Informatica

Informatica® Dynamic Data Masking
9.8.2

Installation and Upgrade Guide

Informatica Dynamic Data Masking Installation and Upgrade Guide
9.8.2
October 2016

© Copyright Informatica LLC 1993, 2018

This software and documentation contain proprietary information of Informatica LLC and are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright law. Reverse engineering of the software is prohibited. 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. This Software may be protected by U.S. and/or international Patents and other Patents Pending.

Use, duplication, or disclosure of the Software by the U.S. Government is subject to the restrictions set forth in the applicable software license agreement and as provided in DFARS 227.7202-1(a) and 227.7702-3(a) (1995), DFARS 252.227-7013©(1)(ii) (OCT 1988), FAR 12.212(a) (1995), FAR 52.227-19, or FAR 52.227-14 (ALT III), as applicable.

The information in this product or documentation is subject to change without notice. If you find any problems in this product or documentation, please report them to us in writing.

Informatica, Informatica Platform, Informatica Data Services, PowerCenter, PowerCenterRT, PowerCenter Connect, PowerCenter Data Analyzer, PowerExchange, PowerMart, Metadata Manager, Informatica Data Quality, Informatica Data Explorer, Informatica B2B Data Transformation, Informatica B2B Data Exchange Informatica On Demand, Informatica Identity Resolution, Informatica Application Information Lifecycle Management, Informatica Complex Event Processing, Ultra Messaging, Informatica Master Data Management, and Live Data Map are trademarks or registered trademarks of Informatica LLC in the United States and in jurisdictions throughout the world. All 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 (c) 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>. 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.

The product includes software copyright © 2004-2007, The Dojo Foundation. All Rights Reserved. Permissions and limitations regarding this software are subject to terms available at http://dojotoolkit.org/license.

This product includes ICU software which is copyright International Business Machines Corporation and others. All rights reserved. Permissions and limitations regarding this software are subject to terms available at http://source.icu-project.org/repos/icu/icu/trunk/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.

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/hsqlLicense.html, http://httpunit.sourceforge.net/doc/ license.html, http://jung.sourceforge.net/license.txt , 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/licence.html; http://www.jgraph.com/jgraphdownload.html; http://www.jcraft.com/jsch/LICENSE.txt; 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/orig/copyright.html; http://www.json.org/license.html; http://forge.ow2.org/projects/javaservice/, http://www.postgresql.org/about/licence.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://srp.stanford.edu/license.txt; http://www.schneier.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.

Publication Date: 2018-06-26

Table of Contents

Preface 6

Informatica Resources. 6

Informatica Network. 6

Informatica Knowledge Base. 6

Informatica Documentation. 6

Informatica Product Availability Matrixes. 7

Informatica Velocity. 7

Informatica Marketplace. 7

Informatica Global Customer Support. 7

Chapter 1: Installation Overview 8

Installation Overview. 8

Chapter 2: Before You Install or Upgrade 9

Overview of Pre-Installation Tasks. 9

Download Software and License Key. 10

Dynamic Data Masking Installer. 10

Verify the Minimum System Requirements. 10

Verify the Temporary Disk Space Requirements. 11

Install Java SE 8 on UNIX. 11

Verify Port Availability. 11

Verify Installation User Account Privileges. 12

Set Up the X Window Server. 12

Chapter 3: Product Installation 14

Product Installation Overview. 14

Installing the Dynamic Data Masking Server and Management Console. 14

Installing in Graphical Mode. 15

Installing in Console Mode. 16

Installing in Silent Mode. 17

Installing the Management Console. 18

Installing in Graphical Mode. 18

Installing in Console Mode. 19

Troubleshooting the Installation. 19

Installation Log File. 19

Starting the Dynamic Data Masking Server. 20

Chapter 4: Upgrade from Dynamic Data Masking 9.5.0 or Later 21

Upgrade from Dynamic Data Masking 9.5.0 or Later Overview. 21

Before You Upgrade. 22

Back Up the Configuration Files. 22
Update the License Key. 22
Upgrade the Server and Management Console. 22
Upgrade the Management Console to the Server and Management Console. 23
Upgrade the Management Console. 25
Upgrade in Silent Mode. 25

Chapter 5: Upgrade from Dynamic Data Masking 9.1.0 or ActiveBase Security 3.1. 27

Upgrade from Dynamic Data Masking 9.1.0 or ActiveBase Security 3.1 Overview. 27
Before You Upgrade. 27
Back Up the Configuration Files. 28
Uninstall Dynamic Data Masking. 28
Dynamic Data Masking 9.1.0 or ActiveBase Security 3.1 Upgrade. 28
Upgrading in Graphical Mode. 28
Upgrading in Console Mode. 30

Chapter 6: After You Install or Upgrade. 32

After You Install the Dynamic Data Masking Server. 32
Verify the Location of Java SE 8. 32
Set User Resource Boundaries. 33
Set Up Authentication. 33
Automatic Restart. 33
Upgrade the Dynamic Data Masking for Microsoft SQL Server Service. 34
After You Install the Management Console. 37

Chapter 7: Uninstallation. 38

Uninstallation Overview. 38
Uninstalling in Graphical Mode. 38
Uninstalling in Console Mode. 39

Index. 40

Preface

The *Informatica Dynamic Data Masking Installation Guide* is written for system administrators who are responsible for the installation or upgrade of Dynamic Data Masking. This guide assumes you have knowledge of your operating systems, relational database concepts, and the database engines in your environment.

Informatica Resources

Informatica Network

Informatica Network hosts Informatica Global Customer Support, the Informatica Knowledge Base, and other product resources. To access Informatica Network, visit https://network.informatica.com.

As a member, you can:

- Access all of your Informatica resources in one place.
- Search the Knowledge Base for product resources, including documentation, FAQs, and best practices.
- View product availability information.
- 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 search Informatica Network for product resources such as documentation, how-to articles, best practices, and PAMs.

To access the Knowledge Base, visit https://kb.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

To get the latest documentation for your product, browse the Informatica Knowledge Base at https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx.

If you have questions, comments, or ideas about this documentation, contact the Informatica Documentation team through email at infa_documentation@informatica.com.

Informatica Product Availability Matrixes

Product Availability Matrixes (PAMs) indicate the versions of operating systems, databases, and other types of data sources and targets that a product release supports. If you are an Informatica Network member, you can access 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. Developed from the real-world experience of hundreds of data management projects, Informatica Velocity represents the collective knowledge of our consultants who have worked with organizations from around the world to plan, develop, deploy, and maintain successful data management solutions.

If you are an Informatica Network member, you can access 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.

Informatica Marketplace

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

Informatica Global Customer Support

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

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
http://www.informatica.com/us/services-and-training/support-services/global-support-centers.

If you are an Informatica Network member, you can use Online Support at http://network.informatica.com.

CHAPTER 1

Installation Overview

This chapter includes the following topic:

- Installation Overview, 8

Installation Overview

Dynamic Data Masking is a data security tool that operates between an application and a database to prevent unauthorized access to sensitive information. The installation includes the Dynamic Data Masking Server and a Management Console that you can use to manage and configure the Dynamic Data Masking Server.

Dynamic Data Masking acts as a proxy between the database and the application. You can install the Dynamic Data Masking Server on the same machine as the database server or on a separate machine.

When you run the Dynamic Data Masking installer, you can select from the following installation options:

Dynamic Data Masking Server and Management Console

Installs the following components in one installation process:

- Dynamic Data Masking Server
- Server Control
- Management Console

You can use the Server Control application and the Management Console to manage the Dynamic Data Masking Server on the same machine.

To run the Dynamic Data Masking Server and manage the connection and security rules on the same machine, you can install the Dynamic Data Masking Server and the Management Console together.

Management Console

Installs the Management Console only. You can install the Management Console on a different machine than where you install the Dynamic Data Masking Server.

To manage the connection and security rules remotely, you can install the Management Console on a different machine. Connect to the Dynamic Data Masking Server through the port number you specify when you install the server.

You can install the Management Console on multiple machines.

You can install Dynamic Data Masking on a machine with Linux, UNIX, or Windows operating system.

CHAPTER 2

Before You Install or Upgrade

This chapter includes the following topics:

- Overview of Pre-Installation Tasks, 9
- Download Software and License Key, 10
- Verify the Minimum System Requirements, 10
- Verify the Temporary Disk Space Requirements, 11
- Install Java SE 8 on UNIX, 11
- Verify Port Availability, 11
- Verify Installation User Account Privileges, 12
- Set Up the X Window Server, 12

Overview of Pre-Installation Tasks

Before you install Dynamic Data Masking, verify the prerequisites for installation and ensure that the machine where you plan to install meets the installation requirements.

Complete the following pre-installation tasks:

- Download the software and license key.
  If you install the Management Console only, you do not need a license key.
- Verify the minimum system requirements.
- Verify the temporary disk space requirements.
- On UNIX, install Java SE 8.
- Verify the availability of port numbers.
- Verify that the installation user account has the appropriate privileges.
- On UNIX, if you install in graphical mode, set up the X Window server.

Download Software and License Key

Download the installation file and license key to the machine where you plan to install Dynamic Data Masking. If you install the Management Console only, you do not need a license key.

You can get the software and the license key from an FTP download. If you choose to download the software, you receive an email that contains the following information:

- Download links. The software is bundled into installation .zip files with a unique link. The download link takes you to the Informatica Download Manager. After you sign in to the Download Manager, save the installation .zip file to a directory that is accessible from the machine where you plan to install the product.
- User ID and password. After you click the download link, sign in to the Download Manager with the user ID and password.
- License key. The license key is included as an attachment to the email message. Copy the license key file to the machine where you plan to install the product.

If you do not have a license key, contact Informatica Global Customer Support.

Dynamic Data Masking Installer

Use the Dynamic Data Masking installer for the platform on which you want to install Dynamic Data Masking.

The following table describes the installation files that you use for each platform:

Installation File	Platform
Informatica_DDM_982_Installer_Win (64 & 32 Bit)	Windows
Informatica_DDM_982_Installer_Unix_nojvm	- HP-UX - AIX - Solaris
Informatica_DDM_982_Installer_linux64	- Red Hat Enterprise Linux - SUSE Linux

The Windows and Linux installers contain the Java SE files required to run Dynamic Data Masking. On UNIX, you must install Java SE before you begin the installation.

Verify the Minimum System Requirements

Verify that the machine where you install Dynamic Data Masking meets the prerequisites for installation.

The following table describes the minimum system requirements for Dynamic Data Masking:

Component	Processor	RAM	Disk Space
Dynamic Data Masking Server and Management Console	Dual Core Processor	256 MB	2.6 GB
Management Console only	Dual Core Processor	256 MB	2.6 GB

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/overview

Verify the Temporary Disk Space Requirements

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 installer requires 2.6 GB of temporary disk space.

Install Java SE 8 on UNIX

If you install Dynamic Data Masking on UNIX, verify that the machine where you perform the installation has Java SE 8.

The Dynamic Data Masking installer, Dynamic Data Masking Server, and Management Console require Java Development Kit (JDK) SE 8 to run. On UNIX, you must install Java SE 8 before you start the installation so that the Dynamic Data Masking installer runs properly. The Java directory must be in the system path.

On Windows or Linux, you do not need to install Java. The Dynamic Data Masking installer contains the Java SE 8 files.

Verify Port Availability

Verify that the port numbers that you plan to use for Dynamic Data Masking are available and open on the machine where you install the Dynamic Data Masking Server.

If necessary, change the firewall configuration to open the ports for the Dynamic Data Masking Server.

The following table lists the minimum system requirements for Dynamic Data Masking:

Port	Description
Dynamic Data Masking service listener port	Port that applications use to connect to the database. The Dynamic Data Masking service listens on this port to intercept database requests sent to the database. If applications connect to multiple databases, you need to verify the availability of multiple port numbers. You must specify a listener port number when you create a Dynamic Data Masking service in the Management Console. Dynamic Data Masking uses the following default listener port numbers: - Dynamic Data Masking Service for Microsoft SQL Server: 1434 - Dynamic Data Masking Service for Informix: 9090 - Dynamic Data Masking Service for Hive: 10001 - Dynamic Data Masking Service for Oracle: 1525 - Dynamic Data Masking Service for DB2: 50001 - Dynamic Data Masking Service for FAS: 8501 - Dynamic Data Masking Service for Teradata: 1025 - Dynamic Data Masking Service for Informix (DRDA): 9089 - Dynamic Data Masking Service for Sybase: 5001
Dynamic Data Masking Server port	Port number that the Management Console uses to connect to the Dynamic Data Masking Server. Default is 8195. You must set the port number during the installation process. After installation, you can use the Server Control command setPort to change the port number.

Verify Installation User Account Privileges

Verify that the user account that you use to run the installer has administrator privileges on the machine where you plan to install the Dynamic Data Masking Server or Management Console.

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.

CHAPTER 3

Product Installation

This chapter includes the following topics:

- Product Installation Overview, 14
- Installing the Dynamic Data Masking Server and Management Console, 14
- Installing the Management Console, 18
- Troubleshooting the Installation, 19

Product Installation Overview

When you install Dynamic Data Masking, you can install the Dynamic Data Masking Server and the Management Console, or you can install the Management Console alone.

The Dynamic Data Masking installer provides the following installation options:

- Dynamic Data Masking Server and Management Console. Installs the Dynamic Data Masking Server and the Management Console in one process.
- Management Console. Installs only the Management Console. Before you can use the Management Console, the Dynamic Data Masking Server must be installed on the same machine or on a different machine.

You can run the Dynamic Data Masking installer in graphical, console, or silent mode.

Installing the Dynamic Data Masking Server and Management Console

You can install the Dynamic Data Masking Server and Management Console in graphical mode, console mode, or silent mode. Use silent mode to install the Dynamic Data Masking Server and Management Console without user interaction.

If you install on UNIX in graphical mode, you must set up an X Window server.

If you install on Windows, the installer updates the system path to include the following path:

```
<Dynamic Data Masking installation>\jre\bin
```

Installing in Graphical Mode

1. Log in to the machine with a user account that has administrator privileges.
2. Navigate to the directory where you downloaded the Dynamic Data Masking installation file.
3. Begin the installation on Linux, UNIX, or Windows.
   - To begin the installation on Linux or UNIX, run the following command on a shell command line: `DDMInstaller.bin`.
   - To begin the installation on Windows, run `DDMInstaller.exe`.

   The **Welcome** page appears.
4. Click **Next**.

   The **Installation Mode** page appears.
5. Select the option to install the Dynamic Data Masking Server and Console.
6. Click **Next**.

   The **Installation Folder** page appears.
7. Enter the absolute path for the installation directory and click **Next**.

   The path must conform to the length and character restrictions of the operating system.

   The **License Key** page appears.
8. Enter the path and file name of the Dynamic Data Masking license key and click **Next**.

   The **Server Details** page appears.
9. Enter the name, port number, and password for the Dynamic Data Masking Server.

   The following table describes the properties that you must specify:

Property	Description
Server Name	Required. Name of the Dynamic Data Masking Server. On UNIX, the installer creates a process with the same name as the Dynamic Data Masking Server. On Windows, the installer creates a Windows service with the same name as the Dynamic Data Masking Server. The server name must be unique and must conform to the naming restrictions for a UNIX process or Windows service.
Server Port Number	Required. Port number that the Management Console uses to connect to the Dynamic Data Masking Server. Default is 8195. If port number 8195 is not available, the installer uses the next available port number as default.
Server Password	Required. Password to log in to the Dynamic Data Masking Server through the Management Console.
Confirm Password	Required. Enter the password again to confirm.

10. Click **Next**.

    The **Pre-installation Summary** page displays the installation details.
11. Verify that the installation details are correct before you continue the installation and then click **Install**.

    The installer copies the Dynamic Data Masking files to the installation directory. When the installation completes, the installer indicates whether the installation is successful.

12. Click **Done** to close the installer.

    You can view the `DDM_Install.log` file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the `DDM_Install.log` file for details. The log file is in the installation directory.

Installing in Console Mode

1. Log in to the machine with a user account that has administrator privileges.
2. Begin the installation on Linux, UNIX, or Windows. Use a shell command line to navigate to the installation directory and run the following commands:
   - On Linux or UNIX, run the following command:

     ```
     DDMInstaller.bin  -i console
     ```

   - On Windows, run the following command

     ```
     DDMInstaller.exe -i console
     ```

   The **Welcome** page appears.
3. Press Enter to continue.

   The **Installation Mode** page appears.
4. Enter 1 to install the Dynamic Data Masking Server and Console.
5. Enter the absolute path for the installation directory.

   The installer displays the installation directory and requests confirmation.
6. Press Enter to continue.

   The **License Key** page appears.
7. Enter the path and file name of the Dynamic Data Masking license key and press Enter.

   The prompts for **Server Details** appears.
8. Enter the name, port number, and password for the Dynamic Data Masking Server.

   The following table describes the properties that you must specify:

Property	Description
Server Name	Required. Name of the Dynamic Data Masking Server. On UNIX, the installer creates a process with the same name as the Dynamic Data Masking Server. On Windows, the installer creates a Windows service with the same name as the Dynamic Data Masking Server. The server name must be unique and must conform to the naming restrictions for a UNIX process or Windows service.
Server Port Number	Required. Port number that the Management Console uses to connect to the Dynamic Data Masking Server. Default is 8195. If port number 8195 is not available, the installer uses the next available port number as default.

Property	Description
Server Password	Required. Password to log in to the Dynamic Data Masking Server through the Management Console. When you type the password, the installer does not display the characters that you enter on the command line.
Confirm Password	Required. Enter the password again to confirm. When you type the password, the installer does not display the characters that you enter on the command line.

9. Press Enter to continue after each entry.

   The **Pre-installation Summary** page displays the installation details.

10. Verify that the installation details are correct and then press Enter to install.

    The installer copies the Dynamic Data Masking files to the installation directory. When the installation completes, the installer indicates whether the installation is successful.

11. Press Enter to close the installer.

    You can view the `DDM_Install.log` file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the `DDM_Install.log` file for details. The log file is in the installation directory.

Installing in Silent Mode

To install the Dynamic Data Masking Server and Management Console without user interaction, install in silent mode.

1. Log in to the machine with a user account that has administrator privileges.
2. Navigate to the directory where you downloaded the Dynamic Data Masking installation file.
3. Locate the SilentInput.properties file.
4. Create a backup copy of the SilentInput.properties file.
5. Use a text editor to open the SilentInput.properties file and modify the values of the installation parameters.

   The following table describes the Dynamic Data Masking installation parameters that you can modify:

Property Name	Description
USER_INSTALL_DIR	Absolute path for the directory in which to install Dynamic Data Masking. If the folder contains a current installation, Dynamic Data Masking will upgrade. Use the default path format. Use two backslashes (\\) before folder names for installation on Windows. Use a slash (/) for installation on Linux and UNIX.
PA_LICENSE_FILE	Absolute path to a valid license file. Use the default path format. Use two backslashes (\\) before folder names for installation on Windows. Use a slash (/) for installation on Linux and UNIX.

Property Name	Description
PA_SERVER_NAME	Dynamic Data Masking Server name. Modify PA_SERVER_NAME to install a Dynamic Data Masking Server with a different name.
PA_PORT_NUMBER	Dynamic Data Masking port. Modify PA_PORT_NUMBER to install a Dynamic Data Masking Server that uses a different port. The number of the port must be valid and not locked.

6. Save the SilentInput.properties file in the same directory as the silent install script file.
7. Begin the installation on Linux, UNIX, or Windows. Use a shell command line to navigate to the installation directory and run the following commands:
   - On Linux or UNIX, run the following command: `silentinstall <administrator password>`
   - On Windows, run the following command `SilentInstall.bat <administrator password>`

   The administrator password is the Dynamic Data Masking administrator password. If you do not provide a password, Dynamic Data Masking uses the default password, admin. If you use the default password, you can change the password after you install.
8. You can view the `DDM_Install.log` file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the `DDM_Install.log` file for details. The log file may be in the installation directory, on the desktop on Windows, or in the /home/user directory on Linux and UNIX.

Installing the Management Console

You can install the Management Console in graphical mode or in console mode.

Installing in Graphical Mode

1. Log in to the machine with a user account that has administrator privileges.
2. Begin the installation. Use a shell command line to navigate to the installation directory and run the following command:

   ```
   DDMInstaller.exe
   ```

   The **Welcome** page appears.
3. Click **Next**.

   The **Installation Mode** page appears.
4. Select the option to install the Management Console.
5. Click **Next**.

   The **Installation Folder** page appears.
6. Enter the absolute path for the installation directory and click **Next**.

   The path must conform to the length and character restrictions of the operating system.

   The **Pre-installation Summary** page displays the installation details.
7. Verify that the installation details are correct before you continue the installation and then click **Install**.

   The installer copies the Management Console files to the installation directory. When the installation completes, the installer indicates whether the installation is successful.

8. Click **Done** to close the installer.

   You can view the `DDM_Install.log` file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the `DDM_Install.log` file for details. The log file is in the installation directory.

Installing in Console Mode

1. Log in to the machine with a user account that has administrator privileges.
2. Begin the installation. Use a shell command line to navigate to the installation directory and run the following command:

   ```
   DDMInstaller.exe -i console
   ```

   The **Welcome** page appears.
3. Press Enter to continue.

   The **Installation Mode** page appears.
4. Enter 2 to install the Management Console.
5. Enter the absolute path for the installation directory.

   The installer displays the installation directory and requests confirmation.
6. Press Enter to continue.

   The **Pre-installation Summary** page displays the installation details.
7. Verify that the installation details are correct and then press Enter to install.

   The installer copies the Dynamic Data Masking Management Console files to the installation directory. When the installation completes, the installer indicates whether the installation is successful.
8. Press Enter to close the installer.

   You can view the `DDM_Install.log` file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the `DDM_Install.log` file for details. The log file is in the installation directory.

Troubleshooting the Installation

When you install Dynamic Data Masking, the installer produces a log file during the installation. Use the log file to get more information about the installation process and to troubleshoot errors that occurred during the installation.

Installation Log File

The installer creates the DDM_Install.log log file during installation. Use the log file to troubleshoot the installation or to view more information about the installation.

The installation log file contains information about the user interactions, installer actions, and installation outcome. If the installation fails, use the installation log file to troubleshoot the error.

The installation log file contains the following information:

- Date and time of the installation

- Memory statistics at the time of the installation
- Class paths and Java extension paths
- Java properties
- Installation start and end times
- Summary of user input during the installation
- Installation mode
- Installation directory
- Directories and files that the installer creates
- Summary of success or failure of installer actions
- List of all installer actions, status of each action, and additional notes for each action

You can find the installation log file in the following directory:

```
<Dynamic Data Masking installation>/DDM_Install.log
```

Starting the Dynamic Data Masking Server

When you install the Dynamic Data Masking Server and Management Console, the installer starts the Dynamic Data Masking Server. To troubleshoot issues when the Dynamic Data Masking Server fails to start, use the information in the DDM_Install.log file to identify the cause of the error.

CHAPTER 4

Upgrade from Dynamic Data Masking 9.5.0 or Later

This chapter includes the following topics:

- Upgrade from Dynamic Data Masking 9.5.0 or Later Overview, 21
- Before You Upgrade, 22
- Upgrade the Server and Management Console, 22
- Upgrade the Management Console to the Server and Management Console, 23
- Upgrade the Management Console, 25
- Upgrade in Silent Mode, 25

Upgrade from Dynamic Data Masking 9.5.0 or Later Overview

You can use the Dynamic Data Masking installer to upgrade from Dynamic Data Masking 9.5.0 or later.

The Dynamic Data Masking installer uninstalls the previous version of Dynamic Data Masking and installs the current version. Dynamic Data Masking preserves the configuration and log information from the previous version.

You must upgrade in graphical mode or silent mode. You cannot upgrade in console mode.

The following table describes the upgrade options:

Current Installation	Upgrade
Dynamic Data Masking Server and Management Console	Dynamic Data Masking Server and Management Console
Management Console	- Dynamic Data Masking Server and Management Console - Management Console

Before You Upgrade

Before you upgrade, perform the following tasks:

- Verify the prerequisites for the installation and ensure that the machine where you plan to install meets the installation requirements.
- Back up the Dynamic Data Masking configuration files.
- Close the Dynamic Data Masking Management Console.
- Stop the Dynamic Data Masking Server.
- Optionally, update the license key.
- Remove the Dynamic Data Masking Windows operating system service.

Back Up the Configuration Files

Dynamic Data Masking stores database connection information and masking rules in configuration files. Before you upgrade, back up the configuration files to safeguard the files during the upgrade process.

You can find the Dynamic Data Masking configuration files in the following directory:

```
<Dynamic Data Masking directory>\cfg
```

Back up the following files:

- config.properties
- config.cfg

Update the License Key

When you upgrade the Dynamic Data Masking Server, the installer prompts you to give the location of the license file if an active license file is not in the Dynamic Data Masking cfg directory. You can optionally update the license file before you run the installer.

1. Stop the Dynamic Data Masking Server. From a Server Control window, run the following command:

   ```
   server stop
   ```

2. If the Dynamic Data Masking Server runs on Windows, remove the Server. From a Server Control window, run the following command:

   ```
   server remove
   ```

3. If an expired license key exists in the installation directory, remove the file. You can find the file in the following location:

   ```
   <Dynamic Data Masking installation>\cfg\license.lic
   ```

4. Save the new license key as license.lic in the following location:

   ```
   <Dynamic Data Masking installation>\cfg\license.lic
   ```

Upgrade the Server and Management Console

Upgrade from Dynamic Data Masking 9.5.0 or later in graphical mode. The upgrade process uninstalls the previous version and installs the current version.

1. Log in to the machine with a user account that has administrator privileges.

2. Close all shells and windows that have the Dynamic Data Masking installation directory current or open.
3. Begin the installation on Linux, UNIX, or Windows.
   - Begin installation on Linux or UNIX in a directory outside of the Dynamic Data Masking installation directory. Run the following command on a shell command line:

     ```
     <Dynamic Data Masking installation>/DDMInstaller.bin
     ```

   - On Windows, use a shell command line to navigate to the installation directory and run the following command

     ```
     DDMInstaller.exe
     ```

   The **Welcome** page appears.
4. Click **Next**.

   The **Installation Mode** page appears.
5. Select the option to install the Dynamic Data Masking Server and Management Console.
6. Click **Next**.

   The **Installation Folder** page appears.
7. Enter the absolute path for the directory where you have Dynamic Data Masking installed and click **Next**.

   The **Upgrade** window appears.
8. Click **OK**.

   The **Uninstall Previous Installation** window appears.
9. Click **OK.**

   The **Pre-Installation Summary** page displays the installation details.
10. Verify that the installation details are correct before you continue the installation and then click **Install.**

    When the installation completes, the installer indicates whether the installation is successful.
11. Click **Done** to close the installer.

You can view the DDM_Install.log file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the DDM_Install.log file for details. The log file is in the installation directory.

Upgrade the Management Console to the Server and Management Console

Upgrade from Dynamic Data Masking 9.5.0 or later in graphical mode. The upgrade process uninstalls the previous version and installs the current version.

1. Log in to the machine with a user account that has administrator privileges.
2. Begin the installation on Linux, UNIX, or Windows. Use a shell command line to navigate to the installation directory and run the following commands:
   - On Linux or UNIX, run the following command:

     ```
     DDMInstaller.bin
     ```

   - On Windows, run the following command

     ```
     DDMInstaller.exe
     ```

   The **Welcome** page appears.

3. Click **Next**.

   The **Installation Mode** page appears.

4. Select the option to install the Dynamic Data Masking Server and Management Console.
5. Click **Next**.

   The **Installation Folder** page appears.

6. Enter the absolute path for the directory where you have the Dynamic Data Masking Management Console installed and click **Next**.

   The **Upgrade Folder Incomplete** window appears.

7. Click **Continue.**

   The **License Key** page appears.

8. Enter the path and file name of the Dynamic Data Masking license key and click **Next**.

   The **Server Details** page appears.

9. Enter the name, port number, and password for the Dynamic Data Masking Server.

   The following table describes the properties that you configure:

Property	Description
Server Name	Required. Name of the Dynamic Data Masking Server. On UNIX, the installer creates a process with the same name as the Dynamic Data Masking Server. On Windows, the installer creates a Windows service with the same name as the Dynamic Data Masking Server. The server name must be unique and must conform to the naming restrictions for a UNIX process or Windows service.
Server Port Number	Required. Port number that the Management Console uses to connect to the Dynamic Data Masking Server. Default is 8195. If port number 8195 is not available, the installer uses the next available port number as default.
Server Password	Required. Password to log in to the Dynamic Data Masking Server through the Management Console.
Confirm Password	Required. Enter the password again to confirm.

10. Click **Next**.

    The **Uninstall Previous Installation** window appears.

11. Click **OK.**

    The **Pre-Installation Summary** page displays the installation details.

12. Verify that the installation details are correct before you continue the installation and then click **Install.**

    When the installation completes, the installer indicates whether the installation is successful.

13. Click **Done** to close the installer.

You can view the DDM_Install.log file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the DDM_Install.log file for details. The log file is in the installation directory.

Upgrade the Management Console

Upgrade from Dynamic Data Masking 9.5.0 or later in graphical mode. The upgrade process uninstalls the previous version and installs the current version.

1. Log in to the machine with a user account that has administrator privileges.
2. Begin the installation. Use a shell command line to navigate to the installation directory and run the following command:

   ```
   DDMInstaller.exe
   ```

   The **Welcome** page appears.
3. Click **Next**.

   The **Installation Mode** page appears.
4. Select the option to install the Dynamic Data Masking Management Console.
5. Click **Next**.

   The **Installation Folder** page appears.
6. Enter the absolute path for the directory where you have the Dynamic Data Masking Management Console installed and click **Next**.

   The **Upgrade** window appears.
7. Click **OK**.

   The **Uninstall Previous Installation** window appears.
8. Click **OK**.

   The **Pre-Installation Summary** page displays the installation details.
9. Verify that the installation details are correct before you continue the installation and then click **Install**.

   When the installation completes, the installer indicates whether the installation is successful.
10. Click **Done** to close the installer.

You can view the DDM_Install.log file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the DDM_Install.log file for details. The log file is in the installation directory.

Upgrade in Silent Mode

To upgrade the Dynamic Data Masking Server and Management Console without user interaction, install in silent mode.

1. Log in to the machine with a user account that has administrator privileges.
2. Navigate to the directory where you downloaded the Dynamic Data Masking installation file.
3. Locate the SilentInput.properties file.
4. Create a backup copy of the SilentInput.properties file.
5. Use a text editor to open the SilentInput.properties file and modify the value of the USER_INSTALL_DIR parameter.

The following table describes the Dynamic Data Masking installation parameters that you can modify:

Property Name	Description
USER_INSTALL_DIR	Absolute path for the directory in which Dynamic Data Masking is installed. Use the default path format. Use two backslashes (\\) before folder names for installation on Windows. Use a slash (/) for installation on Linux and UNIX.
PA_LICENSE_FILE	Absolute path to a valid license file. If you have not uninstalled Dynamic Data Masking, the installation ignores this parameter and uses the license file of the previous installation. If you uninstalled Dynamic Data Masking, the installation uses this parameter. Use the default path format. Use two backslashes (\\) before folder names for installation on Windows. Use a slash (/) for installation on Linux and UNIX.

6. Save the SilentInput.properties file in the same directory as the silent install script file.
7. Close all shells and windows that have the Dynamic Data Masking installation directory current or open.
8. Begin the installation on Linux, UNIX, or Windows.
   - Begin installation on Linux or UNIX in a directory outside of the Dynamic Data Masking installation directory. Run the following command on a shell command line:

     ```
     <Dynamic Data Masking installation>/silentinstall <administrator password>
     ```

   - To begin installation on Windows, open a command window and run the following command from the installation directory:

     ```
     SilentInstall.bat <administrator password>
     ```

   The administrator password is the Dynamic Data Masking administrator password. If you do not provide a password, Dynamic Data Masking uses the default password, admin. If you use the default password, you can chanage the password after you install.

You can view the `DDM_Install.log` file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the `DDM_Install.log` file for details. The log file may be in the installation directory, on the desktop on Windows, or in the /home/user directory on Linux and UNIX.

CHAPTER 5

Upgrade from Dynamic Data Masking 9.1.0 or ActiveBase Security 3.1

This chapter includes the following topics:

- Upgrade from Dynamic Data Masking 9.1.0 or ActiveBase Security 3.1 Overview, 27
- Before You Upgrade, 27
- Dynamic Data Masking 9.1.0 or ActiveBase Security 3.1 Upgrade, 28

Upgrade from Dynamic Data Masking 9.1.0 or ActiveBase Security 3.1 Overview

To upgrade from Dynamic Data Masking 9.1.0 or ActiveBase Security 3.1, you must uninstall the previous version and install the current version.

Upgrade into the folder where you uninstalled the previous version to apply the configuration and log files to the current version.

Before You Upgrade

Before you upgrade, perform the following tasks:

- Verify the prerequisites for the installation and ensure that the machine where you plan to install meets the installation requirements.
- Back up the Dynamic Data Masking configuration files.
- Close the Dynamic Data Masking Management Console.
- Stop the Dynamic Data Masking Server. On Linux and UNIX, navigate to the installation directory and run the command line script ./stop. On Windows, use the command prompt to remove the Dynamic Data Masking Server.

Back Up the Configuration Files

Dynamic Data Masking stores database connection information and masking rules in configuration files. Before you upgrade, back up the configuration files to safeguard the files during the upgrade process.

You can find the Dynamic Data Masking configuration files in the following directory:

```
<Dynamic Data Masking directory>\cfg
```

Back up the following files:

- config.properties
- config.cfg

Uninstall Dynamic Data Masking

You must uninstall Dynamic Data Masking before you can upgrade.

1. Log in to the machine with a user account that has administrator privileges.
2. Begin the uninstallation on Linux, UNIX, or Windows.
   - To begin uninstallation on Linux or UNIX, navigate to the `/Uninstaller` folder of the Dynamic Data Masking installation directory. Run uninstall.bin on a shell command line.
   - To begin uninstallation on Windows, navigate to the Informatica Dynamic Data Masking folder in Windows Explorer and run uninstall.exe.

   The uninstaller requests confirmation to uninstall.
3. Select **Yes** to proceed with the uninstallation process.

   The **Uninstall DDM** page appears.
4. Click **Next** to continue.

   The uninstaller deletes the Dynamic Data Masking files and indicates whether the uninstallation completed successfully. The uninstaller does not remove the configuration file or the log files.
5. Click **Done** to close the uninstaller.

Dynamic Data Masking 9.1.0 or ActiveBase Security 3.1 Upgrade

You can upgrade the Dynamic Data Masking Server and Management Console in graphical mode or in console mode. If you upgrade on Linux or UNIX in graphical mode, you must set up an X Window server.

Upgrading in Graphical Mode

Install Dynamic Data Masking in graphical mode.

1. Log in to the machine with a user account that has administrator privileges.
2. Begin the installation on Linux, UNIX, or Windows. Use a shell command line to navigate to the installation directory and run the following commands:
   - On Linux or UNIX, run the following command:

     ```
     DDMInstaller.bin
     ```

- On Windows, run the following command

  ```
  DDMInstaller.exe
  ```

The **Welcome** page appears.

3. Click **Next**.

   The **Installation Mode** page appears.

4. Select the option to install the Dynamic Data Masking Server and Console.

5. Click **Next**.

   The **Installation Folder** page appears.

6. Enter the absolute path for the installation directory where you uninstalled Dynamic Data Masking and click **Next**.

   Dynamic Data Masking uses the configuration and log files from the previous uninstallation.

   The **License Key** page appears.

7. Enter the path and file name of the Dynamic Data Masking license key and click **Next**.

   The **Server Details** page appears.

8. Enter the name, port number, and password for the Dynamic Data Masking Server.

   The following table describes the properties that you configure:

Property	Description
Server Name	Required. Name of the Dynamic Data Masking Server. On UNIX, the installer creates a process with the same name as the Dynamic Data Masking Server. On Windows, the installer creates a Windows service with the same name as the Dynamic Data Masking Server. The server name must be unique and must conform to the naming restrictions for a UNIX process or Windows service.
Server Port Number	Required. Port number that the Management Console uses to connect to the Dynamic Data Masking Server. Default is 8195. If port number 8195 is not available, the installer uses the next available port number as default.
Server Password	Required. Password to log in to the Dynamic Data Masking Server through the Management Console.
Confirm Password	Required. Enter the password again to confirm.

9. Click **Next**.

   The **Pre-installation Summary** page displays the installation details.

10. Verify that the installation details are correct before you continue the installation and then click **Install**.

    The installer copies the Dynamic Data Masking files to the installation directory. When the installation completes, the installer indicates whether the installation is successful.

11. Click **Done** to close the installer.

    You can view the DDM_Install.log file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the DDM_Install.log file for details. The log file is in the installation directory.

Upgrading in Console Mode

Install Dynamic Data Masking in console mode.

1. Log in to the machine with a user account that has administrator privileges.
2. Begin the installation on Linux, UNIX, or Windows. Use a shell command line to navigate to the installation directory and run the following commands:
   - On Linux or UNIX, run the following command:

     ```
     DDMInstaller.bin  -i console
     ```

   - On Windows, run the following command

     ```
     DDMInstaller.exe -i console
     ```

   The **Welcome** page appears.
3. Press Enter to continue.

   The **Installation Mode** page appears.
4. Enter 1 to install the Dynamic Data Masking Server and Console.
5. Enter the absolute path for the installation directory where you uninstalled Dynamic Data Masking.

   Dynamic Data Masking uses the configuration and log files from the previous uninstallation.

   The installer displays the installation directory and requests confirmation.
6. Press Enter to continue.

   The **License Key** page appears.
7. Enter the path and file name of the Dynamic Data Masking license key and press Enter.

   The prompts for **Server Details** appears.
8. Enter the name, port number, and password for the Dynamic Data Masking Server.

   The following table describes the properties that you configure:

Property	Description
Server Name	Required. Name of the Dynamic Data Masking Server. On UNIX, the installer creates a process with the same name as the Dynamic Data Masking Server. On Windows, the installer creates a Windows service with the same name as the Dynamic Data Masking Server. The server name must be unique and must conform to the naming restrictions for a UNIX process or Windows service.
Server Port Number	Required. Port number that the Management Console uses to connect to the Dynamic Data Masking Server. Default is 8195. If port number 8195 is not available, the installer uses the next available port number as default.
Server Password	Required. Password to log in to the Dynamic Data Masking Server through the Management Console. When you type the password, the installer does not display the characters you enter on the command line.
Confirm Password	Required. Enter the password again to confirm. When you type the password, the installer does not display the characters you enter on the command line.

9. Press Enter to continue after each entry.

The **Pre-installation Summary** page displays the installation details.

10. Verify that the installation details are correct and then press Enter to install.

    The installer copies the Dynamic Data Masking files to the installation directory. When the installation completes, the installer indicates whether the installation is successful.

11. Press Enter to close the installer.

    You can view the DDM_Install.log file to get more information about the installation and to view configuration properties for the installed components. If the installation ends with a warning, check the DDM_Install.log file for details. The log file is in the installation directory.

CHAPTER 6

After You Install or Upgrade

This chapter includes the following topics:

- After You Install the Dynamic Data Masking Server, 32
- After You Install the Management Console, 37

After You Install the Dynamic Data Masking Server

After installation, complete all required post-installation tasks before you log in to the Management Console.

After you install the Dynamic Data Masking Server, complete the following tasks:

- Verify that Java SE 8 is installed on the machine where you installed the Dynamic Data Masking Server.
- On Linux, set the open file resource boundaries.
- Optionally, set up LDAP or Active Directory authentication.
- Optionally, on UNIX, set up the Dynamic Data Masking server to restart when the host machine restarts.
- Optionally, manually upgrade the Dynamic Data Masking for Microsoft SQL Server service from version 9.5.1 or earlier.

Verify the Location of Java SE 8

Verify that Java SE 8 is installed on the machine where you installed the Dynamic Data Masking Server. The Dynamic Data Masking Server requires Java SE 8 to run properly.

Windows or Linux

On Windows, the required Java SE 8 files are installed with Dynamic Data Masking.

UNIX

On UNIX, the Dynamic Data Masking installer does not install the required Java files.

Verify that Java SE 8 is installed on the machine where you installed Dynamic Data Masking. If Java SE 8 is not in the system path, modify the file `JAVA_HOME` environment variable in the `$INSTALL_DIR/setup_server` and `$INSTALL_DIR/LogLoader/logloader` scripts.

Set User Resource Boundaries

On Linux, you must increase the number of open file resources that are available the Dynamic Data Masking user.

Each Dynamic Data Masking client occupies an open file resource to connect to the Dynamic Data Masking Server. In addition, each connection from the Dynamic Data Masking Server to the database occupies an open file resource. Because Dynamic Data Masking requires a large number of resources, you must edit the limits.conf file to increase the number of open file resources available to the Dynamic Data Masking user.

To check the open file descriptor limit, run the following shell command:

```
/proc/<Dynamic Data Masking process ID>/limits
```

Informatica recommends that you set the hard and soft open file descriptor limits to five times the maximum number of database connections that you create through Dynamic Data Masking. For example, if you create 400 connections through Dynamic Data Masking, you might set the open file descriptor limit to 2000.

Setting the Resource Boundaries

Set the open file descriptor limit in the limits.conf file.

1. Open the limits.conf file. You can find the file in the following location:

   ```
   etc/security/limits.conf
   ```

2. In the limits.conf file, edit the Dynamic Data Masking user soft nofile and hard nofile parameters. The following text shows the limits set to 4000:

   ```
   <Dynamic Data Masking user> hard nofile 4000
   <Dynamic Data Masking user> soft nofile 4000
   ```

3. Log out and log back in to the Linux machine.
4. Open a Server Control window and run the following commands:
   - `server stop`
   - `server start`
5. To verify that you set the file descriptor limits correctly, run the following shell command:

   ```
   /proc/<Dynmaic Data Masking procedure ID>/limits
   ```

Set Up Authentication

You can set up LDAP or Active Directory authentication.

To provide security and limit access to the Management Console, use a stronger authentication scheme for Dynamic Data Masking than the default internal authentication. Log in to the Management Console with the user name *admin* and the Dynamic Data Masking Server password, then configure the authentication method that you want to use for Dynamic Data Masking.

Automatic Restart

On Linux and UNIX, you must set up the Dynamic Data Masking Server to restart when the host machine restarts. Dynamic Data Masking works in conjunction with the database to process database requests. If you do not set up automatic restart, no database client application will have access to the database after the host machine restarts.

If you do not set up automatic restart, you must manually restart the Dynamic Data Masking Server after you restart the host machine.

The Dynamic Data Masking installation directory contains an rc.d script file, `S99ddmsrv`, that you can install in the runlevel initialization directories so that the script file will run at startup. A symbolic link references the `S99ddmsrv` script file, which starts the Dynamic Data Masking Server when the host machine restarts or changes runlevels.

On Linux and UNIX, log in as the superuser and create symbolic links to the `S99ddmsrv` script file in each of the runlevel directories to ensure that the script file will run at startup. The initialization process differs depending on the platform. If you are unsure where or how to install the rc.d script file, contact the vendor for instructions.

For example, on Red Hat Enterprise Linux 6, create symbolic links for the appropriate runlevels with the following command format:

```
ln -s <Dynamic Data Masking installation directory>/S99ddmsrv /etc/rc.d/rc<runlevel>.d/
S99ddmsrv
```

If you have more than one Dynamic Data Masking Server on a machine, you can add each server to the automatic startup. Create a symbolic link with a unique name that references the `S99ddmsrv` script file for each Dynamic Data Masking Server.

For example, on Red Hat Enterprise Linux 6, you might run the following commands:

- `ln -s /home/rhel6/Informatica/DDM1/S99ddmsrv /etc/rc.d/rc3.d/S99ddmsrv1`
- `ln -s /home/rhel6/Informatica/DDM2/S99ddmsrv /etc/rc.d/rc3.d/S99ddmsrv2`
- `ln -s /home/rhel6/Informatica/DDM1/S99ddmsrv /etc/rc.d/rc5.d/S99ddmsrv1`
- `ln -s /home/rhel6/Informatica/DDM2/S99ddmsrv /etc/rc.d/rc5.d/S99ddmsrv2`

Before you uninstall Dynamic Data Masking, you must remove the symbolic links that you created in the runlevel directories.

Note: On Windows, the Dynamic Data Masking installer configures the Dynamic Data Masking Server to restart when the host machine restarts.

Upgrade the Dynamic Data Masking for Microsoft SQL Server Service

You must manually upgrade the Dynamic Data Masking for Microsoft SQL Server service from version 9.5.1 or earlier.

Perform the following steps for each Microsoft SQL Server database defined in the Management Console tree:

1. Open the Dynamic Data Masking 9.5.2 or later Management Console.
2. Select a Microsoft SQL Server database node in the Management Console tree and click **Tree** > **Edit**.

   The **Edit** window appears.
3. Note the following Microsoft SQL Server database parameters in the **Edit** window:
   - DDM Database Name
   - SQL Server Databases
   - DDM Port
   - Default Rule Set
4. Click **OK** to close the window.
5. Select the Dynamic Data Masking Server in the Management Console tree and click **Tree** > **Add DDM Services**.

   The **Add DDM Services** window appears.

6. Select **DDM for SQL Server** and click **OK** to close the window.
7. Select the Dynamic Data Masking for Microsoft SQL Server service in the Management Console tree and click **Tree** > **Edit**.

   The **Edit** window appears.
8. Click **Add Port** and enter the port number from the Microsoft SQL Server database node.
9. Click **OK** to close the **Edit** window.
10. Select the Dynamic Data Masking for Microsoft SQL Server service in the Management Console tree and click **Tree** > **Connection Rules**.

    The **Rule Editor** window appears.
11. In the **Rule Editor** window, click **Action** > **Append Rule**.

    The **Append Rule** window appears.
12. Specify the following properties in the **Append Rule** window:

Property	Value
Rule Name	<database name>DB
Matcher	Incoming DDM Listener Port
Incoming Port	Enter the port number from the Microsoft SQL Server database node.
Rule Action	Switch to Database
Database	Enter the DDM Database Name from the Microsoft SQL Server database node.
Processing Action	Continue

13. Click **OK** to close the **Append Rule** window.
14. In the **Rule Editor** window, click **Action** > **Append Rule**.

    The **Append Rule** window appears.
15. Specify the following properties in the **Append Rule** window:

Property	Value
Rule Name	apply<rule set name>
Matcher	All Incoming Connections
Rule Action	Use Rule Set
Rule Set Name	Enter the Rule Set Name specified in the default rule set parameter from the Microsoft SQL Server database node.
Processing Action	Stop if Applied

16. Click **OK** to close the **Append Rule** window.
17. In the **Rule Editor** window, click **File** > **Update Rules** to save the rules.
18. Click **File** > **Exit** to close the Rule Editor.

Create Rule Sets for the Microsoft SQL Server Service

If you defined additional Microsoft SQL Server databases in the Microsoft SQL Server database **Edit** window, you must complete the following steps:

1. Export the default rule set and the rule sets associated with the Microsoft for SQL Server databases you defined in the Microsoft SQL Server Databases section of the database **Edit** window. In the Management Console, select a rule set and click **Tree** > **Security Rule Set**.

   The **Rule Editor** window appears.
2. Click **Action** > **Export**.

   The **Export** window appears.
3. Navigate to the directory where you want to save the rule set and click **Export**.
4. Click **File** > **Exit** to close the **Rule Editor**.
5. In the Management Console tree, select a domain node and click **Tree** > **Security Rule Set**.

   The **Add Rule Set** window appears.
6. Enter a rule set name in the Rule Set Name field and click **OK** to close the **Add Rule Set** window.
7. In the Management Console tree, select the MasterRuleSet security rule set and click **Tree** > **Security Rule Set**.

   The **Rule Editor** window appears.
8. Click **Action** > **Append Rule**.

   The **Append Rule** window appears.
9. Specify the following properties in the **Append Rule** window:

Property	Value
Rule Name	MasterFolder
Matcher	Any
Rule Action	Folder
Processing Action	Stop if Applied

10. Click **OK** to close the **Append Rule** window.
11. Click **File** > **Update Rules** to save the rule folder.
12. In the Rule Editor, select the MasterFolder rule folder and click **Action** > **Import**.

    The **Import** window appears.
13. Navigate to the folder where you exported the Default Rule Set. Select the rule set and click **Import**.
14. Click **File** > **Update Rules** to save the rules.
15. Create a rule folder for each database you defined in the Microsoft SQL Server database **Edit** window.
16. Click **Action** > **Append Rule**.

    The **Append Rule** window appears.

17. Specify the following properties in the **Append Rule** window:

Property	Value
Rule Name	Enter the name of the database.
Matcher	Symbol Matcher
Symbol Name	AUTH_CURRENT_DATABASE
Text	Enter the name of the database. The Text property is case sensitive.
Rule Action	Folder
Processing Action	Stop if Applied

18. Click **OK** to close the **Append Rule** window.
19. Click **File** > **Update Rules** to save the rule folder.
20. In the **Rule Editor**, select the rule folder you created and click **Action** > **Import**.

    The **Import** window appears.
21. Navigate to the folder where you exported the rule set for the database. Select the rule set and click **Import**.
22. Drag the MasterFolder security rule folder to the bottom of the rule tree.
23. Click **File** > **Update Rules** to save the rules.

After You Install the Management Console

After you install the Management Console, verify that Java SE 8 is installed on the machine where you installed the Management Console. The Management Console requires Java SE 8 to run properly.

You can log in to the Management Console to connect to a Dynamic Data Masking Server. If Dynamic Data Masking uses internal authentication, you can log in to the Management Console with the user name *admin* and the Dynamic Data Masking Server password. If Dynamic Data Masking is configured with LDAP or Active Directory authentication, you must log in with a valid user name and password.

CHAPTER 7

Uninstallation

This chapter includes the following topics:

- Uninstallation Overview, 38
- Uninstalling in Graphical Mode, 38
- Uninstalling in Console Mode, 39

Uninstallation Overview

The Dynamic Data Masking installation creates an uninstallation directory that includes an uninstaller.

When you uninstall Dynamic Data Masking, the uninstaller removes the files and folders that were created as part of the installation. The configuration file and the log files are not removed.

If you created symbolic links in the runlevel directories to configure automatic startup of the Dynamic Data Masking Server, you must remove the symbolic links before you uninstall Dynamic Data Masking.

By default, if you run the uninstaller without any parameters, the uninstaller detects the mode in which the product was installed and uses the same mode to uninstall. For example, if you install Dynamic Data Masking in console mode, the uninstaller runs in console mode even if you do not pass the *-i console* parameter.

The Dynamic Data Masking Server must be shut down before you uninstall Dynamic Data Masking.

Uninstalling in Graphical Mode

Uninstall in graphical mode.

1. Log in to the machine with a user account that has administrator privileges.
2. Shut down the Dynamic Data Masking Server and close the Management Console.
3. Close all shells and windows that have the Dynamic Data Masking installation directory current or open.
4. If you created symbolic links for automatic restart in the rc.d directories on Linux or UNIX, remove the links.
5. Begin uninstallation on Linux, UNIX, or Windows.

- Begin uninstallation on Linux or UNIX in a directory outside of the Dynamic Data Masking installation directory. Run the following command on a shell command line:

  ```
  <Dynamic Data Masking installation>/Uninstaller/uninstall.bin -i gui
  ```

- To begin uninstallation on Windows, go to the Informatica Dynamic Data Masking folder in the Start menu and select the option to uninstall the Dynamic Data Masking Server or the Management Console. Or open a command window, and run the following command from the installation directory:

  ```
  Uninstaller\uninstall.exe -i gui
  ```

The uninstaller requests confirmation to uninstall.

6. Select **Yes** to proceed with the uninstallation process.
7. Click **Next** to continue.

   The uninstaller deletes the Dynamic Data Masking files and indicates whether the uninstallation completed successfully. The uninstaller does not remove the configuration file or the log files. You must delete these files manually.
8. Click **Done** to close the uninstaller.

Uninstalling in Console Mode

Uninstall in console mode.

1. Log in to the machine with a user account that has administrator privileges.
2. Shut down the Dynamic Data Masking Server and close the Management Console.
3. Close all shells and windows that have the Dynamic Data Masking installation directory current or open.
4. If you created symbolic links for automatic restart in the rc.d directories on Linux or UNIX, remove the links.
5. Begin uninstallation on Linux, UNIX, or Windows.
   - Begin uninstallation on Linux or UNIX in a directory outside of the Dynamic Data Masking installation directory. Run the following command on a shell command line:

     ```
     <Dynamic Data Masking installation>/Uninstaller/uninstall.bin -i console
     ```

   - To begin uninstallation on Windows, open a command window and run the following command from the installation directory:

     ```
     Uninstaller\uninstall.exe -i console
     ```

   The uninstaller requests confirmation to uninstall.
6. Select **Yes** to proceed with the uninstallation process.
7. Press Enter to continue.

   The uninstaller deletes the Dynamic Data Masking files and indicates whether the uninstallation completed successfully. The uninstaller does not remove the configuration file or the log files. You must delete these files manually.
8. Type Exit to close the uninstaller.

INDEX

D

Dynamic Data Masking
    uninstallation
        console mode 39
        graphical mode 38
Dynamic Data Masking Server
    post-installation steps 32
    Java requirement 11
    port 11
    prerequisites 10
    troubleshooting 20

E

environment variables
    DISPLAY 12

G

graphical mode
    installation requirements 12

I

installation
    license keys for 10
    logs 19
    pre-installation tasks 9
    software 10
    troubleshooting 19
installation requirements
    X Window Server 12
installer
    files 10

J

Java requirement
    Dynamic Data Masking Server 11
    Management Console 11

L

license key
    updating 22
license keys
    installation 10
logs
    DDM_Install.log 19

M

Management Console
    post-installation steps 37
    Java requirement 11
    prerequisites 10

P

port
    Dynamic Data Masking Server 11
post-installation steps
    Dynamic Data Masking Server 32
    Management Console 37
prerequisites
    Dynamic Data Masking Server 10
    Management Console 10

S

software
    installation 10

T

troubleshooting
    Dynamic Data Masking Server 20
    installation 19
    logs 19

U

uninstallation
    Dynamic Data Masking 38, 39

X

X Window Server
    installation requirements 12