9. Select **No content exists under specified connection string. Create new content.**
10. Click **Finish**.

The domain creates the Model Repository Service, creates content for the Model repository in the specified database, and enables the service.

**Note:** When you update the Model Repository Service properties, you must restart the Model Repository Service and the Catalog Service for the modifications to take effect.

After you create the service through the wizard, you can edit the properties or configure other properties.

## Create and Configure the Data Integration Service

The Data Integration Service is an application service that performs data integration jobs for the Analyst tool, the Developer tool, and external clients.

When you preview or run data profiles, SQL data services, and mappings in the Analyst tool or the Developer tool, the client tool sends requests to the Data Integration Service to perform the data integration jobs. When you run SQL data services, mappings, and workflows from the command line program or an external client, the command sends the request to the Data Integration Service.

### Create the Data Integration Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Data Integration Service, verify that you have created and enabled the Model Repository Service. If the domain does not use Kerberos authentication, verify that you have created a Model repository user that the Data Integration Service can use to access the Model Repository Service.

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Services and Nodes** view.
3. In the Domain Navigator, select the domain.
4. Click **Actions > New > Data Integration Service**.  
The **New Data Integration Service** wizard appears.

5. On the **New Data Integration Service - Step 1 of 14** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Assign	Select <b>Node</b> to configure the service to run on a node. If your license includes grid, you can create a grid and assign the service to run on the grid after you create the service.
Node	Node on which the service runs.
Backup Nodes	If your license includes high availability, nodes on which the service can run if the primary node is unavailable.
Model Repository Service	Model Repository Service to associate with the service.
Username	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.

6. Click **Next**.

The **New Data Integration Service - Step 2 of 14** page appears.

7. Enter the HTTP port number to use for the Data Integration Service.
8. Accept the default values for the remaining security properties. You can configure the security properties after you create the Data Integration Service.
9. Select **Enable Service**.
- The Model Repository Service must be running to enable the Data Integration Service.
10. Verify that the **Move to plugin configuration page** is not selected.
11. Click **Next**.
- The **New Data Integration Service - Step 3 of 14** page appears.
12. Set the **Launch Job Options** property to one of the following values:
- In the service process. Configure when you run SQL data service and web service jobs. SQL data service and web service jobs typically achieve better performance when the Data Integration Service runs jobs in the service process.

- In separate local processes. Configure when you run mapping, profile, and workflow jobs. When the Data Integration Service runs jobs in separate local processes, stability increases because an unexpected interruption to one job does not affect all other jobs.

If you configure the Data Integration Service to run on a grid after you create the service, you can configure the service to run jobs in separate remote processes.

13. Accept the default values for the remaining execution options and click **Next**.

The **New Data Integration Service - Step 4 of 14** page appears.

14. If you created the data object cache database for the Data Integration Service, click **Select** to select the cache connection. Select the data object cache connection that you created for the service to access the database.

15. Accept the default values for the remaining properties on this page and click **Next**.

The **New Data Integration Service - Step 5 of 14** page appears.

16. For optimal performance, enable the Data Integration Service modules that you plan to use.

The following table lists the Data Integration Service modules that you can enable:

Module	Description
Web Service Module	Runs web service operation mappings.
Mapping Service Module	Runs mappings and previews.
Profiling Service Module	Runs profiles and scorecards.
SQL Service Module	Runs SQL queries from a third-party client tool to an SQL data service.
Workflow Orchestration Service Module	Runs workflows.

17. Click **Next**.

The **New Data Integration Service - Step 6 of 14** page appears.

You can configure the HTTP proxy server properties to redirect HTTP requests to the Data Integration Service. You can configure the HTTP configuration properties to filter the web services client machines that can send requests to the Data Integration Service. You can configure these properties after you create the service.

18. Accept the default values for the HTTP proxy server and HTTP configuration properties and click **Next**.

The **New Data Integration Service - Step 7 of 14** page appears.

The Data Integration Service uses the result set cache properties to use cached results for SQL data service queries and web service requests. You can configure the properties after you create the service.

19. Accept the default values for the result set cache properties and click **Next**.

The **New Data Integration Service - Step 8 of 14** page appears.

20. If you created the profiling warehouse database for the Data Integration Service, select the Profiling Service module.

21. If you created the workflow database for the Data Integration Service, select the Workflow Orchestration Service module.

22. Verify that the remaining modules are not selected.

You can configure properties for the remaining modules after you create the service.

23. Click **Next**.

The **New Data Integration Service - Step 11 of 14** page appears.

24. If you created the profiling warehouse database for the Data Integration Service, click **Select** to select the database connection. Select the profiling warehouse connection that you created for the service to access the database.

25. Select whether or not content exists in the profiling warehouse database.

If you created a new profiling warehouse database, select **No content exists under specified connection string**.

26. Click **Next**.

The **New Data Integration Service - Step 12 of 14** page appears.

27. Accept the default values for the advanced profiling properties and click **Next**.

The **New Data Integration Service - Step 14 of 14** page appears.

28. If you created the workflow database for the Data Integration Service, click **Select** to select the database connection. Select the workflow database connection that you created for the service to access the database.

29. Click **Finish**.

The domain creates and enables the Data Integration Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

## Create and Configure the Analyst Service

The Analyst Service is an application service that runs the Analyst tool in the Informatica domain. The Analyst Service manages the connections between service components and the users that have access to the Analyst tool.

When you run profiles, scorecards, or mapping specifications in the Analyst tool, the Analyst Service connects to the Data Integration Service to perform the data integration jobs. When you work on Human tasks in the Analyst tool, the Analyst Service connects to the Data Integration Service to retrieve the task metadata from the workflow database.

When you view, create, or delete a Model repository object in the Analyst tool, the Analyst Service connects to the Model Repository Service to access the metadata. When you view data lineage analysis on scorecards in the Analyst tool, the Analyst Service sends the request to the Metadata Manager Service to run data lineage.

### Create the Analyst Service

Use the service creation wizard in the Administrator tool to create the service.

Before you create the Analyst Service, verify that you have created and enabled the following services:

- Model Repository Service

If the domain does not use Kerberos authentication, verify that you have created a Model repository user that the Analyst Service can use to access the Model Repository Service.

- Data Integration Service

1. In the Administrator tool, click the **Manage** tab.
2. Click **Actions > New > Analyst Service**.



The **New Analyst Service** dialog box appears.

3. On the **New Analyst Service - Step 1 of 6** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) [ ]
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

4. Click **Next**.

The **New Analyst Service - Step 2 of 6** page appears.

5. Enter the HTTP port number to use for communication from the Analyst tool to the Analyst Service.
6. To enable secure communication from the Analyst tool to the Analyst Service, select **Enable Secure Communication**.

Enter the following properties to configure secure communication for the Analyst Service:

Property	Description
HTTPS Port	Port number that the Analyst tool runs on when you enable secure communication. Use a different port number than the HTTP port number.
Keystore File	Directory where the keystore file that contains the digital certificates is stored.
Keystore Password	Plain-text password for the keystore file. If this property is not set, the Analyst Service uses the default password <code>changeit</code> .
SSL Protocol	Optional. Indicates the protocol to be used. Set this property to <code>SSL</code> .

7. Select **Enable Service**.

The Model Repository Service and the Data Integration Service must be running to enable the Analyst Service.

8. Click **Next**.

The **New Analyst Service - Step 3 of 6** page appears.

9. Enter the following properties to associate the Model Repository Service with the Analyst Service:

Description	Property
Model Repository Service	Model Repository Service to associate with the service.
User name	User name that the service uses to access the Model Repository Service. Enter the Model repository user that you created.
Password	Password for the Model repository user.
Security Domain	LDAP security domain for the Model repository user. The field appears when the Informatica domain contains an LDAP security domain. Not available for a domain with Kerberos authentication.

10. To enable Analyst tool users to work on Human task data, set the **Data Integration Service** property to the Data Integration Service that you configure to run workflows.

If Analyst tool users do not need to work on Human task records, do not configure this property.

11. Click **Next**.

The **New Analyst Service - Step 4 of 6** page appears.

12. Enter the following run-time properties for the Analyst Service:

Property	Description
Data Integration Service	Data Integration Service to associate with the service. The Analyst Service manages the connection to the Data Integration Service that enables users to perform data preview, mapping specification, scorecard, and profile jobs in the Analyst tool.  You can associate the Analyst Service with the Data Integration Service that you configured to run workflows. Or, you can associate the Analyst Service with different Data Integration Services for the different operations.
Flat File Cache Directory	Directory of the flat file cache where the Analyst tool stores uploaded flat files. The Data Integration Service must also be able to access this directory. If the Analyst Service and the Data Integration Service run on different nodes, configure the flat file directory to use a shared directory.

13. Click **Next**.

The **New Analyst Service - Step 5 of 6** page appears.

14. Enter the directory to store the temporary business glossary files that the business glossary export process creates and the directory to store files that content managers attach to the Glossary assets. These directories must be on the node that runs the Analyst Service.

15. Click **Finish**.

The domain creates and enables the Analyst Service.

After you create the service through the wizard, you can edit the properties or configure other properties.

# Install the Informatica Client

You can install the Informatica client on Windows in graphical or silent mode.

Before you install the Informatica client on Windows, verify that the minimum system and third-party software requirements are met. If the machine where you install the Informatica client is not configured correctly, the installation can fail.

## Verify Installation Requirements

Before you install the Informatica clients, verify the installation requirements to run the Informatica client tools are met.

You can install all the Informatica client tools on the same machine or on separate machines. You can also install the clients on multiple machines. The requirements for the Informatica clients depend on the client tools that you install.

Before you install the Informatica clients, verify the following installation requirements:

### Disk space for the temporary files

The installer writes temporary files to the hard disk. Verify that you have 1 GB disk space on the machine to support the installation. When the installation completes, the installer deletes the temporary files and releases the disk space.

### Permissions to install the clients

Verify that the user account that you use to install the Informatica clients has write permission on the installation directory and Windows registry.

### Minimum system requirements to run the Informatica client tools

The following table lists the minimum system requirements to run the Informatica client tools:

Client	Processor	RAM	Disk Space
PowerCenter Client	1 CPU	1GB	3 GB
Informatica Developer	1 CPU	1GB	6 GB

## PowerCenter Client Requirements

The PowerCenter Client installation includes Mapping Architect for Visio and Mapping Analyst for Excel.

If you plan to use Mapping Architect for Visio, install the following third-party software before you install the PowerCenter Client:

- Microsoft Visio version 2007 or 2010
- Microsoft .NET Framework 3.5.1
- Microsoft .NET Framework 4

**Important:** If you do not install the correct version and service pack level of Microsoft .NET Framework, Mapping Architect for Visio will not install properly.

Mapping Analyst for Excel includes an Excel add-in that adds a Metadata menu or ribbon to Microsoft Excel. You can install the add-in only for Excel 2007 or 2010. If you plan to use Mapping Analyst for Excel, install the following third-party software before you install the PowerCenter Client:

- Microsoft Office Excel version 2007 or 2010
- Java version 1.8 or later

## Installing in Graphical Mode

You can install the Developer tool in graphical mode on Windows.

1. Close all other applications.
2. Go to the root of the directory for the installation files and run `install.bat` as administrator.  
To run the file as administrator, right-click the `install.bat` file and select **Run as administrator**.  
**Note:** If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the Informatica installation directory.  
If you encounter problems when you run the `install.bat` file from the root directory, run the following file:  
`<installer files directory>\client\install.exe`
3. Select **Install Informatica <Version> Clients** and click **Next**.
4. Read the terms and conditions for Informatica installation and the product usage toolkit and select **I agree to the terms and conditions**.  
Informatica DiscoveryIQ is a product usage tool that sends routine reports on data usage and system statistics to Informatica. Informatica DiscoveryIQ uploads data to Informatica 15 minutes after you install and configure Informatica domain. Thereafter, the domain sends the data every 30 days. You can choose to disable usage statistics from the Administrator tool.
  - a. Press **1** if you do not want to accept the terms and conditions.
  - b. Press **2** to accept the terms and conditions.
5. Version 10.2.2 is for big data products only, such as Big Data Management and Big Data Quality. This version does not support non-big data products, such as PowerCenter or Informatica Data Quality.
  - a. Press **1** and type **quit** to quit the installation.
  - b. Press **2** to continue the installation.

If you choose to not accept the terms and condition, the installer prompts you to accept the terms and conditions.
6. The **Installation Pre-requisites** page displays the system requirements. Verify that all installation requirements are met before you continue the installation.
7. On the **Installation Directory** page, enter the absolute path for the installation directory.  
The installation directory must be on the current computer. The maximum length of the path must be less than 260 characters. The directory names in the path must not contain spaces or the following special characters: `@!*$#!%(){}[];,'`  
**Note:** Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.
8. Click **Next**.
9. On the **Pre-Installation Summary** page, review the installation information, and click **Install**.  
The installer copies the Developer tool files to the installation directory.  
The **Post-installation Summary** page indicates whether the installation completed successfully.
10. Click **Done** to close the installer.

You can view the installation log files to get more information about the tasks performed by the installer.

## Installing in Silent Mode

To install the Informatica clients without user interaction, install in silent mode.

Use a properties file to specify the installation options. The installer reads the file to determine the installation options. You can use silent mode installation to install the Informatica clients on multiple machines on the network or to standardize the installation across machines.

To install in silent mode, complete the following tasks:

1. Configure the installation properties file and specify the installation options in the properties file.
2. Run the installer with the installation properties file.

### Configuring the Properties File

Informatica provides a sample properties file that includes the properties required by the installer. Customize the sample properties file to create a properties file and specify the options for your installation. Then run the silent installation.

The sample `SilentInput.properties` file is stored in the installer download location.

1. Go to the root of the directory that contains the installation files.
2. Locate the sample `SilentInput.properties` file.
3. Create a backup copy of the `SilentInput.properties` file.
4. Use a text editor to open and modify the values of the properties in the file.

The following table describes the installation properties that you can modify:

Property Name	Description
INSTALL_TYPE	Indicates whether to install or upgrade the Informatica clients. If the value is 0, the Informatica clients are installed in the directory you specify. If the value is 1, the Informatica clients are upgraded. Default is 0.
UPG_BACKUP_DIR	Directory of the previous version of the Informatica client that you want to upgrade.
USER_INSTALL_DIR	Informatica client installation directory.
DXT_COMP	Indicates whether to install Informatica Developer. If the value is 1, the Developer tool will be installed. If the value is 0, the Developer tool will not be installed. Default is 1.
CLIENT_COMP	Indicates whether to install PowerCenter Client. If the value is 1, PowerCenter Client will be installed. If the value is 0, PowerCenter Client will not be installed. Default is 1.

5. Save the properties file.

## Running the Installer

After you configure the properties file, open a command prompt to start the silent installation.

1. Open a command prompt.
2. Go to the root of the directory that contains the installation files.
3. Verify that the directory contains the file `SilentInput.properties` that you edited and resaved.
4. To run the silent installation, run `silentInstall.bat`.

The silent installer runs in the background. The process can take a while. The silent installation is complete when the `Informatica_<Version>_Client_InstallLog<timestamp>.log` file is created in the installation directory.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. View the installation log files and correct the errors. Then run the silent installation again.

## Starting the PowerCenter Client

When you start PowerCenter Client, you connect to a PowerCenter repository.

1. From the Windows Start menu, click **Programs > Informatica[Version] > Client > [Client Tool Name]**.

The first time you run a PowerCenter Client tool, you must add a repository and connect to it.

2. Click **Repository > Add Repository**.

The **Add Repository** dialog box appears.

3. Enter the repository and user name.

4. Click **OK**.

The repository appears in the Navigator.

5. Click **Repository > Connect**.

The Connect to Repository dialog box appears.

6. In the connection settings section, click **Add** to add the domain connection information.

The **Add Domain** dialog box appears.

7. Enter the domain name, gateway host, and gateway port number.

8. Click **OK**.

9. In the **Connect to Repository** dialog box, enter the password for the Administrator user.

10. Select the security domain.

11. Click **Connect**.

After you connect to the repository, you can create objects.

## CHAPTER 4

# TDM Installation

This chapter includes the following topics:

- [TDM Installation Overview, 55](#)
- [Installing in Graphical Mode, 55](#)
- [Installing in Console Mode, 56](#)
- [Installing in Silent Mode, 57](#)

## TDM Installation Overview

You can install TDM on Windows or UNIX. On Windows, you can run the installer in graphical or silent mode.

On UNIX, you can run the installer in graphical, console, or silent mode.

When you install TDM, you must join an Informatica domain. The Informatica domain is the fundamental administrative unit for services, users, and resources. The gateway node is the entry point to the domain.

When you run the TDM installer, the installer copies the TDM files to the Informatica home location.

After installation, log in to Informatica Administrator and create a Test Data Manager Service and configure the application services for TDM.

Complete the pre-installation tasks to prepare for the installation.

## Installing in Graphical Mode

You can run the installer in graphical mode on UNIX or Windows.

On the SUSE Linux Enterprise 11 operating system, install TDM in console mode or silent mode.

On Windows, if you encounter problems when you run the install.bat file from the installer root directory, run the following file: <TDM Installer Dir>/server/install.exe

1. Log in to the machine with a system user account.
2. Close all other applications.
3. Begin the installation.
  - On Windows, run install.bat from the installer root directory.

- On UNIX, perform the following steps:
  1. Use a shell command line to run `install.sh` from the installer root directory.
  2. Press `g` for graphical mode installation.
- 4. Verify the prerequisites and then click **Next**.
- 5. Select the option to install Test Data Management and then click **Next**.
- 6. Enter the installation directory. The installation directory must be the Informatica home location.
- 7. Click **Next**.
- 8. Verify the TDM installation settings and disk space requirements and click **Install**.  
The installer copies the TDM files to the installation directory. The **Post-Installation Summary** page appears indicating the installation status and the installation directory.
- 9. Click **Done** to close the installer.  
View the installation log files for more information about the tasks performed by the installer and for the configuration properties of the installed components.
- 10. Restart the Informatica domain.

After installation, log in to Informatica Administrator. You must create a Test Data Manager Service and configure the application services for TDM before you can log in to Test Data Manager.

#### RELATED TOPICS:

- [“Starting and Stopping Informatica” on page 100](#)
- [“After You Install TDM” on page 59](#)

## Installing in Console Mode

You can install TDM in console mode on UNIX.

When you run the installer in console mode, the words `quit` and `back` are reserved words. Do not use these words as input text.

1. Log in to the machine with a system user account.
2. Close all other applications.
3. On a shell command line, run the `install.sh` file from the installer root directory.
4. Press `c` to install in console mode.
5. Verify the prerequisites and then press **Enter** to continue.
6. Press `1` to install Test Data Management.
7. Enter the installation directory. The installation directory must be the Informatica home location.
8. Press **Enter** to continue.

9. Review the installation information and press **Enter** to continue.

The installer copies the TDM files to the installation directory.

10. Press **Enter** to exit the installer.

View the installation log files for information about the tasks performed by the installer and for the configuration properties of the installed components.

11. Restart the Informatica domain.



After installation, log in to Informatica Administrator. You must create a Test Data Manager Service and configure the application services for TDM before you can log in to Test Data Manager.

#### RELATED TOPICS:

- [“Starting and Stopping Informatica” on page 100](#)
- [“After You Install TDM” on page 59](#)

## Installing in Silent Mode

To install TDM without user interaction, install in silent mode. Use a properties file to specify the installation parameters. The installer reads the file to determine the installation options.

Copy the installation files to the hard disk on the machine where you plan to install TDM. The user that runs the installer must have read and write permissions on the installer files directory and execute permissions on the `install.bat` and `install.sh` files. If you install on a remote machine, verify that you can access and create files on the remote machine.

To install in silent mode, complete the following tasks:

1. Create the installation properties file and specify the installation parameters.
2. Run the installer with the installation properties file.

## Creating the Properties File

Informatica provides a sample properties file that includes the parameters that the installer requires. You can customize the sample properties file to specify the options for your installation.

The name of the sample properties file is `SilentInput.properties`. The file is located in the installer root directory of the installation DVD or the installer download location. After you customize the file, save the file with the same name in the same directory. Then run the installer in silent mode.

1. Browse to the installer root directory.
2. Find the sample `SilentInput.properties` file.
3. Create a backup copy of the `SilentInput.properties` file.
4. Use a text editor to open the file and enter the values of the installation parameters:

The following table describes the installation parameters:

Property Name	Description
INSTALL_TYPE	Indicates whether to install or upgrade TDM. If the value is 0 the installer performs an installation. If the value is 1 the installer performs an upgrade.
TDM_USER_INSTALL_DIR	Absolute path for the directory in which to install TDM. You must install TDM in the Informatica installation location. The directory names in the path must not contain spaces or the following special characters: @ * \$ # ! % ( ) { } [ ] , ; ' .
PC_OLD_USER_INSTALL_DIR	Absolute path of the installation directory of the previous installed version of Informatica services. Enter this value if you have upgraded Informatica services and INSTALL_TYPE=1.

5. Verify that the values you set are correct. Then save the properties file with the name `SilentInput.properties` in the same directory.

## Running the Silent Installer

After you create the properties file, open a command window to start the silent installation.

1. Open a command window.
2. Go to the TDM installer files directory.
3. Verify that the directory contains the `SilentInput.properties` file that you created.
4. Run the silent installer.  
On Windows, double click the file `silentinstall.bat`.  
On UNIX, run the file `silentinstall.sh`.

The silent installer runs in the background. The process can take a while. View the TDM installation log file in the `<Informatica installation directory>\TDM` location for more information about the tasks performed by the installer and configuration properties for the installed components. If the silent installation fails, the installer creates the `silentErrorLog.log` file.

On UNIX, the installer creates the log file in the `$HOME` directory.

On Windows, the installer creates the log file in the root directory.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. If the installation fails, view the installation log files and correct the errors. Then run the silent installer again.

## CHAPTER 5

# After You Install TDM

This chapter includes the following topics:

- [After You Install TDM Overview, 59](#)
- [Verify File Permissions, 60](#)
- [Verify the Services and Objects in the Informatica Domain, 60](#)
- [Create and Configure the Test Data Warehouse Service, 61](#)
- [Create and Configure the Test Data Manager Service, 65](#)
- [Configure the Informatica Services Machine for Kerberos-Enabled Hadoop HDFS Connections, 71](#)
- [Configure the Test Data Management Machine for Format Preserving Encryption Masking, 72](#)
- [Third-Party JAR Files, 72](#)
- [Storage Tables for Repeatable Masking, 73](#)

## After You Install TDM Overview

After you install TDM, create a Test Data Manager Service. Verify that the Informatica domain contains the services and repositories required for TDM operations before you create the Test Data Manager Service. If the domain does not contain the required services and repositories, you must create them before you can create the Test Data Manager Service.

Create a Test Data Warehouse Service if you want to create and store data sets in a test data warehouse. The Test Data Warehouse Service manages the test data warehouse repository and the test data warehouse.

TDM creates a default connection for substitution masking with repeatable values and creates the storage tables for the connection. To use a different storage connection, you must assign the connection as the default storage connection and create storage tables for the substitution values. You can assign the connection as the default connection and create storage tables from the **Administrator | Preferences** view of Test Data Manager.

# Verify File Permissions

Verify that users have access to the following files:

- On Windows, verify that the user that runs the Informatica Windows service has full access to the TDM files. Navigate to the following directory in the installation directory:  
`<TDM Installation Directory>\TDM\configuration`
- Verify that the user account that runs the Informatica Windows service has full access to the following file:  
`org.eclipse.virgo.kernel.jmxremote.access.properties`
- TDM users must have permission and access to all files and folders that TDM uses in plans and workflows.

# Verify the Services and Objects in the Informatica Domain

Use the Administrator tool to verify that the Informatica domain contains the services and objects required by TDM.

TDM operations require the Test Data Manager Service, PowerCenter Repository Service, PowerCenter Integration Service, and Data Integration Service. If the Informatica domain does not contain these services, you must create them before you use TDM.

Log in to the Administrator tool and verify that the domain contains the following services:

## **PowerCenter Repository Service**

You must associate a repository with a PowerCenter Integration Service. The repository stores the mappings and objects that are required by the PowerCenter Integration Service processes. A PowerCenter Repository Service manages the repository.

Set up a repository for the TDM objects. Create a PowerCenter Repository Service to manage the objects in the repository. After you create the PowerCenter Repository Service, create at least one folder in the repository to organize and store the TDM objects.

## **PowerCenter Integration Service**

The PowerCenter Integration Service runs the sessions and workflows used by the TDM operations.

If you have the Data Discovery option, verify that the domain contains the following services and objects:

## **Model Repository Service**

You must associate the Data Integration Service with a Model repository. The Model Repository Service manages the profiling objects in the Model repository.

## **Profiling warehouse**

To create and run profiles, you must associate the Data Integration Service with a profiling warehouse. The profiling warehouse stores profiling data.

## **Connection to the profiling warehouse**

The Data Integration Service uses the connection when you run a profile.

### **Data Integration Service**

Runs the profiles that you create to perform data discovery.

If you use the Asset Linking feature to link TDM objects with Business Glossary terms, create the following service in the Informatica domain:

### **Analyst Service**

Manages the Analyst tool that TDM uses to link TDM global objects to objects in the Business Glossary. The license for the Analyst Service must support Business Glossary.

If you use the test data warehouse to store data sets, verify that the domain contains the following services and objects:

### **Test Data Warehouse Service**

The Test Data Warehouse Service runs the test data warehouse and manages the test data warehouse repository.

### **Test data warehouse repository**

The test data warehouse repository stores the source table metadata and project metadata for data sets that you create in Test Data Manager.

### **Connection to the test data Warehouse**

The Test Data Warehouse Service uses the connection when you work with data sets.

### **Test Data Manager Service**

The Test Data Manager Service creates and manages the TDM repository. You must create a Test Data Manager Service from the Administrator tool before you can access Test Data Manager.

For more information about the Informatica services and repositories, see the *Informatica Application Service Guide*.

## Create and Configure the Test Data Warehouse Service

Configure a Test Data Warehouse Service if you want to create a test data warehouse in TDM.

The Test Data Warehouse Service manages the test data warehouse repository and the test data warehouse. The test data warehouse repository is a relational database that stores metadata created when you run operations to store data in the test data warehouse. The test data warehouse is a relational database that stores the source data that you include in data sets and data packs. You access data sets from Test Data Manager and data packs from the Test Data Management Self-Service Portal.

Use the Administrator tool or the `infacmd` command line program to administer the Test Data Warehouse Service. When you create a Test Data Warehouse Service you can create a test data warehouse repository or use an existing test data warehouse repository. You can run multiple Test Data Warehouse services on the same node.

Manage the service users, groups, privileges, and roles from the **Security** tab of the Administrator tool. Manage permissions for test data warehouse repository objects in Test Data Manager.

## Test Data Warehouse Service Dependencies

The Test Data Warehouse Service depends on other application services to perform tasks.

Before you create the Test Data Warehouse Service, you must ensure that the services that it depends on exist in the domain.

### PowerCenter Services

Create the PowerCenter services that the Test Data Warehouse Service depends on in the following order:

1. **PowerCenter Repository Service**  
You perform test data warehouse tasks from Test Data Manager. Test Data Manager uses this service to access metadata stored in the PowerCenter repository.
2. **PowerCenter Integration Service**  
You run workflows to create data sets from Test Data Manager. Test Data Manager uses this service to run workflows and sessions.
3. **Data Integration Service**  
Required to run data coverage analysis tasks on data sets in the test data warehouse.
4. **Model Repository Service**  
Required to run data coverage analysis tasks on data sets in the test data warehouse.

### Test Data Manager Service

To work with the test data warehouse, you must create a Test Data Manager Service and associate the Test Data Warehouse Service with it. Alternatively, update the Test Data Manager Service to associate the Test Data Warehouse Service with it.

## Creating the Test Data Warehouse Service

Use the service creation wizard in the Administrator tool to create the service.

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Services and Nodes** view.
3. Click **Actions > New > Test Data Warehouse Service**.  
The **New Test Data Warehouse Service** dialog box appears.
4. On the **New Test Data Warehouse Service - Step 1 of 4** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < >   ! ( ) ] [ You cannot change the name of the service after you create it.
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.

Property	Description
License	License object that allows use of the service.
Node	Node on which the service runs.

- Click **Next**.

The **New Test Data Warehouse Service - Step 2 of 4** page appears.

- Enter the following properties for the test data warehouse repository database:

Property	Description
Repository Name	Name of the test data warehouse repository.
Database Type	The type of database for the test data warehouse repository. <ul style="list-style-type: none"> <li>- Oracle</li> <li>- Microsoft SQL Server</li> <li>- DB2</li> </ul>
User Name	User account for the test data warehouse repository database. Set up this account using the appropriate database client tools.
Password	Password for the test data warehouse repository database user. Must be in 7-bit ASCII.
JDBC URL	JDBC connection URL used to access the test data warehouse repository database. Enter the JDBC URL in one of the following formats: <ul style="list-style-type: none"> <li>- Oracle: jdbc:informatica:oracle://&lt;host name&gt;:&lt;port&gt;;SID=&lt;database name&gt;</li> <li>- IBM DB2: jdbc:informatica:db2://&lt;host name&gt;:&lt;port&gt;;DatabaseName=&lt;database name&gt;</li> <li>- Microsoft SQL Server: jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port&gt;;SelectMethod=cursor;DatabaseName=&lt;database name&gt;</li> </ul>
Schema Name	Available for Microsoft SQL Server. Optional. Name of the schema for the database. If not selected, the service creates the tables in the default schema.
Tablespace Name	Available for DB2. Name of the tablespace in which to create the tables. You must define the tablespace on a single node and the page size must be 32 KB. In a multipartition database, you must select this option. In a single-partition database, if you do not select this option, the installer creates the tables in the default tablespace.
Content creation options for the new Test Data Warehouse Service	Options to create content, or use existing content, and upgrade existing content. <ul style="list-style-type: none"> <li>- Do not create new content. Creates the repository without creating content. Select this option if the database content exists. If the content is of a previous version, the service prompts you to upgrade the content to the current version.</li> <li>- Create new content. Creates repository content.</li> </ul>

- Select **No content exists under specified connection string. Create new content**.
- Choose to enable the Test Data Warehouse Service.
- Click **Next**.

The **New Test Data Warehouse Service - Step 3 of 4** page appears.

10. Enter the following properties for the test data warehouse database:

Property	Description
Test Data Warehouse Name	Name of the test data warehouse.
Description	Description of the test data warehouse. The description cannot exceed 765 characters.
Connection Type	The type of connection for the test data warehouse. <ul style="list-style-type: none"><li>- Oracle</li><li>- ODBC</li></ul>
Target Connection	The database connection to use as the test data warehouse.
Connection Database Type	The type of database for the test data warehouse. Required if you choose the ODBC connection type. <ul style="list-style-type: none"><li>- POSTGRESQL</li></ul>
JDBC Connection for ODBC	The connection that the ODBC test data warehouse uses for the JDBC connection string.
Staging Schema	The schema to use for creation of staging tables. Some jobs that you run from the self-service portal require a staging connection for staging tables. The test data warehouse connection must have access to the schema.

11. Select the required connection from the list of target connections.
12. Click **Next**.
- The **New Test Data Warehouse Service - Step 4 of 4** page appears.
13. Enter the following properties for the test data warehouse server configuration:

Property	Description
HTTP Port	Port number of the Test Data Warehouse Service. The default is 7705.
Enable Transport Layer Security (TLS)	Secures communication between the Test Data Warehouse Service and the domain.
HTTPS Port	Port number for the HTTPS connection.
Keystore File	Path and file name of the keystore file. The keystore file contains the keys and certificates required if you use the SSL security protocol with the test data warehouse. Required if you select Enable Transport Layer Security.
Keystore Password	Password for the keystore file. Required if you select Enable Secured Socket Layer.



Property	Description
SSL Protocol	Secure Sockets Layer protocol to use. Default is TLS.
JVM Params	<p>The heap size allocated for the Test Data Warehouse Service processes.</p> <ul style="list-style-type: none"> <li>- Xms256m -Xmx512m -XX:MaxMetaspaceSize=256m</li> </ul> <p>The time after which database connections are renewed if the Test Data Warehouse Service remains idle. Required if you modified the database configuration settings to values less than the test data warehouse defaults.</p> <p>Configure the following test data warehouse values to be less than the database values:</p> <ul style="list-style-type: none"> <li>- IDLE_TIME. -DIDLE_TIME=&lt;seconds&gt;. Default is 300 seconds.</li> <li>- CONNECT_TIME. DCONNECT_TIME=&lt;seconds&gt;. Default is 5000 seconds.</li> </ul>

14. Click **Finish**.

The domain creates the Test Data Warehouse Service, starts the service, and creates content for the test data warehouse repository.

## Create and Configure the Test Data Manager Service

Before you can use TDM, you must create and configure a Test Data Manager Service from Informatica Administrator.

The Test Data Manager Service manages the TDM repository. When you access a TDM repository object or a test data warehouse object from Test Data Manager, it sends a request to the Test Data Manager Service. The Test Data Manager Service accesses the database content from the TDM repository or connects to the Test Data Warehouse Service associated with it.

Work with the Informatica domain Administrator to create a Test Data Manager Service from Informatica Administrator.

### Test Data Manager Service Dependencies

The Test Data Manager Service depends on other application services to perform tasks. Before you create the Test Data Manager Service, you must create the services that it depends on.

Create the application services that the Test Data Manager Service depends on in the following order:

1. PowerCenter Repository Service  
Test Data Manager requires this service to access metadata stored in the PowerCenter repository.
2. PowerCenter Integration Service  
Test Data Manager requires this service to run workflows and sessions.
3. Model Repository Service  
Test Data Manager requires this service to perform data discovery.
4. Data Integration Service  
Test Data Manager requires this service to perform data discovery.
5. Analyst Service  
Test Data Manager requires this service to link TDM objects with terms in the Business Glossary.
6. Test Data Warehouse Service  
Test Data Manager requires this service to create and store data sets in the test data warehouse.

Create the services before you create the Test Data Manager Service.

## Creating the Test Data Manager Service

Log in to the Administrator tool to create the Test Data Manager Service. You can also create the Test Data Manager Service using the TDM command line program.

1. In the Administrator tool, click the **Manage** tab.
2. Click the **Services and Nodes** view.
3. Click **Actions > New > Test Data Manager Service**.

The **New Test Data Manager Service** dialog box appears.

4. On the **New Test Data Manager Service - Step 1 of 5** page, enter the following properties:

Property	Description
Name	Name of the service. The name is not case sensitive and must be unique within the domain. It cannot exceed 128 characters or begin with @. It also cannot contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > ! ! ( ) ] [ You cannot change the name of the service after you create it.
Description	Description of the service. The description cannot exceed 765 characters.
Location	Domain and folder where the service is created. Click <b>Browse</b> to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.

5. Click **Next**.
6. On the **New Test Data Manager Service - Step 2 of 5** page, enter the following properties:

Property	Description
PowerCenter Repository Service	The PowerCenter Repository Service that the Test Data Manager Service uses to load metadata into the TDM repository.
PowerCenter Integration Service	The PowerCenter Integration Service that runs the workflows that you generate in Test Data Manager for TDM operations.
Model Repository Service	The Model Repository Service associated with the Test Data Manager Service.
User Name	The user name that the Test Data Manager Service uses to connect to the Model Repository Service.
Password	The password that the Test Data Manager Service uses to connect to the Model Repository Service.

Property	Description
Security Domain	The name of the security domain that the user belongs to. Select the security domain from the list.
Data Integration Service	The Data Integration Service associated with the Test Data Manager Service. The Data Integration Service runs the workflows that you generate when you perform data discovery operations in Test Data Manager. If you have enabled profiling, or if you use Hadoop connections, you must select the Data Integration Service in the domain.
Analyst Service	The Analyst Service associated with the Test Data Manager Service. The Analyst Service connects to the Analyst tool, a flat file cache directory to store uploaded flat files and a business glossary export file directory. Required if you want to link TDM global objects to Business Glossary assets.
Test Data Warehouse Service	The Test Data Warehouse Service associated with the Test Data Manager Service. The Test Data Warehouse Service manages the test data warehouse repository. Required if you want to create and store data sets in the test data warehouse.

7. Enable data profiling to perform data discovery tasks in TDM, and click **Next**.
8. On the **New Test Data Manager Service - Step 3 of 5** page, enter the following properties:  
The repository connection information must be valid for the service to work.

Property	Description
Database Type	Type of database for the TDM repository. <ul style="list-style-type: none"> <li>- Oracle</li> <li>- Microsoft SQL Server</li> <li>- DB2</li> </ul> <b>Note:</b> If you use a Microsoft SQL Server database, you must set the collation to <i>case insensitive</i> on the database.
Use Trusted Connection	Available for Microsoft SQL Server. Select this if you want to log in using Windows login credentials.
Custom Driver Class	Custom JDBC parameters. Required if you select Custom database type. Enter the custom JDBC driver parameters.
Username	User account for the TDM repository database. Set up this account using the appropriate database client tools. To apply changes, restart the Test Data Manager Service.
Password	Password for the TDM repository database. Must be in 7-bit ASCII. To apply changes, restart the Test Data Manager Service.
JDBC URL	JDBC connection URL used to access the TDM repository database. Enter the JDBC URL in the following format: <ul style="list-style-type: none"> <li>- Oracle: jdbc:informatica:oracle://&lt;host name&gt;:&lt;port&gt;;ServiceName=&lt;service name&gt;</li> <li>- IBM DB2: jdbc:informatica:db2://&lt;host name&gt;:&lt;port&gt;;DatabaseName=&lt;database name&gt;</li> <li>- Microsoft SQL Server: jdbc:informatica:sqlserver://&lt;host name&gt;:&lt;port&gt;;DatabaseName=&lt;database name&gt;</li> </ul>

Property	Description
Connection String	Native connect string to the TDM repository database. The Test Data Manager Service uses the connect string to create a connection object to the TDM repository and the PowerCenter repository or Model repository. To apply changes, restart the Test Data Manager Service.
Schema Name	Available for Microsoft SQL Server. Name of the schema for the database. If not selected, the service creates the tables in the default schema.
Tablespace Name	Available for DB2. Name of the tablespace in which to create the tables. You must define the tablespace on a single node and the page size must be 32 KB. In a multipartition database, you must select this option. In a single-partition database, if you do not select this option, the installer creates the tables in the default tablespace.
Creation options for the New Test Data Manager Service	<p>Options to create content, or use existing content, and upgrade existing content.</p> <ul style="list-style-type: none"> <li>- Do not create new content. Creates the repository without creating content. Select this option if the database content exists. If the content is of a previous version, the service prompts you to upgrade the content to the current version.</li> <li>- Previous Test Data Manager Service Name: Enter the name of the previous Test Data Manager Service. Required if you create the service with a different name.</li> </ul> <p><b>Note:</b> If you create the Test Data Manager Service with a different name, the source and target connections do not appear in Test Data Manager. Import the connections again if the connections do not appear in Test Data Manager.</p> <ul style="list-style-type: none"> <li>- Upgrade TDM Repository Contents. Upgrades the content to the current version.</li> <li>- Create new content. Creates repository content.</li> </ul>

9. Select the required content creation option.
  - If no content exists, select **Create new content**. You cannot select this option if the database has content.
  - If the database content exists, select **Do not create new content**. If you entered a different name for the Test Data Manager Service, you are prompted to enter the name of the previous Test Data Manager Service. The application checks the version of the content. If the content is of a previous version, an option to upgrade the repository content appears. Upgrade the repository content. Creating the service without upgrading the content to the current version generates a warning.
10. Enable the Test Data Manager Service, and click **Next**.
11. On the **New Test Data Manager Service - Step 4 of 5** page, enter the following properties:

Property	Description
HTTP Port	Port number that TDM runs on. The default is 6605.
Enable Transport Layer Security (TLS)	Secures communication between the Test Data Manager Service and the domain.
HTTPS Port	Port number for the HTTPS connection. The default is 6643.
Keystore File	Path and file name of the keystore file. The keystore file contains the keys and certificates required if you use the SSL security protocol with the Test Data Manager application. Required if you select Enable Transport Layer Security.

Property	Description
Keystore Password	Password for the keystore file. Required if you select Enable Secured Socket Layer.
SSL Protocol	Secure Sockets Layer protocol to use. Default is TLS.

12. Click **Next**.
13. On the **New Test Data Manager Service - Step 5 of 5** page, enter the following properties:

Property	Description
JVM Params	<p>The heap size allocated for Test Data Manager.</p> <ul style="list-style-type: none"> <li>- Xms512m - Xmx1024m -XX:MaxPermSize=512m</li> </ul> <p>The time after which database connections are renewed if the Test Data Manager remains idle. Required if you modified the database configuration settings to values less than the TDM defaults. Configure the following values in TDM to be less than the database values.</p> <ul style="list-style-type: none"> <li>- IDLE_TIME. -DIDLE_TIME=&lt;seconds&gt;. Default is 300 seconds.</li> <li>- CONNECT_TIME. -DCONNECT_TIME=&lt;seconds&gt;. Default is 5000 seconds.</li> </ul>
Connection Pool Size	The JDBC connection pool size.
JMX Port	Port number for the JMX/RMI connections to TDM. Default is 6675.
Shutdown Port	Port number that controls the server shutdown for TDM. The TDM Server listens for shutdown commands on this port. Default is 6607.

## RELATED TOPICS:

- [“infacmd tdm Command Reference” on page 75](#)

## Editing the Test Data Manager Service

You can edit the Test Data Manager Service from the Administrator tool or using the tdm command line program.

Edit the Test Data Manager Service to create or upgrade content and to edit or update the service properties.

## Enabling and Disabling the Test Data Manager Service

You can enable, disable, and recycle the Test Data Manager Service from the service **Actions** menu in the Administrator tool. You can also use the tdm command line program to enable and disable the service.

Disable a Test Data Manager Service to perform maintenance or to temporarily restrict users from accessing Test Data Manager. When you disable the Test Data Manager Service, you also stop Test Data Manager. You might recycle the service if you update a property. When you recycle the service, the Service Manager disables and enables the service.

When you enable the Test Data Manager Service, the Service Manager starts TDM on the node where the service runs.

## Assigning a New License to the Test Data Manager Service

If you buy additional licenses, you can assign a different license to the Test Data Manager Service. Unassign the Test Data Manager Service from the existing license and then assign the service to the new license. You must add the license to the domain before you can assign it to the Test Data Manager Service.

Add the new license to the domain from the Domain **Actions > New > License** option.

To assign a new license to the Test Data Manager Service, perform the following steps in the Administrator tool:

1. Disable the Test Data Manager Service.
2. Select the assigned license in the Domain Navigator.
3. Click **Assigned Services**.
4. Click **Edit Assigned Services**.
5. Select the Test Data Manager Service from the **Assigned Services** list and click **Remove** to unassign it.
6. Select the new license in the Domain Navigator.
7. Click **Assigned Services**.
8. Click **Edit Assigned Services**.
9. Select the Test Data Manager Service from the **Unassigned Services** list and click **Add** to assign it.
10. Click **OK**.
11. Enable the Test Data Manager Service.

## Assigning the Test Data Manager Service to a Different Node

You can assign the Test Data Manager Service to a different node in the domain. The new node that uses the Test Data Manager Service must have TDM installed.

1. Disable the Test Data Manager Service.
2. Click **Edit** in the **General Properties** section.
3. Select a different node for the Node property, and then click **OK**.
4. If the Test Data Manager Service is running in HTTPS security mode, change the Keystore File Location to the path on the new node. Click **Edit** in the **Server Configuration Properties** section and update the Keystore File location, and click **OK**.
5. Enable the Test Data Manager Service.

## Test Data Manager Service Logs

The Test Data Manager Service logs contain detailed information about all Test Data Manager Service actions. View the Test Data Manager Service logs from the **Logs | Services** view in the Administrator tool.

View detailed information about Test Data Manager Service startup and shut down. You can also view console logs and error log messages in the Test Data Manager Service logs in the Administrator tool.

View information about content creation and content upgrade when you perform a service upgrade or create content for the service.

You can access all the Test Data Manager Service logs from the **Logs | Services** view of the Administrator tool.

## Viewing Test Data Manager Service Logs

View the event logs for the Test Data Manager Service that you want to monitor.

You can view messages for events such as enablement, disablement, content creation, and content upgrade of the Test Data Manager Service.

1. In the Administrator tool, click the **Logs** tab.
2. Select the **Service** view.  
The contents panel displays event logs for all services.
3. From the **Service Type** list, select Test Data Manager Service.
4. From the **Service Name** list, select the Test Data Manager Service that you want to monitor.
5. Click the **Filter** button.

The Log Manager retrieves the log events and displays the most recent log events first.

To narrow down the list of log events, select the severity and time period of the events that you want to view. Click the **Filter** button again to refresh the list.

# Configure the Informatica Services Machine for Kerberos-Enabled Hadoop HDFS Connections

If you use a Hadoop cluster with Kerberos authentication, you must configure the Informatica Services machine before you can create and use a Hadoop HDFS connection in Test Data Manager.

Before you begin, perform the following prerequisite tasks:

- Install the latest version of the JCE policy files.
  - Ensure that the KRB5\_CONFIG environment variable contains the `krb5.conf` file location and that the `krb5.conf` file contains the correct entries.
  - Copy the `krb5.conf` file to the following location: `<Informatica installation directory>/TDM/datadirect`
  - Ensure that you have read permission on the ticket cache file.
1. Create a directory in the Informatica installation directory. For example: `<Informatica installation directory>/hadoophdfs/conf/`  
Ensure that the PowerCenter Integration Service is running so that the Informatica administrator user has read/write access to the directory.
  2. Copy the following files from the Hadoop cluster to the directory that you created:
    - `/etc/hadoop/conf/core-site.xml`
    - `/etc/hadoop/conf/mapred-site.xml`
    - `/etc/hadoop/conf/hdfs-site.xml`
    - `/etc/hive/conf/hive-site.xml`
  3. Ensure that the Informatica administrator user exists on all Hadoop cluster nodes and has the same UID. To create the Kerberos ticket cache file, run the `kinit` command on all nodes.
  4. To create the Kerberos ticket cache file, run the `kinit` command on the Informatica node where the PowerCenter Integration Service is running.

The command creates the ticket cache file with the following name format:

/tmp/krb5cc\_<UID>

Use the kinit command to verify, validate, and renew the tickets.

5. Edit the `core-site.xml` file in the directory and add the following parameters:

```
<property>
<name>hadoop.security.kerberos.ticket.cache.path</name>
<value>/tmp/REPLACE_WITH_CACHE_FILENAME</value>
<description>Path to the Kerberos ticket cache.</description>
</property>
```

6. Log in to the Administrator tool, select the PowerCenter Integration Service, and click the **Processes** tab.
7. Click **Edit** on the **Environment Variables** tab. In the CLASSPATH environment variable, add the directory that you created.
8. Restart the PowerCenter Integration Service.

## Configure the Test Data Management Machine for Format Preserving Encryption Masking

Before you can use the format preserving encryption masking type in a plan, you must configure the Test Data Management machine.

1. Create a `tokens` folder on the machine where Informatica service is installed.
2. Go to the `<Informatica installation directory>\TDM\configuration` directory.
3. Open the `softhsm2.conf` file.
4. Set the `directories.tokenidir` property to the `tokens` directory that you create in step 1 and save the change.
5. Set the `SOFTHSM2_CONF` environment variable to the `<Informatica installation directory>\TDM\configuration\softhsm2.conf` directory.
6. Set the `INFA_KEY_LOCATION` environment variable to the `<Informatica installation directory>\isp\config\keys` directory.
7. Restart the Informatica domain.

## Third-Party JAR Files

Ensure that you copy all required third-party JAR files to required locations.

- To use a Teradata or a Teradata Parallel Transporter connection as a staging connection, the Teradata JDBC JAR files `tdgssconfig.jar` and `terajdbc4.jar` must be present in the following location:  
`<Informatica installation directory>\TDM\utilities\mapgen\thirdpartylib.`

Create a `thirdpartylib` folder and copy the JAR files before you configure the connection as a staging connection.

- Before you can test a Teradata or a Teradata Parallel Transporter connection, you must add the Teradata JDBC JAR files `tdgssconfig.jar` and `terajdbc4.jar` to the following location:  
`<Informatica installation directory>\TDM\lib\thirdparty.`



Restart the Test Data Manager Service after you add the files.

- Before you can test a JDBC connection that you configure with a MySQL database, you must add the MySQL JDBC JAR file `mysql-connector-java-5.1.44-bin.jar` to the following location:

`<Informatica installation directory>\TDM\lib\thirdparty.`

Restart the Test Data Manager Service after you add the JAR file.

- Before you can test a Netezza connection, you must add the Netezza JDBC JAR file `nzjdbc.jar` to the following location:

`<Informatica installation directory>\TDM\lib\thirdparty.`

Restart the Test Data Manager Service after you add the JAR file.

## Storage Tables for Repeatable Masking

To perform expression masking or substitution masking with repeatable values, you must assign a storage table for the repeatable values. You can create the table in the TDM repository database or in another database. TDM creates a default storage connection and creates storage tables for this connection.

If you choose to use a different storage connection, you must set this connection as the default connection and create the storage tables for the connection. Set the connection as the default storage and staging connections and create storage tables in Test Data Manager.

Staging connections and storage connections can be on Oracle, Sybase, IBM DB2, or Microsoft SQL Server databases. You can create a staging connection on Teradata and Teradata Parallel Transporter connections.

**Note:** To use a Teradata or a Teradata Parallel Transporter connection as a staging connection, the Teradata JDBC JAR files `tdgssconfig.jar` and `terajdbc4.jar` must be present in the following location:

`<Informatica installation directory>\TDM\utilities\mapgen\thirdpartylib.` Create a `thirdpartylib` folder and copy the JAR files before you configure the connection as a staging connection.

You can create the storage tables for the required staging and storage connection from the **Administrator** view in Test Data Manager.

You can also use the SQL scripts that Informatica provides to create the storage tables. Use your database client tool to run the SQL script and create the table in the database. For example, you can use the SQL\*Plus client for Oracle to create the storage table in an Oracle database.

Run the storage table SQL script for your database. For example, to create the substitution storage table in a Microsoft SQL Server database, run the *Substitution\_SQL\_Server.sql* file. The SQL scripts to create the storage table for repeatable expression masking are installed in the following TDM directory:

`<TDM Installation Directory>/TDM/storage_script/expression_storage`

After you run the expression storage script, verify that the script created the `IDM_EXPRESSION_STORAGE` table in the database. The SQL scripts to create the storage table for repeatable substitution masking are installed in the following TDM directory:

`<TDM Installation Directory>/TDM/storage_script/substitution_storage`

After you run the substitution storage script, verify that the script created the `IDM_SUBSTITUTION_STORAGE` table in the database.

**Important:** The expression and substitution storage tables can contain original values from the source database and the corresponding masked values from the target database. Ensure that access to the storage table is secure. Alternatively, you can create the expression or substitution storage table in a database with limited user access.

## Creating the Storage Tables

Create storage tables if you do not want to use the default staging and storage connection and storage tables that TDM creates.

1. In the **Administrator | Preferences** view, click **Edit** in the **Workflow Generation** section.  
The **Edit Preferences** dialog box appears.
2. Select the required default storage connection from the list.
3. Click **Create Storage Tables** to create the storage tables for this connection.

# CHAPTER 6

## Infacmd

This chapter includes the following topics:

- [infacmd Overview, 75](#)
- [infacmd tdm Command Reference, 75](#)
- [infacmd tdw Command Reference, 86](#)
- [infacmd isp Commands for the Test Data Warehouse Service, 93](#)

### infacmd Overview

*infacmd* is a command line program that allows you to administer services in the domain. You can create the service, add content to the service, enable the service, and disable the service with the *infacmd* command.

Use the *infacmd* command line program to administer the Test Data Manager Service and the Test Data Warehouse Service.

Run the commands from the <INFA\_HOME>\isp\bin path.

You do not need to add the Username and Password options when you run the commands in Kerberos network authentication mode.

### infacmd tdm Command Reference

The *infacmd* tdm program administers the Test Data Manager Service.

You can create the service, add content to the service, enable the service and disable the service with the *infacmd* tdm commands.

#### CreateService

Creates a Test Data Manager Service in a domain.

The *infacmd* tdm CreateService command uses the following syntax:

```
CreateService  
  
<-DomainName|-dn> domain_name  
  
<-ServiceName|-sn> service_name
```

```

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-NodeName|-nn> node_name

<-LicenseName|-ln> license_name

<-PCRSServiceName|-pcrs> power_center_repo_service

<-PCISServiceName|-pcis> power_center_int_service

<-MRSServiceName|-mrs> model_repo_service

<-MRSUserName|-rsun> model_repo_service_username

<-MRSPassword|-rspd> model_repo_service_password

[<-MRSSecurityDomain|-rsdn> model_repo_security_domain]

<-AnalystService|-at> analyst_service

<-EnableProfiling|-ep> enable_profiling

<-TDWServiceName|-tdw> test_data_warehouse_service

<-DISServiceName|-dis> data_integration_service

<-db_type|-dt> database_type (ORACLE, DB2, SQLSERVER or CUSTOM)

<-DBUsername|-du> db_user

<-DBPassword|-dp> db_password

<-DBUrl|-dl> db_url

<-DBConnString|-dc> db_conn_string

[<-DbSchema|-ds> db_schema (used for SQL Server only)]

[<-DbTablespace|-db> db_tablespace (used for DB2 only)]

[<-HttpPort> http_port]

[<-HttpsPort> https_port]

[<-KeystoreFile|-kf> keystore_file_location]

[<-KeystorePassword|-kp> keystore_password]

[<-SSLProtocol|-sp> ssl_protocol]

[<-jvmParams|-jp> jvmParameters]

[<-connPoolSize|-cp> conn_pool_size]

[<-jmxPort> jmx_port]

[<-shutdownPort> shutdown_port]

[<-hadoopDistDir> Hadoop Distribution Directory]

[<-hadoopKerbSPN> Hadoop Kerberos Service Principal Name]

```

[<-hadoopKerbKeytab> Hadoop Kerberos Keytab]

The following table describes infacmd tdm CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the Test Data Manager Service.  The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters:  / * ? < > "
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.
-NodeName -nn	node_name	Required. Name of the node where the service will run.
-LicenseName -ln	license_name	Required. Name of the license. The name is not case sensitive and must be unique within the domain. The name cannot exceed 79 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters: / * ? < > "
-PCRSServicename -pcrs	power_center_repo_service	Name of the PowerCenter Repository Service to which TDM connects.
-PCISServicename -pcis	power_center_int_service	Name of the PowerCenter Integration Service to which TDM connects.
-MRSServiceName -mrs	model_repo_service	Name of the Model Repository Service to which TDM connects.
-MRSUserName -rsun	model_repo_service_username	Required. User name to connect to the Model repository.
-MRSPassword -rspd	model_repo_service_password	Required. Password for the user name to connect to the Model repository. The password is case sensitive.

Option	Argument	Description
-AnalystService -at	analyst_service	Optional. Name of the Analyst Service that TDM uses for asset linking. Required if you use the asset linking feature to link TDM global objects to the Business Glossary objects.
-MRSSecurityDomain -rsdn	model_repo_security_domain	Required if you use LDAP authentication. Name of the security domain that the user belongs to. Security domain is case sensitive. Default is Native.
-EnableProfiling -ep	enable_profiling	Indicates data discovery settings. Set to true to enable data discovery. Set to false to disable data discovery.
-TDWServiceName tdw	test_data_warehouse_service	Optional. Required if you create a test data warehouse. Name of the Test Data Warehouse Service that TDM uses to manage the test data warehouse.
-DISServiceName -dis	data_integration_service	Name of the Data Integration Service to which TDM connects.
-db_type -dt	database_type	Type of TDM repository database. Values are Oracle, SQL Server, DB2, or Custom.
-DBUsername -du	db_user	Required. Account for the repository database. Use the database client to set up this account.
-DBPassword -dp	db_password	Required. Repository database password for the database user.
-DBUrl -dl	db_url	Required. JDBC connect string to the database for the TDM repository. Use one of the following syntaxes:  <b>Oracle:</b>  jdbc:informatica:oracle: // <machineName>:<PortNo>;ServiceName= <DBName>; MaxPooledStatements=20; CatalogOptions=0; EnableServerResultCache=true  <b>DB2:</b>  jdbc:informatica:db2: //<host>:<port>; DatabaseName=<dbname>; BatchPerformanceWorkaround=true;DynamicSections=1000  <b>SQLServer:</b>  jdbc:informatica:sqlserver: // <host>:<port>; DatabaseName=<dbname>; SnapshotSerializable=true

Option	Argument	Description
-DBConnString -dc	db_conn_string	Native connect string to the TDM repository database. The service uses the connect string to create a connection object to the Test Data Manager repository and the PowerCenter repository or Model repository.
-DbSchema -ds	db_schema	Optional. The schema name for a Microsoft SQL Server database.
-DbTablespace -db	db_tablespace	Required for a DB2 database only. When you configure a tablespace name, the Test Data Manager Service creates all repository tables in the same tablespace. You cannot use spaces in the tablespace name.  The tablespace must be defined on a single node and the page size must be 32 KB. In a multipartition database, you must select this option. In a single-partition database, if you do not select this option, the installer creates the tables in the default tablespace.
-HttpPort	http_port	Required. Port number for the service.
-HttpsPort	https_port	Optional. Port number to secure the connection to the Administrator tool. Set this port number if you want to configure HTTPS for a node.
-KeystoreFile -kf	keystore_file_location]	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol with PowerCenter.
-KeystorePassword -kp	keystore_password	Optional. If TLS is enabled, you must specify a password.
-SSLProtocol -pt	SSL Protocol	Optional. Secure Sockets Layer protocol to use. Editable if you enable Transport Layer Security (TLS).



Option	Argument	Description
-jvmParams -jp	jvmParameters	<p>JVM parameters to set:</p> <ul style="list-style-type: none"> <li>- The heap size allocated for Test Data Manager.</li> <li>- The time after which database connections are renewed if the TDM UI remains idle. Required if you have modified the database configuration settings to values less than the TDM defaults. Edit the values in TDM such that the values are less than the database values.</li> </ul> <p>Include the JVM parameters in single quotes and then in double quotes. For example, 'value' and then "value".</p> <p>The -Xms option is case sensitive. For example:</p> <pre>""- Xms512m - Xmx1024m - XX:MaxPermSize=512m"</pre> <ul style="list-style-type: none"> <li>- IDLE_TIME. <ul style="list-style-type: none"> <li>-DIDLE_TIME=&lt;seconds&gt;. Default is 300 seconds.</li> </ul> </li> <li>- CONNECT_TIME. <ul style="list-style-type: none"> <li>-DCONNECT_TIME=&lt;seconds&gt;. Default is 5000 seconds.</li> </ul> </li> </ul>
-connPoolSize -cp	conn_pool_size	Optional. The maximum number of idle connection instances that a pool maintains for a database connection before the maximum idle time is met. Set this value to be more than the minimum number of idle connection instances. Default is 15.
-jmxPort	jmx_port	Port number for the JMX/RMI connections to TDM. Default is 6675.
-shutdownPort	shutdown_port	Port number that controls shutdown for TDM.
-hadoopDistDir -hdd	Hadoop Distribution Directory	The Hadoop distribution directory on the Test Data Manager Service node.
-hadoopKerbSPN -hks	Hadoop Kerberos Service Principal Name	<p>Service Principal Name (SPN) of the Data Integration Service to connect to a Hadoop cluster that uses Kerberos authentication.</p> <p>Not required when you run the MapR Hadoop distribution. Required for other Hadoop distributions.</p>
-hadoopKerbKeytab -hkt	Hadoop Kerberos Keytab	<p>The file path to the Kerberos keytab file on the machine on which the Data Integration Service runs.</p> <p>Not required when you run the MapR Hadoop distribution. Required for other Hadoop distributions.</p>

## CreateContents

Creates repository content for the Test Data Manager repository.

The infacmd tdm CreateContents command uses the following syntax:

```
<-DomainName|-dn> domain_name  
  
[<-SecurityDomain|-sdn> security_domain]  
  
<-UserName|-un> user_name  
  
<-Password|-pd> password  
  
<-ServiceName|-sn> service_name  
  
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd tdm CreateContents options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-ServiceName -sn	service_name	Required. The Test Data Manager Service name.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

## EnableService

Enables the Test Data Manager Service.

The infacmd tdm EnableService command uses the following syntax:

```
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

The following table describes infacmd tdm EnableService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the service you want to run the command against. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.

Option	Argument	Description
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.

## DisableService

Disables the Test Data Manager Service. When you disable the Test Data Manager Service, all the service processes stop.

The infacmd tdm DisableService command uses the following syntax:

```
<-DomainName|-dn> domain_name
<-ServiceName|-sn> service_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-DisableMode|-dm> disable_mode: COMPLETE|ABORT|STOP
```

The following table describes infacmd tdm DisableService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	service_name	Required. Name of the service you want to run the command against. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

Option	Argument	Description
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-DisableMode -dm	disable_mode	Required. Defines how the service is disabled: <ul style="list-style-type: none"> <li>- Complete. Disables the service after all service processes stop.</li> <li>- Abort. Stops all processes immediately, and then disables the service.</li> <li>- Stop. Stops all running workflows, and then disables the service.</li> </ul>

## removeService

Removes the Test Data Manager Service from the domain. Before you remove a service, you must disable it.

The infacmd tdm removeService command uses the following syntax:

```
removeService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
```

```
<-ServiceName|-sn> service_name
```

The following table describes `infacmd tdm removeService` options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable <code>INFA_DEFAULT_DOMAIN</code> . If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable <code>INFA_DEFAULT_DOMAIN_USER</code> . If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that <code>infacmd</code> attempts to establish or reestablish a connection to the domain. If you omit this option, <code>infacmd</code> uses the timeout value specified in the <code>INFA_CLIENT_RESILIENCE_TIMEOUT</code> environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of service you want to remove. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

## infacmd tdw Command Reference

The *infacmd* tdw program administers the Test Data Warehouse Service.

You can create the service and add content to the service with the *infacmd* tdw program.

## CreateService

Creates a Test Data Warehouse Service in a domain.

The infacmd tdw CreateService command uses the following syntax:

```
CreateService

<-DomainName|-dn> Domain Name

<-ServiceName|-sn> Service Name

[<-ServiceDesc|-sd> Service Description]

[<-UserName|-un> Username]

[<-Password|-pd> Password]

[<-SecurityDomain|-sdn> Security Domain]

[<-ResilienceTimeout|-re> Timeout Period in seconds]

<-NodeName|-nn> Node Name

<-LicenseName|-ln> License Name

<-RepoName|-rn> Repository Name

<-RepoDBType|-rdt> Repository Database Type (ORACLE, DB2, SQLSERVER)

<-RepoDBUsername|-rdu> Repository Database User

<-RepoDBPassword|-rdp> Repository Database Password

<-RepoDBUrl|-rdl> Repository Database Url

[<-RepoDbSchema|-rds> Repository Database Schema (used for SQL Server only)]

[<-RepoDbTablespace|-rdts> Repository Database Tablespace (used for DB2 only)]

<-TDWName| -tdwn> Test Data Warehouse Name

[<-TDWDescription| -tdwdesc> Test Data Warehouse Description]

<-TDWConnType|-tdwct> Test Data Warehouse Connection Type (ORACLE/ODBC)

<-TDWConnName|-tdwcn> Test Data Warehouse Connection Name

[<-TDWConnDBType|-tdwcdbt> Test Data Warehouse Connection Database Type (POSTGRESQL)]

[<-TDWJDBCConnName|-tdwjdbccn> Test Data Warehouse JDBC Connection Name]

<-TDWStagingSchema|-tdwstsc> Test Data Warehouse Staging Schema Name

[<-HttpPort> httpPort]

[<-HttpsPort> httpsPort]

[<-KeystoreFile|-kf> Keystore File Location]

[<-KeystorePassword|-kp> Keystore Password]

[<-SSLProtocol|-sp> SSL Protocol]

[<-jvmParams|-jp> JVM Parameters]
```

The following table describes infacmd tdw CreateService options and arguments:

Option	Argument	Description
-DomainName -dn	Domain Name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-ServiceName -sn	Service Name	Required. Name of the Test Data Warehouse Service.  The name is not case sensitive and must be unique within the domain. The characters must be compatible with the code page of the associated repository. The name cannot exceed 230 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters:  / * ? < > "
-ServiceDesc -sd	Service Description	Description of the service. The description cannot exceed 765 characters.
-UserName -un	Username	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.



Option	Argument	Description
-SecurityDomain -sdn	Security Domain	<p>Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.</p> <p>If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.</p>
-ResilienceTimeout -re	Timeout Period in seconds	<p>Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set a the resilience timeout period with both methods, the -re option takes precedence. Default is 180 seconds.</p>
-NodeName -nn	Node Name	Required. Name of the node where the service will run.
-LicenseName -ln	License Name	<p>Required. Name of the license. The name is not case sensitive and must be unique within the domain. The name cannot exceed 79 characters, have leading or trailing spaces, or contain carriage returns, tabs, or the following characters:</p> <p>/ * ? &lt; &gt; "  </p>
-RepoName -rn	Repository Name	Required. Name of the test data warehouse repository.
-RepoDBType -rdt	Database Type	Required. Type of database for the test data warehouse repository. Values are Oracle, SQL Server, or DB2.
-RepoDBUsername -rdu	Repository Database User	Required. Account for the repository database. Use the database client to set up this account.
-RepoDBPassword -rdp	Repository Database Password	Required. Repository database password for the database user.

Option	Argument	Description
-RepoDBUrl -rdl	Repository Database Url	<p>Required. JDBC connect string to the database for the test data warehouse repository. Use one of the following syntaxes:</p> <p><b>Oracle:</b></p> <pre>jdbc:informatica:oracle: //&lt;machine name&gt;:&lt;port number&gt;;ServiceName=&lt;DBName&gt;; MaxPooledStatements=20; CatalogOptions=0; EnableServerResultCache=true</pre> <p><b>DB2:</b></p> <pre>jdbc:informatica:db2: //&lt;host name&gt;:&lt;port number&gt;; DatabaseName=&lt;dbname&gt;; BatchPerformanceWorkaround=true;DynamicSections=1000</pre> <p><b>SQLServer:</b></p> <pre>jdbc:informatica:sqlserver: //&lt;host name&gt;:&lt;port number&gt;; DatabaseName=&lt;database name&gt;; SnapshotSerializable=true</pre>
-RepoDbSchema -rds	Repository Database Schema	Optional. The schema name for a Microsoft SQL Server database.
-RepoDbTablespace -rdts	Repository Database Tablespace	<p>Required for a DB2 database only. When you configure a tablespace name, the Test Data Warehouse Service creates all repository tables in the same tablespace. You cannot use spaces in the tablespace name.</p> <p>The tablespace must be defined on a single node and the page size must be 32 KB. In a multipartition database, you must select this option. In a single-partition database, if you do not select this option, the command creates the tables in the default tablespace.</p>
-TDWName -tdwn	Test Data Warehouse Name	Required. Name of the test data warehouse.
-TDWDescription -tdwdesc	Test Data Warehouse Description	Description of the test data warehouse. The description cannot exceed 765 characters.
TDWConnType -tdwct	Test Data Warehouse Connection Type (ORACLE/ ODBC)	Required. Type of database connection for the test data warehouse.
TDWConnName -tdwcn	Test Data Warehouse Connection Name	Required. The database connection to use as the test data warehouse.
TDWConnDBType tdwcdbt	Test Data Warehouse Connection Database Type (POSTGRESQL)	Required if you choose ODBC connection type. The type of database to use as the test data warehouse connection.

Option	Argument	Description
TDWJDBConnName tdwjdbccn	Test Data Warehouse JDBC Connection Name	Required if you choose ODBC connection type. The connection that the ODBC test data warehouse uses for the JDBC connection string.
TDWStagingSchema tdwstsc	Test Data Warehouse Staging Schema Name	The schema to use for creation of staging tables when required for jobs that you run from the self-service portal. The test data warehouse connection must have access to the schema.
-HttpPort	HttpPort	Required. Port number for the service.
-HttpsPort	HttpsPort	Optional. Port number to secure the connection to the Administrator tool. Set this port number if you want to configure HTTPS for a node.
-KeystoreFile -kf	Keystore File Location	Optional. Keystore file that contains the keys and certificates required if you use the SSL security protocol with PowerCenter.
-KeystorePassword -kp	Keystore Password	Optional. If TLS is enabled, you must specify a password.
-SSLProtocol -sp	SSL Protocol	Optional. Secure Sockets Layer protocol to use. Editable if you enable Transport Layer Security (TLS).
-jvmParams -jp	JVM Parameters	<p>JVM parameters to set:</p> <ul style="list-style-type: none"> <li>- The heap size allocated for the test data warehouse.</li> <li>- The time after which database connections are renewed if the TDM UI remains idle. Required if you have modified the database configuration settings to values less than the TDM defaults. Edit the values in TDM such that the values are less than the database values.</li> </ul> <p>Include the JVM parameters in single quotes and then in double quotes. For example, 'value' and then "value".</p> <p>The -Xms option is case sensitive. For example:</p> <p>""- Xms256m - Xmx512m -  <b>XX</b>:MaxPermSize=256m"</p> <ul style="list-style-type: none"> <li>- IDLE_TIME.  -DIDLE_TIME=&lt;seconds&gt;. Default is 300 seconds.</li> <li>- CONNECT_TIME.  -DCONNECT_TIME=&lt;seconds&gt;. Default is 5000 seconds.</li> </ul>

## CreateService Example

The following sample command creates a Test Data Warehouse Service with the name *tdw1*:

```
infacmd tdw createService -dn Domain -sn tdw1 -un Administrator -pd Administrator -nn
node01 -ln TDM_ALL -rn rep01 -rdt SQLSERVER -rdu test -rdp test -rdl
"jdbc:informatica:sqlserver://ExampleHost:
1433;SelectMethod=cursor;databaseName=tdw_cmd_db" -tdwn TDW1 -tdwct ORACLE -tdwcn
OrclConn -httpport 7705
```

## CreateContents

Creates repository content for the test data warehouse repository.

The `infacmd tdw CreateContents` command uses the following syntax:

```
<-DomainName|-dn> Domain Name

[<-SecurityDomain|-sdn> Security Domain]

<-UserName|-un> Username

<-Password|-pd> Password

<-ServiceName|-sn> Service Name

[<-ResilienceTimeout|-re> Timeout Period in seconds]
```

The following table describes `infacmd tdw CreateContents` options and arguments:

Option	Argument	Description
-DomainName -dn	Domain Name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-SecurityDomain -sdn	Security Domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.

Option	Argument	Description
-UserName -un	Username	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	Password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-ServiceName -sn	Service Name	Required. The Test Data Warehouse Service name.
-ResilienceTimeout -re	Timeout Period in seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. You can set the resilience timeout period with the -re option or the environment variable INFA_CLIENT_RESILIENCE_TIMEOUT. If you set the resilience timeout period with both methods, the -re option takes precedence.

### CreateContents Example

The following sample command creates the content for a Test Data Warehouse Service with the name *tdw1*:

```
infacmd tdw createContents -dn Domain -sn tdw1-un Administrator -pd Administrator
```

## infacmd isp Commands for the Test Data Warehouse Service

The *infacmd* isp program administers the Informatica domain. You can enable, disable, and delete the Test Data Warehouse services with *infacmd* isp commands.

To enable the service, disable the service, and delete the service, use the *infacmd* isp commands.

### EnableService

Enables the application service corresponding to the service name.

Enables the Test Data Warehouse Service and any application service type, including system services. You can also enable Informatica Administrator.

The `infacmd isp EnableService` command uses the following syntax:

```
EnableService

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name
```

The following table describes `infacmd isp EnableService` options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the <code>-dn</code> option or the environment variable <code>INFA_DEFAULT_DOMAIN</code> . If you set a domain name with both methods, the <code>-dn</code> option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the <code>-un</code> option or the environment variable <code>INFA_DEFAULT_DOMAIN_USER</code> . If you set a user name with both methods, the <code>-un</code> option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the <code>-pd</code> option or the environment variable <code>INFA_DEFAULT_DOMAIN_PASSWORD</code> . If you set a password with both methods, the password set with the <code>-pd</code> option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the <code>-sdn</code> option or the environment variable <code>INFA_DEFAULT_SECURITY_DOMAIN</code> . If you set a security domain name with both methods, the <code>-sdn</code> option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the <code>domains.infa</code> file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service you want to enable. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

### EnableService Example

The following sample command enables a Test Data Warehouse Service with the name *tdw1*:

```
infacmd isp enableService -dn Domain -un Administrator -pd Administrator -sn tdw1
```

## DisableService

Disables the application service corresponding to the service name. When you disable a service, all service processes stop.

Disables the Test Data Warehouse Service and any application service type, including system services. The infacmd isp DisableService command uses the following syntax:

```
DisableService
<-DomainName|-dn> domain_name
<-UserName|-un> user_name
<-Password|-pd> password
[<-SecurityDomain|-sdn> security_domain]
[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]
[<-ResilienceTimeout|-re> timeout_period_in_seconds]
<-ServiceName|-sn> service_name
<-Mode|-mo> disable_mode
```

The following table describes infacmd isp DisableService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.

Option	Argument	Description
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive. If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infra file is out of date. The host names and port numbers for the gateway nodes in the domain.
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or re-establish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of the service you want to disable. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.
-Mode -mo	disable_mode	Required. Defines how the service is disabled: <ul style="list-style-type: none"> <li>- Complete. Disables the service after all service processes stop.</li> <li>- Stop. Stops all running jobs and then disables the service.</li> <li>- Abort. Stops all processes immediately, and then disables the service.</li> </ul>

## DisableService Example

The following sample command disables a Test Data Warehouse Service with the name *tdw1*:

```
infacmd isp disableService -dn Domain -un Administrator -pd Administrator -sn tdw1 -Mode
ABORT
```

## RemoveService

Removes the Test Data Warehouse Service and other application services from the domain. Before you remove a service, you must disable it.

The infacmd isp RemoveService command uses the following syntax:

```
RemoveService
```



```

<-DomainName|-dn> domain_name

<-UserName|-un> user_name

<-Password|-pd> password

[<-SecurityDomain|-sdn> security_domain]

[<-Gateway|-hp> gateway_host1:port gateway_host2:port...]

[<-ResilienceTimeout|-re> timeout_period_in_seconds]

<-ServiceName|-sn> service_name

```

The following table describes infacmd isp RemoveService options and arguments:

Option	Argument	Description
-DomainName -dn	domain_name	Required. Name of the Informatica domain. You can set the domain name with the -dn option or the environment variable INFA_DEFAULT_DOMAIN. If you set a domain name with both methods, the -dn option takes precedence.
-UserName -un	user_name	Required if the domain uses Native or LDAP authentication. User name to connect to the domain. You can set the user name with the -un option or the environment variable INFA_DEFAULT_DOMAIN_USER. If you set a user name with both methods, the -un option takes precedence.  Optional if the domain uses Kerberos authentication. To run the command with single sign-on, do not set the user name. If you set the user name, the command runs without single sign-on.
-Password -pd	password	Required if you specify the user name. Password for the user name. The password is case sensitive. You can set a password with the -pd option or the environment variable INFA_DEFAULT_DOMAIN_PASSWORD. If you set a password with both methods, the password set with the -pd option takes precedence.
-SecurityDomain -sdn	security_domain	Required if the domain uses LDAP authentication. Optional if the domain uses native authentication or Kerberos authentication. Name of the security domain to which the domain user belongs. You can set a security domain with the -sdn option or the environment variable INFA_DEFAULT_SECURITY_DOMAIN. If you set a security domain name with both methods, the -sdn option takes precedence. The security domain name is case sensitive.  If the domain uses native or LDAP authentication, the default is Native. If the domain uses Kerberos authentication, the default is the LDAP security domain created during installation. The name of the security domain is the same as the user realm specified during installation.
-Gateway -hp	gateway_host1:port gateway_host2:port ...	Required if the gateway connectivity information in the domains.infra file is out of date. The host names and port numbers for the gateway nodes in the domain.

Option	Argument	Description
-ResilienceTimeout -re	timeout_period_in_seconds	Optional. Amount of time in seconds that infacmd attempts to establish or reestablish a connection to the domain. If you omit this option, infacmd uses the timeout value specified in the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable. If no value is specified in the environment variable, the default of 180 seconds is used.
-ServiceName -sn	service_name	Required. Name of service you want to remove. To enter a name that contains a space or other non-alphanumeric character, enclose the name in quotation marks.

### RemoveService Example

The following sample command deletes a Test Data Warehouse Service with the name *tdw1*:

```
infacmd isp removeService -dn Domain -un Administrator -pd Administrator -sn tdw1
```

## CHAPTER 7

# Starting and Stopping Informatica and TDM

This chapter includes the following topics:

- [Starting and Stopping Informatica and TDM Overview, 99](#)
- [Starting and Stopping Informatica, 100](#)
- [Log In to Informatica Administrator, 102](#)
- [Starting and Stopping the TDM Server, 102](#)
- [Logging in to Test Data Manager, 102](#)

## Starting and Stopping Informatica and TDM Overview

When you install TDM and join an Informatica domain, the Informatica services must be running before you start the TDM Server.

On the node where you install Informatica and TDM, the installer creates a Windows service or UNIX daemon to run Informatica.

On Windows, the installer starts the Informatica service when the installation completes successfully. You can also start or stop the Informatica service from the Control Panel or from the Start menu.

On UNIX, you must start the Informatica daemon manually when the installation completes. Start or stop the Informatica daemon from the command line.

You use the Administrator tool to administer the Informatica domain objects and user accounts. Log in to the Administrator tool to create the user accounts for users of Informatica and TDM and to create and configure the Test Data Manager Service and other application services in the domain. You can also use the Administrator tool to shut down a node. When you shut down a node, you stop Informatica services on the node.

You can use Test Data Manager to configure and run TDM operations. You must create and enable the Test Data Manager Service before you can log in to Test Data Manager.

# Starting and Stopping Informatica

On UNIX, use a command line program to start or stop the Informatica daemon. On Windows, you can start or stop the Informatica service from the Control Panel or the Start menu.

## Starting and Stopping Informatica on UNIX

On UNIX, run `infaservice.sh` to start and stop the Informatica daemon. By default, `infaservice.sh` is installed in the following directory:

```
<InformaticaInstallationDir>/server/tomcat/bin
```

1. Go to the directory where `infaservice.sh` is located.
2. At the command prompt, enter the following command to start the daemon:

```
infaservice.sh startup
```

Enter the following command to stop the daemon:

```
infaservice.sh shutdown
```

**Note:** If you use a softlink to specify the location of `infaservice.sh`, set the `INFA_HOME` environment variable to the location of the Informatica installation directory.

## Starting and Stopping Informatica on Windows

You can use the Services window in the Control Panel, the Start menu shortcut, or a command prompt to start or stop the Informatica services.

### Starting or Stopping Informatica from the Start Menu

To start Informatica from the Windows Start menu, click **Programs > Informatica[Version] > Server**. Right-click **Start Informatica Services** and select **Run as Administrator**.

To stop Informatica from the Windows Start menu, click **Programs > Informatica[Version] > Server**. Right-click **Stop Informatica Services** and select **Run as Administrator**.

### Starting or Stopping Informatica from the Control Panel

The procedure to start or stop the Informatica Windows service is the same as for all other Windows services.

1. Open the Windows Control Panel.
2. Select **Administrative Tools**.
3. Right-click **Services** and select **Run as Administrator**.
4. Right-click the Informatica service.
5. If the service is running, click **Stop**.  
If the service is stopped, click **Start**.

## Configure the Windows Firewall

When you start the Informatica Windows service, the machines where you install the Informatica clients cannot access the Service Manager in the Informatica domain. To allow the clients access to the Service Manager, you must configure the firewall to grant client machines access to the domain.

On the machine where you created the Informatica domain, add the client machines to the list of firewall exceptions.

1. On the Windows Control Panel, open **Windows Firewall**.
2. On the Windows Firewall window, click the **Exceptions** tab.
3. Click **Add Program**.
4. On the Add a Program window, click **Browse**.  
The `infasvcs.exe` file runs the Service Manager in the domain.
5. Go to the following directory:  
`<Informatica installation directory>\tomcat\bin`
6. Select **infasvcs.exe** and click **Open**.  
The `infasvcs.exe` file appears in the list of programs.  
You can click **Change Scope** to specify the machines that you want to access Informatica.
7. Verify that the `infasvcs.exe` file appears in the list of programs and services and that it is enabled.
8. Click **OK**.

## Configuring the Informatica Windows Service

Use the Windows Control Panel to configure the user account that logs in to the Informatica Windows service and to configure the service restart option.

1. Open the Windows Control Panel.
2. Select **Administrative Tools**.
3. Select **Services**.
4. Double-click Informatica <Version>.  
The **Informatica <Version> Properties** dialog box appears.
5. Click the **Log On** tab.
6. Select **This account**.
7. Enter the domain and user name or click **Browse** to locate a system user.
8. Enter and confirm the password for the selected user account.
9. Click the **Recovery** tab. Select the options to restart the Informatica service if the service fails.

For more information about configuring system accounts for services and service restart options on Windows, see the Windows documentation.

# Log In to Informatica Administrator

You must have a user account to log in to the Informatica Administrator web application.

If the Informatica domain runs on a network with Kerberos authentication, you must configure the browser to allow access to the Informatica web applications. In Microsoft Internet Explorer and Google Chrome, add the URL of the Informatica web application to the list of trusted sites. If you are using Chrome version 41 or later, you must also set the `AuthServerWhitelist` and `AuthNegotiateDelegateWhitelist` policies.

1. Start a Microsoft Internet Explorer or Google Chrome browser.
2. In the **Address** field, enter the URL for the Administrator tool:
  - If the Administrator tool is not configured to use a secure connection, enter the following URL:  
`http://<fully qualified hostname>:<http port>/administrator/`
  - If the Administrator tool is configured to use a secure connection, enter the following URL:  
`https://<fully qualified hostname>:<http port>/administrator/`

Host name and port in the URL represent the host name and port number of the master gateway node. If you configured secure communication for the domain, you must use HTTPS in the URL to ensure that you can access the Administrator tool.

If you use Kerberos authentication, the network uses single sign on. You do not need to log in to the Administrator tool with a user name and password.

3. If you do not use Kerberos authentication, enter the user name, password, and security domain for your user account, and then click **Login**.

The **Security Domain** field appears when the Informatica domain contains an LDAP security domain. If you do not know the security domain that your user account belongs to, contact the Informatica domain administrator.

**Note:** If this is the first time you log in with the user name and password provided by the domain administrator, change your password to maintain security.

# Starting and Stopping the TDM Server

You must start the TDM Server before you can access Test Data Manager. The TDM Server is managed by the Test Data Manager Service.

Start the TDM Server by enabling the Test Data Manager Service from the Informatica Administrator. To stop the server, disable the Test Data Manager Service. You cannot use Test Data Manager to access the TDM Server contents when the Test Data Manager service is disabled.

# Logging in to Test Data Manager

You must have an Informatica user account to log in to Test Data Manager. Use the Informatica Administrator to create an Informatica user account.

1. Start a Microsoft Internet Explorer or Google Chrome browser.

2. In the **Address** field, enter the URL for Test Data Manager:

`http://<HostName>:<PortNumber>/tdm`

*HostName* represents the host name of the machine where TDM is installed. *PortNumber* is the startup port number for TDM. The default port number is 6605.

If you configure TDM to use HTTPS, the URL opens the HTTPS site:

`https://<HostName>:<HTTPSPortNumber>/tdm`

3. On the login page, enter an Informatica user name and password.

When you initially log in after installation, you can use the Informatica administrator user account.

4. Click **Login**.

## CHAPTER 8

# Uninstallation

This chapter includes the following topic:

- [Uninstallation Overview, 104](#)

## Uninstallation Overview

On UNIX, uninstall TDM from the command line. On Windows, uninstall from the Windows Start menu.

The uninstallation process deletes the TDM files and clears all configuration. The process does not delete files that are not installed with TDM. For example, the installation process creates temporary directories. The uninstaller does not keep a record of these directories and therefore cannot delete them. You must manually delete these directories for a clean uninstallation.

## Rules and Guidelines for Uninstallation

Use the following rules and guidelines when you uninstall TDM:

- The uninstallation mode depends on the mode that you use to install TDM. For example, you install TDM in console mode. When you run the uninstaller, it runs in console mode.
- Uninstalling TDM does not delete the TDM repository or the test data warehouse repository. The uninstaller removes the TDM files. It does not remove repositories from the database. If you need to move the repositories, you can back them up and restore them to another database.
- The uninstaller does not create a log of the uninstallation process. At the end of the uninstallation process, the uninstaller displays the names of the files and directories that could not be removed.

## Before You Uninstall

Before you uninstall TDM, stop and disable the Test Data Manager Service. The uninstallation process cannot remove the files that are being used by a service that is running.

## Uninstalling TDM

To uninstall TDM, use the uninstaller created during the installation. When you run the installation, the installer creates the following directory for the uninstaller:

```
<TDM installation directory>/Uninstaller_TDM
```

On Windows, do not use the Control Panel to uninstall. Uninstalling from the Control Panel does not completely remove TDM components.



## Running the Uninstaller on UNIX

To uninstall TDM on UNIX, run the uninstaller from the command line.

Go to the following directory:

```
<TDM installation directory>/Uninstaller_TDM
```

Run the uninstaller with the following command:

```
./uninstaller
```

## Running the Uninstaller on Windows

To uninstall TDM on Windows, double click the uninstaller file.

Go to the following directory:

```
<TDM installation directory>/Uninstaller_TDM
```

Double click the uninstaller file `uninstaller.exe`.

## APPENDIX A

# Updating the DynamicSections Parameter of a DB2 Database

This appendix includes the following topics:

- [DynamicSections Parameter Overview, 106](#)
- [Setting the DynamicSections Parameter, 106](#)

## DynamicSections Parameter Overview

IBM DB2 packages contain the SQL statements to be executed on the database server. The DynamicSections parameter of a DB2 database determines the maximum number of executable statements that the database driver can have in a package. You can raise the value of the DynamicSections parameter to allow a larger number of executable statements in a DB2 package. To modify the DynamicSections parameter, connect to the database using a system administrator user account with BINDADD authority.

## Setting the DynamicSections Parameter

Use the DataDirect Connect for JDBC utility to raise the value of the DynamicSections parameter in the DB2 database.

To use the DataDirect Connect for JDBC utility to update the DynamicSections parameter, complete the following tasks:

- Download and install the DataDirect Connect for JDBC utility.
- Run the Test for JDBC tool.

## Downloading and Installing the DDconnect JDBC Utility

Download the DataDirect Connect for JDBC utility from the DataDirect download web site to a machine that has access to the DB2 database server. Extract the contents of the utility file and run the installer.

1. Go to the DataDirect download site:  
<http://www.datadirect.com/support/product-documentation/downloads>
2. Choose the Connect for JDBC driver for an IBM DB2 data source.

3. Register to download the DataDirect Connect for JDBC Utility.
4. Download the utility to a machine that has access to the DB2 database server.
5. Extract the contents of the utility file to a temporary directory.
6. In the directory where you extracted the file, run the installer.

The installation program creates a folder named testforjdbc in the installation directory.

## Running the Test for JDBC Tool

After you install the DataDirect Connect for JDBC Utility, run the Test for JDBC tool to connect to the DB2 database. You must use a system administrator user account with the BINDADD authority to connect to the database.

1. In the DB2 database, set up a system administrator user account with the BINDADD authority.
2. In the directory where you installed the DataDirect Connect for JDBC Utility, run the Test for JDBC tool (testforjdbc).
3. On the Test for JDBC Tool window, click Press Here to Continue.
4. Click Connection > Connect to DB.
5. In the Database field, enter the following text:

```
jdbc:datadirect:db2://  
HostName:PortNumber;databaseName=DatabaseName;CreateDefaultPackage=TRUE;ReplacePackage=TRUE;DynamicSections=3000
```

*HostName* is the name of the machine hosting the DB2 database server.

*PortNumber* is the port number of the database.

*DatabaseName* is the name of the DB2 database.

6. In the User Name and Password fields, enter the system administrator user name and password you use to connect to the DB2 database.
7. Click Connect, and then close the window.

# INDEX

## A

Analyst Service  
    configuring [48](#)  
    creating [48](#)  
applications services  
    enabling [83](#)

## B

before installing the clients  
    verifying installation requirements [51](#)  
    verifying minimum system requirements [51](#)  
    verifying third-party software requirements [51](#)

## C

configuration  
    Windows firewalls [101](#)  
CreateContent (infacmd tdm) [82](#)  
CreateContent (infacmd tdw) [92](#)  
CreateService (infacmd tdm) [75](#)  
CreateService (infacmd tdw) [87](#)

## D

Data Analyzer repository  
    Oracle database requirements [35](#)  
Data Integration Service  
    configuring [45](#)  
    creating [45](#)  
database preparations  
    repositories [32](#)  
database requirements  
    installation requirements [24](#)  
    Model repository [32](#)  
    PowerCenter repository [34](#)  
    profiling warehouse [36](#)  
DisableService (infacmd isp) [95](#)  
DisableService (infacmd tdm) [84](#)  
disk space requirements  
    installation requirements [14, 20](#)  
domain configuration repository  
    IBM DB2 database requirements [32](#)  
    Microsoft SQL Server database requirements [29](#)

## E

EnableService (infacmd isp) [93](#)  
EnableService (infacmd tdm) [83](#)  
environment variables  
    DISPLAY [18](#)

environment variables (*continued*)  
    installation [15, 21](#)

## F

firewalls  
    configuring on Windows [101](#)

## G

graphical mode  
    installation requirements [18](#)  
    installing Informatica clients [52](#)

## H

HTTPS  
    installation requirements [16, 21](#)

## I

IATEMPDIR  
    environment variables [15, 21](#)  
IBM DB2  
    single-node tablespaces [34](#)  
IBM DB2 database requirements  
    domain repository [32](#)  
    Model repository database [32](#)  
    PowerCenter repository [34](#)  
    profiling warehouse [36](#)  
INFA\_HOME  
    environment variables [15, 21](#)  
INFA\_JDK\_HOME  
    environment variables [15](#)  
infacmd isp  
    disabling test data warehouse service [95](#)  
    enabling test data warehouse service [93](#)  
infacmd tdm  
    creating Test Data Manager Service Content in a domain [82](#)  
    creating Test Data Manager Service in a domain [75](#)  
    disabling the Test Data Manager Service [84](#)  
    enabling the Test Data Manager Service [83](#)  
    services, removing [85](#)  
infacmd tdw  
    creating Test Data Warehouse Service Content in a domain [92](#)  
    creating Test Data Warehouse Service in a domain [87](#)  
Informatica Administrator  
    logging in [102](#)  
Informatica clients  
    installing in graphical mode [52](#)  
    installing in silent mode [53](#)

- Informatica services
  - configuring [101](#)
  - starting and stopping on Windows [100](#)
- Informatica Services
  - starting and stopping on UNIX [100](#)
- installation
  - TDM
    - UNIX
      - console mode [56](#)
      - graphical mode [55](#)
    - Windows
      - graphical mode [55](#)
- installation requirements
  - database requirements [24](#)
  - disk space [14](#), [20](#)
  - environment variables [15](#), [21](#)
  - keystore file [16](#), [21](#)
  - minimum system requirements [14](#), [19](#)
  - TDM repository database [24](#)
  - X Window Server [18](#)
- ITDM
  - uninstallation [104](#)

## J

- JAVA\_HOME
  - environment variables [15](#), [21](#)

## K

- keystore file
  - installation requirements [16](#), [21](#)

## L

- LANG
  - locale environment variables [15](#)
- LC\_ALL
  - locale environment variables [15](#)
- LD\_PRELOAD
  - locale environment variables [15](#)
- library path
  - environment variables [15](#)
- license key
  - verifying [14](#), [19](#)
- logs
  - Test Data Manager Service [71](#)

## M

- Microsoft SQL Server database requirements
  - domain configuration repository [29](#)
  - Model repository [33](#)
  - PowerCenter repository [34](#)
  - profiling warehouse [36](#)
  - TDM repository [27](#)
- Model repository
  - database requirements [32](#)
  - IBM DB2 database requirements [32](#)
  - Microsoft SQL Server database requirements [33](#)
  - Oracle database requirements [34](#)
- Model Repository Service
  - configuring [42](#)
  - creating [42](#)

## N

- normal mode
  - PowerCenter Repository Service [39](#)

## O

- operating mode
  - PowerCenter Repository Service [39](#)
- optimization
  - PowerCenter repository [34](#)
- Oracle database requirements
  - Data Analyzer repository [35](#)
  - Model repository [34](#)
  - profiling warehouse [37](#)
  - TDM repository [25](#)
  - test data warehouse repository [29](#)

## P

- PATH
  - environment variables [15](#), [21](#)
- PowerCenter Client
  - third-party software requirements [51](#)
- PowerCenter Integration Service
  - configuring [40](#)
  - creating [40](#), [41](#)
- PowerCenter repository
  - database requirements [34](#)
  - IBM DB2 database requirements [34](#)
  - Microsoft SQL Server database requirements [34](#)
  - optimizing IBM DB2 databases [34](#)
  - Sybase ASE database requirements [35](#)
  - users [39](#)
- PowerCenter Repository Service
  - after creating [39](#)
  - configuring [37](#)
  - creating [37](#)
  - normal mode [39](#)
- profiling warehouse
  - database requirements [36](#)
  - IBM DB2 database requirements [36](#)
  - Microsoft SQL Server database requirements [36](#)
  - Oracle database requirements [37](#)

## R

- RemoveService (infacmd isp)
  - test data warehouse service [96](#)
- removeService (infacmd tdm)
  - description [85](#)
- repositories
  - preparing databases [32](#)

## S

- services
  - starting and stopping [100](#)
- silent mode
  - installing Informatica clients [53](#)
- Sybase ASE database requirements
  - PowerCenter repository [35](#)
- system requirements
  - minimum installation requirements [14](#), [19](#)

system requirements (*continued*)

TDM Server [14](#), [20](#)

## T

tablespaces

single nodes [34](#)

TDM repository

Microsoft SQL Server database requirements [27](#)

Oracle database requirements [25](#)

requirements [24](#)

TDM repository database

installation requirements [24](#)

TDM Server

system requirements [14](#), [20](#)

TDM service

disabling [84](#)

Test Data Manager Service

assign a new license [70](#)

creating [66](#)

creating in a domain [75](#), [82](#)

removing using infacmd tdm [85](#)

test data warehouse repository

Oracle database requirements [29](#)

test data warehouse service

disabling [95](#)

enabling [93](#)

removing using infacmd isp [96](#)

Test Data Warehouse Service

creating in a domain [87](#), [92](#)

third-party software requirements

PowerCenter Client [51](#)

## U

uninstallation

process [104](#)

rules and guidelines [104](#)

user accounts

PowerCenter repository [39](#)

## W

Windows

configuring firewalls [101](#)

installing Informatica clients in graphical mode [52](#)

starting and stopping Informatica services [100](#)

## X

X Window Server

installation requirements [18](#)