Informatica® Dynamic Data Masking
9.9.3

Data Archive Accelerator Guide

Informatica Dynamic Data Masking Data Archive Accelerator Guide
9.9.3
September 2021

© Copyright Informatica LLC 1993, 2021

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 © 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.

Revision: 1
Publication Date: 2021-09-15

Table of Contents

Preface 6

Informatica Resources 6

- Informatica Network 6
- Informatica Knowledge Base 6
- Informatica Documentation 6
- Informatica Product Availability Matrices 7
- Informatica Velocity 7
- Informatica Marketplace 7
- Informatica Global Customer Support 7

Chapter 1: Introduction to the Data Archive Accelerator 8

Data Archive Accelerator Overview 8

Masking Data in Data Archive 8

Chapter 2: Data Archive Accelerator Setup 10

Data Archive Accelerator Setup Overview 10

Step 1. Verify the Requirements 11

Step 2. Add the Data Vault Service 11

Step 3. Add the Listener Port to the Data Vault Service 11

Step 4. Define the Data Vault Connection 11

Step 5. Create the Security Rules 12

- Creating the Security Rule Set 13
- Creating the DataArchiveAction Rule 13

Step 6. Create the Connection Rules 14

- Creating the SwichToDataVault Rule 14
- Creating the UseDataArchiveAccelerator Rule 15

Step 7. Enable Dynamic Data Masking in Data Archive 16

Step 8. Define the Data Vault Host and Port 17

Step 9. Create Data Archive Access Roles 17

Step 10. Assign Access Roles to Users 18

Chapter 3: Data Archive Accelerator Rules 19

Data Archive Accelerator Rules Overview 19

Create and Assign Loyalty Level Access Roles 21

Importing the Data Archive Accelerator Rules 21

Match Tables Rule 22

MaskRequired(NonAdministrator) Rule 22

- Loyalty Levels 23

MatchLevel Rules 23

MaskLevel Rules 24

MaskLevel0 Rule. . . . 24
MaskLevel1 Rules. . . . 24
MaskLevel2 Rule. . . . 25
MaskLevel3 Rule. . . . 25
MaskDefaultLevel Rule. . . . 25
Print Roles Rule. . . . 26
GenericDataArchiveAction Rule. . . . 26
PrintDataArchiveSymbols Rule. . . . 26

Chapter 4: Dynamic Data Masking. . . . 27

Dynamic Data Masking Overview. . . . 27
Dynamic Data Masking Components. . . . 28
Management Console. . . . 29
Menu. . . . 29
Management Console Tree. . . . 31
Logging In to the Management Console. . . . 31
Database Management. . . . 32
Dynamic Data Masking Server Management. . . . 32
Dynamic Data Masking Service Management. . . . 33
Dynamic Data Masking Listener Ports. . . . 33
Domain Management. . . . 33
Connection Management Overview. . . . 34
Data Vault Connection Management. . . . 34
Data Vault Connection Parameters. . . . 34
Rules. . . . 35
Rule Components. . . . 35
Rule Trees. . . . 35
Connection Rules. . . . 37
Security Rules. . . . 37
Rule Folders. . . . 38
Rule Management. . . . 39
Server Control. . . . 39
Running Server Control. . . . 40
Server Control Commands. . . . 40

Index. . . . 42

Preface

Read the *Data Archive Accelerator Guide* to learn how to route requests made to the Data Vault through Dynamic Data Masking. Learn how to use a pre-defined set of security rules to mask sensitive data in Data Vault.

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.

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.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at 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.

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

Introduction to the Data Archive Accelerator

This chapter includes the following topics:

- Data Archive Accelerator Overview, 8
- Masking Data in Data Archive, 8

Data Archive Accelerator Overview

Use the Data Archive accelerator to implement Dynamic Data Masking for Data Vault.

Configure Data Archive to route requests made to the Data Vault through Dynamic Data Masking. Configure connection and security rules in Dynamic Data Masking to specify which users see masked data and how data is masked.

The Data Archive accelerator is in the Dynamic Data Masking installation folder as an additional component that you can configure to work with Data Vault.

The Data Archive accelerator package contains a .jar file that Dynamic Data Masking uses to extract user and user role information from the SQL request and an example set of security rules that mask sensitive data in the Loyalty demo database.

Masking Data in Data Archive

When you enable Dynamic Data Masking in Data Archive, Data Archive and Dynamic Data Masking work together to mask sensitive data.

You can mask data based on the user name or the Data Archive access role of a user. It is recommended to mask data based on the Data Archive access role. When you create a security rule in Dynamic Data Masking, you specify the user or access role that the rule applies to.

When the Data Archive client sends an SQL request to the Data Vault, it appends a multi-line SQL comment to the request that contains encrypted user and user role information. Dynamic Data Masking decrypts the comment and uses the Java class GetUsersAndRolesFromComment to create symbols.

The following table describes the symbols that the GetUsersAndRolesFromComment Java class creates:

Symbol	Description
DataArchive_User	The Data Archive user.
DataArchive_Roles	A list of shuffled Data Archive access roles separated by commas.

You must create a rule in Dynamic Data Masking that uses the GetUsersAndRolesFromComment Java class so that Dynamic Data Masking decrypts the SQL comment.

Because Data Vault does not allow multi-line comments, the request fails if Dynamic Data Masking does not decrypt the comment. If Dynamic Data Masking encounters an error during decryption such as a missing comment or the wrong comment format, Dynamic Data Masking returns the original SQL statement and does not define values for the DataArchive_User and DataArchive_Roles symbols.

CHAPTER 2

Data Archive Accelerator Setup

This chapter includes the following topics:

- Data Archive Accelerator Setup Overview, 10
- Step 1. Verify the Requirements, 11
- Step 2. Add the Data Vault Service, 11
- Step 3. Add the Listener Port to the Data Vault Service, 11
- Step 4. Define the Data Vault Connection, 11
- Step 5. Create the Security Rules, 12
- Step 6. Create the Connection Rules, 14
- Step 7. Enable Dynamic Data Masking in Data Archive, 16
- Step 8. Define the Data Vault Host and Port, 17
- Step 9. Create Data Archive Access Roles, 17
- Step 10. Assign Access Roles to Users , 18

Data Archive Accelerator Setup Overview

Set up the Data Archive accelerator to mask data in the Data Vault.

You can find the Data Archive accelerator in the following location:

```
<Dynamic Data Masking installation>\Accelerators\DataArchive
```

To set up the Data Archive Accelerator, perform the following tasks:

1. Verify the setup requirements.
2. Add the Data Vault service in the Management Console.
3. Define the listener port for the Data Vault service.
4. Define the Data Vault connection in the Management Console.
5. Create a security rule set and define security rules.
6. Create the connection rules.
7. Enable Dynamic Data Masking in Data Archive.
8. Define the Data Vault host and port parameters in Data Archive.
9. Create Data Archive access roles.
10. Assign access roles to users.

Step 1. Verify the Requirements

Verify the following requirements before you use the Data Archive accelerator:

- You must have Dynamic Data Masking version 9.6.0 or later installed.
- You must have Data Archive 6.2.0 or later installed.

Step 2. Add the Data Vault Service

Add the Data Vault service in the Management Console. If the service exists in the Management Console, add the listener port for Data Vault.

1. In the Management Console, click the Dynamic Data Masking Server in the tree.
2. Click **Tree** > **Add DDM Services**.

   The **Add DDM Services** window appears.
3. Select the DDM for FAS service in the **Add DDM Services** window.
4. Click **OK**.

   The service appears in the Management Console tree.

Step 3. Add the Listener Port to the Data Vault Service

If the Dynamic Data Masking service Data Vault listener port is not defined, you must add it in the Management Console.

1. In the Management Console, click the DDM for FAS service in the tree.
2. Click **Tree** > **Edit**.

   The **Edit** window appears.
3. Click **Add Port**.
4. Enter the port number of the Data Vault and click **OK**. For example, you might enter 8501.

   The **Edit** window closes.

Step 4. Define the Data Vault Connection

Define the Data Vault connection in the Management Console.

1. In the Management Console, click **Tree** > **Add Database**.

   The **Add Database** window appears.

2. Select the FAS database type.
3. Define the following properties for the Data Vault connection:

   DDM Database Name

   Name of the database node that appears in the Management Console tree. For example, you might enter DataVault.

   Server Address

   Server host name or TCP/IP address for the Data Vault.

   Note: Verify that there is no firewall that prohibits the Dynamic Data Masking Server from connecting to the Data Vault server and port number.

   Server Port

   TCP/IP listener port for the Data Vault.

   FAS Database Name

   Database name for the Data Vault.

   DBA Username

   User name for the database user account to log in to the Data Vault.

   DBA Password

   Password for Data Vault user.
4. Click **Test Connection** to validate the connection to the database.
5. Click **OK**.

   The Data Vault database node appears in the Management Console tree.

Step 5. Create the Security Rules

To return masked data to the user, create security rules that define which users see masked data and how the data is masked.

The Data Archive accelerator contains pre-defined masking rules for the Data Archive Loyalty demo database. Use the accelerator rules as a guide to create rules based on the type of data that you want to mask.

You must create a security rule set and add security rules to the rule set. The first rule that you add to the rule set must be a rule like the DataArchiveAction rule that decrypts the user and user roles from the SQL comment that Data Archive appends to the request. The Data Archive accelerator contains an example GenericDataArchiveAction rule that decrypts the SQL comment. Create additional security rules based on the data that you want to mask.

The access roles that you specify in the security rules must match the access roles that you create in Data Archive. You can mask data based on the user name or the Data Archive access role of a user. It is recommended to mask data based on the Data Archive access role.

Creating the Security Rule Set

Create the security rule set to hold security rules.

1. In the Management Console, select a domain node and click **Tree** > **Add Rule Set**.

   The **Add Rule Set** window appears.
2. Enter the name of the rule set. For example, enter DataArchiveAccelerator.
3. Click **OK**.

   The rule set appears in the Management Console tree.

Creating the DataArchiveAction Rule

Create the DataArchiveAction rule to decrypt the SQL comment that contains user and user role information.

1. In the Management Console, select the DataArchiveAccelerator security rule set and click **Tree** > **Security Rule Set**.

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

   The **Append Rule** window appears.
3. Define the following rule parameters:

   Rule Name

   Enter the name of the rule. For example, you might enter DataArchiveAction.

   Matching Method

   Select Any.

   Action Type

   Select Java Action.

   Class Path

   Enter the path to the DataArchiveAccelerator.jar file. For example, you might enter:

   ```
   <Dynamic Data Masking installation>\DDM\Accelerators\DataArchive\lib
   \DataArchiveAccelerator.jar
   ```

   Class Name

   Enter GetUsersAndRolesFromComment.

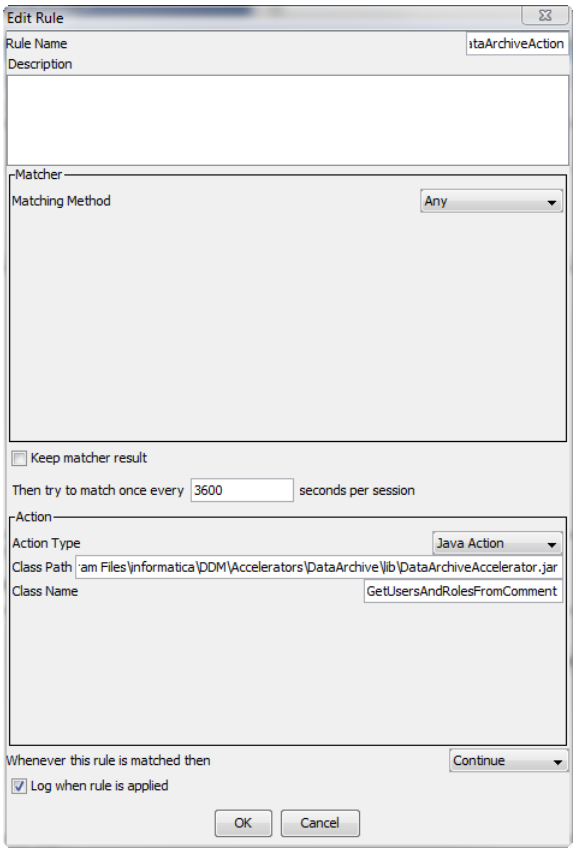
   Processing Action

   Select Continue to direct the request to the next rule in the tree.

   Log when Rule is Applied

   Select this option to create a log entry when a request goes through the security rule set.

   The following figure shows the DataArchiveAction rule:



4. Click **OK**.

   The rule appears in the rule tree.

5. Click **File** > **Update Rules** to save the rule.

Step 6. Create the Connection Rules

Create connection rules to direct incoming requests from the Data Archive client to the security rule set before the request is sent to the Data Vault.

You must create two connection rules to mask Data Vault data. The SwitchToDataVault rule directs requests to the Data Vault. The UseDataArchiveAccelerator rule directs requests to the security rule set that defines how to mask Data Vault data.

Creating the SwichToDataVault Rule

The SwitchToDataVault rule directs requests to the Data Vault.

1. In the Management Console, select the Data Vault service node and click **Tree** > **Connection Rules**.

   The **Rule Editor** window appears.

2. Click **Action** > **Append Rule**.

   The **Append Rule** window appears.

3. Define the following rule parameters:

   Rule Name

   Enter SwitchToDataVault.

   Matcher

   Select Incoming DDM Listener Port.

   Incoming Port

   Enter the listener port that you defined for the Data Vault database node in the Management Console. For example, you might enter 8501.

   Action

   Select Switch to Database.

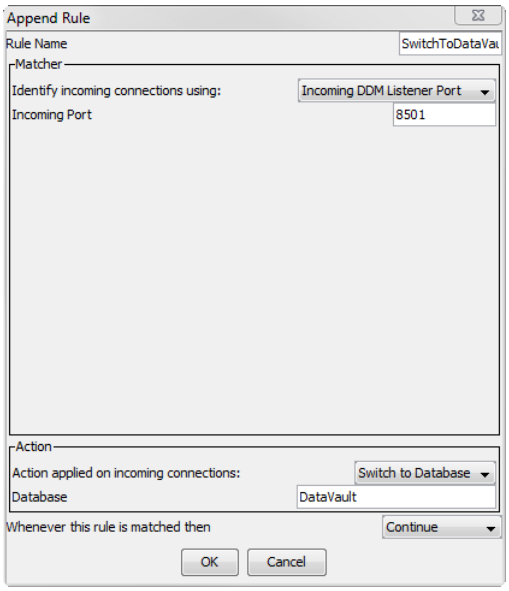
   Database

   Enter the name of the database node that you defined for the Data Vault database in the Management Console. For example, you might enter DataVault.

   Processing Action

   Select Continue.

   The following figure shows the SwitchToDataVault rule:



4. Click **OK** to add the rule to the rule tree.

Creating the UseDataArchiveAccelerator Rule

The UseDataArchiveAccelerator rule directs requests to the DataArchiveAccelerator security rule set.

1. In the connection rule **Rule Editor** window, click **Action** > **Append Rule**.

   The **Append Rule** window appears.

2. Define the following rule parameters:

   Rule Name

   Enter UseDataArchiveAccelerator

   Matcher

   Select All Incoming Connections.

   Action

   Select Use Rule Set.

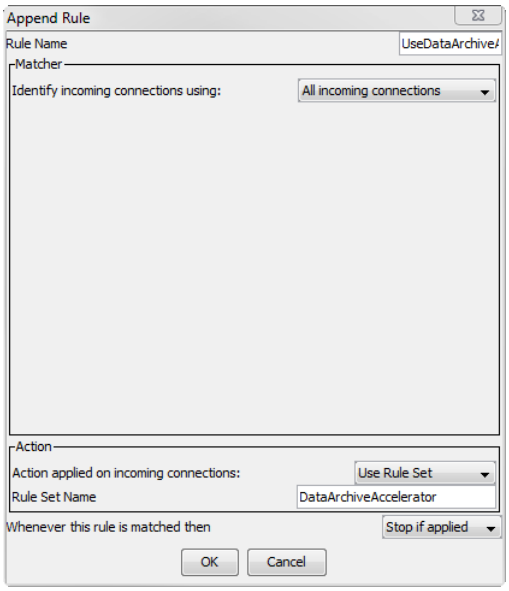
   Rule Set Name

   Enter the name of the security rule set that you created to mask Data Vault data. For example, enter DataArchiveAccelerator.

   Processing Action

   Select Stop if Applied.

   The following figure shows the UseDataArchiveAccelerator rule:



3. Click **OK** to add the rule to the rule tree.
4. Click **File** > **Update Rules** to save the connection rules.

Step 7. Enable Dynamic Data Masking in Data Archive

Enable Dynamic Data Masking in the Data Archive conf.properties file. When you enable Dynamic Data Masking, Data Archive appends the encrypted SQL comment to the SQL request that it sends to Dynamic Data Masking.

1. Open the Data Archive `conf.properties` file.

   You can find the `conf.properties` file in the root Data Archive installation directory.

2. Set the informia.enableDDMSecurity property to `Yes`.
3. Save and close the `conf.properties` file.

Step 8. Define the Data Vault Host and Port

Update the Data Vault host and port in Data Archive to match the host and port information that you entered in the Dynamic Data Masking Management Console.

1. From the Data Archive interface, click **Administration** > **Manage Connections**.

   The **Manage Connections** page appears.
2. Click the **Target** tab.
3. Click the Data Vault target connection.

   The Data Vault connection properties appear.
4. Enter the Dynamic Data Masking proxy host name in the **Data Vault Host** property.

   If you installed Dynamic Data Masking on the same machine as Data Vault, the host name remains the same as the Data Vault host name.
5. Enter the port number of the Dynamic Data Masking service for Data Vault in the Data Vault Port property. For example, you might enter 8501.
6. Click **Save**.

Step 9. Create Data Archive Access Roles

Create access roles in Data Archive to determine what data is masked for a user and what unmasked data a user can view. Assign the roles to users based on the security model.

1. From the Data Archive interface, click **Administration** > **Managing Roles**.
2. Click **New Access Role**.
3. Define the following access role parameters:

   Role Name

   Unique Name for the role. Note that after you create the role, you cannot edit the role name. Role names cannot contain special characters.

   Description

   Description of the role.

   Valid From

   Start date of the period of time that the role is valid.

   Valid Until

   End date of the period fo time that the role is valid. The date is optional. By default, roles do not have an end date. Roles without an end date are valid indefinitely.
4. Click **Save**.

Step 10. Assign Access Roles to Users

Assign the access roles you created in step nine to users in Data Archive.

1. Click **Administration** > **Manage Users**.

   A list of users appears.
2. Click **Edit** next to the user you want to assign the role to.

   The user details appears.
3. Click **Add Role**.

   A new line appears in the list of roles.
4. Select the role that you want to assign and enter the validity dates of the role assignment.
5. Click **Save**.

CHAPTER 3

Data Archive Accelerator Rules

This chapter includes the following topics:

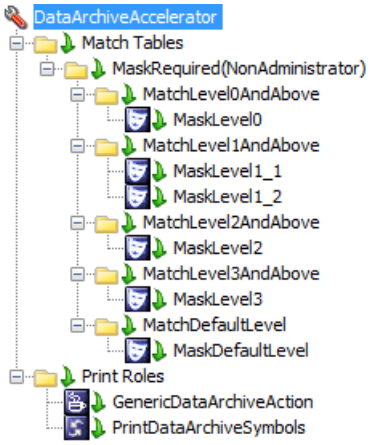
- Data Archive Accelerator Rules Overview, 19
- Create and Assign Loyalty Level Access Roles, 21
- Importing the Data Archive Accelerator Rules, 21
- Match Tables Rule, 22
- MaskRequired(NonAdministrator) Rule, 22
- MatchLevel Rules, 23
- MaskLevel Rules, 24
- Print Roles Rule, 26
- GenericDataArchiveAction Rule, 26
- PrintDataArchiveSymbols Rule, 26

Data Archive Accelerator Rules Overview

The Data Archive accelerator contains a pre-defined security rule set to mask data in the Data Archive Loyalty database. The masking rules in the rule set are an example of the type of rules that you can create to mask Data Vault data. The Print Roles rules allow you to view the users and roles that receive masked data.

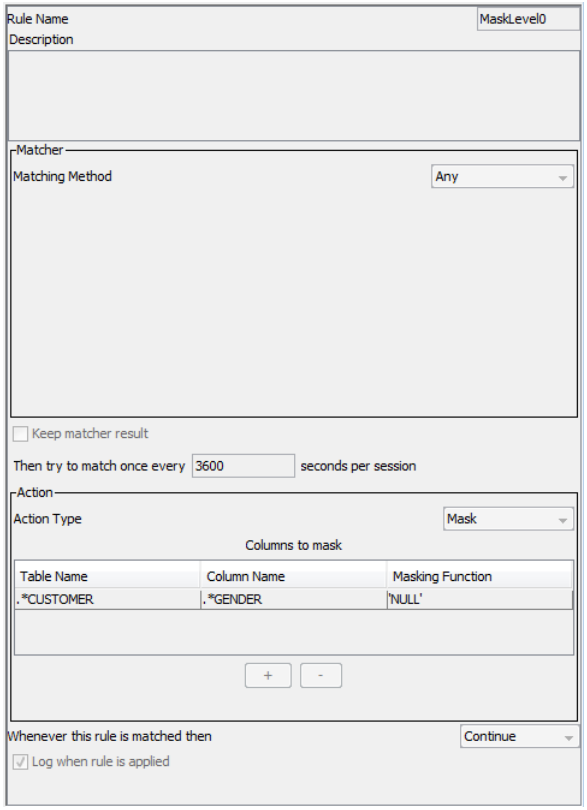
The rules in the DataArchiveAccelerator rule set are sample rules that you use with the Data Archive Loyalty demo database. Use the rules as a guide to create masking rules to mask Data Vault data.

The following figure shows the Data Archive accelerator rule tree:



Select a rule in the rule tree to view the properties in the pane on the left.

The following image shows the MaskLevel0 rule properties:



The MaskLevel0 rule uses the any rule matcher, which applies the rule to all requests that reach the MaskLevel0 rule in the rule tree. The mask rule action masks data. In the mask rule action, the NULL masking function on the GENDER column in the CUSTOMER table nullifies gender data in the result set. The continue processing action directs the request to the next rule in the rule tree.

Create and Assign Loyalty Level Access Roles

Create Data Archive access roles and assign the access roles to users to mask data with the Data Archive accelerator rules.

The Data Archive accelerator uses access roles to determine what masked and unmasked data a user sees.

Create the following access roles in the Data Archive interface:

- Administrator
- Loyalty_PI_LEVEL_0
- Loyalty_PI_LEVEL_1
- Loyalty_PI_LEVEL_2
- Loyalty_PI_LEVEL_3
- Loyalty_PI_DEFAULT_LEVEL

Assign the access roles to users based on the security model.

Note: You must create a new Administrator access role to use the Data Archive accelerator. The Administrator role is not the ILM Admin role.

Importing the Data Archive Accelerator Rules

Import the Data Archive accelerator rules to mask data in the Loyalty demo database.

1. In the Management Console, select a domain node in the rule tree and click **Tree** > **Add Rule Set**.

   The **Add Rule Set** window appears.
2. Enter DataArchiveAccelerator as the name for the security rule set and click **OK**.

   The security rule set appears in the Management Console rule.
3. Select the DataArchiveAccelerator rule set in the rule tree and click **Tree** > **Security Rule Set**.

   The **Rule Editor** appears.
4. Click **Action** > **Import**.

   The **Import** window appears.
5. Browse to the location of the DataArchiveAccelerator.xml file and click **Import**. You can find the file in the following location:

   ```
   <Dynamic Data Masking installation>/Accelerators/DataArchive/rules/FAS
   ```

   The rules appear in the security rule tree.
6. Select **File** > **Update Rules** to save the security rules.

Match Tables Rule

The Match Tables rule identifies requests to the Loyalty database and directs the requests to the masking rules in the rule tree.

The Match Tables rule uses the text matcher to identify requests sent to tables in the Loyalty database that contain sensitive data. The rule matcher identifies the following tables that contain sensitive data:

- CUSTOMER
- TICKET
- TICKET_COUPON
- ADDRESS
- AIRPORTS

The rule uses the folder rule action and the continue processing action to direct requests to the next rule inside the rule folder.

When a request is sent to a table that contains sensitive information, the Rule Engine directs the request to the MaskRequired(NonAdministrator) rule. If the request does not access a table that contains sensitive information, the Rule Engine directs the request to the Print Roles rule.

MaskRequired(NonAdministrator) Rule

The MaskRequired(NonAdministrator) rule identifies user roles and sets the LOYALTY_ROLE symbol.

Dynamic Data Masking uses the LOYALTY_ROLE symbol to determine whether a user can view unmasked data. The MaskRequired(NonAdministrator) rule sets the LOYALTY_ROLE symbol for the user that sent the request.

Dynamic Data Masking sets the LOYALTY_ROLE symbol to one of the following values:

- Administrator
- Loyalty_PI_LEVEL_0
- Loyalty_PI_LEVEL_1
- Loyalty_PI_LEVEL_2
- Loyalty_PI_LEVEL_3
- Loyalty_PI_DEFAULT_LEVEL

A user with the Administrator loyalty level views unmasked data. A user with the Loyalty_PI_LEVEL_0 level views some masked data. A user with the Loyalty_PI_DEFAULT_LEVEL level views the most masked data.

The MaskRequired(NonAdministrator) rule uses the Java matcher matching method. The class path field contains the location of the DataArchiveAccelerator.jar file and the class name field contains the GetLoyaltyRoleFromComment class.

You can find the DataArchiveAccelerator.jar in the following location:

```
<Dynamic Data Masking installation>\Accelerators\DataArchive\lib
\DataArchiveAccelerator.jar
```

The rule uses the folder rule action and the continue processing action. If the user that sent the request is not an administrator, the Rule Engine sends the request to the next rule in the tree. If the use is an administrator, the Rule Engine sends the request to the Print Roles rule.

Loyalty Levels

Loyalty levels determine what masked and unmasked data a user views.

The MaskRequired(NonAdministrator) rule sets the LOYALTY_ROLE symbol for the user. If the user is an administrator, the rule matcher returns FALSE and the rule sets the LOYALTY_ROLE symbol to Administrator. The Rule Engine does not continue processing the request and the request goes to the Print Roles rule.

If the user does not have an administrator role, the matcher returns TRUE. The LOYALTY_ROLE symbol is set based on the user role. For example, if the user has a loyalty level 2, the LOYALTY_ROLE symbol is set to Loyalty_PI_LEVEL_2.

If the user has a default user level or does not have a user role, the LOYALTY_ROLE symbol is set to Loyalty_PI_DEFAULT_LEVEL.

If the user has more than one loyalty role, the LOYALTY_ROLE symbol is set to the weakest loyalty level. For example, if the user has loyalty role one (1) and loyalty role three (3), the symbol is set to Loyalty_PI_LEVEL_3.

MatchLevel Rules

The MatchLevel rules use the folder processing action to direct requests to the appropriate masking rules.

The MatchLevel rules use the symbol matcher matching method. The symbol matcher retrieves the value of the LOYALTY_ROLE symbol.

If the LOYALTY_ROLE symbol value is a match, the rule uses the folder rule action and the continue processing action to direct the request to the masking rule in the folder. If the LOYALTY_ROLE symbol value of the user is not a match for the MatchLevel rule, the request goes down the rule tree to the next MatchLevel rule.

The following table lists the MatchLevel rules and the LOYALTY_ROLE symbol values that each rule matches:

Rule	Loyalty Levels
MatchLevel0AndAbove	- Loyalty_PI_LEVEL_0 - Loyalty_PI_LEVEL_1 - Loyalty_PI_LEVEL_2 - Loyalty_PI_LEVEL_3 - Loyalty_PI_DEFAULT_LEVEL
MatchLevel1AndAbove	- Loyalty_PI_LEVEL_1 - Loyalty_PI_LEVEL_2 - Loyalty_PI_LEVEL_3 - Loyalty_PI_DEFAULT_LEVEL
MatchLevel2AndAbove	- Loyalty_PI_LEVEL_2 - Loyalty_PI_LEVEL_3 - Loyalty_PI_DEFAULT_LEVEL
MatchLevel3AndAbove	- Loyalty_PI_LEVEL_3 - Loyalty_PI_DEFAULT_LEVEL
MatchDefaultLevel	Loyalty_PI_DEFAULT_LEVEL

MaskLevel Rules

The MaskLevel rules use the mask rule action to mask data.

Each time the loyalty level of a user is a match for a MatchLevel rule, the request goes to the masking rule below the MatchLevel rule. If the request is not a match for the MatchLevel rule, the request goes to the next MatchLevel rule until it reaches the end of the rule tree.

For example, a user with a loyalty level of one sends a request. The request moves through the rule tree in the following order:

1. The user is a match for the MatchLevel0AndAbove rule, so the rule directs the request to the MaskLevel0 masking rule and the Rule Engine applies the rule.
2. The request continues to the MatchLevel1AndAbove rule, which matches the request and directs the request to the MaskLevel1_1 rule.
3. The Rule Engine applies the MaskLevel1_1 and MaskLevel1_2 rules to the request.
4. The request continues to the MatchLevel2AndAbove, which is not a match. The request continues to the MatchLevel3AndAbove and MatchDefaultLevel rules. The request is not a match for the rules and the Rule Engine does not apply any more masking rules.

MaskLevel0 Rule

The MaskLevel0 masking rule masks data to users that have a loyalty level of zero (0) or higher.

The following table describes the column that the MaskLevel0 rule masks:

Table	Column
CUSTOMER	GENDER. Nullifies the values.

MaskLevel1 Rules

The MaskLevel1_1 and MaskLevel1_2 rules mask data to users that have a loyalty level of one (1) or higher.

The MatchLevel1AndAbove rule folder contains two rules because the rules mask columns with the same name in different tables.

The following table describes the columns that the MaskLevel1 rules mask:

Table	Column
CUSTOMER	CREDITCARD. Shows only last four digits.
TICKET	- CREDITCARD. Shows only last four digits. - ID_NUM. Shows as XXX-XX-XXX.
TICKET_COUPON	ID_NUM. Shows as XXX-XX-XXX.

MaskLevel2 Rule

The MaskLevel2 rule masks data to users that have a loyalty level of two (2) or higher.

The following table describes the columns that the MaskLevel2 rule masks:

Table	Column
ADDRESS	- ADDRESS. Shows the following text: `Hidden for compliance reasons.` - PHONE_NUMBER. Shows only the last four digits.
CUSTOMER	- FIRST_NAME. Shows first three characters and replaces the remaining characters with asterisks (*). - LAST_NAME. Shows the first three characters and replaces the remaining characters with asterisks (*).
TICKET	PASSENGER_NAME. Shows first three characters and replaces the remaining characters with asterisks (*).

MaskLevel3 Rule

The MaskLevel3 masking rule masks data to users that have a loyalty level of one (3) or higher.

The following table describes the columns that the MaskLevel3 rule masks:

Table	Column
ADDRESS	- ZIP_CODE. Shows first three characters and replaces the remaining characters with asterisks (*). - CITY. Shows first three characters and replaces the remaining characters with asterisks (*). - STATE. Changes all values to ZZ.

MaskDefaultLevel Rule

The MaskDefaultLevel masking rule masks data to default users.

The following table describes the columns that the MaskDefaultLevel rule masks:

Table	Column
AIRPORTS	CODE. Changes all values to x.
CUSTOMER	- LAST_ACTIVITY_DATE. Shows only the day and month. - MEMBER_SINCE_DATE. Shows only the date and month. - MEMBERSHIP_STATUS. Shows the following text: `* CONFIDENTIAL *`
TICKET-COUPON	- FROM_CITY. Changes all values to F. - TO_CITY. Changes all values to T.

Print Roles Rule

The Print Roles rule uses the folder processing action to direct requests to the GenericDataArchiveAction and PrintDataArchiveSymbols rules.

The Print Roles rule uses the text matcher to match ".*select 1.*." When the request is a match, the folder processing action directs the request to the GenericDataArchiveAction rule and the PrintDataArchiveSymbols rules.

GenericDataArchiveAction Rule

The GenericDataArchiveAction rule retrieves the user name and user role information from the SQL request and creates symbols based on the information. Create a rule similar to the GenericDataArchiveAction rule when you create a rule set to mask Data Vault data.

When you create a rule set to mask Data Vault data, you can create a rule similar to the GenericDataArchiveAction rule that decrypts the SQL comment from the Data Archive client and creates the DataArchive_User and DataArchive_Roles symbols. The rule uses the Java rule action. The class path parameter must contain the location of the DataArchiveAcclerator.jar file and the class name must be GetUsersAndRolesFromComment.

PrintDataArchiveSymbols Rule

The PrintDataArchiveSymbols rule prints a list of the Data Archive users and user roles.

The PrintDataArchiveSymbols is a rule that you can use to print the Data Archive users and user roles to verify that the GetUsersAndRolesFromComment correctly decrypted the SQL comment that the Data Archive client sent to Dynamic Data Masking.

CHAPTER 4

Dynamic Data Masking

This chapter includes the following topics:

- Dynamic Data Masking Overview, 27
- Dynamic Data Masking Components, 28
- Management Console, 29
- Database Management, 32
- Dynamic Data Masking Server Management, 32
- Dynamic Data Masking Service Management, 33
- Domain Management, 33
- Connection Management Overview, 34
- Rules, 35
- Server Control, 39

Dynamic Data Masking Overview

Dynamic Data Masking is a data security product that operates between an application and a database to prevent unauthorized access to sensitive information. Dynamic Data Masking intercepts requests sent to the database and applies data masking rules to the request to mask the data before it is sent back to the application.

You can use Dynamic Data Masking to mask or prevent access to sensitive data stored in production and non-production databases. You set up the rules to specify the database requests to intercept and the masking actions to apply. Dynamic Data Masking monitors incoming database requests from the application. Dynamic Data Masking applies the data masking rules to the database request before it sends it to the database. The database processes the modified request as normal and returns masked results to Dynamic Data Masking. Dynamic Data Masking then sends the results to the application.

You can use Dynamic Data Masking to mask data for specific types of database requests or you can restrict access to data from certain groups within an organization. For example, you can create a rule to apply a masking function to credit card numbers when the database request comes from a support team member. When the database sends the data back to the application, the support team member sees the masked numbers instead of the real credit card numbers.

Dynamic Data Masking Components

Dynamic Data Masking includes server components to intercept and process database requests and a client component to manage the server.

Dynamic Data Masking has the following components:

Dynamic Data Masking Server

The Dynamic Data Masking Server provides services and resources to intercept database requests and perform data masking tasks.

The Dynamic Data Masking Server includes the following components:

- Dynamic Data Masking services
- Rule Engine

Dynamic Data Masking Service

The Dynamic Data Masking service listens on the listener port to monitor and route incoming database requests.

You can run the following Dynamic Data Masking services:

Service	Description
DDM for Azure	Listens for and routes database requests for a Microsoft Azure SQL database. The service supports the SSL mode of communication.
DDM for DB2	Listens for and routes database requests for an IBM Db2 database. The service supports SSL and non-SSL modes of communication.
DDM for FAS	Listens for and routes database requests for Data Vault. The service supports SSL and non-SSL modes of communication.
DDM for Hive	Listens for and routes database requests for a Hive database. The service supports SSL and non-SSL modes of communication as well as Kerberos Authentication and Kerberos encrypted data.
DDM for Hive HTTP	Listens for and routes database requests for Hive databases using HTTP transport. The service supports SSL and non-SSL modes of communication, and Kerberos Authentication.
DDM for Impala	Listens for and routes database requests for an Impala database. The service supports SSL and non-SSL modes of communication as well as Kerberos Authentication.
DDM for Informix	Listens for and routes database requests in Informix native protocol to Informix databases.
DDM for Informix (DRDA)	Listens for and routes database requests in Distributed Relational Database Architecture protocol to Informix databases.
DDM for JDBC	Listens for database requests for a database that uses JDBC connectivity.
DDM for ODBC	Listens for database requests for a database that uses ODBC connectivity.
DDM for Oracle	Listens for and routes database requests for an Oracle database. The service supports SSL and non-SSL modes of communication.

Service	Description
DDM for PostgreSQL	Listens for and routes database requests for a PostgreSQL database.
DDM for SQL Server	Listens for and routes database requests for a Microsoft SQL Server database. The service supports SSL and non-SSL modes of communication.
DDM for Sybase	Listens for and routes database requests for a Sybase database.
DDM for Teradata	Listens for and routes database requests for a Teradata database.

Rule Engine

The Rule Engine evaluates incoming database requests and applies connection and security rules to determine how to route requests and mask data. The Rule Engine can modify the database request based on the rules defined in the Dynamic Data Masking Server.

The Rule Engine applies the following types of rules:

- Connection rule. Defines the conditions and actions that the Rule Engine applies to determine how to route a database connection request received from an application.
- Security rule. Contains the conditions and actions that define what to do with the database SQL request and how to apply SQL rewrites that manipulate the returned SQL result set.

Server Control

Server Control is a command line program that you use to configure and manage the Dynamic Data Masking Server. Use Server Control to start or stop the Dynamic Data Masking Server and services or to change the port number or password for the Dynamic Data Masking Server.

Management Console

The Management Console is a client application that you use to manage the Dynamic Data Masking Server. You can use the Management Console to create and manage rules and to configure and manage connections to databases.

Management Console

The Management Console is the client component of the Dynamic Data Masking Server.

You can install the Management Console on a remote machine or the local system to manage the Dynamic Data Masking service. Use the Management Console to manage and configure domains and Dynamic Data Masking services, define connection rules for Dynamic Data Masking services, define security rules, and configure target databases.

Menu

The Management Console Tree menu contains options that you use to edit the nodes within the Management Console tree. The toolbar contains shortcuts to options in the menu. Available menu items change based on

the type of node you select in the tree. Items that are not available for the tree node you select are grayed out.

The Management Console Tree menu contains the following options:

Menu Item	Action
Login	Shows the server host, port, and username for the last login.
Exit	Exits the Dynamic Data Masking session.
Add Domain	Creates a domain in the Management Console tree. Add Domain is available when a domain node is selected.
Add Database	Defines the connection properties for an additional database in the Management Console tree. Add Database is available when a domain node is selected.
Add DDM Services	Adds a Dynamic Data Masking service to the Management Console tree. Add DDM Services is available when the server node is selected.
Add Rule Set	Adds a security rule set to the Management Console tree. Add Rule Set is available when a domain node is selected.
Edit	Opens a window to edit domain and rule set names, define service listener ports, and edit connection information for databases and the Dynamic Data Masking Server.
Security Rule Set	Opens a security rule set. Security Rule Set is available when a security rule set is selected.
Connection Rules	Opens a connection rule set. Connection Rules is available when a Dynamic Data Masking service is selected.
Authorization	Opens a window to set and edit permissions for the selected node. Authorization is available when a database, domain, or security rule set node is selected.
Cut	Copies and deletes the selected Management Console tree node. You can cut server, database, domain, and security rule set nodes. You cannot cut service nodes or the root domain node.
Copy	Copies the selected Management Console tree node. You can copy database, domain, and security rule set nodes. You cannot copy service nodes, server nodes, or the root domain node.
Paste	Pastes the cut or copied Management Console tree node. You can paste on domain nodes.
Remove	Removes a node from the Management Console tree. **Note:** You cannot remove the Dynamic Data Masking Server or the Management Console root domain.
Start Service	Starts a Dynamic Data Masking service. The Start Service option is available when a Dynamic Data Masking service is selected.
Stop Service	Stops a Dynamic Data Masking service. The Stop Service option is available when a Dynamic Data Masking service is selected.
Add Logger	Adds a custom logger to the Management Console tree. Add Logger is available when the Loggers node is selected.
Add Appender	Adds an appender to the Management Console tree. Add Appender is available when a logger node is selected.

Menu Item	Action
Support	Creates an encrypted .zip archive of Dynamic Data Masking logs. You can send the log archive to Informatica Global Customer Support to troubleshoot issues with Dynamic Data Masking.
Manage Licenses	Allows you to select a new license file. Use the Manage Licenses option if the Dynamic Data Masking license file has expired. The Manage Licenses option is available when the Dynamic Data Masking Server node is selected.
Sort by Name	Sorts child nodes and nested child nodes in alphabetical order by the name of the node. Sort by Name is available when a node with child nodes is selected.
Sort by Owner	Sorts child nodes and nested child nodes in alphabetical order by the login name of the user that created the nodes. Sort by Owner is available when a node with child nodes is selected.
Sort by Type	Sorts child nodes and nested child nodes in alphabetical order by the type of node. Sort by Type is available when a node with child nodes is selected.

Management Console Tree

The Management Console tree is a navigation tree organized by nodes. When the Management Console is not connected to a Dynamic Data Masking Server, it shows a default domain node. All actions are disabled, except Login, Exit, and About. After successful login to a Dynamic Data Masking Server, the Management Console shows a tree with the Dynamic Data Masking Server node that it is connected to.

The Management Console tree can contain domain, database, server, service, logger, appender, and rule set nodes. Tree nodes are arranged hierarchically.

On the Management Console, the relationship between the Dynamic Data Masking Server and a database is based on the domain organization. The Dynamic Data Masking Server will connect to databases that are in the same domain or a sub domain of the Dynamic Data Masking Server. The Dynamic Data Masking Server will not connect to any database that is outside the domain that contains the Dynamic Data Masking Server.

Logging In to the Management Console

You can access the Dynamic Data Masking components through the Management Console. Log in to the Management Console to manage target databases, configure listener ports, and define rules.

To log in to the Management Console, you need the server address and port number of the server that Dynamic Data Masking operates on and the administrator credentials.

Logging In to the Management Console on Windows

On Windows, open the Management Console through the Start menu.

1. On Windows 7 and earlier, select **Start** > **All Programs** > **Informatica** > **Dynamic Data Masking** > **Management Console**.

   On Windows 10 and later, select **Search the Web and Windows** > **All apps** > **Informatica Dynamic Data Masking** > **Management Console**.

   The **Login** window appears.
2. Verify that the **Server Host** and **Port** display the correct information for the Dynamic Data Masking Server.

3. Enter the Dynamic Data Masking administrator user name and password. If you use LDAP authentication, the user name must be in LDAP format. Click **Connect**.

   A tree is visible in the Management Console after you login successfully.

Logging In to the Management Console on Linux

On Linux, start the Management Console with the `mng` script.

You must have the X Window server installed on the machine that you use to log in to the Management Console.

1. Open a terminal and navigate to the Dynamic Data Masking installation directory.

   For example, you might enter the following command:

   ```
   cd /home/Informatica/DDM
   ```

2. Run the following command to start the Management Console:

   ```
   ./mng
   ```

   The **Login** window appears.

3. Verify that the **Server Host** and **Port** display the correct information for the Dynamic Data Masking Server.
4. Enter the Dynamic Data Masking administrator user name and password. If you use LDAP authentication, the user name must be in LDAP format. Click **Connect**.

   A tree is visible in the Management Console after you log in.

Database Management

A database node contains references to databases. The Dynamic Data Masking Server controls access to the databases that the database nodes reference.

A database node can reference an Oracle, Microsoft SQL Server, Db2, Informix, Sybase, Data Vault, Hive, or Teradata database. The Management Console tree can contain an unlimited number of database nodes. You can create database nodes under domain nodes. Database nodes do not have child nodes. You can set user permissions on database nodes.

Dynamic Data Masking Server Management

A server node contains a reference to the Dynamic Data Masking Server. By default, the server node is located under the root domain after a new installation of the Dynamic Data Masking Server.

The Management Console contains one server node. Each Dynamic Data Masking instance associates with one Dynamic Data Masking Server. You connect to a server when you log into the Management Console. The Dynamic Data Masking Server manages databases located under a parent domain or all sub domains of the server node in the tree.

The server node has a domain node parent. The server node can have Dynamic Data Masking service child nodes. You can edit and move the server node.

Note: You cannot add or remove the Dynamic Data Masking Server node with the Add or Remove options in the Management Console menu.

Dynamic Data Masking Service Management

The Dynamic Data Masking service routes SQL queries to Oracle, Microsoft SQL Server, Db2, Informix, Sybase, Data Vault, Hive, and Teradata databases.

The Dynamic Data Masking Server can contain single service nodes for each database. Create service nodes under the server node. Service nodes cannot have child nodes. You can add, edit, and remove service nodes.

Each Dynamic Data Masking service routes requests to a specific type of database. For example, the Dynamic Data Masking for Oracle service routes requests to Oracle databases and the Dynamic Data Masking for DB2 service routes requests to Db2 databases.

Dynamic Data Masking Listener Ports

The Dynamic Data Masking service controls connections between the client and the database through the listener port.

You must configure the database listener port to forward connections to the Dynamic Data Masking listener port. How you configure the listener ports depends on whether the Dynamic Data Masking service runs on the database server or on a standalone server. You can define the listener port that the Dynamic Data Masking service uses through the Services Editor in the Management Console.

If the Dynamic Data Masking service runs on a standalone server, you must route application connection requests to the Dynamic Data Masking listener port.

Defining a Dynamic Data Masking Listener Port

Before you can define a listener port, you must run the netstat system utility to verify port availability.

1. In the Management Console, right-click on a Dynamic Data Masking service and select **Edit**.

   The Service Editor appears.
2. Click **Add Port**.
3. Enter the listener port for the Dynamic Data Masking service.
4. Click **OK**.

Domain Management

A domain is a virtual node in the Management Console tree that you use to group other nodes. The Management Console contains a default root domain. You can use domains to create a visual representation of the structure of the databases within an organization.

You can create an unlimited number of domains in the Management Console tree. A domain can contain other domains, databases, and server child nodes. You can set user permissions on domain nodes.

You can add, edit, cut, copy, paste, and remove a domain. You cannot remove the root domain. Drag a domain up or down in the Management Console tree to change the position of the domain within the tree.

Connection Management Overview

Use the **Add Database** window to add a database to the Management Console tree. Select a database type and define database parameters. Test the database connection to verify that the Dynamic Data Masking service can access the database.

Data Vault Connection Management

To add an Informatica Data Vault connection node to the Management Console tree, select the FAS database type.

You can enable SSL communication between the Data Vault and the Dynamic Data Masking Server. For more information about enabling SSL communication, see the "Security" chapter. Communication is encrypted between the Dynamic Data Masking FAS service and the Data Vault, and between the Dynamic Data Masking FAS service and the Data Vault client. For information on how to enable SSL in the Data Vault, see the *Data Vault Administrator Guide*. To use SSL communication, you must have Data Archive version 6.4.3 or later installed.

Click **Test Connection** to verify that the Dynamic Data Masking service can access the database.

Data Vault Connection Parameters

Define the following connection parameters for a Data Vault connection:

DDM Database Name

Name for the database node that appears in the Management Console tree.

Server Address

Server host name or TCP/IP address for the Data Vault.

Note: Verify that there is no firewall that prohibits the Dynamic Data Masking Server from connecting to the Data Vault Server and port number.

Server Port

TCP/IP listener port for the Data Vault.

FAS Database Name

Database name for the Data Vault.

Keystore

Select **Custom** if you have configured a custom keystore. Select **Default** if you want to use the default keystore preconfigured for use with Dynamic Data Masking.

DBA Username

User name for the Data Vault user account to log in to the Data Vault. The Data Vault user must have the SELECT access privilege for all the tables to which the client user has the SELECT access privilege. This parameter is valid for the default keystore.

DBA Password

Password for the Data Vault user. This parameter is valid for the default keystore.

Key Store Name

Name of the custom keystore, defined in the `ddm.security` file. This parameter is valid for custom keystores.

Alias

Alias name for the custom keystore. For CyberArk accounts, the alias name was defined when the CyberArk account was created. This parameter is valid for custom keystores.

SSL

Select to enable SSL communication between the database and the Dynamic Data Masking Server. For more information on SSL configuration, see the chapter "Security."

Rules

A rule contains the conditions and actions that the Rule Engine uses to process a request. Connection rules process application connection requests. Security rules process SQL statements. You create and define rules to manage the SQL requests that the client or application sends to the target database.

A rule defines connection criteria and masking techniques. The Rule Engine uses connection criteria to forward requests and masking techniques to mask data. Rules can be connection rules or security rules, placed in a rule tree. The organization of the rule tree determines the order in which the Rule Engine applies the rules. You can create and edit rules within the Management Console.

Rule Components

A rule consists of a matcher, an action, and a processing action. Each rule component defines how the Rule Engine identifies and processes a request to the database.

The Rule Engine applies a connection rule to incoming connection requests and applies security rules to SQL statements. A connection rule defines how the Dynamic Data Masking service establishes a connection with the application. A security rule defines the conditions and masking rules that the Rule Engine applies to the SQL statement request. The Rule Engine applies a security rule if you configure a connection rule to apply a rule set.

A rule consists of the following components:

Matcher

Defines the criteria that the Rule Engine uses to identify a match.

Action

Defines the action that the Rule Engine applies to the request.

Processing action

Defines the action that the Rule Engine applies to the request after the Rule Engine applies the rule. The processing action manages how the Rule Engine processes the request through the rule tree. A processing action can specify that the Rule Engine does not process further rules in the rule tree or that the Rule Engine continues to evaluate other rules.

Rule Trees

A rule tree represents the organizational structure of rules and rule folders. The position that you assign a rule or rule folder within the rule tree determines the order in which the Rule Engine processes the rule. You build conditional relationships between rules through the rule tree.

A rule tree can be a connection rule tree or a security rule tree. Each rule tree uses a system of folders and rules to determine the hierarchical order for rule processing.

When the Dynamic Data Masking Server receives a connection request, the Rule Engine parses the request through the connection rule tree. If the connection rule assigns a security rule set, then the Rule Engine parses the SQL request through the security rule tree. The security rule set defines the security techniques that the Rule Engine applies to rewrite the SQL statement.

Rule Tree Components

Connection rules and security rules work together to define when and how data is masked.

Use the following components to identify and manage application requests:

Rule

The conditions and actions that you want to apply to a request. A rule can be a connection rule or a security rule. You can create an individual rule or create a rule as part of a rule folder.

A rule consists of a matcher, action, and processing action.

Rule folder

A rule that uses the Folder rule action. You can use a rule folder to group conditional rules. The Rule Engine processes the contents of a rule folder hierarchically.

A connection rule folder contains connection rules. A security rule folder contains security rules.

Connection rule

A rule that defines the criteria that the Rule Engine uses to identify the target database for the request. A connection rule consists of a matcher and an action that you define to identify and route a connection request from an application.

Connection rule tree

The connection rule tree defines the order in which the Rule Engine processes connection rules. The connection rule tree contains all the connection rules that you define for the target databases. The Rule Engine processes the first rule or rule folder in the connection rule tree and stops at the end of the rule tree or when there is a stop processing action.

Security rule

A rule that defines the criteria that the Rule Engine uses to parse and alter the SQL statement request. A security rule consists of a matcher and action that you define to identify and mask a SQL request.

Security rule set

A security rule set is a container for security rules. You use rule folders to organize and nest rules within the rule set. A security rule set can contain multiple rule folders. The Rule Engine processes the SQL statement through the rule set until the Rule Engine encounters a stop processing action.

Security rule tree

Each security rule set has an individual security rule tree. The security rule tree defines the order in which the Rule Engine processes security rules. The security rule tree contains the security rules for a particular security rule set. The Rule Engine processes the first rule or rule folder in the security rule tree and stops when there is a stop processing action.

Connection Rules

A connection rule defines the connection criteria that the Rule Engine uses to identify a connection and the target database.

A connection rule uses a matcher and a rule action to identify and route a connection. The matcher defines the criteria that the Rule Engine uses to identify a match. The rule action determines how the Rule Engine processes the matched connection.

When the Dynamic Data Masking service receives a connection request, the Rule Engine applies connection rules to the connection. If the connection request matches the criteria defined by the matcher, the Rule Engine applies the rule action to the connection. After the Rule Engine applies the rule action, the Rule Engine applies processing action. The processing action defines the next action that the Rule Engine applies to the request.

Creating a Connection Rule

Create a connection rule to manage how the Dynamic Data Masking service forwards incoming connections. Define the connection criteria and processing action for a connection rule. Add a single connection rule to the rule tree or nest a connection rule within a rule folder.

1. In the Management Console, select the Dynamic Data Masking service that you want to add the connection rule to, and click **Tree** > **Connection Rules**.

   The **Rule Editor** window appears.
2. Select **Action** > **Append Rule**.

   The **Append Rule** window appears.
3. Enter a rule name in the **Rule Name** box.
4. Select and define a matcher.
5. Select and define an action.
6. Select a processing action.
7. Click **OK**.

   The connection rule appears in the rule tree.
8. Select **File** > **Update Rules**.

   The connection rule is saved.

Security Rules

A security rule defines the criteria that the Rule Engine uses to parse and rewrite an SQL request. A security rule is part of a security rule set. You can create a security rule in a rule folder or as a rule in a rule tree.

Security rules specify the technique that the Rule Engine uses to mask data. Security rules consist of a matcher, a rule action, and a processing action. Security rules mask data in a row or column. For example, create a security rule that rewrites SQL requests that reference the Social Security column from the Employee table.

Connection rules define the security rules that the Rule Engine applies. Use the connection properties to define security rules for Microsoft SQL Server.

Note: Dynamic Data Masking supports request packets in UTF-8 format. If the machine on which you install Dynamic Data Masking has a different default encoding method, you can change the method by updating the `jvm.params` file. Dynamic Data Masking might not work as expected for requests sent in non UTF-8 format.

Creating a Security Rule Set

Create a security rule set to group security rules that share a relational link.

1. In the Management Console, click on a domain node in the rule tree.
2. Click **Tree** > **Add Rule Set**.

   The **Add Rule Set** window appears.
3. Enter a name for the security rule set and click **OK**.

   The security rule set appears inside the rule tree in the Management Console.

You can add security rules to the rule set.

Creating a Security Rule

Create a security rule to define the criteria that the Rule Engine uses to parse an SQL request. To create a security rule, configure a matcher, action, and processing action.

Use the following high-level steps to create a security rule. The steps vary based on the types of matcher methods and actions that the rule uses.

1. In the Management Console, click the security rule set that you want to add the rule to.
2. Select **Tree** > **Security Rule Set**.

   The **Rule Editor** appears.
3. Click **Action** > **Append Rule**.

   The **Append Rule** window appears.
4. Enter a name for the rule in the **Rule Name** field.
5. Enter an optional description for the rule.
6. Select a matcher type and define the matching criteria.
7. Select **Keep matcher result** to store the result if a match occurs.
8. Choose a rule action and define the rule action criteria.
9. Choose a rule processing action.
10. Select **Log when rule is applied** to log the rule information in the rule log.
11. Click **OK**.

    The rule appears in the rule tree.
12. Select **File** > **Update Rules** to save the rule in the rule tree.

Rule Folders

A rule folder is a container for rules that share conditional relationships. You can rename, reconfigure, move, cut, copy, paste, delete, disable, and enable a rule folder. Create rule folders to organize related rules and define the order in which the Rule Engine applies them.

A rule folder can contain connection rules or security rules. A connection rule folder groups rules that you apply to connection requests. A security rule folder contains rules that you apply to SQL request statements.

To create a rule folder, specify the folder action for the rule. Within the rule folder, create relational rules that help the Rule Engine identify, match, and rewrite requests. Before you can add rules to a folder, you must outline the relationships between the rules that you want the folder to contain.

You can group rules that share the same purpose. For example, group masking rules together in a rule folder and group access control rules in another rule folder.

Note: When you create a rule folder, you must set the processing action to **Continue**. When the Rule engine encounters a continue processing action, the Rule Engine processes the request through the rules that the folder contains.

Rule Management

You can rename, reconfigure, move, cut, copy, paste, delete, disable, and enable a rule. When you make changes to a rule, you must update the rule tree for the change to take effect.

When you create, edit, or add a connection rule, you must restart the current session with the application before the Rule Engine can apply the connection rule. Updates to a security rule take effect immediately. You do not need to start a new session for the Rule Engine to apply a security rule.

You can move a rule to change the position of the rule in the rule tree. You can move a rule folder to change the position of the folder in the rule tree. You cannot move a rule into or out of a folder. Move a rule to change the order in which the Rule Engine applies the rule.

You can enable or disable a rule or rule set. By default, the rule or rule set is enabled. When you enable a rule or rule set, the Rule Engine applies the rule or rule set to the request. When you disable a rule, the Rule Engine skips the rule or rule set and applies the next rule or rule set in the rule tree.

You can delete a rule or rule folder from the rule tree. When you delete a rule folder, you delete the content that the rule folder contains. You cannot undo the changes after you delete a rule or rule folder from the rule tree.

Editing a Rule

You can edit the matcher, action, processing action, and name for any rule.

1. Open the **Rule Editor** for connection rules or security rules.
2. Click on a rule in the rule tree.
3. Click **Edit**.

   The **Edit** window appears.
4. Make the changes that you want to the rule components.
5. Click **OK**.
6. Select **File** > **Update Rules**.

   The rule tree is updated.

Server Control

The Dynamic Data Masking Server Control program is a command line interface that you use to manage the Dynamic Data Masking Server and start and stop the Dynamic Data Masking services. Server Control reads administrative requests and writes the results of the requests to the standard system output and error streams.

Server Control has a set of commands that simplify management and configuration of local and remote Dynamic Data Masking Servers. Server Control is installed with the Dynamic Data Masking Server. Run Server Control on the machine where you installed the Dynamic Data Masking Server.

For a complete list of Server Control commands, see the *Dynamic Data Masking Administrator Guide*.

Running Server Control

Run Server Control to manage the Dynamic Data Masking Server from a command line interface.

If you run the Dynamic Data Masking Server on Windows, Server Control runs as a batch file with a .bat extension.

If you run the Dynamic Data Masking Server on Linux, Server Control runs as a shell script with no extension. You can run the `server` shell script to use the Server Control commands. Alternatively, you can run a subset of the Server Control commands from individual shell scripts. For example, to start the Dynamic Data Masking Server, you can run the `server` shell script with the start command or you can run the `start` shell script directly.

Running Server Control on Windows

On Windows, run the Server Control command line program from the Start Menu.

1. Select **Start** > **Informatica** > **Dynamic Data Masking** > **Server Control**.
2. At the command line, enter commands with the following syntax:

```
server <command name> <parameter>
```

For example, the following command sets the port for the Dynamic Data Masking Server to 8195:

```
server setPort 8195
```

Running Server Control on Linux or UNIX

On Linux, use the `server` shell script to run Server Control commands. Alternatively, run Server Control commands from individual shell scripts.

1. Open a terminal, and navigate to the Dynamic Data Masking Server installation directory.

   For example, you might navigate to the following directory:

   ```
   /home/Informatica/DDM
   ```

2. Run the shell script for the Server Control command that you want to use.
   - If you run the `server` shell script, enter commands with the following syntax:

     ```
     ./server <command name> <parameter>
     ```

   - If you run a shell script for a specific command, run the shell script with the following syntax:

     ```
     ./<shell script name> <parameter>
     ```

For example, the following command uses the `server` shell script to start the DDM for Oracle service:

```
./server startDDMService "DDM for Oracle"
```

Alternatively, the following command uses the `startDDMService` shell script to start the DDM for Oracle service:

```
./startDDMService "DDM for Oracle"
```

Server Control Commands

Enter commands and parameters in the Server Control command line program to manage the Dynamic Data Masking Servers and services.

Use the following rules when you enter commands and parameters:

- The first word after a command is the parameter.
- If a parameter contains spaces, enclose the parameter in double quotes.

- Server Control commands are not case sensitive.

Help

Displays descriptions and parameters for each Server Control command.

The command uses the following syntax:

```
server
  help
```

Start

Starts the Dynamic Data Masking Server. Creates an operating system service in Windows if the service does not exist. The Dynamic Data Masking Server must be shut down to run the command.

The command uses the following syntax:

```
server
  start
```

On Linux, you can also run the `start` shell script to start the Dynamic Data Masking Server.

Stop

Stops the Dynamic Data Masking Server.

The command uses the following syntax:

```
server
  stop
```

On Linux, you can also run the `stop` shell script to stop the Dynamic Data Masking Server.

INDEX

A

accelerator
  overview 8
  setup 10

C

command line
  parameters 40
connection management
  Data Vault 34
  overview 34
connection parameters
  Data Vault 34
connection rule
  creating 37
connection rule tree 36
connection rules
  creating 14

D

Data Archive accelerator
  overview 8
Data Vault
  connection management 34
  connection parameters 34
  define 11
databases
  Data Vault 34
  management 32
domains
  management 33
Dynamic Data Masking
  components 28
  databases 32
  listener ports 33
  Server 32
  service 33
Dynamic Data Masking service
  Data Vault 28
  Hive 28
  IBM Db2 28
  Informix 28
  Microsoft SQL Server 28
  Oracle 28
  Sybase 28
  Teradata 28

I

importing
  rules 21

L

listener port
  define 11
listener ports
  defining 33

M

Management Console
  logging in 31
  menu 30
  overview 29
  tree 31

R

roles
  loyalty roles 23
rule
  creating 37, 38
Rule Engine 28
rule folder 36, 38
rule set 36
rule tree 35, 36
rules
  components 35
  connection rules 14
  editing 39
  folders 38
  GenericDataArchiveAction 26
  importing 21
  management 39
  MaskDefaultLevel 25
  MaskLevel 24
  MaskLevel2 25
  MaskLevel3 25
  MaskRequired(NonAdministrator) 22
  matcher 35
  MatchLevel 23
  overview 19
  Print Roles 26
  PrintDataArchiveSymbols 26
  processing action 35
  rule action 35
  rule tree 35
  security rules 12
  SwitchToDataVault 14

rules *(continued)*
updating 39
UseDataArchiveAccelerator 15

S

security rule
creating 38
security rule set
creating 38
security rule tree 36
security rules
creating 12
Server
management 32
Server Control
commands
help 41
start 41
stop 41
Server Control *(continued)*
running 40
service
add 11
management 33
symbol
LOYALTY_ROLE 23
symbols
DataArchive_Roles 26
DataArchive_User 26