Informatica

Informatica® Dynamic Data Masking
9.8.2

Siebel Accelerator Guide

Informatica Dynamic Data Masking Siebel Accelerator 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 5

Informatica Resources. 5

Informatica Network. 5

Informatica Knowledge Base. 5

Informatica Documentation. 5

Informatica Product Availability Matrixes. 6

Informatica Velocity. 6

Informatica Marketplace. 6

Informatica Global Customer Support. 6

Chapter 1: Introduction to the Siebel Accelerator 7

Siebel Accelerator Overview. 7

Chapter 2: Siebel Accelerator Setup 8

Siebel Accelerator Setup Overview. 8

Verify Requirements. 9

Create Dynamic Data Masking Database Administrator User. 9

Compile the Database Objects. 9

Create a Database Connection. 10

Import Connection Rules. 10

Import Application Security Rules. 11

Import Development Security Rules. 11

Chapter 3: Siebel Accelerator Rules 13

Siebel Accelerator Rules Overview. 13

Siebel Accelerator Connection Rules. 13

SiebelDevConnRule Connection Rule. 14

SiebelAppConnRule Connection Rule 14

SiebelDevRuleSet Security Rule Set. 14

SiebelAppRuleSet Security Rule Set. 15

MatchSiebelTables Rule Folder. 15

UserHandling and PositionHandling Rule Folders. 16

BlackList Rule Folder. 16

WhiteList Rule Folder 16

Index 18

Preface

The *Siebel Accelerator Guide* contains information to help administrators use the Siebel accelerator to implement Dynamic Data Masking for an Oracle database configured for Siebel. This guide assumes that you have knowledge of Dynamic Data Masking.

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

Introduction to the Siebel Accelerator

This chapter includes the following topic:

- Siebel Accelerator Overview, 7

Siebel Accelerator Overview

Use the Siebel accelerator to implement Dynamic Data Masking for an Oracle database configured for Siebel. The accelerator package contains predefined Dynamic Data Masking connection and security rules for common masking requirements.

The Siebel accelerator is in the Dynamic Data Masking installation folder as an additional component that you can configure to work with a Siebel database. You can use the accelerator rules to mask data based on the Siebel user and the Siebel position of the user that accesses the database.

CHAPTER 2

Siebel Accelerator Setup

This chapter includes the following topics:

- Siebel Accelerator Setup Overview, 8
- Verify Requirements, 9
- Create Dynamic Data Masking Database Administrator User, 9
- Compile the Database Objects, 9
- Create a Database Connection, 10
- Import Connection Rules, 10
- Import Application Security Rules, 11
- Import Development Security Rules, 11

Siebel Accelerator Setup Overview

Set up the Siebel accelerator to use predefined connection and security rules.

You can find the Siebel accelerator in the following directory:

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

To set up the Siebel accelerator, perform the following tasks:

1. Verify the installation requirements.
2. Create a Dynamic Data Masking database administrator user.
3. Compile the database objects.
4. Create a Dynamic Data Masking Oracle database connection.
5. Import the Siebel accelerator connection rules.
6. Import the Siebel accelerator application security rules.
7. Import the Siebel accelerator development security rules.

Verify Requirements

Verify the following requirements before you use the Siebel accelerator:

- Dynamic Data Masking version 9.1.0 or later must be installed.
- The database must be an Oracle database configured for Siebel.

Create Dynamic Data Masking Database Administrator User

Create a Dynamic Data Masking database administrator user to use the Siebel accelerator.

Connect to the database with the sys user and run the following database commands:

```
CREATE USER DDMUSER IDENTIFIED BY DDMUSER
ALTER USER DDMUSER QUOTA UNLIMITED ON USERS
GRANT BECOME USER TO DDMUSER
GRANT CREATE SESSION TO DDMUSER
GRANT ALTER SESSION TO DDMUSER
GRANT SELECT ANY TABLE TO DDMUSER
GRANT SELECT ANY DICTIONARY TO DDMUSER ACTIVE
GRANT DBA TO DDMUSER
```

Note: The database commands create a database user with the user name DDMUSER and password DDMUSER. You can change the values of the user name and password.

Compile the Database Objects

Use the SQL scripts in the Siebel folder to compile the database objects.

You can find the SQL script files in the following directory:
`<Dynamic Data Masking installation>\Accelerators\Siebel\sql\Oracle`

1. Connect to the database with the Dynamic Data Masking database user you created to use the Siebel accelerator.
2. Compile the Siebel matchers spec package with the following script:

   `DDM_SIEBEL_MATCHERS_spec.sql`
3. Compile the Siebel matchers body package with the following script:

   `DDM_SIEBEL_MATCHERS_body.sql`
4. Grant execute privileges to all users with the following database command:

   ```
   GRANT EXECUTE ON DDM_SIEBEL_MATCHERS TO PUBLIC
   ```
5. Create a public synonym for the Siebel matchers package with the following database command:

   ```
   CREATE PUBLIC SYNONYM DDM_SIEBEL_MATCHERS FOR DDM_SIEBEL_MATCHERS
   ```

Create a Database Connection

Create a Dynamic Data Masking database connection for Oracle in the Management Console.

1. Log in to the Dynamic Data Masking Management Console.
2. Highlight the Dynamic Data Masking Server in the Management Console tree and select **Tree** > **Add DDM Services**.

   The **Add DDM Services** window appears.
3. Check **DDM for Oracle** and click **OK.**

   The **DDM for Oracle** node appears in the Management Console tree.
4. Highlight a domain node or the Management Console tree root node and select **Tree** > **Add Database**.

   The **Add Database** window appears.
5. Select the Oracle database type.
6. Configure the Oracle database connection parameters.

   The following table describes the database connection parameters:

Parameter	Description
Database Name	Logical name defined for the target database.
Instance Name	Instance name for the target database.
Listener Address	Server host name or TCP/IP address for the target database.
Listener Port	TCP/IP listener port for the target database.
Listener Service Name	Service name for the target database.
DBA Username	The user name of the user you created to use the Siebel accelerator.
DBA Password	Password for the user you created to use the Siebel accelerator.

7. Click **Test Connection** and verify that Dynamic Data Masking is connected to the database.
8. Click **OK**.

   The database node appears in the Management Console.

Import Connection Rules

Import the Siebel accelerator connection rules into the Management Console.

1. Highlight the DDM for Oracle node in the Management Console tree and select **Tree** > **Connection Rules**.

   The Rule Editor opens.
2. In the Rule Editor, highlight the DDM for Oracle node in the tree and select **Action** > **Import**.

   The **Import** window opens.
3. Navigate to the following directory:

```
<Dynamic Data Masking installation>\Accelerators\Siebel\rules\Oracle
```

4. Select the SiebelConnectionRules.xml file and click **Import**.

   The SiebelAppConnRule and SiebelDevConnRule connection rules appear in the Rule Editor.
5. Select **File** > **Update Rules** to save the connection rules.
6. Select **File** > **Exit** to close the Rule Editor.

Note: If you modify the Siebel connection rules, you must log out of the Siebel application and log in again.

Import Application Security Rules

Import the Siebel accelerator application security rules into the Management Console.

1. Highlight the Management Console tree root node in the Management Console tree and select **Tree** > **Security Rule Set**.

   The **Add Rule Set** window opens.
2. Enter SiebelAppRuleSet as the rule set name and click **OK**.

   The SiebelAppRuleSet rule appears in the Management Console tree.
3. Highlight the SiebelAppRuleSet rule set and select **Tree** > **Security Rule Set**.

   The Rule Editor opens.
4. In the Rule Editor, select **Action** > **Import**.

   The **Import** window opens.
5. Navigate to the following directory:

   ```
   <Dynamic Data Masking installation>\Accelerators\Siebel\rules\Oracle
   ```
6. Select the SiebelAppRuleSet.xml file and click **Import**.

   The MatchSiebelTables rule folder appears in the Rule Editor.
7. Expand the MatchSiebelTables rule folder to view the UserHandling and PositionHandling rules.
8. Define BlackList and WhiteList rules in the Rule Editor. Highlight a rule and select **Action** > **Edit** to open the **Edit Rule** window.
9. Select **File** > **Update Rules** to save the security rules.
10. Select **File** > **Exit** to close the Rule Editor.

Import Development Security Rules

Import the Siebel accelerator development security rules into the Management Console.

1. Highlight the Dynamic Data Masking Server node in the Management Console tree and select **Tree** > **Add Rule Set**.

   The **Add Rule Set** window opens.
2. Enter SiebelDevRuleSet as the rule set name and click **OK**.

   The SiebelDevRuleSet rule set appears in the Management Console tree.

3. Highlight the SiebelDevRuleSet rule set and select **Tree** > **Security Rule Set**.

   The Rule Editor opens.

4. In the Rule Editor, select **Action** > **Import**.

   The **Import** window opens.

5. Navigate to the following directory:

   ```
   <Dynamic Data Masking installation>\Accelerators\Siebel\rules\Oracle
   ```

6. Select the SiebelDevRuleSet.xml file and click **Import**.

   The SiebelDevRuleSet rule appears in the Rule Editor.

7. Highlight the SiebelDevRuleSet rule set and select **Action** > **Edit** to open the **Edit Rule** window and edit the rule.

8. Create security rules for Siebel development tools. Select **Action** > **Insert Rule** to create new rules.

9. Select **File** > **Update Rules** to save the security rules.

10. Select **File** > **Exit** to close the Rule Editor.

CHAPTER 3

Siebel Accelerator Rules

This chapter includes the following topics:

- Siebel Accelerator Rules Overview, 13
- Siebel Accelerator Connection Rules, 13
- SiebelDevRuleSet Security Rule Set, 14
- SiebelAppRuleSet Security Rule Set, 15

Siebel Accelerator Rules Overview

The Siebel accelerator contains an Oracle connection rule set and multiple security rule sets. The rule sets contain predefined rules that are common masking techniques.

The connection rule set contains rules that direct the SQL statement to the security rule sets. The security rule sets determine how the data is masked. You can modify the rules to alter the masking techniques.

The following table describes the Siebel accelerator rule sets:

Rule Set	Description
Connection Rule Set	An Oracle connection rule set that directs SQL requests to the SiebelDevRuleSet and SiebelAppRuleSet security rule sets.
SiebelDevRuleSet	A security rule set that masks rules that do not come from a Siebel client. You use the SiebelDevRuleSet for SQL requests from the development team.
SiebelAppRuleSet	A security rule set that masks rules that come from a Siebel client. The SiebelAppRuleSet masks requests sent from non-development team users.

Siebel Accelerator Connection Rules

The Siebel accelerator connection rules direct SQL requests to security rule sets.

The SiebelDevConnRule connection rule matches SQL requests that do not come from a Siebel client. It directs requests to the SiebelDevRuleSet security rule set. You can use the SiebelDevConnRule to direct requests from development tools such as Toad and SQL Developer.

The SiebelAppConnRule connection rule matches SQL requests that come from a Siebel client. It directs requests to the SiebelAppRuleSet security rule set. You can use SiebelAppConnRule to direct requests that come from non-development tools.

The following table describes the Siebel accelerator connection rules:

Rule	Description
SiebelDevConnRule	Directs requests that do not come from a Siebel client to the SiebelDevRuleSet security rule set.
SiebelAppConnRule	Directs requests that come from a Siebel client to the SiebelAppRuleSet security rule set.

Note: Changes that you make to the Siebel connection rules take effect the next time you log in.

SiebelDevConnRule Connection Rule

The SiebelDevConnRule connection rule directs all database requests that do not come from a Siebel client to the SiebelDevRuleSet security rule set. You can use the SiebelDevConnRule rule to direct requests that come from the development team.

The SiebelDevConnRule connection rule uses the Client/Application Information matcher to identify incoming requests. The matcher contains items on the exclude list that identify Siebel thick and thin clients. The connection rule is applied to any request that comes from a tool that is not on the exclude list. The rule action specifies that Dynamic Data Masking uses the SiebelDevRuleSet security rule set for the request.

For example, if the development team accesses the database through SQL Developer, the SiebelDevConnRule connection rule directs the request to the SiebelDevRuleSet security rule set.

SiebelAppConnRule Connection Rule

The SiebelAppConnRule connection rule directs all database requests from a Siebel client to the SiebelAppRuleSet security rule set. You can use the SiebelAppConnRule rule for non-development purposes.

The SiebelAppConnRule connection rule uses the Client/Application Information matcher to identify incoming requests. The matcher contains items on the include list that identify Siebel thick and thin clients. The connection rule is applied to any request that comes from a tool that is on the include list. The rule action specifies that Dynamic Data Masking uses the SiebelAppRuleSet security rule set for the request.

For example, if a user accesses the database through Siebel Web Client, the SiebelAppConnRule connection rule directs the request to the SiebelAppRuleSet security rule set.

SiebelDevRuleSet Security Rule Set

The SiebelDevRuleSet security rule set receives requests from the SiebelDevConnRule connection rule directs SQL if the request does not come from a Siebel client.

The SiebelDevRuleSet security rule set contains the TestSiebelDevRuleSet security rule. The TestSiebelDevRuleSet rule does not mask data. You can modify the TestSiebelDevRuleSet security rule and add rules to the rule set to mask data when a request comes from a development tool.

For example, the development team works from 8:00 a.m. to 5:00 p.m. You want to block access to the database from development tools when the development team is not at work. Create a security rule in the

SiebelDevRuleSet security rule set that uses the Time of Day matcher to block requests to the database at all other times of day.

The following table describes the rule in the SiebelDevRuleSet security rule set:

Rule	Description
TestSiebelDevRuleSet	Security rule that you modify to mask data for requests that come from development tools.

SiebelAppRuleSet Security Rule Set

The SiebelAppRuleSet security rule receives requests from the SiebelAppConnRule connection rule if the request comes from a Siebel client. You can mask data based on the user or the position of the user that sends the SQL request.

The following table describes the rule folders in the SiebelAppRuleSet security rule set:

Rule Folder	Description
BlackList	A rule folder that contains a BlockUpdates folder and a MaskingRule rule. Use the Symbol matcher in the BlackList folder to define groups of users and positions of users that receive masked data.
MatchSiebelTables	A rule folder that contains the UserHandling and PositionHandling folders.
PositionHandling	A rule folder that contains BlackList and WhiteList folders. The rules in the PositionHandling folder mask data based on the position of the user that sends the SQL request.
UserHandling	A rule folder that contains BlackList and WhiteList folders. The rules in the UserHandling folder mask data based on the user that sends the SQL request.
WhiteList	A rule folder that contains a StopIfWhiteList rule, a BlockUpdates folder, and a MaskingRule rule.

The following table describes the rules in the SiebelAppRuleSet:

Rule	Description
BlockUpdates	A rule folder that contains rules that prevent updates of masked data.
MaskingRule	A masking rule. Define masking functions in the MaskingRule rule.
StopIfWhiteList	A rule that defines the users or positions of users that receive unmasked data.

MatchSiebelTables Rule Folder

The MatchSiebelTables folder is a security rule folder in the SiebelAppConnRule security rule set that contains all the accelerator rules and folders.

The MatchSiebelTables folder uses the Text matching method to identify tables that contain personally identifiable information. The matcher contains a list of common tables that contain personally identifiable information. You can add and remove tables from the list.

The MatchSiebelTables folder uses the Continue rule processing action. If the SQL request matches the rule, the request continues to the folders inside the MatchSiebelTables folder.

UserHandling and PositionHandling Rule Folders

The UserHandling and PositionHandling folders are security rule folders in the MatchSiebelTables folder that contain masking rules.

The UserHandling folder contains rules that mask data based on the user that sends the SQL request. The PositionHandling folder contains rules that mask data based on the position of the user that sends the SQL request.

If you want to mask data based on the user that accesses the database, enable the UserHandling folder and disable the PositionHandling folder. If you want to mask data based on the position of the user that accesses the database, enable the PositionHandling folder and disable the UserHandling folder.

The UserHandling and PositionHandling folders do not contain a rule matcher or rule action. They are containers for groups of rules.

Note: Disable the UserHandling or PositionHandling folder based on how you want to mask data. If you enable the UserHandling folder and the PositionHandling folder, the SQL request will go to the first folder in the tree.

BlackList Rule Folder

The BlackList rule folder is a security rule folder in the UserHandling and PositionHandling folders that defines the users and positions of users that receive masked data.

You can define the list of BlackList users and user positions in the BlackList folder. Define BlackList users in the UserHandling folder and BlackList user positions in the PositionHandling folder.

If you want to mask data based on the users or user positions in the BlackList, enable the BlackList folder and disable the WhiteList folder.

The BlackList folder contains a BlockUpdates folder. The BlockUpdates folder contains rules that prevent updates of masked data.

The BlackList folder contains a masking rule that masks columns that contain personally identifiable information. You can modify the masking rule in the Rule Editor.

For example, you have 100 users. You want to mask data when 20 of the users access the database. Enable the UserHandling folder and disable the PositionHandling folder. In the UserHandling folder, enable the BlackList folder and disable the WhiteList folder. List the 20 users in the BlackList folder. Dynamic Data Masking will mask data when a request is sent from the users in the BlackList folder.

WhiteList Rule Folder

The WhiteList rule folder is a security rule folder in the UserHandling and PositionHandling folders that defines the users and positions of users that receive unmasked data.

You can define the list of WhiteList users and user positions in the StopIfWhiteList rule within the WhiteList folder. Define WhiteList users in the UserHandling folder and WhiteList user positions in the PositionHandling folder.

If you want to mask data based on the users or user positions in the WhiteList folder, enable the WhiteList folder and disable the BlackList folder.

The WhiteList folder contains a BlockUpdates folder. The BlockUpdates folder contains rules that prevent updates of masked data.

The WhiteList folder contains a masking rule that masks columns that contain personally identifiable information. You can modify the masking rule in the Rule Editor.

INDEX

A

accelerator
  setup 8
application security rule
  import 11

C

connection rule
  import 10
  siebelappconnrule 14
  siebeldevconnrule 14

D

development security rule
  import 11

F

folder
  blacklist 16
  blockupdates 16
  matchsiebeltables 15
  positionhandling 16
folder *(continued)*
  userhandling 16
  whitelist 16

R

rule
  blacklist 16
  blockupdates 16
  matchsiebeltables 15
  positionhandling 16
  userhandling 16
  whitelist 16
rule set
  connection rules 13
  siebelappruleset 15
  siebeldevruleset 14

S

security rule
  import 11
security rule set
  siebelappruleset 15
  siebeldevruleset 14
security rules
  import 11