

# **Oracle® Database Vault**

Administrator's Guide

12c Release 2 (12.2)

**E49709-15**

May 2017

Oracle Database Vault Administrator's Guide, 12c Release 2 (12.2)

E49709-15

Copyright © 2006, 2017, Oracle and/or its affiliates. All rights reserved.

Primary Author: Patricia Huey

Contributors: Taousif Ansari , Tom Best, Sanjay Bharadwaj , Todd Bottger, Ji-won Byun, Ben Chang, Martin Cheng, Chi Ching Chui, Scott Gaetjen, Viksit Gaur, Rishabh Gupta, Lijie Heng, Dominique Jeunot, Peter Knaggs, Suman Kumar, Chon Lee, Rudregowda Mallegowda, Paul Needham, Yi Ouyang, Hozefa Palitanawala, Robert Pang, Gayathri Sairamkrishnan, Vipin Samar, James Spiller, Srividya Tata, Kamal Tbeileh, Saravana Soundararajan, Sudheesh Varma, Peter Wahl, Alan Williams

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

---

---

# Contents

Preface .....	xxvii
Audience .....	xxvii
Documentation Accessibility .....	xxvii
Related Documents.....	xxvii
Conventions.....	xxviii
Changes in This Release for Oracle Database Vault Administrator's Guide .....	xxix
Changes in Oracle Database Vault 12c Release 2 (12.2.0.1) .....	xxix
New Features .....	xxix
Deprecated Features.....	xxxvii
<b>1 Introduction to Oracle Database Vault</b>	
1.1 What Is Oracle Database Vault? .....	1-1
1.1.1 About Oracle Database Vault .....	1-2
1.1.2 Controls for Privileged Accounts.....	1-2
1.1.3 Controls for Database Configuration .....	1-3
1.1.4 Enterprise Applications Protection Policies .....	1-3
1.1.5 Run-time Privilege Analysis for Users and Applications .....	1-3
1.2 What Privileges Do You Need to Use Oracle Database Vault? .....	1-3
1.3 Components of Oracle Database Vault.....	1-4
1.3.1 Oracle Database Vault Access Control Components .....	1-4
1.3.2 Oracle Enterprise Manager Cloud Control Database Vault Administrator Pages .....	1-5
1.3.3 Oracle Database Vault DVSYS and DVF Schemas .....	1-6
1.3.4 Oracle Database Vault PL/SQL Interfaces and Packages .....	1-6
1.3.5 Oracle Database Vault Reporting and Monitoring Tools.....	1-6
1.4 How Oracle Database Vault Addresses Compliance Regulations .....	1-7
1.5 How Oracle Database Vault Protects Privileged User Accounts.....	1-8
1.6 How Oracle Database Vault Allows for Flexible Security Policies .....	1-8
1.7 How Oracle Database Vault Addresses Database Consolidation Concerns.....	1-9
1.8 How Oracle Database Vault Works in a Multitenant Environment .....	1-10

<b>2</b>	<b>What to Expect After You Enable Oracle Database Vault</b>	
2.1	Initialization and Password Parameter Settings That Change.....	2-1
2.2	How Oracle Database Vault Restricts User Authorizations.....	2-3
2.3	New Database Roles to Enforce Separation of Duties.....	2-3
2.4	Privileges That Are Revoked from Existing Users and Roles .....	2-3
2.5	Privileges That Are Prevented for Existing Users and Roles .....	2-5
2.6	Modified AUDIT Statement Settings for a Non-Unified Audit Environment .....	2-5
<b>3</b>	<b>Getting Started with Oracle Database Vault</b>	
3.1	Manually Installing Oracle Database Vault in a Multitenant Environment .....	3-1
3.2	Registering Oracle Database Vault with an Oracle Database .....	3-2
3.2.1	About Registering Oracle Database Vault with an Oracle Database.....	3-2
3.2.2	Registering Database Vault in a Non-Multitenant Environment.....	3-3
3.2.3	Registering Database Vault with Common Users to Manage the CDB Root.....	3-5
3.2.4	Registering Database Vault Common Users to Manage Specific PDBs .....	3-7
3.2.5	Plugging in a Database That Has Database Vault Enabled .....	3-9
3.2.6	Verifying That Database Vault Is Configured and Enabled .....	3-9
3.3	Logging into Oracle Database Vault.....	3-10
3.4	Quick Start Tutorial: Securing a Schema from DBA Access.....	3-11
3.4.1	About This Tutorial.....	3-12
3.4.2	Step 1: Log On as SYSTEM to Access the HR Schema .....	3-12
3.4.3	Step 2: Create a Realm .....	3-13
3.4.4	Step 3: Create the SEBASTIAN User Account .....	3-14
3.4.5	Step 4: Have User SEBASTIAN Test the Realm.....	3-15
3.4.6	Step 5: Create an Authorization for the Realm .....	3-15
3.4.7	Step 6: Test the Realm .....	3-16
3.4.8	Step 7: If Unified Auditing Is Not Enabled, Then Run a Report .....	3-16
3.4.9	Step 8: Remove the Components for This Tutorial .....	3-17
<b>4</b>	<b>Performing Privilege Analysis to Find Privilege Use</b>	
4.1	What Is Privilege Analysis?.....	4-1
4.1.1	About Privilege Analysis .....	4-2
4.1.2	How Privilege Analysis Works with Pre-Compiled Database Objects.....	4-2
4.1.3	Who Can Perform Privilege Analysis?.....	4-3
4.1.4	Types of Privilege Analysis.....	4-3
4.1.5	Benefits and Use Cases of Privilege Analysis .....	4-3
4.1.6	How Does a Multitenant Environment Affect Privilege Analysis? .....	4-4
4.2	Creating and Managing Privilege Analysis Policies .....	4-5
4.2.1	About Creating and Managing Privilege Analysis Policies.....	4-5
4.2.2	General Steps for Managing Privilege Analysis .....	4-6
4.2.3	Creating a Privilege Analysis Policy .....	4-6
4.2.4	Examples of Privilege Analysis Policies .....	4-11

4.2.5	Enabling a Privilege Analysis Policy .....	4-12
4.2.6	Disabling a Privilege Analysis Policy .....	4-14
4.2.7	Generating a Privilege Analysis Report.....	4-15
4.2.8	Dropping a Privilege Analysis Policy .....	4-18
4.3	Creating Roles and Managing Privileges Using Cloud Control.....	4-19
4.3.1	Creating a Role from a Privilege Analysis Report in Cloud Control.....	4-19
4.3.2	Revoking and Regranting Roles and Privileges Using Cloud Control .....	4-20
4.3.3	Generating a Revoke or Regrant Script Using Cloud Control.....	4-20
4.4	Tutorial: Using Capture Runs to Analyze ANY Privilege Use .....	4-23
4.4.1	Step 1: Create User Accounts.....	4-23
4.4.2	Step 2: Create and Enable a Privilege Analysis Policy.....	4-24
4.4.3	Step 3: Use the READ ANY TABLE System Privilege .....	4-25
4.4.4	Step 4: Disable the Privilege Analysis Policy .....	4-25
4.4.5	Step 5: Generate and View a Privilege Analysis Report.....	4-25
4.4.6	Step 6: Create a Second Capture Run .....	4-26
4.4.7	Step 7: Remove the Components for This Tutorial .....	4-27
4.5	Tutorial: Analyzing Privilege Use by a User Who Has the DBA Role.....	4-28
4.5.1	Step 1: Create User Accounts.....	4-28
4.5.2	Step 2: Create and Enable a Privilege Analysis Policy.....	4-29
4.5.3	Step 3: Perform the Database Tuning Operations .....	4-30
4.5.4	Step 4: Disable the Privilege Analysis Policy .....	4-30
4.5.5	Step 5: Generate and View Privilege Analysis Reports .....	4-31
4.5.6	Step 6: Remove the Components for This Tutorial .....	4-32
4.6	Privilege Analysis Policy and Report Data Dictionary Views .....	4-33

## 5 Configuring Realms

5.1	What Are Realms? .....	5-2
5.1.1	About Realms.....	5-2
5.1.2	Mandatory Realms to Restrict User Access to Objects within a Realm.....	5-3
5.1.3	Realms in a Multitenant Environment .....	5-5
5.1.4	Object Types That Realms Can Protect .....	5-5
5.2	Default Realms .....	5-5
5.2.1	Oracle Database Vault Realm .....	5-6
5.2.2	Database Vault Account Management Realm .....	5-7
5.2.3	Oracle Enterprise Manager Realm.....	5-7
5.2.4	Oracle Default Schema Protection Realm .....	5-7
5.2.5	Oracle System Privilege and Role Management Realm .....	5-8
5.2.6	Oracle Default Component Protection Realm.....	5-8
5.3	Creating a Realm.....	5-8
5.4	About Realm-Secured Objects .....	5-12
5.5	About Realm Authorization.....	5-13
5.6	Realm Authorizations in a Multitenant Environment .....	5-13
5.7	Modifying the Enablement Status of a Realm .....	5-14

5.8	Deleting a Realm .....	5-15
5.9	How Realms Work .....	5-15
5.10	How Authorizations Work in a Realm .....	5-17
5.10.1	About Authorizations in a Realm .....	5-17
5.10.2	Examples of Realm Authorizations .....	5-17
5.11	Access to Objects That Are Protected by a Realm.....	5-19
5.12	Example of How Realms Work .....	5-19
5.13	How Realms Affect Other Oracle Database Vault Components .....	5-20
5.14	Guidelines for Designing Realms.....	5-20
5.15	How Realms Affect Performance .....	5-21
5.16	Realm Related Reports and Data Dictionary Views.....	5-22

## 6 Configuring Rule Sets

6.1	What Are Rule Sets? .....	6-2
6.2	Rule Sets and Rules in a Multitenant Environment.....	6-2
6.3	Default Rule Sets.....	6-3
6.4	Creating a Rule Set .....	6-5
6.5	Creating a Rule to Add to a Rule Set .....	6-8
6.5.1	About Creating Rules .....	6-8
6.5.2	Default Rules.....	6-9
6.5.3	Creating a New Rule.....	6-12
6.5.4	Adding Existing Rules to a Rule Set.....	6-14
6.5.5	Removing a Rule from a Rule Set .....	6-14
6.6	Removing Rule Set References to Oracle Database Vault Components.....	6-15
6.7	Deleting a Rule Set.....	6-15
6.8	How Rule Sets Work .....	6-16
6.8.1	How Oracle Database Vault Evaluates Rules .....	6-16
6.8.2	Nested Rules within a Rule Set .....	6-16
6.8.3	Creating Rules to Apply to Everyone Except One User.....	6-17
6.9	Tutorial: Creating an Email Alert for Security Violations .....	6-17
6.9.1	About This Tutorial.....	6-17
6.9.2	Step 1: Install and Configure the UTL_MAIL PL/SQL Package.....	6-18
6.9.3	Step 2: Create an Email Security Alert PL/SQL Procedure .....	6-19
6.9.4	Step 3: Configure an Access Control List File for Network Services.....	6-20
6.9.5	Step 4: Create a Rule Set and a Command Rule to Use the Email Security Alert.....	6-21
6.9.6	Step 5: Test the Email Security Alert .....	6-22
6.9.7	Step 6: Remove the Components for This Tutorial .....	6-23
6.10	Tutorial: Configuring Two-Person Integrity, or Dual Key Security .....	6-24
6.10.1	About This Tutorial.....	6-25
6.10.2	Step 1: Create Users for This Tutorial.....	6-25
6.10.3	Step 2: Create a Function to Check if User patch_boss Is Logged In.....	6-26
6.10.4	Step 3: Create Rules, a Rule Set, and a Command Rule to Control User Access .....	6-27
6.10.5	Step 4: Test the Users' Access .....	6-28

6.10.6	Step 5: Remove the Components for This Tutorial .....	6-29
6.11	Guidelines for Designing Rule Sets.....	6-30
6.12	How Rule Sets Affect Performance.....	6-30
6.13	Rule Set and Rule Related Reports and Data Dictionary Views.....	6-31
<b>7</b>	<b>Configuring Command Rules</b>	
7.1	What Are Command Rules?.....	7-2
7.1.1	About Command Rules.....	7-2
7.1.2	Command Rules in a Multitenant Environment .....	7-3
7.1.3	Types of Command Rules .....	7-4
7.2	Default Command Rules .....	7-7
7.3	SQL Statements That Can Be Protected by Command Rules.....	7-8
7.4	Creating a Command Rule.....	7-9
7.5	Modifying the Enablement Status of a Command Rule .....	7-11
7.6	Deleting a Command Rule .....	7-11
7.7	How Command Rules Work.....	7-11
7.8	Tutorial: Using a Command Rule to Control Table Creations by a User.....	7-12
7.8.1	Step 1: Create a Table.....	7-12
7.8.2	Step 2: Create a Command Rule.....	7-13
7.8.3	Step 3: Test the Command Rule .....	7-14
7.8.4	Step 4: Remove the Components for this Tutorial.....	7-14
7.9	Guidelines for Designing Command Rules .....	7-15
7.10	How Command Rules Affect Performance .....	7-16
7.11	Command Rule Related Reports and Data Dictionary View.....	7-16
<b>8</b>	<b>Configuring Factors</b>	
8.1	What Are Factors?.....	8-1
8.2	Default Factors .....	8-2
8.3	Creating a Factor .....	8-5
8.3.1	Accessing the Create Factors Page.....	8-5
8.3.2	Completing the General Page for Factor Creation .....	8-6
8.3.3	Configurations Page for Factor Creation .....	8-7
8.3.4	Options Page of Factor Creation .....	8-12
8.4	Adding an Identity to a Factor.....	8-14
8.4.1	About Factor Identities .....	8-14
8.4.2	About Trust Levels .....	8-15
8.4.3	About Label Identities .....	8-15
8.4.4	Creating and Configuring a Factor Identity .....	8-16
8.4.5	Deleting a Factor Identity.....	8-17
8.4.6	Using Identity Mapping to Configure an Identity to Use Other Factors.....	8-17
8.5	Deleting a Factor .....	8-19
8.6	How Factors Work.....	8-20
8.6.1	How Factors Are Processed When a Session Is Established.....	8-20

8.6.2	How Factors Are Retrieved.....	8-21
8.6.3	How Factors Are Set .....	8-22
8.7	Tutorial: Preventing Ad Hoc Tool Access to the Database.....	8-23
8.7.1	About This Tutorial.....	8-23
8.7.2	Step 1: Enable the HR and OE User Accounts .....	8-24
8.7.3	Step 2: Create the Factor .....	8-24
8.7.4	Step 3: Create the Rule Set and Rules .....	8-25
8.7.5	Step 4: Create the CONNECT Command Rule.....	8-26
8.7.6	Step 5: Test the Ad Hoc Tool Access Restriction .....	8-27
8.7.7	Step 6: Remove the Components for This Tutorial .....	8-28
8.8	Tutorial: Restricting User Activities Based on Session Data .....	8-28
8.8.1	About This Tutorial.....	8-29
8.8.2	Step 1: Create an Administrative User .....	8-29
8.8.3	Step 2: Add Identities to the Domain Factor .....	8-30
8.8.4	Step 3: Map the Domain Factor Identities to the Client_IP Factor.....	8-31
8.8.5	Step 4: Create a Rule Set to Set the Hours and Select the Factor Identity .....	8-33
8.8.6	Step 5: Create a Command Rule That Uses the Rule Set .....	8-34
8.8.7	Step 6: Test the Factor Identity Settings .....	8-34
8.8.8	Step 7: Remove the Components for This Tutorial .....	8-35
8.9	Guidelines for Designing Factors .....	8-36
8.10	How Factors Affect Performance .....	8-37
8.11	Factor Related Reports and Data Dictionary Views .....	8-37

## 9 Configuring Secure Application Roles for Oracle Database Vault

9.1	What Are Secure Application Roles in Oracle Database Vault?.....	9-1
9.2	Creating an Oracle Database Vault Secure Application Role .....	9-2
9.3	Modifications to a Secure Application Role.....	9-3
9.4	Security for Oracle Database Vault Secure Application Roles.....	9-4
9.5	Deleting an Oracle Database Vault Secure Application Role.....	9-4
9.6	How Oracle Database Vault Secure Application Roles Work.....	9-4
9.7	Tutorial: Granting Access with Database Vault Secure Application Roles.....	9-5
9.7.1	About This Tutorial.....	9-5
9.7.2	Step 1: Create Users for This Tutorial.....	9-6
9.7.3	Step 2: Enable the OE User Account.....	9-6
9.7.4	Step 3: Create the Rule Set and Its Rules.....	9-6
9.7.5	Step 4: Create the Database Vault Secure Application Role .....	9-7
9.7.6	Step 5: Grant the SELECT Privilege to the Secure Application Role .....	9-8
9.7.7	Step 6: Test the Database Vault Secure Application Role.....	9-8
9.7.8	Step 7: Remove the Components for This Tutorial .....	9-9
9.8	How Secure Application Roles Affect Performance.....	9-10
9.9	Secure Application Role Related Reports and Data Dictionary View .....	9-10



<b>10</b>	<b>Configuring Oracle Database Vault Policies</b>	
10.1	What Are Database Vault Policies?.....	10-1
10.1.1	About Oracle Database Vault Policies.....	10-1
10.1.2	Oracle Database Vault Policies in a Multitenant Environment.....	10-3
10.2	Default Oracle Database Vault Policies.....	10-3
10.3	Creating an Oracle Database Policy.....	10-4
10.4	Modifying an Oracle Database Vault Policy.....	10-6
10.5	Deleting an Oracle Database Vault Policy.....	10-6
10.6	Related Data Dictionary Views.....	10-6
<b>11</b>	<b>Using Simulation Mode for Logging Realm and Command Rule Activities</b>	
11.1	About Simulation Mode.....	11-1
11.2	Simulation Mode Use Cases.....	11-2
11.3	Tutorial: Tracking Violations to a Realm Using Simulation Mode.....	11-3
11.3.1	About This Tutorial.....	11-4
11.3.2	Step 1: Create Users for This Tutorial.....	11-4
11.3.3	Step 2: Create a Realm and an Oracle Database Vault Policy.....	11-5
11.3.4	Step 3: Test the Realm and Policy.....	11-6
11.3.5	Step 4: Query the DBA_DV_SIMULATION_LOG View for Violations.....	11-7
11.3.6	Step 5: Enable and Re-test the Realm.....	11-7
11.3.7	Step 6: Remove the Components for This Tutorial.....	11-8
<b>12</b>	<b>Integrating Oracle Database Vault with Other Oracle Products</b>	
12.1	Integrating Oracle Database Vault with Enterprise User Security.....	12-1
12.1.1	About Integrating Oracle Database Vault with Enterprise User Security.....	12-2
12.1.2	Configuring an Enterprise User Authorization.....	12-2
12.2	Configuring Oracle Database Vault Accounts as Enterprise User Accounts.....	12-2
12.3	Integration of Oracle Database Vault with Transparent Data Encryption.....	12-4
12.4	Attaching Factors to an Oracle Virtual Private Database.....	12-5
12.5	Integrating Oracle Database Vault with Oracle Label Security.....	12-5
12.5.1	How Oracle Database Vault Is Integrated with Oracle Label Security.....	12-6
12.5.2	Requirements for Using Oracle Database Vault with Oracle Label Security.....	12-7
12.5.3	Using Oracle Database Vault Factors with Oracle Label Security Policies.....	12-7
12.5.4	Tutorial: Integrating Oracle Database Vault with Oracle Label Security.....	12-10
12.5.5	Related Reports and Data Dictionary Views.....	12-14
12.6	Integrating Oracle Database Vault with Oracle Data Guard.....	12-15
12.6.1	Step 1: Configure the Primary Database.....	12-15
12.6.2	Step 2: Configure the Standby Database.....	12-16
12.7	Registering Oracle Internet Directory Using Oracle Database Configuration Asssitant.....	12-17
<b>13</b>	<b>DBA Operations in an Oracle Database Vault Environment</b>	
13.1	Using Oracle Database Vault with Oracle Enterprise Manager.....	13-2

13.1.1	Propagating Oracle Database Vault Configurations to Other Databases .....	13-2
13.1.2	Enterprise Manager Cloud Control Alerts for Oracle Database Vault Policies .....	13-4
13.1.3	Oracle Database Vault-Specific Reports in Enterprise Manager Cloud Control .....	13-4
13.1.4	Changing the DBSNMP Account Password in a Database Vault Environment.....	13-5
13.2	Using Oracle Data Pump with Oracle Database Vault .....	13-5
13.2.1	About Using Oracle Data Pump with Oracle Database Vault.....	13-6
13.2.2	Authorizing Users for Data Pump Regular Export and Import Operations.....	13-6
13.2.3	Authorizing Users for Data Pump Transportable Export and Import Operations ..	13-9
13.2.4	Guidelines for Exporting or Importing Data in a Database Vault Environment...	13-13
13.3	Using Oracle Scheduler with Oracle Database Vault.....	13-14
13.3.1	About Using Oracle Scheduler with Oracle Database Vault .....	13-14
13.3.2	Granting a Job Scheduling Administrator Authorization for Database Vault.....	13-15
13.3.3	Revoking Authorization from Job Scheduling Administrators.....	13-16
13.4	Using Information Lifecycle Management with Oracle Database Vault.....	13-16
13.4.1	About Using Information Lifecycle Management with Oracle Database Vault ....	13-17
13.4.2	Authorizing Users for ILM Operations in Database Vault .....	13-17
13.4.3	Revoking Information Lifecycle Management Authorization from Users .....	13-18
13.5	Oracle Recovery Manager and Oracle Database Vault .....	13-18
13.6	Privileges for Using Oracle Streams with Oracle Database Vault.....	13-19
13.7	Privileges for Using XStream with Oracle Database Vault .....	13-19
13.8	Privileges for Using Oracle GoldenGate in with Oracle Database Vault .....	13-20
13.9	Using Data Masking in an Oracle Database Vault Environment .....	13-21
13.9.1	About Data Masking in an Oracle Database Vault Enabled Database.....	13-21
13.9.2	Adding Data Masking Users to the Data Dictionary Realm Authorizations .....	13-21
13.9.3	Giving Users Access to Tables or Schemas That They Want to Mask.....	13-22
13.9.4	Creating a Command Rule to Control Data Masking Privileges .....	13-22
13.10	Plugging a Database Vault-Enabled PDB to a CDB .....	13-23
13.11	Using the ORADEBUG Utility with Oracle Database Vault.....	13-26

## 14 Oracle Database Vault Schemas, Roles, and Accounts

14.1	Oracle Database Vault Schemas .....	14-1
14.1.1	DVSYSC Schema .....	14-1
14.1.2	DVF Schema .....	14-2
14.2	Oracle Database Vault Roles .....	14-3
14.2.1	About Oracle Database Vault Roles .....	14-4
14.2.2	Privileges of Oracle Database Vault Roles.....	14-6
14.2.3	Granting Oracle Database Vault Roles to Users .....	14-8
14.2.4	DV_OWNER Database Vault Owner Role .....	14-9
14.2.5	DV_ADMIN Database Vault Configuration Administrator Role.....	14-11
14.2.6	DV_MONITOR Database Vault Monitoring Role.....	14-12
14.2.7	DV_SECANALYST Database Vault Security Analyst Role .....	14-13
14.2.8	DV_AUDIT_CLEANUP Audit Trail Cleanup Role .....	14-13
14.2.9	DV_DATAPUMP_NETWORK_LINK Data Pump Network Link Role .....	14-14

14.2.10	DV_STREAMS_ADMIN Oracle Streams Configuration Role.....	14-15
14.2.11	DV_XSTREAM_ADMIN XStream Administrative Role.....	14-16
14.2.12	DV_GOLDENGATE_ADMIN GoldenGate Administrative Role .....	14-17
14.2.13	DV_GOLDENGATE_REDO_ACCESS GoldenGate Redo Log Role .....	14-18
14.2.14	DV_PATCH_ADMIN Database Vault Database Patch Role.....	14-18
14.2.15	DV_ACCTMGR Database Vault Account Manager Role.....	14-19
14.2.16	DV_REALM_OWNER Database Vault Realm DBA Role.....	14-21
14.2.17	DV_REALM_RESOURCE Database Vault Application Resource Owner Role...	14-21
14.2.18	DV_POLICY_OWNER Database Vault Owner Role .....	14-22
14.2.19	DV_PUBLIC Database Vault PUBLIC Role.....	14-23
14.3	Oracle Database Vault Accounts Created During Registration.....	14-23
14.4	Backup Oracle Database Vault Accounts.....	14-25

## 15 Oracle Database Vault Realm APIs

15.1	ADD_AUTH_TO_REALM Procedure.....	15-2
15.2	ADD_OBJECT_TO_REALM Procedure.....	15-4
15.3	CREATE_REALM Procedure.....	15-5
15.4	DELETE_AUTH_FROM_REALM Procedure .....	15-8
15.5	DELETE_OBJECT_FROM_REALM Procedure.....	15-9
15.6	DELETE_REALM Procedure .....	15-9
15.7	DELETE_REALM_CASCADE Procedure.....	15-10
15.8	RENAME_REALM Procedure.....	15-11
15.9	UPDATE_REALM Procedure.....	15-11
15.10	UPDATE_REALM_AUTH Procedure.....	15-13

## 16 Oracle Database Vault Rule Set APIs

16.1	DBMS_MACADM Rule Set Procedures.....	16-1
16.1.1	ADD_RULE_TO_RULE_SET Procedure .....	16-2
16.1.2	CREATE_RULE Procedure .....	16-3
16.1.3	CREATE_RULE_SET Procedure.....	16-5
16.1.4	DELETE_RULE Procedure.....	16-8
16.1.5	DELETE_RULE_FROM_RULE_SET Procedure .....	16-8
16.1.6	DELETE_RULE_SET Procedure.....	16-9
16.1.7	RENAME_RULE Procedure .....	16-9
16.1.8	RENAME_RULE_SET Procedure .....	16-10
16.1.9	UPDATE_RULE Procedure .....	16-11
16.1.10	UPDATE_RULE_SET Procedure .....	16-12
16.2	Oracle Database Vault PL/SQL Rule Set Functions.....	16-14
16.2.1	DV_SYSEVENT Function.....	16-15
16.2.2	DV_LOGIN_USER Function.....	16-15
16.2.3	DV_INSTANCE_NUM Function.....	16-15
16.2.4	DV_DATABASE_NAME Function.....	16-16
16.2.5	DV_DICT_OBJ_TYPE Function.....	16-16

16.2.6	DV_DICT_OBJ_OWNER Function .....	16-17
16.2.7	DV_DICT_OBJ_NAME Function .....	16-17
16.2.8	DV_SQL_TEXT Function .....	16-18

## 17 Oracle Database Vault Command Rule APIs

17.1	CREATE_COMMAND_RULE Procedure .....	17-2
17.2	CREATE_CONNECT_COMMAND_RULE Procedure .....	17-9
17.3	CREATE_SESSION_EVENT_CMD_RULE Procedure .....	17-11
17.4	CREATE_SYSTEM_EVENT_CMD_RULE Procedure .....	17-12
17.5	DELETE_COMMAND_RULE Procedure .....	17-14
17.6	DELETE_CONNECT_COMMAND_RULE Procedure .....	17-16
17.7	DELETE_SESSION_EVENT_CMD_RULE Procedure .....	17-17
17.8	DELETE_SYSTEM_EVENT_CMD_RULE Procedure .....	17-17
17.9	UPDATE_COMMAND_RULE Procedure .....	17-18
17.10	UPDATE_CONNECT_COMMAND_RULE Procedure .....	17-21
17.11	UPDATE_SESSION_EVENT_CMD_RULE Procedure .....	17-22
17.12	UPDATE_SYSTEM_EVENT_CMD_RULE Procedure .....	17-24

## 18 Oracle Database Vault Factor APIs

18.1	DBMS_MACADM Factor Procedures and Functions .....	18-1
18.1.1	ADD_FACTOR_LINK Procedure .....	18-3
18.1.2	ADD_POLICY_FACTOR Procedure .....	18-4
18.1.3	CHANGE_IDENTITY_FACTOR Procedure .....	18-4
18.1.4	CHANGE_IDENTITY_VALUE Procedure .....	18-5
18.1.5	CREATE_DOMAIN_IDENTITY Procedure .....	18-6
18.1.6	CREATE_FACTOR Procedure .....	18-7
18.1.7	CREATE_FACTOR_TYPE Procedure .....	18-9
18.1.8	CREATE_IDENTITY_MAP Procedure .....	18-10
18.1.9	CREATE_IDENTITY Procedure .....	18-11
18.1.10	DELETE_FACTOR Procedure .....	18-12
18.1.11	DELETE_FACTOR_LINK Procedure .....	18-13
18.1.12	DELETE_IDENTITY Procedure .....	18-13
18.1.13	DELETE_FACTOR_TYPE Procedure .....	18-14
18.1.14	DELETE_IDENTITY_MAP Procedure .....	18-14
18.1.15	DROP_DOMAIN_IDENTITY Procedure .....	18-15
18.1.16	GET_SESSION_INFO Function .....	18-16
18.1.17	GET_INSTANCE_INFO Function .....	18-17
18.1.18	RENAME_FACTOR Procedure .....	18-17
18.1.19	RENAME_FACTOR_TYPE Procedure .....	18-18
18.1.20	UPDATE_FACTOR Procedure .....	18-18
18.1.21	UPDATE_FACTOR_TYPE Procedure .....	18-21
18.1.22	UPDATE_IDENTITY Procedure .....	18-21
18.2	Oracle Database Vault Run-Time PL/SQL Procedures and Functions .....	18-22

18.2.1	About Oracle Database Vault Run-Time PL/SQL Procedures and Functions .....	18-23
18.2.2	SET_FACTOR Procedure .....	18-23
18.2.3	GET_FACTOR Function.....	18-24
18.2.4	GET_FACTOR_LABEL Function.....	18-24
18.2.5	GET_TRUST_LEVEL Function.....	18-25
18.2.6	GET_TRUST_LEVEL_FOR_IDENTITY Function.....	18-26
18.2.7	ROLE_IS_ENABLED Function.....	18-27
18.3	Oracle Database Vault DVF PL/SQL Factor Functions .....	18-27
18.3.1	About Oracle Database Vault DVF PL/SQL Factor Functions .....	18-29
18.3.2	F\$AUTHENTICATION_METHOD Function.....	18-29
18.3.3	F\$CLIENT_IP Function .....	18-30
18.3.4	F\$DATABASE_DOMAIN Function .....	18-31
18.3.5	F\$DATABASE_HOSTNAME Function .....	18-31
18.3.6	F\$DATABASE_INSTANCE Function .....	18-31
18.3.7	F\$DATABASE_IP Function .....	18-32
18.3.8	F\$DATABASE_NAME Function .....	18-32
18.3.9	F\$DOMAIN Function .....	18-33
18.3.10	F\$ENTERPRISE_IDENTITY Function.....	18-33
18.3.11	F\$IDENTIFICATION_TYPE Function .....	18-34
18.3.12	F\$LANG Function .....	18-34
18.3.13	F\$LANGUAGE Function .....	18-35
18.3.14	F\$MACHINE Function.....	18-35
18.3.15	F\$NETWORK_PROTOCOL Function.....	18-36
18.3.16	F\$PROXY_ENTERPRISE_IDENTITY Function.....	18-36
18.3.17	F\$SESSION_USER Function.....	18-37

## 19 Oracle Database Vault Secure Application Role APIs

19.1	DBMS_MACADM Secure Application Role Procedures.....	19-1
19.1.1	ASSIGN_ROLE Procedure .....	19-2
19.1.2	CREATE_ROLE Procedure .....	19-2
19.1.3	DELETE_ROLE Procedure.....	19-3
19.1.4	RENAME_ROLE Procedure .....	19-4
19.1.5	UPDATE_ROLE Procedure .....	19-4
19.1.6	UNASSIGN_ROLE Procedure.....	19-5
19.2	DBMS_MACSEC_ROLES Secure Application Role Procedure and Function.....	19-6
19.2.1	CAN_SET_ROLE Function .....	19-6
19.2.2	SET_ROLE Procedure .....	19-7

## 20 Oracle Database Vault Oracle Label Security APIs

20.1	CREATE_MAC_POLICY Procedure.....	20-1
20.2	CREATE_POLICY_LABEL Procedure .....	20-3
20.3	DELETE_MAC_POLICY_CASCADE Procedure.....	20-4
20.4	DELETE_POLICY_FACTOR Procedure .....	20-5

20.5	DELETE_POLICY_LABEL Procedure .....	20-5
20.6	UPDATE_MAC_POLICY Procedure .....	20-6

## 21 Oracle Database Vault Utility APIs

21.1	DBMS_MACUTL Constants .....	21-1
21.1.1	DBMS_MACUTL Listing of Constants .....	21-1
21.1.2	Example: Creating a Realm Using DBMS_MACUTL Constants .....	21-6
21.1.3	Example: Creating a Rule Set Using DBMS_MACUTL Constants .....	21-6
21.1.4	Example: Creating a Factor Using DBMS_MACUTL Constants.....	21-7
21.2	DBMS_MACUTL Package Procedures and Functions .....	21-7
21.2.1	CHECK_DVSYSDML_ALLOWED Procedure .....	21-8
21.2.2	GET_CODE_VALUE Function.....	21-9
21.2.3	GET_SECOND Function .....	21-10
21.2.4	GET_MINUTE Function.....	21-11
21.2.5	GET_HOUR Function.....	21-11
21.2.6	GET_DAY Function .....	21-12
21.2.7	GET_MONTH Function .....	21-13
21.2.8	GET_YEAR Function .....	21-13
21.2.9	IS_ALPHA Function .....	21-14
21.2.10	IS_DIGIT Function .....	21-15
21.2.11	IS_DVSYSDOWNER Function .....	21-15
21.2.12	IS_OLS_INSTALLED Function .....	21-16
21.2.13	IS_OLS_INSTALLED_VARCHAR Function.....	21-16
21.2.14	USER_HAS_OBJECT_PRIVILEGE Function.....	21-17
21.2.15	USER_HAS_ROLE Function.....	21-18
21.2.16	USER_HAS_ROLE_VARCHAR Function.....	21-19
21.2.17	USER_HAS_SYSTEM_PRIVILEGE Function.....	21-20

## 22 Oracle Database Vault General Administrative APIs

22.1	DBMS_MACADM General System Maintenance Procedures.....	22-1
22.1.1	ADD-NLS_DATA Procedure.....	22-3
22.1.2	AUTHORIZE_DATAPUMP_USER Procedure.....	22-3
22.1.3	AUTHORIZE_DDL Procedure.....	22-4
22.1.4	AUTHORIZE_MAINTENANCE_USER Procedure.....	22-5
22.1.5	AUTHORIZE_PROXY_USER Procedure.....	22-6
22.1.6	AUTHORIZE_SCHEDULER_USER Procedure.....	22-7
22.1.7	AUTHORIZE_TTS_USER Procedure .....	22-7
22.1.8	UNAUTHORIZE_DATAPUMP_USER Procedure .....	22-8
22.1.9	UNAUTHORIZE_DDL Procedure .....	22-9
22.1.10	UNAUTHORIZE_MAINTENANCE_USER Procedure .....	22-10
22.1.11	UNAUTHORIZE_PROXY_USER Procedure .....	22-11
22.1.12	UNAUTHORIZE_SCHEDULER_USER Procedure .....	22-12
22.1.13	UNAUTHORIZE_TTS_USER Procedure.....	22-13

22.1.14	DISABLE_DV Procedure.....	22-13
22.1.15	DISABLE_DV_DICTIONARY_ACCTS Procedure .....	22-14
22.1.16	DISABLE_DV_PATCH_ADMIN_AUDIT Procedure.....	22-14
22.1.17	DISABLE_ORADEBUG Procedure.....	22-15
22.1.18	ENABLE_DV Procedure .....	22-15
22.1.19	ENABLE_DV_PATCH_ADMIN_AUDIT Procedure.....	22-16
22.1.20	ENABLE_DV_DICTIONARY_ACCTS Procedure .....	22-17
22.1.21	ENABLE_ORADEBUG Procedure .....	22-17
22.2	CONFIGURE_DV General System Maintenance Procedure .....	22-18

## 23 Oracle Database Vault Policy APIs

23.1	ADD_CMD_RULE_TO_POLICY Procedure.....	23-2
23.2	ADD_OWNER_TO_POLICY Procedure.....	23-4
23.3	ADD_REALM_TO_POLICY Procedure.....	23-4
23.4	CREATE_POLICY Procedure .....	23-5
23.5	DELETE_CMD_RULE_FROM_POLICY Procedure.....	23-6
23.6	DELETE_OWNER_FROM_POLICY Procedure .....	23-8
23.7	DELETE_REALM_FROM_POLICY Procedure.....	23-9
23.8	DROP_POLICY Procedure.....	23-10
23.9	RENAME_POLICY Procedure .....	23-10
23.10	UPDATE_POLICY_DESCRIPTION Procedure .....	23-11
23.11	UPDATE_POLICY_STATE Procedure.....	23-11

## 24 Oracle Database Vault API Reference

24.1	DBMS_MACADM PL/SQL Package Contents.....	24-1
24.2	DBMS_MACSEC_ROLES PL/SQL Package Contents.....	24-8
24.3	DBMS_MACUTL PL/SQL Package Contents.....	24-8
24.4	CONFIGURE_DV PL/SQL Procedure .....	24-9
24.5	DVF PL/SQL Interface Contents.....	24-9

## 25 Oracle Database Vault Data Dictionary Views

25.1	About the Oracle Database Vault Data Dictionary Views.....	25-5
25.2	CDB_DV_STATUS View .....	25-5
25.3	DBA_DV_CODE View.....	25-6
25.4	DBA_DV_COMMAND_RULE View.....	25-8
25.5	DBA_DV_DATAPUMP_AUTH View.....	25-10
25.6	DBA_DV_DDL_AUTH View.....	25-10
25.7	DBA_DV_DICTIONARY_ACCTS View .....	25-11
25.8	DBA_DV_FACTOR View .....	25-11
25.9	DBA_DV_FACTOR_TYPE View .....	25-13
25.10	DBA_DV_FACTOR_LINK View.....	25-14
25.11	DBA_DV_IDENTITY View .....	25-15
25.12	DBA_DV_IDENTITY_MAP View.....	25-15

25.13	DBA_DV_JOB_AUTH View .....	25-16
25.14	DBA_DV_MAC_POLICY View .....	25-17
25.15	DBA_DV_MAC_POLICY_FACTOR View .....	25-17
25.16	DBA_DV_MAINTENANCE_AUTH View .....	25-18
25.17	DBA_DV_ORADEBUG View .....	25-18
25.18	DBA_DV_PATCH_ADMIN_AUDIT View .....	25-19
25.19	DBA_DV_POLICY View.....	25-19
25.20	DBA_DV_POLICY_LABEL View .....	25-20
25.21	DBA_DV_POLICY_OBJECT View .....	25-21
25.22	DBA_DV_POLICY_OWNER View .....	25-22
25.23	DBA_DV_PROXY_AUTH View .....	25-23
25.24	DBA_DV_PUB_PRIVS View .....	25-23
25.25	DBA_DV_REALM View .....	25-24
25.26	DBA_DV_REALM_AUTH View .....	25-25
25.27	DBA_DV_REALM_OBJECT View .....	25-27
25.28	DBA_DV_ROLE View.....	25-28
25.29	DBA_DV_RULE View .....	25-29
25.30	DBA_DV_RULE_SET View.....	25-30
25.31	DBA_DV_RULE_SET_RULE View .....	25-32
25.32	DBA_DV_STATUS View .....	25-33
25.33	DBA_DV_SIMULATION_LOG View.....	25-34
25.34	DBA_DV_TTS_AUTH View .....	25-36
25.35	DBA_DV_USER_PRIVS View.....	25-36
25.36	DBA_DV_USER_PRIVS_ALL View.....	25-37
25.37	DVSYSDV\$CONFIGURATION_AUDIT View .....	25-38
25.38	DVSYSDV\$ENFORCEMENT_AUDIT View .....	25-43
25.39	DVSYSDV\$REALM View .....	25-46
25.40	DVSYSDV.POLICY_OWNER_COMMAND_RULE View .....	25-48
25.41	DVSYSDV.POLICY_OWNER_POLICY View .....	25-49
25.42	DVSYSDV.POLICY_OWNER_REALM View .....	25-49
25.43	DVSYSDV.POLICY_OWNER_REALM_AUTH View .....	25-51
25.44	DVSYSDV.POLICY_OWNER_REALM_OBJECT View.....	25-52
25.45	DVSYSDV.POLICY_OWNER_RULE View .....	25-53
25.46	DVSYSDV.POLICY_OWNER_RULE_SET View .....	25-54
25.47	DVSYSDV.POLICY_OWNER_RULE_SET_RULE View .....	25-56
25.48	SYS.DV\$CONFIGURATION_AUDIT View .....	25-56
25.49	SYS.DV\$ENFORCEMENT_AUDIT View .....	25-57

## 26 Monitoring Oracle Database Vault

26.1	About Monitoring Oracle Database Vault .....	26-1
26.2	Monitoring Security Violations and Configuration Changes .....	26-1



## 27 Oracle Database Vault Reports

27.1	About the Oracle Database Vault Reports .....	27-1
27.2	Who Can Run the Oracle Database Vault Reports?.....	27-2
27.3	Running the Oracle Database Vault Reports .....	27-2
27.4	Oracle Database Vault Configuration Issues Reports .....	27-3
27.4.1	Command Rule Configuration Issues Report .....	27-3
27.4.2	Rule Set Configuration Issues Report.....	27-3
27.4.3	Realm Authorization Configuration Issues Report.....	27-4
27.4.4	Factor Configuration Issues Report .....	27-4
27.4.5	Factor Without Identities Report .....	27-4
27.4.6	Identity Configuration Issues Report .....	27-4
27.4.7	Secure Application Configuration Issues Report .....	27-5
27.5	Oracle Database Vault Auditing Reports.....	27-5
27.5.1	Realm Audit Report .....	27-5
27.5.2	Command Rule Audit Report .....	27-6
27.5.3	Factor Audit Report .....	27-6
27.5.4	Label Security Integration Audit Report.....	27-6
27.5.5	Core Database Vault Audit Trail Report.....	27-6
27.5.6	Secure Application Role Audit Report.....	27-6
27.6	Oracle Database Vault General Security Reports.....	27-7
27.6.1	Object Privilege Reports .....	27-7
27.6.2	Database Account System Privileges Reports.....	27-9
27.6.3	Sensitive Objects Reports .....	27-10
27.6.4	Privilege Management - Summary Reports .....	27-12
27.6.5	Powerful Database Accounts and Roles Reports.....	27-13
27.6.6	Initialization Parameters and Profiles Reports .....	27-16
27.6.7	Database Account Password Reports.....	27-17
27.6.8	Security Audit Report: Core Database Audit Report.....	27-17
27.6.9	Other Security Vulnerability Reports.....	27-17

## A Auditing Oracle Database Vault

A.1	About Auditing in Oracle Database Vault.....	A-1
A.2	Protection of the Unified Audit Trail in an Oracle Database Vault Environment .....	A-2
A.3	Oracle Database Vault Specific Audit Events.....	A-3
A.3.1	Oracle Database Vault Policy Audit Events .....	A-3
A.3.2	Oracle Database Vault Audit Trail Record Format .....	A-3
A.4	Archiving and Purging the Oracle Database Vault Audit Trail .....	A-6
A.4.1	About Archiving and Purging the Oracle Database Vault Audit Trail.....	A-6
A.4.2	Archiving the Oracle Database Vault Audit Trail.....	A-6
A.4.3	Purging the Oracle Database Vault Audit Trail.....	A-8
A.5	Oracle Database Audit Settings Created for Oracle Database Vault .....	A-9

<b>B</b>	<b>Disabling and Enabling Oracle Database Vault</b>	
B.1	When You Must Disable Oracle Database Vault .....	B-1
B.2	Step 1: Disable Oracle Database Vault .....	B-2
B.3	Step 2: Perform the Required Tasks.....	B-2
B.4	Step 3: Enable Oracle Database Vault .....	B-3
<b>C</b>	<b>Postinstallation Oracle Database Vault Procedures</b>	
C.1	Configuring Oracle Database Vault on Oracle RAC Nodes.....	C-1
C.2	Adding Languages to Oracle Database Vault .....	C-2
C.3	Deinstalling Oracle Database Vault .....	C-2
C.4	Reinstalling Oracle Database Vault.....	C-4
<b>D</b>	<b>Oracle Database Vault Security Guidelines</b>	
D.1	Separation of Duty Guidelines .....	D-1
D.1.1	How Oracle Database Vault Handles Separation of Duty .....	D-2
D.1.2	Separation of Tasks in an Oracle Database Vault Environment .....	D-2
D.1.3	Separation of Duty Matrix for Oracle Database Vault.....	D-3
D.1.4	Identification and Documentation of the Tasks of Database Users.....	D-4
D.2	Managing Oracle Database Administrative Accounts.....	D-5
D.2.1	SYSTEM User Account for General Administrative Uses.....	D-6
D.2.2	SYSTEM Schema for Application Tables .....	D-6
D.2.3	Limitation of the SYSDBA Administrative Privilege.....	D-6
D.2.4	Root and Operating System Access to Oracle Database Vault.....	D-6
D.3	Accounts and Roles Trusted by Oracle Database Vault .....	D-7
D.4	Accounts and Roles That Should be Limited to Trusted Individuals.....	D-8
D.4.1	Management of Users with Root Access to the Operating System.....	D-8
D.4.2	Management of the Oracle Software Owner .....	D-8
D.4.3	Management of SYSDBA Access .....	D-9
D.4.4	Management of SYSOPER Access .....	D-9
D.5	Guidelines for Using Oracle Database Vault in a Production Environment .....	D-9
D.6	Secure Configuration Guidelines .....	D-10
D.6.1	General Secure Configuration Guidelines.....	D-10
D.6.2	UTL_FILE and DBMS_FILE_TRANSFER Package Security Considerations.....	D-11
D.6.3	CREATE ANY JOB Privilege Security Considerations.....	D-14
D.6.4	CREATE EXTERNAL JOB Privilege Security Considerations .....	D-14
D.6.5	LogMiner Package Security Considerations .....	D-14
D.6.6	ALTER SYSTEM and ALTER SESSION Privilege Security Considerations.....	D-14
<b>E</b>	<b>Troubleshooting Oracle Database Vault</b>	
E.1	Using Trace Files to Diagnose Oracle Database Vault Events.....	E-1
E.1.1	About Using Trace Files to Diagnose Oracle Database Vault Events .....	E-2
E.1.2	Types of Oracle Database Vault Trace Events That You Can and Cannot Track.....	E-2

E.1.3	Levels of Oracle Database Vault Trace Events .....	E-3
E.1.4	Performance Effect of Enabling Oracle Database Vault Trace Files .....	E-3
E.1.5	Enabling Oracle Database Vault Trace Events .....	E-3
E.1.6	Finding Oracle Database Vault Trace File Data .....	E-5
E.1.7	Example: Low Level Oracle Database Vault Realm Violations in a Trace File.....	E-7
E.1.8	Example: High Level Trace Enabled for Oracle Database Vault Authorization .....	E-8
E.1.9	Example: Highest Level Traces on Violations on Realm-Protected Objects .....	E-9
E.1.10	Disabling Oracle Database Vault Trace Events .....	E-10
E.2	General Diagnostic Tips .....	E-11
E.3	Configuration Problems with Oracle Database Vault Components.....	E-12
E.4	Resetting Oracle Database Vault Account Passwords.....	E-12
E.4.1	Resetting the DV_OWNER User Password .....	E-12
E.4.2	Resetting the DV_ACCTMGR User Password .....	E-13

## Index



## List of Figures

1-1	Oracle Database Vault Realm Blocking DBA Access to Data.....	1-2
1-2	Oracle Database Vault Security.....	1-10
1-3	Oracle Database Vault in a Multitenant Environment with Regular Mode.....	1-11
5-1	How Authorizations Work for Realms and Realm Owners.....	5-20
12-1	Encrypted Data and Oracle Database Vault.....	12-5
14-1	How Oracle Database Vault Roles Are Categorized.....	14-5



## List of Tables

1-1	Regulations That Address Potential Security Threats.....	1-7
2-1	Modified Database Initialization Parameter Settings.....	2-2
2-2	Privileges Oracle Database Vault Revokes.....	2-4
4-1	Data Dictionary Views That Display Privilege Analysis Information.....	4-33
5-1	Reports Related to Realms.....	5-22
5-2	Data Dictionary Views Used for Realms.....	5-23
6-1	Current Default Oracle Database Vault Rules.....	6-9
6-2	Reports Related to Rule Sets.....	6-31
6-3	Data Dictionary Views Used for Rules and Rule Sets.....	6-31
7-1	Default Command Rules.....	7-7
7-2	Reports Related to Command Rules.....	7-16
8-1	Reports Related to Factors and Their Identities.....	8-37
8-2	Data Dictionary Views Used for Factors and Factor Identities.....	8-38
9-1	Reports Related to Secure Application Roles.....	9-10
10-1	Data Dictionary Views Used for Oracle Database Vault Policies.....	10-6
12-1	Reports Related to Database Vault and Oracle Label Security Integration.....	12-14
12-2	Data Dictionary Views Used for Oracle Label Security.....	12-15
13-1	Levels of Authorization for Oracle Data Pump Regular Operations.....	13-7
13-2	Levels of Authorization for Oracle Data Pump Transportable Operations.....	13-10
14-1	Privileges of Oracle Database Vault Roles.....	14-6
14-2	Database Accounts Used by Oracle Database Vault.....	14-24
14-3	Model Oracle Database Vault Database Accounts.....	14-25
15-1	ADD_AUTH_TO_REALM Parameters.....	15-2
15-2	ADD_OBJECT_TO_REALM Parameters.....	15-4
15-3	CREATE_REALM Parameters.....	15-6
15-4	DELETE_AUTH_FROM_REALM Parameters.....	15-8
15-5	DELETE_OBJECT_FROM_REALM Parameters.....	15-9
15-6	DELETE_REALM Parameter.....	15-10
15-7	DELETE_REALM_CASCADE Parameter.....	15-10
15-8	RENAME_REALM Parameters.....	15-11
15-9	UPDATE_REALM Parameters.....	15-12
15-10	UPDATE_REALM_AUTH Parameters.....	15-13
16-1	ADD_RULE_TO_RULE_SET Parameters.....	16-2
16-2	CREATE_RULE Parameters.....	16-4
16-3	CREATE_RULE_SET Parameters.....	16-5
16-4	DELETE_RULE Parameter.....	16-8
16-5	DELETE_RULE_FROM_RULE_SET Parameters.....	16-8
16-6	DELETE_RULE_SET Parameter.....	16-9
16-7	RENAME_RULE Parameters.....	16-10
16-8	RENAME_RULE_SET Parameters.....	16-10
16-9	UPDATE_RULE Parameters.....	16-11
16-10	UPDATE_RULE_SET Parameters.....	16-12
17-1	CREATE_COMMAND_RULE Parameters.....	17-3
17-2	ALTER SYSTEM Command Rule Settings.....	17-4
17-3	ALTER SESSION Command Rule Settings.....	17-6
17-4	CREATE_CONNECT_COMMAND_RULE Parameters.....	17-9
17-5	CREATE_SESSION_EVENT_CMD_RULE Parameters.....	17-11
17-6	CREATE_SYSTEM_EVENT_CMD_RULE Parameters.....	17-13
17-7	DELETE_COMMAND_RULE Parameters.....	17-15
17-8	DELETE_CONNECT_COMMAND_RULE Parameters.....	17-16
17-9	DELETE_SESSION_EVENT_CMD_RULE Parameters.....	17-17

17-10	DELETE_SYSTEM_EVENT_CMD_RULE Parameters.....	17-18
17-11	UPDATE_COMMAND_RULE Parameters.....	17-19
17-12	UPDATE_CONNECT_COMMAND_RULE Parameters.....	17-21
17-13	UPDATE_SESSION_EVENT_CMD_RULE Parameters.....	17-23
17-14	UPDATE_SYSTEM_EVENT_CMD_RULE Parameters.....	17-25
18-1	ADD_FACTOR_LINK Parameters.....	18-3
18-2	ADD_POLICY_FACTOR Parameters.....	18-4
18-3	CHANGE_IDENTITY_FACTOR Parameters.....	18-5
18-4	CHANGE_IDENTITY_VALUE Parameters.....	18-5
18-5	CREATE_DOMAIN_IDENTITY Parameters.....	18-6
18-6	CREATE_FACTOR Parameters.....	18-7
18-7	CREATE_FACTOR_TYPE Parameters.....	18-10
18-8	CREATE_IDENTITY_MAP Parameters.....	18-10
18-9	CREATE_IDENTITY Parameters.....	18-12
18-10	DELETE_FACTOR Parameter.....	18-12
18-11	DELETE_FACTOR_LINK Parameters.....	18-13
18-12	DELETE_IDENTITY Parameters.....	18-13
18-13	DELETE_FACTOR_TYPE Parameters.....	18-14
18-14	DELETE_IDENTITY_MAP Parameters.....	18-15
18-15	DROP_DOMAIN_IDENTITY Parameters.....	18-16
18-16	GET_SESSION_INFO Parameter.....	18-16
18-17	GET_INSTANCE_INFO Parameter.....	18-17
18-18	RENAME_FACTOR Parameters.....	18-17
18-19	RENAME_FACTOR_TYPE Parameters.....	18-18
18-20	UPDATE_FACTOR.....	18-19
18-21	UPDATE_FACTOR_TYPE Parameters.....	18-21
18-22	UPDATE_IDENTITY Parameters.....	18-22
18-23	SET_FACTOR Parameters.....	18-23
18-24	GET_FACTOR Parameter.....	18-24
18-25	GET_FACTOR_LABEL Parameters.....	18-25
18-26	GET_TRUST_LEVEL Parameter.....	18-26
18-27	GET_TRUST_LEVEL_FOR_IDENTITY Parameters.....	18-26
18-28	ROLE_IS_ENABLED Parameter.....	18-27
19-1	ASSIGN_ROLE Parameters.....	19-2
19-2	CREATE_ROLE Parameters.....	19-3
19-3	DELETE_ROLE Parameter.....	19-3
19-4	RENAME_ROLE Parameters.....	19-4
19-5	UPDATE_ROLE Parameters.....	19-5
19-6	UNASSIGN_ROLE Parameters.....	19-5
19-7	CAN_SET_ROLE Parameter.....	19-6
19-8	SET_ROLE Parameter.....	19-7
20-1	CREATE_MAC_POLICY Parameters.....	20-2
20-2	Oracle Label Security Merge Algorithm Codes.....	20-2
20-3	CREATE_POLICY_LABEL Parameters.....	20-4
20-4	DELETE_MAC_POLICY_CASCADE Parameter.....	20-5
20-5	DELETE_POLICY_FACTOR Parameters.....	20-5
20-6	DELETE_POLICY_LABEL Parameters.....	20-6
20-7	UPDATE_MAC_POLICY.....	20-7
21-1	DBMS_MACUTL Listing of Constants.....	21-2
21-2	CHECK_DVSYSDML_ALLOWED Parameter.....	21-9
21-3	GET_CODE_VALUE Parameters.....	21-9
21-4	GET_SECOND Parameter.....	21-10
21-5	GET_MINUTE Parameter.....	21-11
21-6	GET_HOUR Parameter.....	21-12



21-7	GET_DAY Parameter.....	21-12
21-8	GET_MONTH Parameter.....	21-13
21-9	GET_YEAR Parameter.....	21-14
21-10	IS_ALPHA Parameter.....	21-14
21-11	IS_DIGIT Parameter.....	21-15
21-12	IS_DVSYST_OWNER Parameter.....	21-16
21-13	USER_HAS_OBJECT_PRIVILEGE Parameters.....	21-17
21-14	USER_HAS_ROLE Parameters.....	21-19
21-15	USER_HAS_ROLE_VARCHAR Parameters.....	21-20
21-16	USER_HAS_SYSTEM_PRIVILEGE Parameters.....	21-20
22-1	ADD-NLS_DATA.....	22-3
22-2	AUTHORIZE_DATAPUMP_USER.....	22-4
22-3	AUTHORIZE_DDL.....	22-5
22-4	AUTHORIZE_MAINTENANCE_USER.....	22-5
22-5	AUTHORIZE_PROXY_USER.....	22-6
22-6	AUTHORIZE_SCHEDULER_USER.....	22-7
22-7	AUTHORIZE_TTS_USER.....	22-8
22-8	UNAUTHORIZE_DATAPUMP_USER.....	22-9
22-9	UNAUTHORIZE_DDL.....	22-9
22-10	UNAUTHORIZE_MAINTENANCE_USER.....	22-10
22-11	UNAUTHORIZE_PROXY_USER.....	22-11
22-12	UNAUTHORIZE_SCHEDULER_USER.....	22-12
22-13	UNAUTHORIZE_TTS_USER.....	22-13
22-14	ENABLE_DV.....	22-16
22-15	CONFIGURE_DV.....	22-19
23-1	ADD_CMD_RULE_TO_POLICY Parameters.....	23-2
23-2	ADD_OWNER_TO_POLICY Parameters.....	23-4
23-3	ADD_REALM_TO_POLICY Parameters.....	23-5
23-4	CREATE_POLICY Parameters.....	23-6
23-5	DELETE_CMD_RULE_FROM_POLICY Parameters.....	23-7
23-6	DELETE_OWNER_FROM_POLICY Parameters.....	23-9
23-7	DELETE_REALM_FROM_POLICY Parameters.....	23-9
23-8	DROP_POLICY Parameters.....	23-10
23-9	RENAME_POLICY Parameters.....	23-10
23-10	UPDATE_POLICY_DESCRIPTION Parameters.....	23-11
23-11	UPDATE_POLICY_STATE Parameters.....	23-12
24-1	DBMS_MACADM Realm Procedures.....	24-1
24-2	DBMS_MACADM Rule Set and Rule Procedures.....	24-2
24-3	DBMS_MACADM Command Rule Procedures.....	24-3
24-4	DBMS_MACADM Factor Procedures and Functions.....	24-4
24-5	DBMS_MACADM Secure Application Role Procedures.....	24-5
24-6	DBMS_MACADM Oracle Label Security Procedures.....	24-5
24-7	DBMS_MACADM Database Vault Policy Procedures.....	24-6
24-8	DBMS_MACADM General Administrative Procedures.....	24-7
24-9	DBMS_MACSEC_ROLES PL/SQL Package Contents.....	24-8
24-10	DBMS_MACUTL PL/SQL Package Contents.....	24-8
24-11	DVF PL/SQL Interface Contents.....	24-10
25-1	DBA_DV_CODE View CODE_GROUP Values.....	25-7
25-2	DBA_DV_SIMULATION_LOG_VIOLATION_TYPE Code Values.....	25-35
25-3	DVSYSDV\$CONFIGURATION_AUDIT View ACTION Values.....	25-40
25-4	DVSYSDV\$ENFORCEMENT_AUDIT View ACTION Values.....	25-46
A-1	Oracle Database Vault Audit Trail Format.....	A-4
A-2	Audit Policy Settings Oracle Database Vault Adds to Oracle Database.....	A-10
D-1	Example Separation of Duty Matrix.....	D-4

D-2	Example Application Protection Maxtrix.....	D-5
D-3	Trusted Oracle Database Vault Roles and Privileges.....	D-7
E-1	Contents of Oracle Database Vault Trace Files.....	E-2

---

# Preface

*Oracle Database Vault Administrator's Guide* explains how to configure access control-based security in an Oracle Database environment by using Oracle Database Vault.

[Audience](#) (page xxvii)

[Documentation Accessibility](#) (page xxvii)

[Related Documents](#) (page xxvii)

[Conventions](#) (page xxviii)

## Audience

This document is intended for security managers, audit managers, label administrators, and Oracle database administrators (DBAs) who are involved in the configuration of Oracle Database Vault.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

## Related Documents

For more information refer to the following documents:

- *Oracle Database Security Guide*
- *Oracle Label Security Administrator's Guide*
- *Oracle Database Administrator's Guide*
- *Oracle Database SQL Language Reference*

## Oracle Technology Network (OTN)

You can download free release notes, installation documentation, updated versions of this guide, white papers, or other collateral from the Oracle Technology Network (OTN). Visit

<http://www.oracle.com/technetwork/database/security/index.html>

For security-specific information on OTN, visit

<http://www.oracle.com/technetwork/topics/security/whatsnew/index.html>

For the latest version of the Oracle documentation, including this guide, visit

<http://www.oracle.com/technetwork/documentation/index.html>

## Oracle Database Vault-Specific Sites

For OTN information specific to Oracle Database Vault, visit

<http://www.oracle.com/us/products/database/options/database-vault/overview/index.html>

For frequently asked questions about Oracle Database Vault, visit

<http://www.oracle.com/technetwork/database/options/oracle-database-vault-external-faq-2032888.pdf>

## Oracle Store

Printed documentation is available for sale in the Oracle Store at:

<https://shop.oracle.com>

## My Oracle Support (formerly Oracle*MetaLink*)

You can find information about security patches, certifications, and the support knowledge base by visiting My Oracle Support at:

<https://support.oracle.com>

# Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

---

# Changes in This Release for Oracle Database Vault Administrator's Guide

This preface contains:

[Changes in Oracle Database Vault 12c Release 2 \(12.2.0.1\)](#) (page xxix)

## Changes in Oracle Database Vault 12c Release 2 (12.2.0.1)

The following are changes in *Oracle Database Vault Administrator's Guide* for Oracle Database 12c release 2 (12.2.0.1):

[New Features](#) (page xxix)

[Deprecated Features](#) (page xxxvii)

### New Features

The following features are new for this release:

[Ability to Create Oracle Database Vault Policies](#) (page xxx)

An Oracle Database Vault policy groups and manages realms and command rules that have something in common in a single policy.

[Ability to Configure Simulation Mode Protection](#) (page xxxi)

Simulation mode protects Oracle Database Vault security objects so that SQL commands are not blocked, but violations to the security controls are logged.

[Privilege Analysis Enhancements](#) (page xxxiii)

Privilege analysis policies now capture more privilege use than in previous releases, find unused privilege grants, and create named capture runs.

[Ability to Create Common Realms and Common Command Rules for Oracle Multitenant](#) (page xxxiii)

In a multitenant environment, you now can create common realms and common command rules within the application PDB context.

[ALTER SESSION, ALTER SYSTEM, and CONNECT Command Rule Enhancements](#) (page xxxiv)

Command rules now provide more ALTER SESSION and ALTER SYSTEM functionality, and CONNECT command rule enhancements.

[Enhancements for the Authentication\\_Method Default Factor](#) (page xxxv)

Starting with this release, the Authentication\_Method default factor can be used for external and global user authentication.

[Changed Default Value for SQL92\\_SECURITY Parameter](#) (page xxxvi)

Starting with this release, the default value for the SQL92\_SECURITY parameter has changed from FALSE to TRUE.

[Oracle Database Vault Support for Flashback Technology and ILM](#) (page xxxvii)

You now can use Oracle Flashback Technology features and Information Lifecycle Management (ILM) features in an Oracle Database Vault-enabled database.

[Support for Rolling Upgrades for Data Guard Logical Standby Databases](#) (page xxxvii)

Oracle Data Guard logical standby databases can perform rolling upgrades for Oracle Database Vault-enabled systems using transient logical standby and the DBMS\_ROLLING package.

### **Ability to Create Oracle Database Vault Policies**

An Oracle Database Vault policy groups and manages realms and command rules that have something in common in a single policy.

For example, the realms and command rules can have an application or schema in common.

The status of the realms and command rules in this policy can be updated at once, in a single command, instead of performing the update individually on each security object. Also new to this release is the DV\_POLICY\_OWNER role, which provides the grantee user the authority to perform basic administration tasks. This user can add authorized users to the realms that are included in the policy and change the policy state without being granted the powerful DV\_OWNER role.

The following new functionality supports this feature:

- DBMS\_MACADM PL/SQL procedures:
  - DBMS\_MACADM.ADD\_CMD\_RULE\_TO\_POLICY
  - DBMS\_MACADM.ADD\_OWNER\_TO\_POLICY
  - DBMS\_MACADM.ADD\_REALM\_TO\_POLICY
  - DBMS\_MACADM.CREATE\_POLICY
  - DBMS\_MACADM.DELETE\_CMD\_RULE\_FROM\_POLICY
  - DBMS\_MACADM.DELETE\_OWNER\_FROM\_POLICY
  - DBMS\_MACADM.DELETE\_REALM\_FROM\_POLICY
  - DBMS\_MACADM.DROP\_POLICY
  - DBMS\_MACADM.RENAME\_POLICY
  - DBMS\_MACADM.UPDATE\_POLICY\_DESCRIPTION
  - DBMS\_MACADM.UPDATE\_POLICY\_STATE
- Role:

- DV\_POLICY\_OWNER
- Data dictionary views:
  - DVSYS.DBA\_DV\_POLICY
  - DVSYS.DBA\_DV\_POLICY\_OBJECT
  - DVSYS.DBA\_DV\_POLICY\_OWNER
  - DVSYS.POLICY\_OWNER\_COMMAND\_RULE
  - DVSYS.POLICY\_OWNER\_POLICY
  - DVSYS.POLICY\_OWNER\_REALM
  - DVSYS.POLICY\_OWNER\_REALM\_AUTH
  - DVSYS.POLICY\_OWNER\_REALM\_OBJECT
  - DVSYS.POLICY\_OWNER\_RULE
  - DVSYS.POLICY\_OWNER\_RULE\_SET
  - DVSYS.POLICY\_OWNER\_RULE\_SET\_RULE

#### **Related Topics:**

##### [Configuring Oracle Database Vault Policies](#) (page 10-1)

You can use Oracle Database Vault policies to implement frequently used realm and command rule settings.

##### [DV\\_POLICY\\_OWNER Database Vault Owner Role](#) (page 14-22)

The DV\_POLICY\_OWNER role enables database users to manage to a limited degree Oracle Database Vault policies.

##### [Oracle Database Vault Data Dictionary Views](#) (page 25-1)

You can find information about the Oracle Database Vault configuration settings by querying the Database Vault-specific data dictionary views.

#### **Ability to Configure Simulation Mode Protection**

Simulation mode protects Oracle Database Vault security objects so that SQL commands are not blocked, but violations to the security controls are logged.

Simulation mode can also be set for the new Oracle Database Vault policy, which then sets it on embedded objects. This status is between the full protection of being enabled and blocking the access of SQL statements and being disabled. When realms and command rules are set to the simulation mode, violations that occur to these security controls are only logged to the simulation log file. They are not enforced or deny access to the user. This enables you to more quickly certify applications with Oracle Database Vault and to move new realms and command rules to production. You can implement a mandatory realm on a test application database schema and then set it to simulation mode. After running the full test application regression test, you then can analyze the simulation mode log to determine which users and which trusted paths to authorize to the test application schema. You can also develop new command rules and migrate them to production in simulation mode for a period of time to determine the impact they would have when they are enabled.

The simulation mode log is available for viewing in the DBA\_DV\_SIMULATION\_LOG data dictionary view. After you have finished testing the realm and command rule,

you can clear the contents of the DBA\_DV\_SIMULATION\_LOG view for the next time you need to test Database Vault configurations in a test environment.

The following functionality supports this features:

- New or changed DBMS\_MACADM PL/SQL procedures:
  - DBMS\_MACADM.CREATE\_REALM (changed)
  - DBMS\_MACADM.UPDATE\_REALM (changed)
  - DBMS\_MACADM.CREATE\_COMMAND\_RULE (changed)
  - DBMS\_MACADM.UPDATE\_COMMAND\_RULE (changed)
  - DBMS\_MACADM.DELETE\_COMMAND\_RULE (changed)
  - DBMS\_MACADM.CREATE\_CONNECT\_COMMAND\_RULE (new)
  - DBMS\_MACADM.UPDATE\_CONNECT\_COMMAND\_RULE (new)
  - DBMS\_MACADM.DELETE\_CONNECT\_COMMAND\_RULE (new)
  - DBMS\_MACADM.CREATE\_SESSION\_EVENT\_CMD\_RULE (new)
  - DBMS\_MACADM.UPDATE\_SESSION\_EVENT\_CMD\_RULE (new)
  - DBMS\_MACADM.DELETE\_SESSION\_EVENT\_CMD\_RULE (new)
  - DBMS\_MACADM.CREATE\_SYSTEM\_EVENT\_CMD\_RULE (new)
  - DBMS\_MACADM.UPDATE\_SYSTEM\_EVENT\_CMD\_RULE (new)
  - DBMS\_MACADM.DELETE\_SYSTEM\_EVENT\_CMD\_RULE (new)
- New data dictionary view and table:
  - DBA\_DV\_SIMULATION\_LOG data dictionary view
  - DVSYS.SIMULATION\_LOG\$ table

### Related Topics:

[Using Simulation Mode for Logging Realm and Command Rule Activities](#)  
(page 11-1)

Simulation mode writes the activities performed on realms and command rules to a log file, which is accessible through a data dictionary view.

[Oracle Database Vault Realm APIs](#) (page 15-1)

The DBMS\_MACADM PL/SQL package enables you to configure Oracle Database Vault realms.

[Oracle Database Vault Command Rule APIs](#) (page 17-1)

The DBMS\_MACADM PL/SQL package provides procedures for configuring command rules. .

[DBA\\_DV\\_SIMULATION\\_LOG View](#) (page 25-34)

The DBA\_DV\_SIMULATION\_LOG data dictionary view captures simulation log information for realms and command rules that have had simulation mode enabled.



## Privilege Analysis Enhancements

Privilege analysis policies now capture more privilege use than in previous releases, find unused privilege grants, and create named capture runs.

- **Additional privilege captures:** You now can create privilege analysis policies that capture compilation privileges that are used for definer's rights and invoker's rights program units, that capture privileges that were used for Code Based Access Control (CBAC) role use, and that capture secure application role use.
- **Unused privilege grants:** The privilege capture reports now indicate which privilege grants were not used by users or roles.
- **Capture runs:** A capture run defines the period of time that a privilege capture takes place. You define the capture run when you enable the policy. You can create multiple capture runs for use with one policy and then use these capture runs in comparison reports.

### Related Topics:

[Performing Privilege Analysis to Find Privilege Use](#) (page 4-1)

Privilege analysis dynamically analyzes the privileges and roles that users use and do not use.

## Ability to Create Common Realms and Common Command Rules for Oracle Multitenant

In a multitenant environment, you now can create common realms and common command rules within the application PDB context.

The benefit of creating common realms and command rules (that is, in the application root) is that you can manage them from a central location in a multitenant environment, rather than in individual pluggable databases (PDBs). Realms for the application root common objects must be configured in the application PDB or root. Local realms and local command rules can still be implemented on individual PDBs over and above any common realms and common command rules.

Common realms can only be created on common objects in the application root. You cannot create common realms in the CDB root. However, you can create common command rules in either the application root or the CDB root. A common command rule in the application root applies to its associated PDBs. Common command rules that are in the CDB root will apply to all PDBs in the CDB environment. When you create a common object in the application root, you must synchronize it so that it is visible in the individual PDBs, but if you create a common object in the CDB root, it is synchronized automatically. To synchronize an object in the application root, you use the `ALTER PLUGGABLE DATABASE APPLICATION` statement with the `SYNC` clause.

The following functionality supports this feature:

- New or changed `DBMS_MACADM` PL/SQL procedures:
  - All realm-related `DBMS_MACADM` PL/SQL procedures
  - All command rule-related `DBMS_MACADM` PL/SQL procedures
  - `DBMS_MACADM.ADD_CMD_RULE_TO_POLICY` (new)
  - `DBMS_MACADM.DELETE_CMD_RULE_FROM_POLICY` (new)

- New or changed data dictionary views:
  - DBA\_DV\_COMMAND\_RULE
  - DVSYS.DBA\_DV\_POLICY\_OBJECT (new)
  - DBA\_DV\_REALM
  - DVSYS.DV\$REALM
  - DBA\_DV\_REALM\_AUTH
  - DBA\_DV\_REALM\_OBJECT
  - DBA\_DV\_RULE\_SET
  - DBA\_DV\_RULE\_SET\_RULE

### Related Topics:

#### [Realms in a Multitenant Environment](#) (page 5-5)

In a multitenant environment, you can create a realm to protect common objects in the application root.

#### [Command Rules in a Multitenant Environment](#) (page 7-3)

In a multitenant environment, you can create common and local command rules in either the CDB root or the application root.

#### [Oracle Database Vault Realm APIs](#) (page 15-1)

The DBMS\_MACADM PL/SQL package enables you to configure Oracle Database Vault realms.

#### [Oracle Database Vault Command Rule APIs](#) (page 17-1)

The DBMS\_MACADM PL/SQL package provides procedures for configuring command rules. .

#### [Oracle Database Vault Policy APIs](#) (page 23-1)

You can use the DBMS\_MACADM PL/SQL package to manage Oracle Database Vault policies.

#### [Oracle Database Vault Data Dictionary Views](#) (page 25-1)

You can find information about the Oracle Database Vault configuration settings by querying the Database Vault-specific data dictionary views.

## **ALTER SESSION, ALTER SYSTEM, and CONNECT Command Rule Enhancements**

Command rules now provide more ALTER SESSION and ALTER SYSTEM functionality, and CONNECT command rule enhancements.

In previous releases, you could create command rules for the ALTER SESSION and ALTER SYSTEM statements, but the functionality that you could include was limited. Starting with this release, Oracle Database Vault provides the ability to include event settings that are commonly used by ALTER SESSION and ALTER SYSTEM. The options for these special command rules enable you to use many of the features of the ALTER SESSION and ALTER SYSTEM statements, such as the ability to use the SET clause for parameter settings.

In addition, Oracle has made the management of the CONNECT command rule easier to maintain. In previous releases, you could create a CONNECT command rule, but if, for example, you had to create four different command rules for four different users, then you had to create a complex rule with OR and AND keywords to account for the

multiple users in one command rule. With this release, you can create a CONNECT command rule for each user.

The changed and new DBMS\_MACADM PL/SQL procedures to manage the ALTER SESSION, ALTER SYSTEM, and CONNECT command rules are as follows:

- DBMS\_MACADM.CREATE\_COMMAND\_RULE (changed)
- DBMS\_MACADM.UPDATE\_COMMAND\_RULE (changed)
- DBMS\_MACADM.CREATE\_CONNECT\_COMMAND\_RULE (new)
- DBMS\_MACADM.UPDATE\_CONNECT\_COMMAND\_RULE (new)
- DBMS\_MACADM.DELETE\_CONNECT\_COMMAND\_RULE (new)
- DBMS\_MACADM.CREATE\_SESSION\_EVENT\_CMD\_RULE (new)
- DBMS\_MACADM.UPDATE\_SESSION\_EVENT\_CMD\_RULE (new)
- DBMS\_MACADM.DELETE\_SESSION\_EVENT\_CMD\_RULE (new)
- DBMS\_MACADM.CREATE\_SYSTEM\_EVENT\_CMD\_RULE (new)
- DBMS\_MACADM.UPDATE\_SYSTEM\_EVENT\_CMD\_RULE (new)
- DBMS\_MACADM.DELETE\_SYSTEM\_EVENT\_CMD\_RULE (new)

#### **Related Topics:**

##### [ALTER SESSION and ALTER SYSTEM Command Rules](#) (page 7-5)

You can create different kinds of ALTER SESSION and ALTER SYSTEM command rules that provide fine-grained control for these SQL statements.

##### [CONNECT Command Rule](#) (page 7-4)

The DBMS\_MACADM.CREATE\_CONNECT\_CMD\_RULE procedure creates a user-specific CONNECT command rule.

##### [Ability to Configure Simulation Mode Protection](#) (page xxxi)

Simulation mode protects Oracle Database Vault security objects so that SQL commands are not blocked, but violations to the security controls are logged.

##### [Ability to Create Common Realms and Common Command Rules for Oracle Multitenant](#) (page xxxiii)

In a multitenant environment, you now can create common realms and common command rules within the application PDB context.

#### **Enhancements for the Authentication\_Method Default Factor**

Starting with this release, the Authentication\_Method default factor can be used for external and global user authentication.

This enhancement provides for global and external authentication when the Kerberos and Secure Sockets Layer (SSL) strong authentication features are used.

#### **Related Topics:**

##### [Default Factors](#) (page 8-2)

Oracle Database Vault provides a set of default factors.

## Changed Default Value for SQL92\_SECURITY Parameter

Starting with this release, the default value for the SQL92\_SECURITY parameter has changed from FALSE to TRUE.

---

---

**See Also:** *Oracle Database Reference* for more information about the SQL92\_SECURITY parameter

---

---

## Oracle Database Vault Support for Flashback Technology and ILM

You now can use Oracle Flashback Technology features and Information Lifecycle Management (ILM) features in an Oracle Database Vault-enabled database.

The Oracle Flashback Technology enhancement enables you to use Database Vault realms and command rules to control access to database objects while you are using the Oracle Flashback features. You can protect the PURGE TABLE, PURGE INDEX, FLASHBACK TABLE, PURGE TABLESPACE, PURGE RECYCLEBIN, PURGE DBA\_RECYCLEBIN, CREATE FLASHBACK ARCHIVE, ALTER FLASHBACK ARCHIVE, DROP FLASHBACK ARCHIVE SQL statements with Database Vault command rules.

The ILM enhancement enables you to use Database Vault realms and command rules with the Automatic Data Optimization (ADO) features, including granting to users the authorization to enable an ADO administrative user to perform ILM operations on Database Vault-protected objects. This enhancement enables ILM to meet regulatory compliance requirements for data retention and protection, and to store large amounts of data at the lowest cost, using storage tiering. To manage authorizations for users to perform ILM operations, two new procedures are introduced with this release: DBMS\_MACADM.AUTHORIZE\_MAINTENANCE\_USER and DBMS\_MACADM.UNAUTHORIZE\_MAINTENANCE\_USER. To find information about ILM authorization grants, a new data dictionary view, DBA\_DV\_MAINTENANCE\_AUTH, is provided.

---

---

**See Also:**

- [About Realms](#) (page 5-2) for more information about how realms are affected by this enhancement
  - [About Command Rules](#) (page 7-2) for more information about command rules
  - [SQL Statements That Can Be Protected by Command Rules](#) (page 7-8) for a list of the Oracle Flashback Technology SQL statements that can be protected by Database Vault command rules
  - [Using Information Lifecycle Management with Oracle Database Vault](#) (page 13-16) for information about granting users authorization to perform ILM tasks in a Database Vault environment
  - [AUTHORIZE\\_MAINTENANCE\\_USER Procedure](#) (page 22-5) for information about the `DBMS_MACADM.AUTHORIZE_MAINTAINANCE_USER` procedure
  - [UNAUTHORIZE\\_MAINTENANCE\\_USER Procedure](#) (page 22-10) for information about the `DBMS_MACADM.UNAUTHORIZE_MAINTAINANCE_USER` procedure
  - [DBA\\_DV\\_MAINTENANCE\\_AUTH View](#) (page 25-18) for information about the `DBA_DV_MAINTENANCE_USER` data dictionary view
  - *Oracle Database VLDB and Partitioning Guide* for more information about ILM
  - *Oracle Database Backup and Recovery User's Guide* for more information about Oracle Flashback Recovery
- 
- 

### **Support for Rolling Upgrades for Data Guard Logical Standby Databases**

Oracle Data Guard logical standby databases can perform rolling upgrades for Oracle Database Vault-enabled systems using transient logical standby and the `DBMS_ROLLING` package.

See [Integrating Oracle Database Vault with Oracle Data Guard](#) (page 12-15) for more information.

#### **Related Topics:**

[Integrating Oracle Database Vault with Oracle Data Guard](#) (page 12-15)

An Oracle Database Vault-Oracle Data Guard integration requires first, the primary database configuration, then the standby database configuration.

### **Deprecated Features**

The following features have been deprecated for this release.

[Deprecated Rules and Rule Sets](#) (page xxxviii)

Several default rules and rule sets are no longer included in a fresh installation of Oracle Database Vault.

### [Deprecated UTL\\_FILE\\_DIR Parameter](#) (page xxxviii)

The UTL\_FILE\_DIR parameter has been deprecated for this release.

## Deprecated Rules and Rule Sets

Several default rules and rule sets are no longer included in a fresh installation of Oracle Database Vault.

The following rules are no longer included in a fresh installation of an Oracle Database 12c release 2 (12.2) database:

- Is \_system\_trig\_enabled Parameters Allowed
- Is o7\_dictionary\_accessibility Parameters Allowed
- Is \_dynamic\_ols\_init Parameters Allowed
- Is Alter DVSYS Allowed
- Are System Security Parameters Allowed
- Are Dump or Dest Parameters Allowed
- Are Backup Restore Parameters Allowed
- Are Database File Parameters Allowed
- Are Optimizer Parameters Allowed
- Are PL-SQL Parameters Allowed
- Are Security Parameters Allowed

The following default rule sets are not included in fresh installations of Oracle Database 12c release 2 (12.2):

- Allow System Parameters
- Allow Fine Grained Control of System Parameters

These rules and rule sets are replaced by new rules and rule sets that are more secure.

### Related Topics:

#### [Default Rules](#) (page 6-9)

Default rules are rules that have commonly used behavior, such as checking if an action evaluates to true or false.

#### [Default Rule Sets](#) (page 6-3)

Oracle Database Vault provides a set of default rules sets that you can customize for your needs.

## Deprecated UTL\_FILE\_DIR Parameter

The UTL\_FILE\_DIR parameter has been deprecated for this release.

This parameter is still supported for backward compatibility. However, Oracle recommends that you use directory objects instead.

---

---

**See Also:** *Oracle Database Reference* for more information about the UTL\_FILE\_DIR parameter

---

---

---

# Introduction to Oracle Database Vault

Oracle Database Vault enables you to control administrative access to your data.

[What Is Oracle Database Vault?](#) (page 1-1)

Oracle Database Vault provides controls to prevent unauthorized privileged users from accessing sensitive data and to prevent unauthorized database changes.

[What Privileges Do You Need to Use Oracle Database Vault?](#) (page 1-3)

Oracle Database Vault provides database roles that enable different users to perform specific tasks, based on separation-of-duty guidelines.

[Components of Oracle Database Vault](#) (page 1-4)

Oracle Database Vault has a set of components that include PL/SQL packages and other special tools.

[How Oracle Database Vault Addresses Compliance Regulations](#) (page 1-7)

One of the biggest side benefits resulting from regulatory compliance has been security awareness.

[How Oracle Database Vault Protects Privileged User Accounts](#) (page 1-8)

Many security breaches, both external and internal, target privileged users database accounts to steal data from databases.

[How Oracle Database Vault Allows for Flexible Security Policies](#) (page 1-8)

Oracle Database Vault helps you design flexible security policies for your database.

[How Oracle Database Vault Addresses Database Consolidation Concerns](#) (page 1-9)

Consolidation and cloud environments reduce cost but can expose sensitive application data to those without a true need-to-know.

[How Oracle Database Vault Works in a Multitenant Environment](#) (page 1-10)

Oracle Database Vault can be used with Oracle Multitenant to provide increased security for consolidation.

## 1.1 What Is Oracle Database Vault?

Oracle Database Vault provides controls to prevent unauthorized privileged users from accessing sensitive data and to prevent unauthorized database changes.

[About Oracle Database Vault](#) (page 1-2)

The Oracle Database Vault security controls protect application data from unauthorized access, and comply with privacy and regulatory requirements.

[Controls for Privileged Accounts](#) (page 1-2)

Privileged database accounts are one of the most commonly used pathways for gaining access to sensitive applications data in the database.

[Controls for Database Configuration](#) (page 1-3)

Common audit findings are unauthorized changes to database entitlements and grants of the DBA role to too many users.

[Enterprise Applications Protection Policies](#) (page 1-3)

Application-specific Oracle Database Vault protection policies and guidelines are available for major enterprise applications.

[Run-time Privilege Analysis for Users and Applications](#) (page 1-3)

Oracle Database Vault enables you to identify the actual privileges and roles that are used at run-time.

### 1.1.1 About Oracle Database Vault

The Oracle Database Vault security controls protect application data from unauthorized access, and comply with privacy and regulatory requirements.

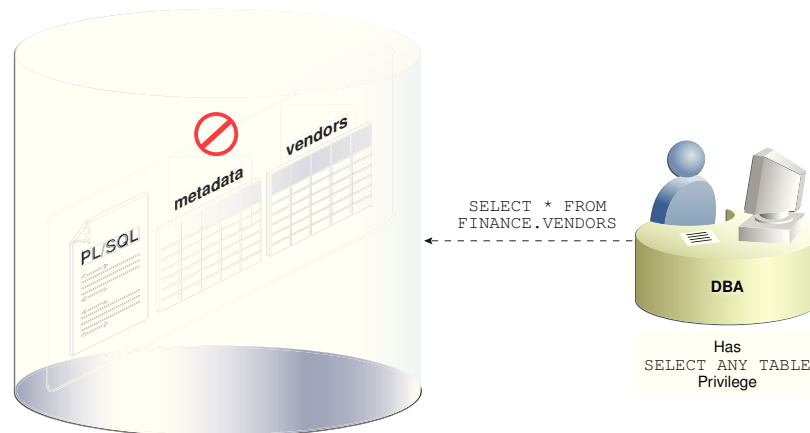
You can deploy controls to block privileged account access to application data and control sensitive operations inside the database using trusted path authorization. Through the analysis of privileges and roles, you can increase the security of existing applications by using least privilege best practices. Oracle Database Vault secures existing database environments transparently, eliminating costly and time consuming application changes.

### 1.1.2 Controls for Privileged Accounts

Privileged database accounts are one of the most commonly used pathways for gaining access to sensitive applications data in the database.

While their broad and unrestricted access facilitates database maintenance, the same access also creates a point of attack for gaining access to large amounts of data. Oracle Database Vault realms around application schemas, sensitive tables, and stored procedures provide controls to prevent privileged accounts from being exploited by intruders and insiders to access sensitive application data.

**Figure 1-1 Oracle Database Vault Realm Blocking DBA Access to Data**





### 1.1.3 Controls for Database Configuration

Common audit findings are unauthorized changes to database entitlements and grants of the DBA role to too many users.

Preventing unauthorized changes to production environments is important not only for security, but also for compliance as such changes can weaken security and open doors to intruders, violating privacy and compliance regulations. Oracle Database Vault SQL command rules enable you to control operations inside the database, including commands such as `CREATE TABLE`, `TRUNCATE TABLE`, and `CREATE USER`. Various out-of-the-box factors such as IP address, authentication method, and program name help implement trusted path authorization to deter attacks leveraging stolen passwords. These controls prevent accidental configuration changes and also prevent hackers and malicious insiders from tampering with applications.

The Oracle Database Vault realms with the mandatory mode enables you to seal off access to application objects, even to those with direct object grants, including the object owner. With mandatory realms, you do not need to analyze who has access because this is clear from the list of authorized users. You can enable mandatory realms at runtime and use them in response to a cyber threat, preventing all access until the threat has been analyzed.

### 1.1.4 Enterprise Applications Protection Policies

Application-specific Oracle Database Vault protection policies and guidelines are available for major enterprise applications.

These enterprise applications include Oracle Fusion Applications, Oracle E-Business Suit, Oracle PeopleSoft, Oracle Siebel, Oracle Financial Services (i-Flex), Oracle Primavera, SAP, and Finacle from Infosys.

### 1.1.5 Run-time Privilege Analysis for Users and Applications

Oracle Database Vault enables you to identify the actual privileges and roles that are used at run-time.

The additional unused roles and privileges can then be audited or revoked by the security administrators to reduce the attack surface and implement least privilege model. Privilege analysis can also be used on administrators to help limit the roles and privileges they are granted to fulfill their responsibilities. You do not need to have Oracle Database Vault enabled to perform privilege analysis.

## 1.2 What Privileges Do You Need to Use Oracle Database Vault?

Oracle Database Vault provides database roles that enable different users to perform specific tasks, based on separation-of-duty guidelines.

The most commonly used roles are as follows:

- `DV_OWNER` and `DV_ADMIN` enable you to create and manage Database Vault policies.
- `DV_ACCTMGR` enables you to manage user accounts.

When you register Oracle Database Vault, the `DV_OWNER` role is granted to a user who must exist before you begin the configuration process, and the `DV_ACCTMGR` role is granted to a second, optional user, who must also exist before configuration. You can grant the Database Vault roles to other users, but ensure that these users are trusted.

During the registration process, you must create backup accounts for the DV\_OWNER and DV\_ACCTMGR users. As a best practice, Oracle strongly recommends that you keep and maintain these backup accounts.

**Related Topics:**[Oracle Database Vault Roles](#) (page 14-3)

Oracle Database Vault provides default roles that are based on specific user tasks and adhere to separation of duty concepts.

[Backup Oracle Database Vault Accounts](#) (page 14-25)

As a best practice, you should maintain backup accounts for the DV\_OWNER and DV\_ACCTMGR roles.

## 1.3 Components of Oracle Database Vault

Oracle Database Vault has a set of components that include PL/SQL packages and other special tools.

[Oracle Database Vault Access Control Components](#) (page 1-4)

Oracle Database Vault enables you to create a set of components to manage security for your database instance.

[Oracle Enterprise Manager Cloud Control Database Vault Administrator Pages](#) (page 1-5)

Oracle Database Vault is pre-installed by default and can be enabled easily.

[Oracle Database Vault DVSYS and DVF Schemas](#) (page 1-6)

Oracle Database Vault database objects and public functions are stored in the DVSYS and DVF schemas, respectively.

[Oracle Database Vault PL/SQL Interfaces and Packages](#) (page 1-6)

Oracle Database Vault provides PL/SQL interfaces and packages for security managers or application developers to configure access control policies.

[Oracle Database Vault Reporting and Monitoring Tools](#) (page 1-6)

You can generate reports on the various activities that Oracle Database Vault monitors.

### 1.3.1 Oracle Database Vault Access Control Components

Oracle Database Vault enables you to create a set of components to manage security for your database instance.

These components are as follows:

- **Realms.** A realm is a protection zone inside the database where database schemas, objects, and roles can be secured. For example, you can secure a set of schemas, objects, and roles that are related to accounting, sales, or human resources. After you have secured these into a realm, you can use the realm to control the use of system and object privileges to specific accounts or roles. This enables you to provide fine-grained access controls for anyone who wants to use these schemas, objects, and roles. [Configuring Realms](#) (page 5-1), discusses realms in detail. See also [Oracle Database Vault Realm APIs](#) (page 15-1).
- **Command rules.** A command rule is a special security policy that you can create to control how users can execute almost any SQL statement, including `SELECT`,

ALTER SYSTEM, database definition language (DDL), and data manipulation language (DML) statements. Command rules must work with rule sets to determine whether the statement is allowed. [Configuring Command Rules](#) (page 7-1), discusses command rules in detail. See also [Oracle Database Vault Command Rule APIs](#) (page 17-1).

- **Factors.** A factor is a named variable or attribute, such as a user location, database IP address, or session user, which Oracle Database Vault can recognize and use as a trusted path. You can use factors in rules to control activities such as authorizing database accounts to connect to the database or the execution of a specific database command to restrict the visibility and manageability of data. Each factor can have one or more identities. An identity is the actual value of a factor. A factor can have several identities depending on the factor retrieval method or its identity mapping logic. [Configuring Factors](#) (page 8-1), discusses factors in detail. See also [Oracle Database Vault Factor APIs](#) (page 18-1).
- **Rule sets.** A rule set is a collection of one or more rules that you can associate with a realm authorization, command rule, factor assignment, or secure application role. The rule set evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (All True or Any True). The rule within a rule set is a PL/SQL expression that evaluates to true or false. You can have the same rule in multiple rule sets. [Configuring Rule Sets](#) (page 6-1), discusses rule sets in detail. See also [Oracle Database Vault Rule Set APIs](#) (page 16-1).
- **Secure application roles.** A secure application role is a special Oracle Database role that can be enabled based on the evaluation of an Oracle Database Vault rule set. [Configuring Secure Application Roles for Oracle Database Vault](#) (page 9-1), discusses secure application roles in detail. See also [Oracle Database Vault Secure Application Role APIs](#) (page 19-1).

To augment these components, Oracle Database Vault provides a set of PL/SQL interfaces and packages. [Oracle Database Vault PL/SQL Interfaces and Packages](#) (page 1-6) provides an overview.

In addition to these components, you can analyze the privilege use of your users. [Performing Privilege Analysis to Find Privilege Use](#) (page 4-1) describes how to use privilege analysis.

In general, the first step you take is to create a realm composed of the database schemas or database objects that you want to secure. You can further secure the realm by creating rules, command rules, factors, identities, rule sets, and secure application roles. In addition, you can run reports on the activities these components monitor and protect. [Getting Started with Oracle Database Vault](#) (page 3-1), provides a simple tutorial that will familiarize you with basic Oracle Database Vault functionality. Later chapters provide more advanced tutorials. [Oracle Database Vault Reports](#) (page 27-1), provides more information about how you can run reports to check the configuration and other activities that Oracle Database Vault performs.

### 1.3.2 Oracle Enterprise Manager Cloud Control Database Vault Administrator Pages

Oracle Database Vault is pre-installed by default and can be enabled easily.

Oracle Database Vault administration is fully integrated with Oracle Enterprise Manager Cloud Control, providing security administrators with a streamlined and centralized interface to manage Oracle Database Vault.

In Oracle Enterprise Manager Cloud Control, you can access the Oracle Database Vault Administrator pages if you prefer to use a graphical user interface to configure

Database Vault policies, and view Database Vault alerts and reports. Oracle Database Vault Administrator provides an extensive collection of security-related reports that assist in understanding the baseline security configuration. These reports also help point out deviations from this baseline.

[Getting Started with Oracle Database Vault](#) (page 3-1) through [DBA Operations in an Oracle Database Vault Environment](#) (page 13-1) explain how to use the Oracle Database Vault Administrator pages to configure access control policy defined in realms, command rules, factors, rule sets, secure application roles, and how to integrate Oracle Database Vault with other Oracle products. [Monitoring Oracle Database Vault](#) (page 26-1) explains how to use these pages to monitor Database Vault activity, and [Oracle Database Vault Reports](#) (page 27-1), explains Oracle Database Vault reporting.

### 1.3.3 Oracle Database Vault DVSYS and DVF Schemas

Oracle Database Vault database objects and public functions are stored in the *DVSYS* and *DVF* schemas, respectively.

Oracle Database Vault provides a schema, *DVSYS*, which stores the database objects needed to process Oracle data for Oracle Database Vault. This schema contains the roles, views, accounts, functions, and other database objects that Oracle Database Vault uses. The *DVF* schema contains public functions to retrieve (at run time) the factor values set in the Oracle Database Vault access control configuration.

#### Related Topics:

[Oracle Database Vault Schemas, Roles, and Accounts](#) (page 14-1)

Oracle Database Vault provides schemas that contain Database Vault objects, roles that provide separation of duty for specific tasks, and default user accounts.

### 1.3.4 Oracle Database Vault PL/SQL Interfaces and Packages

Oracle Database Vault provides PL/SQL interfaces and packages for security managers or application developers to configure access control policies.

The PL/SQL procedures and functions allow the general database account to operate within the boundaries of access control policy in the context of a given database session.

See [Oracle Database Vault Realm APIs](#) (page 15-1) through [Oracle Database Vault API Reference](#) (page 24-1) for more information.

### 1.3.5 Oracle Database Vault Reporting and Monitoring Tools

You can generate reports on the various activities that Oracle Database Vault monitors.

In addition, you can monitor policy changes, security violation attempts, and database configuration and structural changes.

#### Related Topics:

[Oracle Database Vault Reports](#) (page 27-1)

Oracle Database Vault provides reports that track activities, such as the Database Vault configuration settings.

[Monitoring Oracle Database Vault](#) (page 26-1)

You can monitor Oracle Database Vault by checking for violations to the Database Vault configurations and by tracking changes to policies.

## 1.4 How Oracle Database Vault Addresses Compliance Regulations

One of the biggest side benefits resulting from regulatory compliance has been security awareness.

Historically, the focus of the information technology (IT) department has been on high availability and performance. The focus on regulatory compliance has required everyone to take a step back and look at their IT infrastructure, databases, and applications from a security angle. Common questions include:

- Where is the sensitive information stored?
- Who has access to this information?

Regulations such as the Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA), International Convergence of Capital Measurement and Capital Standards: a Revised Framework (Basel II), Japan Privacy Law, Payment Card Industry Data Security Standard (PCI DSS), and the European Union Directive on Privacy and Electronic Communications have common themes that include internal controls, separation of duty, and access control.

While most changes required by regulations such as Sarbanes-Oxley and HIPAA are procedural in nature, the remainder may require technology investments. A common security requirement found in regulations is stringent internal controls. The degree to which Oracle Database Vault helps an organization achieve compliance varies with the regulation. In general, Oracle Database Vault realms, command rules, factors and separation of duty features, help reduce the overall security risks that regulation provisions worldwide address.

[Table 1-1](#) (page 1-7) lists regulations that address potential security threats.

**Table 1-1 Regulations That Address Potential Security Threats**

Regulation	Potential Security Threat
Sarbanes-Oxley Section 302	Unauthorized changes to data
Sarbanes-Oxley Section 404	Modification to data, unauthorized access
Sarbanes-Oxley Section 409	Denial of service, unauthorized access
Gramm-Leach-Bliley	Unauthorized access, modification, or disclosure
Health Insurance Portability and Accountability Act (HIPAA) 164.306	Unauthorized access to data
HIPAA 164.312	Unauthorized access to data
Basel II – Internal Risk Management	Unauthorized access to data
CFR Part 11	Unauthorized access to data
Japan Privacy Law	Unauthorized access to data

**Table 1-1 (Cont.) Regulations That Address Potential Security Threats**

<b>Regulation</b>	<b>Potential Security Threat</b>
EU Directive on Privacy and Electronic Communications	Unauthorized access to data
Payment Card Industry Data Security Standard (PCI DSS)	Unauthorized changes to data

## 1.5 How Oracle Database Vault Protects Privileged User Accounts

Many security breaches, both external and internal, target privileged users database accounts to steal data from databases.

Oracle Database Vault protects against compromised privilege user account attacks by using realms, factors, and command rules. Combined, these provide powerful security tools to help secure access to databases, applications, and sensitive information. You can combine rules and factors to control the conditions under which commands in the database are allowed to execute, and to control access to data protected by a realm. For example, you can create rules and factors to control access to data based on IP addresses, the time of day, and specific programs. These can limit access to only those connections that pass these conditions. This can prevent unauthorized access to application data and access to the database by unauthorized applications.

Oracle Database Vault provides built-in factors that you can use in combination with rules to control access to the database, realm-protected applications, and commands within the database.

You can associate rules and factors with many SQL statements in the database to provide stronger internal controls within the database. You can customize these to meet the operational policies for your site. For example, you could define a rule to limit execution of the `ALTER SYSTEM` statement to a specific IP address and host name.

## 1.6 How Oracle Database Vault Allows for Flexible Security Policies

Oracle Database Vault helps you design flexible security policies for your database.

For example, any database user who has the DBA role can make modifications to basic parameters in a database. Suppose an inexperienced administrator who has system privileges decides to start a new redo log file but does not realize that doing so at a particular time may cause problems for the database. With Oracle Database Vault, you can create a command rule to prevent this user from making such modifications by limiting his or her usage of the `ALTER SYSTEM SWITCH LOGFILE` statement. Furthermore, you can attach rule sets to the command rule to restrict activity further, such as limiting the statement's execution in the following ways:

- By time (for example, only during 4 p.m. and 5 p.m. on Friday afternoons)
- By local access only, that is, not remotely
- By IP address (for example, allowing the action to only a specified range of IP addresses)

You can customize Oracle Database Vault separation of duties to fit the requirements of business of any size. For example, large customers with dedicated IT staff and some out sourced back end operations can further fine tune separation of duties to control

what out sourced database administrators can do. For smaller organizations with some users handling multiple responsibilities, separation of duties can be tuned down and these users can create separate dedicated accounts for each responsibility. This helps such users keep track of all actions made and prevents intruders from exploiting compromised privileged database accounts to steal sensitive data. In addition, it helps auditors verify compliance.

## 1.7 How Oracle Database Vault Addresses Database Consolidation Concerns

Consolidation and cloud environments reduce cost but can expose sensitive application data to those without a true need-to-know.

Data from one country may be hosted in an entirely different country, but access to that data must be restricted based on regulations of the country to which the data belongs. Oracle Database Vault controls provide increased security for these environments by preventing database administrators from accessing the applications data. In addition, controls can be used to help block application bypass and enforce a trusted-path from the application tier to the application data.

Oracle Database Vault provides four distinct separation of duty controls for security administration:

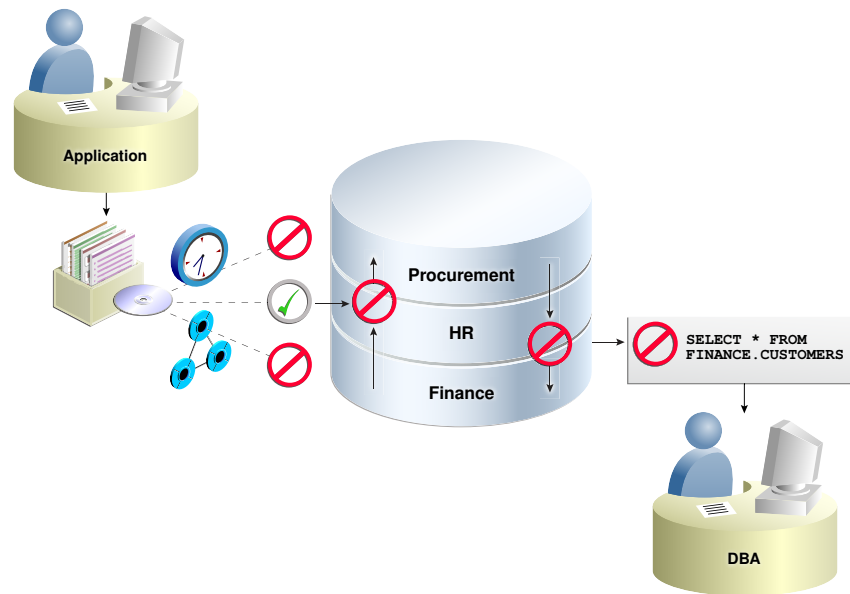
- Day-to-day database administrator tasks using the default Oracle Database DBA role
- Security administrator tasks using the DV\_OWNER and DV\_ADMIN roles
- Account administrator tasks using the DV\_ACCTMGR role
- Grants of roles and privileges by a named trusted user

Oracle Database Vault separation of duty controls can be customized and organizations with limited resources can assign multiple Oracle Database Vault responsibilities to the same administrator, but using separate accounts for each separation-of-duty role to minimize damage to the database if any one account is stolen and leveraged.

Oracle customers today still have hundreds and even thousands of databases distributed throughout the enterprise and around the world. However, for database consolidation as a cost-saving strategy in the coming years to be effective, the physical security provided by the distributed database architecture must be available in the consolidated environment. Oracle Database Vault addresses the primary security concerns of database consolidation.

[Figure 1-2](#) (page 1-10) illustrates how Oracle Database Vault addresses the following database security concerns:

- **Administrative privileged account access to application data:** In this case, Oracle Database Vault prevents the database administrator from accessing the schemas that are protected by the Finance realm. Although the database administrator is the most powerful and trusted user, this administrator does not need access to application data residing within the database.
- **Separation of duties for application data access:** In this case, the HR realm owner, created in Oracle Database Vault, has access to the HR realm schemas.

**Figure 1-2 Oracle Database Vault Security**

Database consolidation can result in multiple powerful user accounts residing in a single database. This means that in addition to the overall database administrator, individual application schema owners also may have powerful privileges. Revoking some privileges may adversely affect existing applications. Using Oracle Database Vault realms, you can enforce access to applications through a trusted path, preventing database users who have not been specifically authorized access from using powerful privileges to look at other application data. For example, a database administrator who has the `SELECT ANY TABLE` system privilege can be prevented from using that privilege to view other application data residing in the same database.

## 1.8 How Oracle Database Vault Works in a Multitenant Environment

Oracle Database Vault can be used with Oracle Multitenant to provide increased security for consolidation.

Oracle Database Vault can prevent privileged user access inside a pluggable database (PDB) and between the PDB and the common privileged user at the container database. Each pluggable database (PDB) has its own Database Vault metadata, such as realms, rule sets, command rules, default policies (such as default realms) and so on. In addition, the objects within the `DVSYS` and `DVF` schemas are automatically available to any child PDBs. Both of these schemas are common user schemas.

You can configure common realms in the application root only, but you can create common rule sets and command rules in either the application root or the CDB root. A common command rule in the application root applies to its associated PDBs, and common command rules in the CDB root apply to all PDBs in the CDB environment. The ability to create common realms and command rules enables you to create policies that use a shared set of realms, rule sets, or command rules throughout the CDB environments, rather than having to create these same components for every PDB in the multitenant environment. The common protection applies for all PDBs associated with the application root that have Oracle Database Vault enabled.

You can create individual local policies for each PDB. When you use Database Vault to protect an object, Database Vault subjects common privileges for common objects to the same enforcement rules as local system privileges.

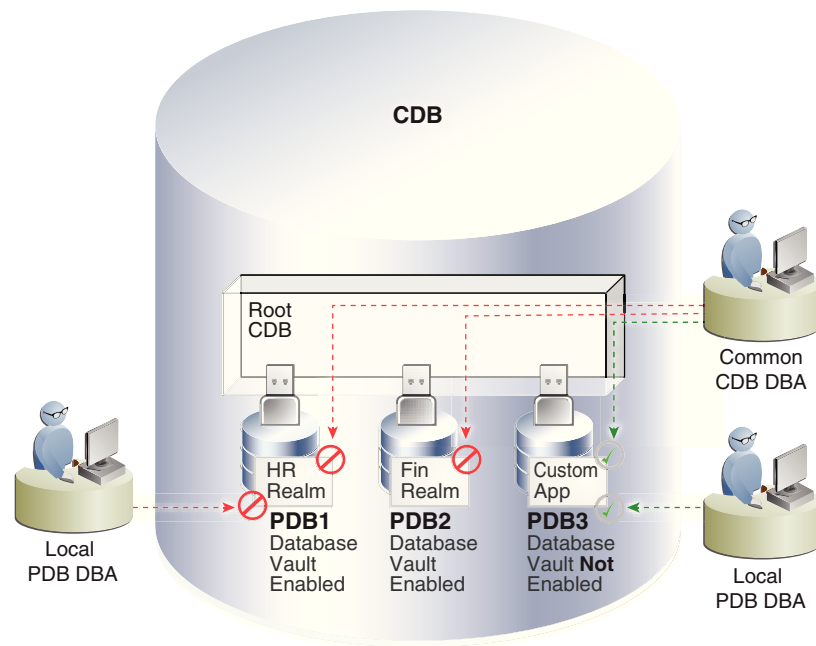


When you configure a PDB that has Database Vault enabled, the `DVSYS` schema is a common user schema that is stored in the root. This means that all the objects within the `DVSYS` schema (tables, data dictionary views, user accounts, PL/SQL packages, default policies, and so on) are subject to the common privileges available for this schema. In other words, you can create realms, factors, and so on in the root to protect the schema in the root. Ensure that you configure Database Vault in the root first, before you configure it in the associated PDBs.

When you enable Oracle Database Vault in the CDB root, you can choose either regular mode or strict mode. The settings propagate throughout the CDB based on the setting you choose. For example, suppose a CDB contains both Database Vault-enabled PDBs and PDBs in which Database Vault is not enabled. If you enable Database Vault using regular mode, then both types of PDBs will continue to function normally. If you enable Database Vault using strict mode, then the Database Vault-disabled PDBs will operate in restricted mode.

[Figure 1-3](#) (page 1-11) illustrates how the database in regular mode allows different access for common and local database administrators depending if Database Vault is enabled. In this scenario, neither the common user nor the local users have access to the realms in PDB1 and PDB2. Both the common user and the PDB3 local user have access to the Custom App application in PDB3, where Database Vault is not enabled.

**Figure 1-3 Oracle Database Vault in a Multitenant Environment with Regular Mode**



#### Related Topics:

##### [Realms in a Multitenant Environment](#) (page 5-5)

In a multitenant environment, you can create a realm to protect common objects in the application root.

##### [Rule Sets and Rules in a Multitenant Environment](#) (page 6-2)

In a multitenant environment, you can create a rule set and its associated rules in the application root.

[Command Rules in a Multitenant Environment](#) (page 7-3)

In a multitenant environment, you can create common and local command rules in either the CDB root or the application root.

[Plugging a Database Vault-Enabled PDB to a CDB](#) (page 13-23)

You can plug a legacy Database Vault-enabled PDB to a multitenant container database (CDB).

---

# What to Expect After You Enable Oracle Database Vault

When you enable Oracle Database Vault, several Oracle Database security features, such as default user authorizations, are modified to provide stronger security restrictions.

## [Initialization and Password Parameter Settings That Change](#) (page 2-1)

The Oracle Database Vault configuration modifies several database initialization parameter settings to better secure your database configuration.

## [How Oracle Database Vault Restricts User Authorizations](#) (page 2-3)

The Oracle Database configuration requires two additional administrative database account names.

## [New Database Roles to Enforce Separation of Duties](#) (page 2-3)

The Oracle Database Vault configuration implements the concept of *separation of duty* so that you can meet regulatory, privacy and other compliance requirements.

## [Privileges That Are Revoked from Existing Users and Roles](#) (page 2-3)

The Oracle Database Vault configuration revokes privileges from several Oracle Database-supplied users and roles, for better separation of duty.

## [Privileges That Are Prevented for Existing Users and Roles](#) (page 2-5)

The Oracle Database Vault configuration prevents several privileges for all users and roles who have been granted these privileges, including users SYS and SYSTEM.

## [Modified AUDIT Statement Settings for a Non-Unified Audit Environment](#) (page 2-5)

When you configure Oracle Database Vault and if you decide not to use unified auditing, then Database Vault configures several AUDIT statements.

## 2.1 Initialization and Password Parameter Settings That Change

The Oracle Database Vault configuration modifies several database initialization parameter settings to better secure your database configuration.

If these changes adversely affect your organizational processes or database maintenance procedures, then contact Oracle Support for help in resolving the issue.

[Table 2-1](#) (page 2-2) describes the initialization parameter settings that Oracle Database Vault modifies. Initialization parameters are stored in the `init.ora` initialization parameter file. On UNIX and Linux, this file is located in `$ORACLE_HOME/dbs`. On Windows, this file is located in `$ORACLE_HOME/database`. For more information about this file, see *Oracle Database Reference*.

**Table 2-1 Modified Database Initialization Parameter Settings**

Parameter	Default Value in Database	New Value Set by Database Vault	Impact of the Change
AUDIT_SYS_OPERATIONS	FALSE	TRUE	<p>Enables the auditing of top-level operations directly issued by user SYS, and users connecting with SYSDBA or SYSOPER privilege.</p> <p>For more information about AUDIT_SYS_OPERATIONS, see <i>Oracle Database Reference</i>.</p>
OS_ROLES	Not configured	FALSE	<p>Disables the operating system to completely manage the granting and revoking of roles to users. Any previous grants of roles to users using GRANT statements do not change, because they are still listed in the data dictionary. Only the role grants made at the operating system-level to users apply. Users can still grant privileges to roles and users.</p> <p>For more information about OS_ROLES, see <i>Oracle Database Reference</i>.</p>
REMOTE_LOGIN_PASSWORDFILE	EXCLUSIVE	EXCLUSIVE	<p>Specifies whether Oracle Database checks for a password file. The EXCLUSIVE setting enforces the use of the password file, if you installed Oracle Database Vault into a database where REMOTE_LOGIN_PASSWORDFILE is not set to EXCLUSIVE.</p> <p>For more information about REMOTE_LOGIN_PASSWORDFILE, see <i>Oracle Database Reference</i>.</p>
SQL92_SECURITY	TRUE	TRUE	<p>Ensures that if a user has been granted the UPDATE or DELETE object privilege, then the user must also be granted the SELECT object privilege before being able to perform UPDATE or DELETE operations on tables that have WHERE or SET clauses.</p> <p>Be aware that if the user is only granted the READ object privilege (instead of SELECT), then the user is not able to perform UPDATE or DELETE operations.</p> <p>For more information about SQL92_SECURITY, see <i>Oracle Database Reference</i>.</p>

## 2.2 How Oracle Database Vault Restricts User Authorizations

The Oracle Database configuration requires two additional administrative database account names.

In addition, several database roles are created. These accounts are part of the separation of duties provided by Oracle Database Vault. One common audit problem that has affected several large organizations is the unauthorized creation of new database accounts by a database administrator within a production instance. Upon installation, Oracle Database Vault prevents anyone other than the Oracle Database Vault account manager or a user granted the Oracle Database Vault account manager role from creating users in the database.

### Related Topics:

[Separation of Duty Guidelines](#) (page D-1)

Oracle Database Vault is designed to easily implement separation of duty guidelines.

## 2.3 New Database Roles to Enforce Separation of Duties

The Oracle Database Vault configuration implements the concept of *separation of duty* so that you can meet regulatory, privacy and other compliance requirements.

Oracle Database Vault makes clear separation between the account management responsibility, data security responsibility, and database management responsibility inside the database. This means that the concept of a super-privileged user (for example, DBA) is divided among several new database roles to ensure no one user has full control over both the data and configuration of the system. Oracle Database Vault prevents privileged users (those with the DBA and other privileged roles and system privileges) from accessing designated protected areas of the database called realms. It also introduces new database roles called the Oracle Database Vault Owner (DV\_OWNER) and the Oracle Database Vault Account Manager (DV\_ACCTMGR). These new database roles separate the data security and the account management from the traditional DBA role. You should map these roles to distinct security professionals within your organization.

### Related Topics:

[Separation of Duty Guidelines](#) (page D-1)

Oracle Database Vault is designed to easily implement separation of duty guidelines.

[Oracle Database Vault Roles](#) (page 14-3)

Oracle Database Vault provides default roles that are based on specific user tasks and adhere to separation of duty concepts.

[Oracle Database Vault Accounts Created During Registration](#) (page 14-23)

You must create accounts for the Oracle Database Vault Owner and Oracle Database Vault Account Manager during the registration process.

## 2.4 Privileges That Are Revoked from Existing Users and Roles

The Oracle Database Vault configuration revokes privileges from several Oracle Database-supplied users and roles, for better separation of duty.

[Table 2-2](#) (page 2-4) lists privileges that Oracle Database Vault revokes from the Oracle Database-supplied users and roles. Be aware that if you disable Oracle

Database Vault, these privileges remain revoked. If your applications depend on these privileges, then grant them to application owner directly.

**Table 2-2 Privileges Oracle Database Vault Revokes**

User or Role	Privilege That Is Revoked
DBA role	<ul style="list-style-type: none"> <li>• BECOME USER</li> <li>• SELECT ANY TRANSACTION</li> <li>• CREATE ANY JOB</li> <li>• CREATE EXTERNAL JOB</li> <li>• EXECUTE ANY PROGRAM</li> <li>• EXECUTE ANY CLASS</li> <li>• MANAGE SCHEDULER</li> <li>• DEQUEUE ANY QUEUE</li> <li>• ENQUEUE ANY QUEUE</li> <li>• MANAGE ANY QUEUE</li> </ul>
IMP_FULL_DATABASE role <sup>1</sup>	<ul style="list-style-type: none"> <li>• BECOME USER</li> <li>• MANAGE ANY QUEUE</li> </ul>
EXECUTE_CATALOG_ROLE role	<ul style="list-style-type: none"> <li>• EXECUTE ON DBMS_LOGMNR</li> <li>• EXECUTE ON DBMS_LOGMNR_D</li> <li>• EXECUTE ON DBMS_LOGMNR_LOGREP_DICT</li> <li>• EXECUTE ON DBMS_LOGMNR_SESSION</li> <li>• EXECUTE ON DBMS_FILE_TRANSFER</li> </ul>
PUBLIC user	<ul style="list-style-type: none"> <li>• EXECUTE ON UTL_FILE</li> </ul>
SCHEDULER_ADMIN role <sup>2</sup>	<ul style="list-style-type: none"> <li>• CREATE ANY JOB</li> <li>• CREATE EXTERNAL JOB</li> <li>• EXECUTE ANY PROGRAM</li> <li>• EXECUTE ANY CLASS</li> <li>• MANAGE SCHEDULER</li> </ul>

<sup>1</sup> To authorize users to export and import data using Oracle Data Pump, see [Using Oracle Data Pump with Oracle Database Vault](#) (page 13-5).

<sup>2</sup> To authorize users to schedule database jobs, see [Using Oracle Scheduler with Oracle Database Vault](#) (page 13-14).

---



---

**Note:**

Both the SYS and SYSTEM users retain the SELECT privilege for the DBA\_USERS\_WITH\_DEFPWD data dictionary view, which lists user accounts that use default passwords. If you want other users to have access to this view, grant them the SELECT privilege on it.

---



---

**Related Topics:**

[Table 14-1](#) (page 14-6)

[DV\\_ACCTMGR Database Vault Account Manager Role](#) (page 14-19)

The DV\_ACCTMGR role is a powerful role, used for accounts management.

## 2.5 Privileges That Are Prevented for Existing Users and Roles

The Oracle Database Vault configuration prevents several privileges for all users and roles who have been granted these privileges, including users `SYS` and `SYSTEM`.

The `DV_ACCTMGR` role has these privileges for separation of duty.

- `ALTER PROFILE`
- `ALTER USER`
- `CREATE PROFILE`
- `CREATE USER`
- `DROP PROFILE`
- `DROP USER`

For better security and to maintain separation-of-duty standards, do not enable `SYS` or `SYSTEM` users the ability to create or manage user accounts.

## 2.6 Modified AUDIT Statement Settings for a Non-Unified Audit Environment

When you configure Oracle Database Vault and if you decide not to use unified auditing, then Database Vault configures several `AUDIT` statements.

### Related Topics:

[Oracle Database Audit Settings Created for Oracle Database Vault](#) (page A-9)

When you install Oracle Database Vault, it creates several `AUDIT` settings in the database.





---

# Getting Started with Oracle Database Vault

Before you can start using Oracle Database Vault, you must register it with the Oracle database.

[Manually Installing Oracle Database Vault in a Multitenant Environment](#) (page 3-1)

Under certain conditions, for a multitenant environment, you must manually install Oracle Database Vault.

[Registering Oracle Database Vault with an Oracle Database](#) (page 3-2)

You can register Oracle Database Vault for either a non-multitenant environment or a multitenant environment.

[Logging into Oracle Database Vault](#) (page 3-10)

Oracle Enterprise Manager Cloud Control (Cloud Control) provides pages for Oracle Database Vault.

[Quick Start Tutorial: Securing a Schema from DBA Access](#) (page 3-11)

This tutorial shows how to create a realm around the HR schema.

## 3.1 Manually Installing Oracle Database Vault in a Multitenant Environment

Under certain conditions, for a multitenant environment, you must manually install Oracle Database Vault.

You must manually install Oracle Database Vault (and Oracle Label Security) in a PDB if this PDB does not have these products when the PDB has been plugged into a CDB where Database Vault and Label Security are installed.

1. As user who has been granted the SYSDBA administrative privilege, log in to the PDB in which you want to install Oracle Database Vault.

For example, to log in to a PDB named `hr_pdb`:

```
sqlplus sec_admin@hr_pdb as sysdba
Enter password: password
```

To find the available PDBs, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

2. If necessary, follow the instructions in [Verifying That Database Vault Is Configured and Enabled](#) (page 3-9) to check if Oracle Database Vault and Oracle Label Security are already installed on this PDB.
3. Install Oracle Label Security by executing the `catols.sql` script.

```
@${ORACLE_HOME}/rdbms/admin/catols.sql
```

Oracle Label Security must be installed before you can use Oracle Database Vault.

4. Install Oracle Database Vault by executing the `catmac.sql` script.

```
@$ORACLE_HOME/rdbms/admin/catmac.sql
```

5. At the `Enter value for 1` prompt, enter the default tablespace for the PDB.
6. At the `Enter value for 2` prompt, enter the temporary tablespace for the PDB.

After the installation is complete, you can register Oracle Database Vault.

**Related Topics:**

[Registering Oracle Database Vault with an Oracle Database](#) (page 3-2)

You can register Oracle Database Vault for either a non-multitenant environment or a multitenant environment.

## 3.2 Registering Oracle Database Vault with an Oracle Database

You can register Oracle Database Vault for either a non-multitenant environment or a multitenant environment.

[About Registering Oracle Database Vault with an Oracle Database](#) (page 3-2)

After you install Oracle Database, you must register (that is, configure and enable) Oracle Database Vault with the Oracle database in which it was installed.

[Registering Database Vault in a Non-Multitenant Environment](#) (page 3-3)

You can register Oracle Database Vault from SQL\*Plus in a non-multitenant environment.

[Registering Database Vault with Common Users to Manage the CDB Root](#) (page 3-5)

In a multitenant environment, you can register Oracle Database Vault with a common user who will manage the CDB root.

[Registering Database Vault Common Users to Manage Specific PDBs](#) (page 3-7)

In a multitenant environment, you must register Oracle Database Vault in the root first, then in the PDBs afterward.

[Plugging in a Database That Has Database Vault Enabled](#) (page 3-9)

From SQL\*Plus, in a multitenant environment, you can plug in a database that already has Database Vault enabled.

[Verifying That Database Vault Is Configured and Enabled](#) (page 3-9)

The `DBA_DV_STATUS`, `CDB_DV_STATUS`, `DBA_OLS_STATUS`, and `CDB_OLS_STATUS` data dictionary views verify if Oracle Database is configured and enabled.

### 3.2.1 About Registering Oracle Database Vault with an Oracle Database

After you install Oracle Database, you must register (that is, configure and enable) Oracle Database Vault with the Oracle database in which it was installed.

Oracle Database includes Database Vault when you choose to include a default database in the installation process, but you must register it before you can use it. If you create a custom database, then you can use DBCA to install and enable Database

Vault for it. As part of the registration process, you create the Database Vault administrative accounts. The registration process enables Oracle Label Security if it is not already enabled. Oracle Label Security is required for Oracle Database Vault but it does not require a separate license unless you begin using Oracle Label Security separately and create Oracle Label Security policies. This procedure applies to the CDB root, application root, and the current pluggable database (PDB), as well as to both single-instance and Oracle Real Application Clusters (Oracle RAC) installations.

This section explains how to register Oracle Database Vault in a non-multitenant environment, and several ways that you can register it in a multitenant environment.

---



---

**Note:** If you have upgraded from a release earlier than Oracle Database 12c, and if the earlier Oracle Database Vault had been enabled in that earlier release, then after the upgrade process is complete, you must enable Oracle Database Vault by using the `DBMS_MACADM.ENABLE_DV` procedure.

---



---

### Related Topics:

[Verifying That Database Vault Is Configured and Enabled](#) (page 3-9)

The `DBA_DV_STATUS`, `CDB_DV_STATUS`, `DBA_OLS_STATUS`, and `CDB_OLS_STATUS` data dictionary views verify if Oracle Database is configured and enabled.

## 3.2.2 Registering Database Vault in a Non-Multitenant Environment

You can register Oracle Database Vault from SQL\*Plus in a non-multitenant environment.

1. Log into the database instance as a user who has privileges to create user accounts and grant the `CREATE SESSION` privilege to other users.

For example:

```
sqlplus sec_admin
Enter password: password
```

2. Create accounts that will be used for the Database Vault Owner (`DV_OWNER` role) and Database Vault Account Manager (`DV_ACCTMGR` role) accounts.

Oracle strongly recommends that you create two accounts for each role. One account, the primary account, will be used on a day-to-day basis and the other account will be used as a backup account in case the password of the primary account is lost and must be reset.

For example:

```
GRANT CREATE SESSION TO dbv_owner IDENTIFIED BY password;
GRANT CREATE SESSION TO dbv_owner_backup IDENTIFIED BY password;
GRANT CREATE SESSION TO dbv_acctmgr IDENTIFIED BY password;
GRANT CREATE SESSION TO dbv_acctmgr_backup IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace `password` with a password that is secure.

3. Connect with the `SYSDBA` administrative privilege.

```
CONNECT / AS SYSDBA
Enter password: password
```

**4. Configure the primary Database Vault user accounts.**

```
BEGIN
CONFIGURE_DV (
  dvowner_username      => 'dbv_owner',
  dvacctmgr_username    => 'dbv_acctmgr');
END;
/
```

Do not enter the names DV\_OWNER, DV\_ACCTMGR, or the names of any other Database Vault roles for these user accounts.

**5. Run the utlrlp.sql script to recompile invalidated objects.**

```
@?/rdbms/admin/utlrlp.sql
```

If the script gives you any instructions, follow them, and then run the script again. If the script terminates abnormally without giving any instructions, run it again.

**6. Connect as the primary Database Vault Owner user that you just configured.**

For example:

```
CONNECT dbv_owner
Enter password: password
```

**7. Enable Oracle Database Vault.**

```
EXEC DBMS_MACADM.ENABLE_DV;
```

**8. Connect with the SYSDBA administrative privilege.**

```
CONNECT / AS SYSDBA
```

**9. Restart the database.**

```
SHUTDOWN IMMEDIATE
STARTUP
```

**10. Connect as the primary DV\_OWNER user and then grant the DV\_OWNER role to the backup DV\_OWNER user that you created earlier.**

For example:

```
CONNECT dbv_owner
Enter password: password

GRANT DV_OWNER TO dbv_owner_backup;
```

**11. Connect as the primary DV\_ACCTMGR user and then grant the DV\_ACCTMGR role to the backup DV\_ACCTMGR user.**

For example:

```
CONNECT dbv_acctmgr
Enter password: password

GRANT DV_ACCTMGR TO dbv_acctmgr_backup;
```

**12. Store the two backup accounts in a safe location in case they are needed in the future.**

**Related Topics:**[Verifying That Database Vault Is Configured and Enabled](#) (page 3-9)

The `DBA_DV_STATUS`, `CDB_DV_STATUS`, `DBA_OLS_STATUS`, and `CDB_OLS_STATUS` data dictionary views verify if Oracle Database is configured and enabled.

[Oracle Database Vault Roles](#) (page 14-3)

Oracle Database Vault provides default roles that are based on specific user tasks and adhere to separation of duty concepts.

[Logging into Oracle Database Vault](#) (page 3-10)

Oracle Enterprise Manager Cloud Control (Cloud Control) provides pages for Oracle Database Vault.

### 3.2.3 Registering Database Vault with Common Users to Manage the CDB Root

In a multitenant environment, you can register Oracle Database Vault with a common user who will manage the CDB root.

1. In a multitenant environment, log into the root of the database instance as a user who has privileges to create users and grant the `CREATE SESSION` and `SET CONTAINER` privileges.

For example:

```
sqlplus c##sec_admin
Enter password: password
```

2. Create accounts that will be used for the Database Vault Owner (`DV_OWNER` role) and Database Vault Account Manager (`DV_ACCTMGR` role) accounts.

Oracle strongly recommends that you create two accounts for each role. One account, the primary account, will be used on a day-to-day basis and the other account will be used as a backup account in case the password of the primary account is lost and must be reset.

Prepend the names of these accounts with `c##` or `C##`. For example:

```
GRANT CREATE SESSION, SET CONTAINER TO c##dbv_owner_root IDENTIFIED BY password
CONTAINER = ALL;
GRANT CREATE SESSION, SET CONTAINER TO c##dbv_owner_root_backup IDENTIFIED BY
password CONTAINER = ALL;
GRANT CREATE SESSION, SET CONTAINER TO c##dbv_acctmgr_root IDENTIFIED BY password
CONTAINER = ALL;
GRANT CREATE SESSION, SET CONTAINER TO c##dbv_acctmgr_root_backup IDENTIFIED BY
password CONTAINER = ALL;
```

Replace `password` with a password that is secure. See *Oracle Database Security Guide* for the minimum requirements for creating passwords.

3. Connect to the root as user `SYS` with the `SYSDBA` administrative privilege

```
CONNECT SYS AS SYSDBA
Enter password: password
```

4. Configure the primary Database Vault user accounts.

```
BEGIN
CONFIGURE_DV (
  dvowner_uname          => 'c##dbv_owner_root',
```

```

    dvacctmgr_uname      => 'c##dbv_acctmgr_root');
END;
/

```

5. Run the `utlrlp.sql` script to recompile invalidated objects in the root.

```
@?/rdbms/admin/utlrlp.sql
```

If the script provides instructions, follow them, and then run the script again. If the script terminates abnormally without giving any instructions, run it again.

6. Connect to the root as the primary Database Vault Owner user that you just configured.

For example:

```
CONNECT c##dbv_owner_root
Enter password: password
```

7. Enable Oracle Database Vault using one of the following options:

- To enable Oracle Database Vault to use regular mode, which puts the PDB in restricted mode until you enable Database Vault in the PDB and then restart the PDB:

```
EXEC DBMS_MACADM.ENABLE_DV (strict_mode => 'n');
```

- To enable Oracle Database Vault to use strict mode, which enables Database Vault in each PDB:

```
EXEC DBMS_MACADM.ENABLE_DV (strict_mode => 'y');
```

8. Connect with the `SYSDBA` administrative privilege.

```
CONNECT / AS SYSDBA
```

9. Restart the database.

```
SHUTDOWN IMMEDIATE
STARTUP
```

10. Connect as the primary `DV_OWNER` user and then grant the `DV_OWNER` role to the backup `DV_OWNER` user that you created earlier.

For example:

```
CONNECT c##dbv_owner_root
Enter password: password

GRANT DV_OWNER TO c##dbv_owner_root_backup;
```

11. Connect as the primary `DV_ACCTMGR` user and then grant the `DV_ACCTMGR` role to the backup `DV_ACCTMGR` user.

For example:

```
CONNECT c##dbv_acctmgr_root
Enter password: password

GRANT DV_ACCTMGR TO c##dbv_acctmgr_root_backup;
```

12. Store the two backup accounts in a safe location in case they are needed in the future.

**Related Topics:**[Verifying That Database Vault Is Configured and Enabled](#) (page 3-9)

The `DBA_DV_STATUS`, `CDB_DV_STATUS`, `DBA_OLS_STATUS`, and `CDB_OLS_STATUS` data dictionary views verify if Oracle Database is configured and enabled.

[Oracle Database Vault Roles](#) (page 14-3)

Oracle Database Vault provides default roles that are based on specific user tasks and adhere to separation of duty concepts.

[Logging into Oracle Database Vault](#) (page 3-10)

Oracle Enterprise Manager Cloud Control (Cloud Control) provides pages for Oracle Database Vault.

**3.2.4 Registering Database Vault Common Users to Manage Specific PDBs**

In a multitenant environment, you must register Oracle Database Vault in the root first, then in the PDBs afterward.

If you try to register in a PDB first, then an `ORA-47503: Database Vault is not enabled on CDB$ROOT` error appears.

1. In a multitenant environment, log into the root of the database instance as a user who has privileges to create users and to grant the `CREATE SESSION` and `SET CONTAINER` privileges.

For example:

```
sqlplus c##sec_admin
Enter password: password
```

2. If you have not already done so, then create user accounts to be used as the Database Vault accounts.

See Step 2 (page 3-5) under [Registering Database Vault with Common Users to Manage the CDB Root](#) (page 3-5) for more information about creating these accounts.

3. Ensure that you have registered Oracle Database Vault in the CDB root, as described in [Registering Database Vault with Common Users to Manage the CDB Root](#) (page 3-5).
4. Connect to the PDB to which the common users will need access.

For example:

```
CONNECT c##sec_admin@pdb_name
Enter password: password
```

To find the available PDBs, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

5. Grant the `CREATE SESSION` and `SET CONTAINER` privileges to the users for this PDB.

For example:

```
GRANT CREATE SESSION, SET CONTAINER TO c##dbv_owner_root CONTAINER = CURRENT;
GRANT CREATE SESSION, SET CONTAINER TO c##dbv_acctmgr_root CONTAINER = CURRENT;
```

6. Connect as user `SYS` with the `SYSDBA` administrative privilege

```
CONNECT SYS@pdb_name AS SYSDBA
Enter password: password
```

7. While still in the PDB, configure the two primary Database Vault user accounts.

For example:

```
BEGIN
CONFIGURE_DV (
  dvowner_username      => 'c##dbv_owner_root',
  dvacctmgr_username    => 'c##dbv_acctmgr_root');
END;
/
```

8. Run the `utlrlp.sql` script to recompile invalidated objects in this PDB.

```
@?/rdbms/admin/utlrlp.sql
```

If the script provides instructions, follow them, and then run the script again. If the script terminates abnormally without giving any instructions, run it again.

9. Connect to the PDB as the primary Database Vault Owner user that you just configured.

For example:

```
CONNECT c##dbv_owner_root@pdb_name
Enter password: password
```

10. Enable Oracle Database Vault in this PDB.

```
EXEC DBMS_MACADM.ENABLE_DV;
```

11. Connect to the CDB with the `SYSDBA` administrative privilege.

```
CONNECT / AS SYSDBA
```

12. Close and reopen the PDB.

For example:

```
ALTER PLUGGABLE DATABASE pdb_name CLOSE IMMEDIATE;

ALTER PLUGGABLE DATABASE pdb_name OPEN;
```

### Related Topics:

[Verifying That Database Vault Is Configured and Enabled](#) (page 3-9)

The `DBA_DV_STATUS`, `CDB_DV_STATUS`, `DBA_OLS_STATUS`, and `CDB_OLS_STATUS` data dictionary views verify if Oracle Database is configured and enabled.

[Oracle Database Vault Roles](#) (page 14-3)

Oracle Database Vault provides default roles that are based on specific user tasks and adhere to separation of duty concepts.

[Logging into Oracle Database Vault](#) (page 3-10)

Oracle Enterprise Manager Cloud Control (Cloud Control) provides pages for Oracle Database Vault.



### 3.2.5 Plugging in a Database That Has Database Vault Enabled

From SQL\*Plus, in a multitenant environment, you can plug in a database that already has Database Vault enabled.

In this scenario, the plugged in database has its own local Database Vault accounts. Be aware that if you plug a Database Vault-enabled database into a CDB that is not Database Vault enabled, the PDB will remain in restricted mode until you enable Database Vault in the CDB and then restart the CDB. If you plug a non-Database Vault-enabled PDB into a CDB that is Database Vault enabled, then the PDB remains in restricted mode until you enable Database Vault in the PDB and then restart the PDB.

To enable a common user to manage the Database Vault configuration for this PDB:

1. Log into the PDB as the local primary Database Vault owner.

For example:

```
sqlplus dbv_owner@pdb_name
Enter password: password
```

To find the available PDBs, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

2. Grant the common Database Vault users the `CREATE SESSION` and `SET CONTAINER` privileges, and the appropriate Database Vault roles.

The following accounts will be the primary and the backup accounts:

```
GRANT CREATE SESSION, SET CONTAINER, DV_OWNER TO c##dbv_owner_root;
GRANT CREATE SESSION, SET CONTAINER, DV_OWNER TO c##dbv_owner_root_backup;
GRANT CREATE SESSION, SET CONTAINER, DV_ACCTMGR TO c##dbv_acctmgr_root;
GRANT CREATE SESSION, SET CONTAINER, DV_ACCTMGR TO c##dbv_acctmgr_root_backup;
```

#### Related Topics:

##### [Verifying That Database Vault Is Configured and Enabled](#) (page 3-9)

The `DBA_DV_STATUS`, `CDB_DV_STATUS`, `DBA_OLS_STATUS`, and `CDB_OLS_STATUS` data dictionary views verify if Oracle Database is configured and enabled.

##### [Oracle Database Vault Roles](#) (page 14-3)

Oracle Database Vault provides default roles that are based on specific user tasks and adhere to separation of duty concepts.

##### [Logging into Oracle Database Vault](#) (page 3-10)

Oracle Enterprise Manager Cloud Control (Cloud Control) provides pages for Oracle Database Vault.

### 3.2.6 Verifying That Database Vault Is Configured and Enabled

The `DBA_DV_STATUS`, `CDB_DV_STATUS`, `DBA_OLS_STATUS`, and `CDB_OLS_STATUS` data dictionary views verify if Oracle Database is configured and enabled.

In addition to Oracle Database Vault administrators, the Oracle Database `SYS` user and users who have been granted the `DBA` role can query these views.

- For Database Vault:
  - If you want to find the Database Vault status for a non-multitenant database, or in a multitenant environment for the root only or an individual PDB, then query `DBA_DV_STATUS`. For example:
 

```
SELECT * FROM DBA_DV_STATUS;
```

Output similar to the following appears:

NAME	STATUS
DV_CONFIGURE_STATUS	TRUE
DV_ENABLE_STATUS	TRUE
  - If you want to find the Database Vault status of all PDBs in a multitenant environment, as a common user with administrative privileges, then query `CDB_DV_STATUS`, which provides the addition of a container ID (`CON_ID`) field..
- For Oracle Label Security, query the following data dictionary views, which are similar to their Database Vault equivalent views:
  - `DBA_OLS_STATUS`
  - `CDB_OLS_STATUS`

### 3.3 Logging into Oracle Database Vault

Oracle Enterprise Manager Cloud Control (Cloud Control) provides pages for Oracle Database Vault.

The Oracle Database Vault pages can be used to administer and monitor Database Vault-protected databases from a centralized console. This console enables you to automate alerts, view Database Vault reports, and propagate Database Vault policies to other Database Vault-protected databases.

Before you try to log in, ensure that you have configured the Cloud Control target databases that you plan to use with Database Vault by following the Oracle Enterprise Manager online help and *Oracle Enterprise Manager Advanced Configuration*. Oracle Database Vault must also be registered with the Oracle database, using the instructions in [Registering Oracle Database Vault with an Oracle Database](#) (page 3-2).

1. Start Cloud Control.

For example:

```
https://myserver.example.com:7799/em
```

2. Log in to Cloud Control as a security administrator.
3. In the Cloud Control home page, from the **Targets** menu, select **Databases**.
4. In the Databases page, select the link for the Oracle Database Vault-protected database to which you want to connect.

The Database home page appears.

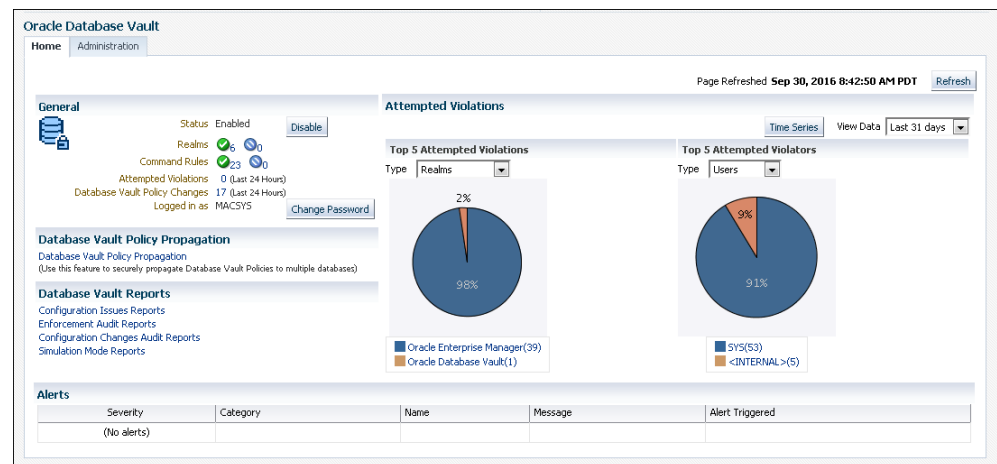
5. From the **Security** menu, select **Database Vault**.

The Database Login page appears.

## 6. Enter the following information:

- **Username:** Enter the name of a user who has been granted the appropriate Oracle Database Vault role:
  - Creating and propagating Database Vault policies: DV\_OWNER or DV\_ADMIN role, SELECT ANY DICTIONARY privilege
  - Viewing Database Vault alerts and reports: DV\_OWNER, DV\_ADMIN, or DV\_SECANALYST role, SELECT ANY DICTIONARY privilege
- **Password:** Enter your password.
- **Role:** Select **NORMAL** from the list.
- **Save as:** Select this check box if you want these credentials to be automatically filled in for you the next time that this page appears. The credentials are stored in Enterprise Manager in a secured manner. Access to these credentials depends on the user who is currently logged in.

The Database Vault home page appears.



### Related Topics:

[About Oracle Database Vault Roles](#) (page 14-4)

Oracle Database Vault provides a set of roles that are required for managing Oracle Database Vault.

[Using Oracle Database Vault with Oracle Enterprise Manager](#) (page 13-2)

Oracle Database Vault administrators can perform tasks in Oracle Enterprise Manager Cloud Control such as propagating policies to other databases.

## 3.4 Quick Start Tutorial: Securing a Schema from DBA Access

This tutorial shows how to create a realm around the HR schema.

[About This Tutorial](#) (page 3-12)

In this tutorial, you create a realm around for the HR sample database schema by using the Oracle Database Vault PL/SQL packages.

**Step 1: Log On as SYSTEM to Access the HR Schema** (page 3-12)

You must enable the HR schema for this tutorial.

**Step 2: Create a Realm** (page 3-13)

Realms can protect one or more schemas, individual schema objects, and database roles.

**Step 3: Create the SEBASTIAN User Account** (page 3-14)

At this stage, there are no database accounts or roles authorized to access or otherwise manipulate the database objects the realm will protect.

**Step 4: Have User SEBASTIAN Test the Realm** (page 3-15)

At this stage, have user SEBASTIAN test the realm, even though he has the READ ANY TABLE system privilege.

**Step 5: Create an Authorization for the Realm** (page 3-15)

Next, user SEBASTIAN must be granted authorization to the HR Apps realm, so that he can access the HR.EMPLOYEES table.

**Step 6: Test the Realm** (page 3-16)

To test the realm, you must try to access the EMPLOYEES table as a user other than HR.

**Step 7: If Unified Auditing Is Not Enabled, Then Run a Report** (page 3-16)

Because you enabled auditing on failure for the HR Apps realm, you can generate a report to find any security violations.

**Step 8: Remove the Components for This Tutorial** (page 3-17)

You can remove the components that you created for this tutorial if you no longer need them.

### 3.4.1 About This Tutorial

In this tutorial, you create a realm around for the HR sample database schema by using the Oracle Database Vault PL/SQL packages.

In the HR schema, the EMPLOYEES table has information such as salaries that should be hidden from most employees in the company, including those with administrative access. To accomplish this, you add the HR schema to the secured objects of the protection zone, which in Oracle Database Vault is called a *realm*, inside the database. Then you grant limited authorizations to this realm. Afterward, you test the realm to make sure it has been properly secured. And finally, to see how Oracle Database Vault provides an audit trail on suspicious activities like the one you will try when you test the realm, you will run a report.

### 3.4.2 Step 1: Log On as SYSTEM to Access the HR Schema

You must enable the HR schema for this tutorial.

Before you begin this tutorial, ensure that the HR sample schema is installed. *Oracle Database Sample Schemas* describes how to install the sample schemas.

1. Log into the database instance as a user who has been granted the DBA role, and then access the HR schema.

For example:

```
sqlplus system  
Enter password: password
```

- In a multitenant environment, connect to the appropriate PDB.

For example:

```
CONNECT SYSTEM@my_pdb
Enter password: password
```

To find the available PDBs, in the CDB, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

- Query the `HR.EMPLOYEES` table as follows.

```
SELECT FIRST_NAME, LAST_NAME, SALARY FROM HR.EMPLOYEES WHERE ROWNUM < 10;
```

Output similar to the following appears:

FIRST_NAME	LAST_NAME	SALARY
Steven	King	24000
Neena	Kochhar	17000
Lex	De Haan	17000
Alexander	Hunold	9000
Bruce	Ernst	6000
David	Austin	4800
Valli	Pataballa	4800
Diana	Lorentz	4200
Nancy	Greenberg	12008

9 rows selected.

- If the `HR` schema is locked and expired, log into the database instance as the `DV_ACCTMGR` user and unlock and unexpire the account. For example:

```
sqlplus bea_dvacctmgr -- For a multitenant environment, sqlplus
bea_dvacctmgr@hrpdb
Enter password: password
```

```
ALTER USER HR ACCOUNT UNLOCK IDENTIFIED BY password
```

Follow the guidelines in *Oracle Database Security Guide* to replace `password` with a password that is secure.

As you can see, `SYSTEM` has access to the salary information in the `EMPLOYEES` table of the `HR` schema. This is because `SYSTEM` is automatically granted the `DBA` role, which includes the `SELECT ANY TABLE` system privilege.

- Do not exit `SQL*Plus`.

### 3.4.3 Step 2: Create a Realm

Realms can protect one or more schemas, individual schema objects, and database roles.

Once you create a realm, you can create security restrictions that apply to the schemas and their schema objects within the realm. You will need to create a realm for the `HR` schema.

- Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.

2. In the Administration page, under Database Vault Components, click **Realms**.
3. In the Realms page of Oracle Database Vault Administrator, click **Create**.
4. In the Create Realm page, under General, enter HR Apps after **Name**.
5. In the **Description** field, enter Realm to protect the HR schema.
6. Leave the **Mandatory Realm** check box unchecked.
7. After Status, ensure that **Enabled** is selected so that the realm can be used.
8. Under Audit Options, ensure that **Audit On Failure** is selected so that you can create an audit trail later on.
9. Click **Next** to display the Realm secured objects page.
10. Click the **Add** button and in the Add Secured Object dialog box, enter the following information:
  - **Owner:** Enter HR to select the HR schema.
  - **Object Type:** Enter TABLE.
  - **Object Name:** Enter EMPLOYEES.
11. Click **OK**.

The HR.EMPLOYEES table is added to the Create Realm : Realm Secured Objects page.

12. Click **Done**, and then click **Finish**.

At this stage, you have created the realm but you have not assigned any authorizations to it. You will take care of that later on in this tutorial.

### 3.4.4 Step 3: Create the SEBASTIAN User Account

At this stage, there are no database accounts or roles authorized to access or otherwise manipulate the database objects the realm will protect.

So, the next step is to authorize database accounts or database roles so that they can have access to the schemas within the realm. You will create the SEBASTIAN user account.

1. In SQL\*Plus, connect as the Database Vault Account Manager, who has the DV\_ACCTMGR role, and create the local user SEBASTIAN.

For example:

```
CONNECT bea_dvacctmgr -- Or, CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

```
GRANT CREATE SESSION TO SEBASTIAN IDENTIFIED BY password;
```

Replace *password* with a password that is secure. See *Oracle Database Security Guide* for the minimum requirements for creating passwords.

2. Connect as SYS with the SYSDBA privilege, and then grant SEBASTIAN the following additional privilege.

```
CONNECT SYS AS SYSDBA -- Or, CONNECT SYS@hrpdb AS SYSDBA
Enter password: password
```

```
GRANT READ ANY TABLE TO SEBASTIAN;
```

Do not exit SQL\*Plus; you will need it for [Step 6: Test the Realm](#) (page 3-16), when you test the realm.

### 3.4.5 Step 4: Have User SEBASTIAN Test the Realm

At this stage, have user SEBASTIAN test the realm, even though he has the READ ANY TABLE system privilege.

1. Connect as user SEBASTIAN.

```
CONNECT sebastian
Enter password: password
```

2. Query the HR.EMPLOYEES table.

```
SELECT COUNT(*) FROM HR.EMPLOYEES;
```

The following output should appear:

```
ERROR at line 1:
ORA-01031: insufficient privileges
```

Even though user SEBASTIAN has the READ ANY TABLE system privilege, he cannot query the HR.EMPLOYEES table, because the HR Apps realm takes precedence over the READ ANY TABLE system privilege.

### 3.4.6 Step 5: Create an Authorization for the Realm

Next, user SEBASTIAN must be granted authorization to the HR Apps realm, so that he can access the HR.EMPLOYEES table.

1. In the Realms page of Database Vault Administrator, select the **HR Apps** in the list of realms, and then click **Edit**.
2. Click the **Next** button until you reach the Realm authorizations page.
3. Click **Add** and then enter the following information in the Add Authorizations dialog box:
  - **Realm Authorization Grantee:** Enter SEBASTIAN.
  - **Realm Authorization Type:** Select **Participant** from the list.
  - **Realm Authorization Ruleset:** Leave this field blank.
4. Click **OK**.

The Participant authorization allows the user SEBASTIAN in the HR Apps realm to manage access, manipulate, and create objects protected by the HR Apps realm. In this case, the HR user and SEBASTIAN are the only users allowed to view the EMPLOYEES table.

5. Click **Done**, and then **Finish**.

### 3.4.7 Step 6: Test the Realm

To test the realm, you must try to access the `EMPLOYEES` table as a user other than HR. The `SYSTEM` account normally has access to all objects in the HR schema, but now that you have safeguarded the `EMPLOYEES` table with Oracle Database Vault, this is no longer the case.

1. In SQL\*Plus, connect as `SYSTEM`.

```
CONNECT SYSTEM -- Or, CONNECT SYSTEM@hrpdb
Enter password: password
```

2. Try accessing the salary information in the `EMPLOYEES` table again:

```
SELECT FIRST_NAME, LAST_NAME, SALARY FROM HR.EMPLOYEES WHERE ROWNUM <10;
```

The following output should appear:

```
Error at line 1:
ORA-01031: insufficient privileges
```

`SYSTEM` no longer has access to the salary information in the `EMPLOYEES` table. (In fact, even user `SYS` does not have access to this table.) However, user `SEBASTIAN` does have access to this information.

3. Connect as user `SEBASTIAN`.

```
CONNECT sebastian -- Or, CONNECT sebastian@hrpdb
Enter password: password
```

4. Perform the following query:

```
SELECT FIRST_NAME, LAST_NAME, SALARY FROM HR.EMPLOYEES WHERE ROWNUM <10;
```

Output similar to the following appears:

FIRST_NAME	LAST_NAME	SALARY
Steven	King	24000
Neena	Kochhar	17000
Lex	De Haan	17000
Alexander	Hunold	9000
Bruce	Ernst	6000
David	Austin	4800
Valli	Pataballa	4800
Diana	Lorentz	4200
Nancy	Greenberg	12008

```
9 rows selected.
```

### 3.4.8 Step 7: If Unified Auditing Is Not Enabled, Then Run a Report

Because you enabled auditing on failure for the HR Apps realm, you can generate a report to find any security violations.

For example, you could generate a report for the violation that you attempted in [Step 6: Test the Realm](#) (page 3-16).

1. In SQL\*Plus, connect as user `SYSTEM` and ensure that unified auditing is not enabled.



```
CONNECT SYSTEM -- Or, CONNECT SYSTEM@hrpdb
Enter password: password
```

```
SQL> SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing';
```

If VALUE returns TRUE, then you cannot complete this section. Go to [Step 8: Remove the Components for This Tutorial](#) (page 3-17).

If unified auditing is enabled, then you must create a unified audit policy to capture events. See *Oracle Database Security Guide* for information about how to create unified audit policies for Oracle Database Vault.

2. In the Database Vault Administrator page, click **Home** to display the home page.
3. In the Database Vault Home page, under **Reports**, select **Database Vault Reports**.
4. In the Database Vault Reports page, select **Database Vault Enforcement Audit Report**.
5. From the **Database Vault Audit Report** list, select **Realm Audit Report**.
6. In the Search area, from the **Command** menu, select **Equals** and in the text field, enter `SELECT`. Then click **Search**.

The report appears in the table that follows the Search region.

7. Click **OK** to exit the report.

Oracle Database Vault generates a report listing the type of violation (in this case, the `SELECT` statement entered in the previous section), when and where it occurred, the login account who tried the violation, and what the violation was.

### 3.4.9 Step 8: Remove the Components for This Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. Drop user SEBASTIAN.

In SQL\*Plus, log on as the Oracle Database Vault account manager (for example, `bea_dvacctmgr`) and then drop SEBASTIAN as follows:

```
sqlplus bea_dvacctmgr -- Or, CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

```
DROP USER SEBASTIAN;
```

2. Delete the HR Apps realm.
  - a. In Cloud Control, ensure that you are logged in as a user who has the `DV_OWNER` role.
  - b. In the Database Vault Home page, click **Administration**.
  - c. In the Realms page, select `HR Apps` from the list of realms.
  - d. Click **Delete**, and in the Confirmation window, click **Yes**.
3. If necessary, in SQL\*Plus, lock and expire the HR account.

```
ALTER USER HR ACCOUNT LOCK PASSWORD EXPIRE;
```



---

# Performing Privilege Analysis to Find Privilege Use

Privilege analysis dynamically analyzes the privileges and roles that users use and do not use.

## [What Is Privilege Analysis?](#) (page 4-1)

Oracle Database Vault with Oracle Database Release 12c includes a feature called privilege analysis to help you increase the security of your applications and database operations.

## [Creating and Managing Privilege Analysis Policies](#) (page 4-5)

You can create and manage privilege analysis policies in either SQL\*Plus or in Enterprise Manager Cloud Control.

## [Creating Roles and Managing Privileges Using Cloud Control](#) (page 4-19)

You can create new roles using privileges found in a privilege analysis report and then grant this role to users.

## [Tutorial: Using Capture Runs to Analyze ANY Privilege Use](#) (page 4-23)

This tutorial demonstrates how to create capture runs to analyze the use of the `READ ANY TABLE` system privilege.

## [Tutorial: Analyzing Privilege Use by a User Who Has the DBA Role](#) (page 4-28)

This tutorial demonstrates how to analyze the privilege use of a user who has the `DBA` role and performs database tuning operations.

## [Privilege Analysis Policy and Report Data Dictionary Views](#) (page 4-33)

Oracle Database provides data dictionary views that show information about analyzed privileges.

## 4.1 What Is Privilege Analysis?

Oracle Database Vault with Oracle Database Release 12c includes a feature called privilege analysis to help you increase the security of your applications and database operations.

### [About Privilege Analysis](#) (page 4-2)

Because it is a dynamic analysis, it captures real privileges and roles that were actually used.

### [How Privilege Analysis Works with Pre-Compiled Database Objects](#) (page 4-2)

Privilege analysis can be used to capture the privileges that have been exercised on pre-compiled database objects.

### [Who Can Perform Privilege Analysis?](#) (page 4-3)

To use privilege analysis, you must be granted the `CAPTURE_ADMIN` role.

[Types of Privilege Analysis](#) (page 4-3)

You can create different types of privilege analysis policies to achieve specific goals.

[Benefits and Use Cases of Privilege Analysis](#) (page 4-3)

Analyzing privilege use is beneficial in finding unnecessarily granted privileges.

[How Does a Multitenant Environment Affect Privilege Analysis?](#) (page 4-4)

You can create and use privilege analysis policies in a multitenant environment.

## 4.1.1 About Privilege Analysis

Because it is a dynamic analysis, it captures real privileges and roles that were actually used.

Because it is a dynamic analysis, it captures real privileges and roles that were actually used.

Privilege analysis captures privileges used by database users and applications at runtime. If your applications include definer's rights and invoker's rights procedures, then privilege analysis captures the privileges that are required to compile a procedure and execute it, even if the procedure was compiled before the privilege capture was created and enabled.

Running inside the Oracle Database kernel, privilege analysis helps reduce the attack surface of applications and increase operational security by identifying used and unused privileges. Privilege analysis can be used after you install Oracle Database Release 12c without any additional configuration steps.

---

---

**Note:**

If you want to configure privilege analysis by using Oracle Enterprise Manager Cloud Control, then ensure that you have the latest plug-in. For information about how to deploy a plug-in, see *Enterprise Manager Cloud Control Administrator's Guide*.

---

---

## 4.1.2 How Privilege Analysis Works with Pre-Compiled Database Objects

Privilege analysis can be used to capture the privileges that have been exercised on pre-compiled database objects.

Examples of these objects are PL/SQL packages, procedures, functions, views, triggers, and Java classes and data.

Because these privileges may not be exercised during run time when a stored procedure is called, these privileges are collected when you generate the results for any database-wide capture, along with run-time captured privileges. A privilege is treated as an unused privilege when it is not used in either pre-compiled database objects or run-time capture, and it is saved under the run-time capture name. If a privilege is used for pre-compiled database objects, then it is saved under the capture name `ORA$DEPENDENCY`. If a privilege is captured during run time, then it is saved under the run-time capture name. If you want to know what the used privileges are for both pre-compiled database objects and run-time usage, then you must query both the `ORA$DEPENDENCY` and run-time captures. For unused privileges, you only need to query with the run-time capture name.

To find a full list of the pre-compiled objects on which privilege analysis can be used, query the `TYPE` column of the `ALL_DEPENDENCIES` data dictionary view.

### 4.1.3 Who Can Perform Privilege Analysis?

To use privilege analysis, you must be granted the `CAPTURE_ADMIN` role.

You use the `DBMS_PRIVILEGE_CAPTURE` PL/SQL package to manage privilege capture. You use the data dictionary views provided by privilege analysis to analyze your privilege use.

### 4.1.4 Types of Privilege Analysis

You can create different types of privilege analysis policies to achieve specific goals.

- **Role-based privilege use capture.** You must provide a list of roles. If the roles in the list are enabled in the database session, then the used privileges for the session will be captured. You can capture privilege use for the following types of roles: Oracle default roles, user-created roles, Code Based Access Control (CBAC) roles, and secure application roles.
- **Context-based privilege use capture.** You must specify a Boolean expression only with the `SYS_CONTEXT` function. The used privileges will be captured if the condition evaluates to `TRUE`.
- **Role- and context-based privilege use capture.** You must provide both a list of roles that are enabled and a `SYS_CONTEXT` Boolean expression for the condition. When any of these roles is enabled in a session and the given context condition is satisfied, then privilege analysis starts capturing the privilege use.
- **Database-wide privilege capture.** If you do not specify any type in your privilege analysis policy, then the used privileges in the database will be captured, except those for the user `SYS`. (This is also referred to as unconditional analysis, because it is turned on without any conditions.)

Note the following restrictions:

- You can enable only one privilege analysis policy at a time. The only exception is that you can enable a database-wide privilege analysis policy at the same time as a non-database-wide privilege analysis policy, such as a role or context attribute-driven analysis policy.
- You cannot analyze the privileges of the `SYS` user.
- Privilege analysis shows the grant paths to the privilege but it does not suggest which grant path to keep.
- If the role, user, or object has been dropped, then the values that reflect the privilege captures for these in the privilege analysis data dictionary views are dropped as well.

### 4.1.5 Benefits and Use Cases of Privilege Analysis

Analyzing privilege use is beneficial in finding unnecessarily granted privileges.

#### [Unnecessarily Granted Privileges of Applications](#) (page 4-4)

The privileges of the account that accesses a database should only be limited to the privileges that are strictly required by the application.

#### [Development of Secure Applications](#) (page 4-4)

During the application development phase, some administrators may grant many powerful system privileges and roles to application developers.

##### **4.1.5.1 Unnecessarily Granted Privileges of Applications**

The privileges of the account that accesses a database should only be limited to the privileges that are strictly required by the application.

But when an application is developed, especially by a third party, more privileges than necessary may be granted to the application connection pool accounts for convenience. In addition, some developers grant system and application object privileges to the `PUBLIC` role.

For example, to select from application data and run application procedures, the system privileges `SELECT ANY TABLE` and `EXECUTE ANY PROCEDURE` are granted to an application account `appsys`. The account `appsys` now can access non-application data even if he or she does not intend to. In this situation, you can analyze the privilege usage by user `appsys`, and then based on the results, revoke and grant privileges as necessary.

##### **4.1.5.2 Development of Secure Applications**

During the application development phase, some administrators may grant many powerful system privileges and roles to application developers.

The administrators may do this because at that stage they may not know what privileges the application developer needs.

Once the application is developed and working, the privileges that the application developer needs — and does not need — become more apparent. At that time, the security administrator can begin to revoke unnecessary privileges. However, the application developer may resist this idea on the basis that the application is currently working without problems. The administrator can use privilege analysis to examine each privilege that the application uses, to ensure that when he or she does revoke any privileges, the application will continue to work.

For example, `app_owner` is an application database user through whom the application connects to a database. User `app_owner` must query tables in the `OE`, `SH`, and `PM` schemas. Instead of granting the `SELECT` object privilege on each of the tables in these schemas, a security administrator grants the `SELECT ANY TABLE` privilege to `app_owner`. After a while, a new schema, `HR`, is created and sensitive data are inserted into `HR.EMPLOYEES` table. Because user `app_owner` has the `SELECT ANY TABLE` privilege, he can query this table to access its sensitive data, which is a security issue. Instead of granting system privileges (particularly the `ANY` privileges), it is far better to grant object privileges for specific tables.

#### **4.1.6 How Does a Multitenant Environment Affect Privilege Analysis?**

You can create and use privilege analysis policies in a multitenant environment.

If you are using a multitenant environment, then you can create privilege analysis policies in either the CDB root or in individual PDBs. The privilege analysis policy applies only to the container in which it is created, either to the privileges used within the CDB root or the application root, or to the privileges used within a PDB. It cannot be applied globally throughout the multitenant environment. You can grant the `CAPTURE_ADMIN` role locally to a local user or a common user. You can grant the `CAPTURE_ADMIN` role commonly to common users.

---

**See Also:**

*Oracle Database Administrator's Guide* for more information about multitenant container databases (CDBs)

---

## 4.2 Creating and Managing Privilege Analysis Policies

You can create and manage privilege analysis policies in either SQL\*Plus or in Enterprise Manager Cloud Control.

[About Creating and Managing Privilege Analysis Policies](#) (page 4-5)

You can use Oracle Enterprise Manager Cloud Control or the DBMS\_PRIVILEGE\_CAPTURE PL/SQL package to analyze privileges.

[General Steps for Managing Privilege Analysis](#) (page 4-6)

You must follow a general set of steps to analyze privileges.

[Creating a Privilege Analysis Policy](#) (page 4-6)

You can create a privilege analysis policy in either Enterprise Manager Cloud Control or from SQL\*Plus, using the DBMS\_PRIVILEGE\_CAPTURE PL/SQL package.

[Examples of Privilege Analysis Policies](#) (page 4-11)

You can create a variety of privilege analysis policies.

[Enabling a Privilege Analysis Policy](#) (page 4-12)

You can enable a privilege analysis policy using either Enterprise Manager Cloud Control or from SQL\*Plus, using the DBMS\_PRIVILEGE\_CAPTURE PL/SQL package.

[Disabling a Privilege Analysis Policy](#) (page 4-14)

You can disable a privilege analysis policy using either Enterprise Manager Cloud Control or from SQL\*Plus, using the DBMS\_PRIVILEGE\_CAPTURE PL/SQL package.

[Generating a Privilege Analysis Report](#) (page 4-15)

You can generate a privilege analysis policy report using either Enterprise Manager Cloud Control or from SQL\*Plus, using the DBMS\_PRIVILEGE\_CAPTURE PL/SQL package.

[Dropping a Privilege Analysis Policy](#) (page 4-18)

You can drop a privilege analysis policy report using either Enterprise Manager Cloud Control or from SQL\*Plus, using the DBMS\_PRIVILEGE\_CAPTURE PL/SQL package.

### 4.2.1 About Creating and Managing Privilege Analysis Policies

You can use Oracle Enterprise Manager Cloud Control or the DBMS\_PRIVILEGE\_CAPTURE PL/SQL package to analyze privileges.

Before you can do so, you must be granted the CAPTURE\_ADMIN role. The DBMS\_PRIVILEGE\_CAPTURE package enables you to create, enable, disable, and drop privilege analysis policies. It also generates reports that show the privilege usage, which you can view in DBA\_\* views.

---



---

**See Also:**

*Oracle Database PL/SQL Packages and Types Reference* for detailed information about the `DBMS_PRIVILEGE_CAPTURE` PL/SQL package

---



---

## 4.2.2 General Steps for Managing Privilege Analysis

You must follow a general set of steps to analyze privileges.

1. Define the privilege analysis policy.
2. Enable the privilege analysis policy.

This step begins recording the privilege use that the policy defined. Optionally, specify a name for this capture run. Each time you enable a privilege analysis policy, you can create a different capture run for it. In this way, you can create multiple named capture runs for comparison analysis later on.

3. Optionally, enable the policy to capture dependency privileges if you want to capture the privileges that are used by definer's rights and invoker's rights program units.
4. After a sufficient period of time to gather data, disable the privilege analysis policy's recording of privilege use.

This step stops capturing the privilege use for the policy.

5. Generate privilege analysis results.

This step writes the results to the data dictionary views described in [Privilege Analysis Policy and Report Data Dictionary Views](#) (page 4-33).

6. Optionally, disable and then drop the privilege analysis policy and capture run.

Dropping a privilege analysis policy deletes the data captured by the policy.

## 4.2.3 Creating a Privilege Analysis Policy

You can create a privilege analysis policy in either Enterprise Manager Cloud Control or from SQL\*Plus, using the `DBMS_PRIVILEGE_CAPTURE` PL/SQL package.

### [About Creating a Privilege Analysis Policy](#) (page 4-6)

When a policy is created, it resides in the Oracle data dictionary and the SYS schema.

### [Creating a Privilege Analysis Policy in Enterprise Manager Cloud Control](#) (page 4-7)

You can create a privilege analysis policy in Cloud Control.

### [Creating a Privilege Analysis Policy Using `DBMS\_PRIVILEGE\_CAPTURE`](#) (page 4-9)

The `DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE` procedure creates a privilege analysis policy.

### 4.2.3.1 About Creating a Privilege Analysis Policy

When a policy is created, it resides in the Oracle data dictionary and the SYS schema.



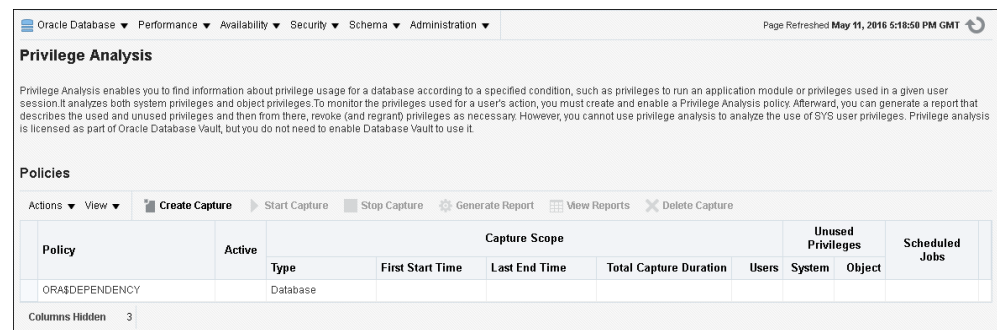
However, both `SYS` and the user who created the policy can drop it. After you create the policy, you must manually enable it so that it can begin to analyze privilege use. If you want to configure privilege analysis by using Oracle Enterprise Manager Cloud Control, then ensure that you have the latest plug-in. For information about how to deploy a plug-in, see *Enterprise Manager Cloud Control Administrator's Guide*.

### 4.2.3.2 Creating a Privilege Analysis Policy in Enterprise Manager Cloud Control

You can create a privilege analysis policy in Cloud Control.

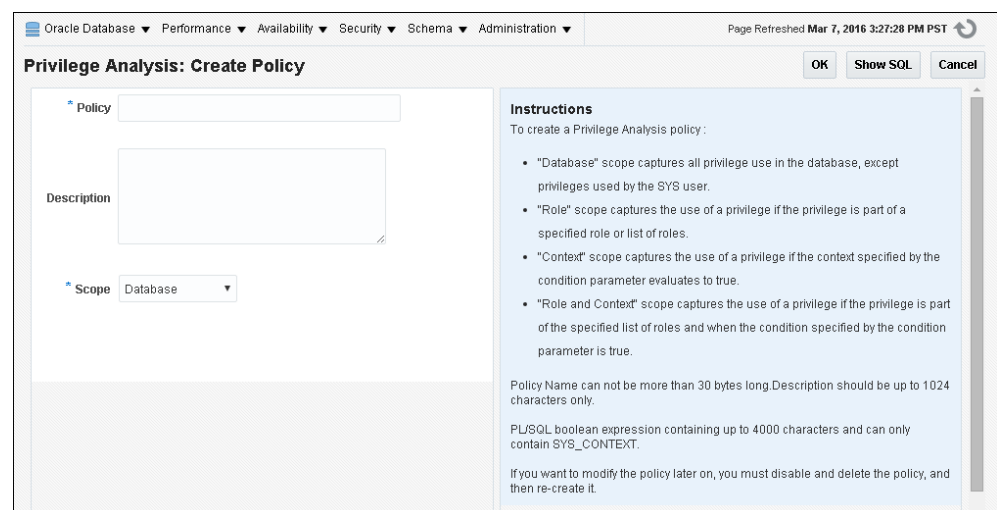
1. Log in to Cloud Control as a user who has been granted the `CAPTURE_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. *Oracle Database 2 Day DBA* explains how to log in.
2. From the **Security** menu, select **Privilege Analysis**.

The Privilege Analysis home page appears.



3. In the Privilege Analysis page, under Policies, select **Create Capture**.

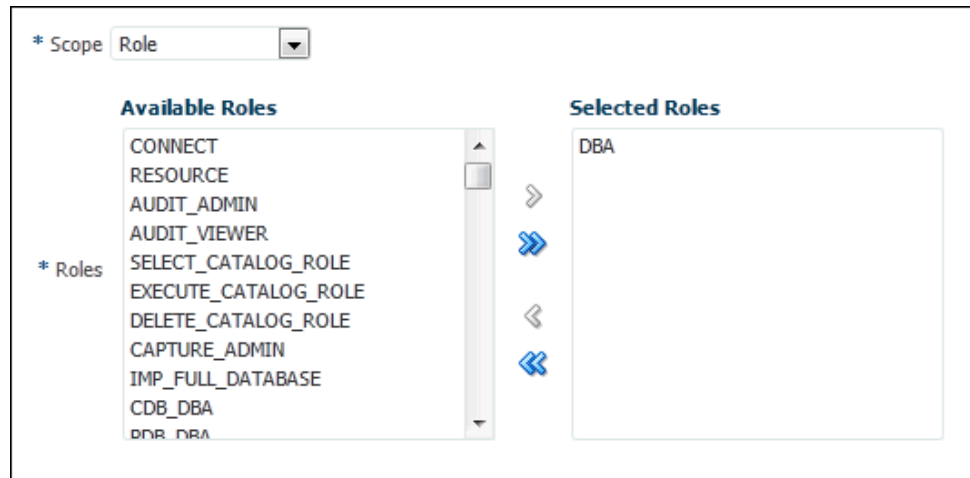
The Privilege Analysis: Create Policy page appears.



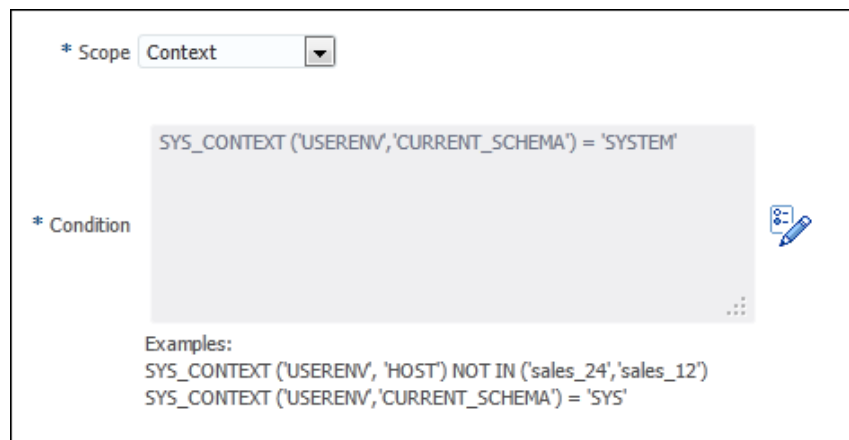
4. Enter the following information:

- **Policy:** Enter a unique name for the privilege analysis policy. You can find the names of existing policies by querying the `NAME` column of the `DBA_PRIV_CAPTURES` view. You can include spaces in the name and have a maximum of 128 characters in this name.

- **Description:** Optionally, enter a description for the policy, in up to 1024 characters.
- **Scope:** Select from the following types:
  - **Database** captures all privileges that were used in the entire database, except privileges from user SYS.
  - **Role** captures privileges from one or more roles that you specify. If the roles in the list are enabled in the database session, then the used privileges for the session will be captured. If you select this option, then the Create Policy page displays the **Available Roles** list.



- **Context** captures privileges when the condition that you specify evaluates to TRUE. If you select this option, then the Capture Policy page displays a **Condition** field. To build the condition, select the edit icon on the right of this field to display the Policy Expression Builder dialog box.



- **Role and Context** captures privileges from one of the specified roles when the context condition evaluates to TRUE. If you select this option, then both the list of available roles and **Condition** field appear.

5. Click **OK**.

The new policy appears in the Policies area of the Privilege Analysis page.

6. To enable the policy so that it can begin to capture privilege use, return to the main Privilege Analysis policy page, select the policy under **Policies**, and then click **Start Capture**.

The Privilege Analysis: Start Capture dialog box appears.

7. Enter the following information to set the time in which the capture will begin:
  - To start the privilege capture process immediately, click **Immediate** and then click the **OK** button.
  - To start the privilege capture at a later date, click **Later**, specify the date and time that you want to capture process to begin, and then click **OK**.

The Privilege Analysis page appears. The time that you set for the policy to begin is listed under **First Start Time** for the policy. If you want to modify the start time, select the policy and click **Start Capture**.

#### 4.2.3.3 Creating a Privilege Analysis Policy Using DBMS\_PRIVILEGE\_CAPTURE

The `DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE` procedure creates a privilege analysis policy.

After you create the privilege analysis policy, you can find it listed in the `DBA_PRIV_CAPTURES` data dictionary view.

- Use the following syntax for the `DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE` procedure:

```
DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
  name           VARCHAR2,
  description    VARCHAR2 DEFAULT NULL,
  type           NUMBER DEFAULT DBMS_PRIVILEGE_CAPTURE.G_DATABASE,
  roles          ROLE_NAME_LIST DEFAULT ROLE_NAME_LIST(),
  condition      VARCHAR2 DEFAULT NULL);
```

In this specification:

- **name**: Specifies the name of the privilege analysis policy to be created. Ensure that this name is unique and no more than 128 characters. You can include spaces in the name, but you must enclose the name in single quotation marks whenever you refer to it. To find the names of existing policies, query the `NAME` column of the `DBA_PRIV_CAPTURES` view.

- `description`: Describes the purpose of the privilege analysis policy, up to 1024 characters in mixed-case letters. Optional.
- `type`: Specifies the type of capture condition. If you omit the `type` parameter, then the default is `DBMS_PRIVILEGE_CAPTURE.G_DATABASE`. Optional.

Enter one of the following types:

- `DBMS_PRIVILEGE_CAPTURE.G_DATABASE`: Captures all privileges used in the entire database, except privileges from user `SYS`.
- `DBMS_PRIVILEGE_CAPTURE.G_ROLE`: Captures privileges for the sessions that have the roles enabled. If you enter `DBMS_PRIVILEGE_CAPTURE.G_ROLE` for the `type` parameter, then you must also specify the `roles` parameter. For multiple roles, separate each role name with a comma.
- `DBMS_PRIVILEGE_CAPTURE.G_CONTEXT`: Captures privileges for the sessions that have the condition specified by the `condition` parameter evaluating to `TRUE`. If you enter `DBMS_PRIVILEGE_CAPTURE.G_CONTEXT` for the `type` parameter, then you must also specify the `condition` parameter.
- `DBMS_PRIVILEGE_CAPTURE.G_ROLE_AND_CONTEXT`: Captures privileges for the sessions that have the role enabled and the context condition evaluating to `TRUE`. If you enter `DBMS_PRIVILEGE_CAPTURE.G_ROLE_AND_CONTEXT` for the `type` parameter, then you must also specify both the `roles` and `condition` parameters.
- `roles`: Specifies the roles whose used privileges will be analyzed. That is, if a privilege from one of the given roles is used, then the privilege will be analyzed. You must specify this argument if you specify `DBMS_PRIVILEGE_CAPTURE.G_ROLE` or `DBMS_PRIVILEGE_CAPTURE.G_ROLE_AND_CONTEXT` for the `type` argument. Each role you enter must exist in the database. (You can find existing roles by querying the `DBA_ROLES` data dictionary view.) For multiple roles, use `varray` type `role_name_list` to enter the role names. You can specify up to 10 roles.

For example, to specify two roles:

```
roles => role_name_list('role1', 'role2'),
```

- `condition`: Specifies a Boolean expression up to 4000 characters. You must specify this argument if you specify `DBMS_PRIVILEGE_CAPTURE.G_CONTEXT` or `DBMS_PRIVILEGE_CAPTURE.G_ROLE_AND_CONTEXT` for the `type` argument. Only `SYS_CONTEXT` expressions with relational operators(`==`, `>`, `>=`, `<`, `<=`, `<>`, `BETWEEN`, and `IN`) are permitted in this Boolean expression.

The `condition` expression syntax is as follows:

```
predicate ::= SYS_CONTEXT(namespace, attribute) relop constant_value |
              SYS_CONTEXT(namespace, attribute)
              BETWEEN
              constant_value
              AND constant_value | SYS_CONTEXT(namespace, attribute)
              IN {constant_value (,constant_value)* }
```

```
relop ::= = | < | <= | > | >= | <>
```

```

context_expression ::= predicate | (context_expression)
                    AND (context_expression) | (context_expression)
                    OR (context_expression )

```

For example, to use a condition to specify the IP address 192.0.2.1:

```
condition => 'SYS_CONTEXT(''USERENV'', ''IP_ADDRESS'')='''192.0.2.1''';
```

\* You can add as many constant values as you need (for example, IN {*constant\_value1*}, or IN {*constant\_value1*, *constant\_value2*, *constant\_value3*}).

Remember that after you create the privilege analysis policy, you must enable it, as described in [Enabling a Privilege Analysis Policy](#) (page 4-12).

## 4.2.4 Examples of Privilege Analysis Policies

You can create a variety of privilege analysis policies.

**Example: Privilege Analysis of Database-Wide Privileges** (page 4-11)

The DBMS\_PRIVILEGE\_CAPTURE.CREATE\_CAPTURE can be used to analyze database-wide privileges.

**Example: Privilege Analysis of Privilege Usage of Two Roles** (page 4-11)

The DBMS\_PRIVILEGE\_CAPTURE.CREATE\_CAPTURE procedure can be used to analyze the privilege usage of multiple roles.

**Example: Privilege Analysis of Privileges During SQL\*Plus Use** (page 4-12)

The DBMS\_PRIVILEGE\_CAPTURE.CREATE\_CAPTURE procedure can be used to capture privileges for analysis.

**Example: Privilege Analysis of PSMITH Privileges During SQL\*Plus Access** (page 4-12)

The DBMS\_PRIVILEGE\_CAPTURE.CREATE\_CAPTURE can be used to analyze user access when the user is running SQL\*Plus.

### 4.2.4.1 Example: Privilege Analysis of Database-Wide Privileges

The DBMS\_PRIVILEGE\_CAPTURE.CREATE\_CAPTURE can be used to analyze database-wide privileges.

[Example 4-1](#) (page 4-11) shows how to use the DBMS\_PRIVILEGE\_CAPTURE package to create and enable a privilege analysis policy to record all privilege use in the database.

#### **Example 4-1 Privilege Analysis of Database-Wide Privileges**

```

BEGIN
  DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
    name          => 'db_wide_capture_pol',
    description   => 'Captures database-wide privileges',
    type          => DBMS_PRIVILEGE_CAPTURE.G_DATABASE);
END;
/
EXEC DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE ('db_wide_capture_pol');

```

### 4.2.4.2 Example: Privilege Analysis of Privilege Usage of Two Roles

The DBMS\_PRIVILEGE\_CAPTURE.CREATE\_CAPTURE procedure can be used to analyze the privilege usage of multiple roles.

[Example 4-2](#) (page 4-12) shows how to analyze the privilege usage of two roles.

**Example 4-2 Privilege Analysis of Privilege Usage of Two Roles**

```

BEGIN
  DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
    name          => 'dba_roles_capture_pol',
    description    => 'Captures DBA and LBAC_DBA role use',
    type           => DBMS_PRIVILEGE_CAPTURE.G_ROLE,
    roles         => role_name_list('dba', 'lbac_dba'));
END;
/
EXEC DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE ('dba_roles_capture_pol');

```

**4.2.4.3 Example: Privilege Analysis of Privileges During SQL\*Plus Use**

The `DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE` procedure can be used to capture privileges for analysis.

[Example 4-3](#) (page 4-12) shows how to analyze privileges used to run SQL\*Plus.

**Example 4-3 Privilege Analysis of Privileges During SQL\*Plus Use**

```

BEGIN
  DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
    name          => 'sqlplus_capture_pol',
    description    => 'Captures privilege use during SQL*Plus use',
    type           => DBMS_PRIVILEGE_CAPTURE.G_CONTEXT,
    condition     => 'SYS_CONTEXT(''USERENV'', ''MODULE'')='''sqlplus''');
END;
/
EXEC DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE ('sqlplus_capture_pol');

```

**4.2.4.4 Example: Privilege Analysis of PSMITH Privileges During SQL\*Plus Access**

The `DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE` can be used to analyze user access when the user is running SQL\*Plus.

[Example 4-4](#) (page 4-12) shows how to analyze the privileges used by session user PSMITH when running SQL\*Plus.

**Example 4-4 Privilege Analysis of PSMITH Privileges During SQL\*Plus Access**

```

BEGIN
  DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
    name          => 'psmith_sqlplus_analysis_pol',
    description    => 'Analyzes PSMITH role priv use for SQL*Plus module',
    type           => DBMS_PRIVILEGE_CAPTURE.G_CONTEXT,
    condition     => 'SYS_CONTEXT(''USERENV'', ''MODULE'')='''sqlplus''
                    AND SYS_CONTEXT(''USERENV'', ''SESSION_USER'')='''PSMITH''');
END;
/
EXEC DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE ('psmith_sqlplus_analysis_pol');

```

**4.2.5 Enabling a Privilege Analysis Policy**

You can enable a privilege analysis policy using either Enterprise Manager Cloud Control or from SQL\*Plus, using the `DBMS_PRIVILEGE_CAPTURE` PL/SQL package.

[About Enabling a Privilege Analysis Policy](#) (page 4-13)

After you create a privilege analysis policy, you must enable it.

[Enabling a Privilege Analysis Policy Using Cloud Control](#) (page 4-13)

You can enable a privilege analysis policy using Cloud Control.

## Enabling a Privilege Analysis Policy Using `DBMS_PRIVILEGE_CAPTURE` (page 4-14)

The `DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE` procedure enables a privilege policy and creates a capture run name for it.

### 4.2.5.1 About Enabling a Privilege Analysis Policy

After you create a privilege analysis policy, you must enable it.

When you enable a privilege analysis policy, you can create a named capture run for the policy's findings. The capture run defines a period of time from when the capture is enabled (begun) and when it is disabled (stopped). This way, you can create multiple runs and then compare them when you generate the privilege capture results. [Tutorial: Using Capture Runs to Analyze ANY Privilege Use](#) (page 4-23) provides an example of how you can create and generate multiple capture runs.

The general process for managing multiple named capture runs is as follows:

1. Create the policy.
2. Enable the policy for the first run.
3. After a period time to collect user behavior data, disable this policy and its run.
4. Generate the results and then query the privilege analysis data dictionary views for information about this capture run.

If you omit the `run_name` parameter from the `DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT` procedure, then this procedure looks at all records as a whole and then analyzes them.

5. Re-enable the policy for the second run. You cannot create a new capture run if the policy has not been disabled first.
6. After you have collected the user data, disable the policy and the second run.
7. Generate the results.
8. Query the privilege analysis data dictionary views. The results from both capture runs are available in the views. If you only want to show the results of one of the capture runs, then you can regenerate the results and requery the privilege analysis views.

Once enabled, the privilege analysis policy will begin to record the privilege usage when the condition is satisfied. At any given time, only one privilege analysis policy in the database can be enabled. The only exception is that a privilege analysis policy of type `DBMS_PRIVILEGE_CAPTURE.G_DATABASE` can be enabled at the same time with a privilege analysis of a different type.

When you drop a privilege analysis policy, its associated capture runs are dropped as well and are not reflected in the privilege analysis data dictionary views.

Restarting a database does not change the status of a privilege analysis. For example, if a privilege analysis policy is enabled before a database shutdown, then the policy is still enabled after the database shutdown and restart.

### 4.2.5.2 Enabling a Privilege Analysis Policy Using Cloud Control

You can enable a privilege analysis policy using Cloud Control.

1. Log in to Cloud Control as a user who has been granted the `CAPTURE_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. *Oracle Database 2 Day DBA* explains how to log in.
2. From the **Security** menu, select **Privilege Analysis**.
3. Under Policies, select the policy that you want to enable.
4. Select the **Start Capture** button.
5. In the Privilege Analysis: Start Capture dialog box, specify a time to begin the privilege analysis policy.

To run the policy now, select **Immediate**. To run the policy later, select **Later**, and then specify the hour, minute, second, and the time zone for the policy to begin.

6. Click **OK**.

#### 4.2.5.3 Enabling a Privilege Analysis Policy Using `DBMS_PRIVILEGE_CAPTURE`

The `DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE` procedure enables a privilege policy and creates a capture run name for it.

The run name defines the period of time that the capture took place.

1. Query the `NAME` and `ENABLED` columns of the `DBA_PRIV_CAPTURES` data dictionary view to find the existing privilege analysis policies and whether they are currently enabled.
2. Run the `DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE` procedure to enable the policy and optionally create a name for a capture run.

For example, to enable the privilege analysis policy `logon_users_analysis`:

```
BEGIN
  DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE (
    name      => 'logon_users_analysis_pol',
    run_name => 'logon_users_04092016');
END;
/
```

## 4.2.6 Disabling a Privilege Analysis Policy

You can disable a privilege analysis policy using either Enterprise Manager Cloud Control or from SQL\*Plus, using the `DBMS_PRIVILEGE_CAPTURE` PL/SQL package.

[About Disabling a Privilege Analysis Policy](#) (page 4-15)

You must disable the privilege analysis policy before you can generate a privilege analysis report.

[Disabling a Privilege Analysis Policy Using Cloud Control](#) (page 4-15)

You can disable a privilege analysis policy using Cloud Control.

[Disabling a Privilege Analysis Policy Using `DBMS\_PRIVILEGE\_CAPTURE`](#) (page 4-15)

The `DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE` procedure disables a privilege analysis policy.



#### 4.2.6.1 About Disabling a Privilege Analysis Policy

You must disable the privilege analysis policy before you can generate a privilege analysis report.

After you disable the policy, then the privileges are no longer recorded. Disabling a privilege analysis policy takes effect immediately for user sessions logged on both before and after the privilege analysis policy is disabled.

#### 4.2.6.2 Disabling a Privilege Analysis Policy Using Cloud Control

You can disable a privilege analysis policy using Cloud Control.

1. Log in to Cloud Control as a user who has been granted the `CAPTURE_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. *Oracle Database 2 Day DBA* explains how to log in.
2. From the **Security** menu, select **Privilege Analysis**.
3. Under Policies, select the policy that you want to disable.
4. Select **Stop Capture**.
5. In the Privilege Analysis: Stop Capture dialog box, do the following: specify a time to stop the privilege analysis policy.
  - a. To stop the policy now, select **Immediate**. To stop the policy later, select **Later**, and then specify the hour, minute, second, and the time zone for the policy to stop.
  - b. To generate a report, click the **Generate Report** button. You can view the reports from the Privilege Analysis page by selecting the policy and clicking **View Reports**.
6. Click **OK**.

#### 4.2.6.3 Disabling a Privilege Analysis Policy Using `DBMS_PRIVILEGE_CAPTURE`

The `DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE` procedure disables a privilege analysis policy.

1. Query the `NAME` and `ENABLED` columns of the `DBA_PRIV_CAPTURES` data dictionary view to find the existing privilege analysis policies and whether they are currently disabled.
2. Run the `DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE` procedure to enable the policy.

For example, to disable the privilege analysis policy `logon_users_analysis`:

```
EXEC DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE ('logon_users_analysis_pol');
```

### 4.2.7 Generating a Privilege Analysis Report

You can generate a privilege analysis policy report using either Enterprise Manager Cloud Control or from SQL\*Plus, using the `DBMS_PRIVILEGE_CAPTURE` PL/SQL package.

[About Generating a Privilege Analysis Report](#) (page 4-16)

After the privilege analysis policy has been disabled, you can generate a report.

[Generating a Privilege Analysis Report Using Cloud Control](#) (page 4-16)

You can generate a privilege analysis report using Cloud Control.

[Accessing Privilege Analysis Reports Using Cloud Control](#) (page 4-16)

A privilege analysis report provides information about both used and unused privileges.

[Generating a Privilege Analysis Report Using DBMS\\_PRIVILEGE\\_CAPTURE](#) (page 4-17)

The `DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT` procedure generates a report showing the results of a privilege capture.

#### 4.2.7.1 About Generating a Privilege Analysis Report

After the privilege analysis policy has been disabled, you can generate a report.

In Enterprise Manager Cloud Control, you can view the reports from the Privilege Analysis page **Actions** menu, and from there, revoke and regrant roles and privileges as necessary. To view the report results in SQL\*Plus, query the data dictionary views in [Privilege Analysis Policy and Report Data Dictionary Views](#) (page 4-33). If a privilege is used during the privilege analysis process and then revoked before you generate the report, then the privilege is still reported as a used privilege, but without the privilege grant path.

#### 4.2.7.2 Generating a Privilege Analysis Report Using Cloud Control

You can generate a privilege analysis report using Cloud Control.

1. Log in to Cloud Control as a user who has been granted the `CAPTURE_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. *Oracle Database 2 Day DBA* explains how to log in.
2. From the **Security** menu, select **Privilege Analysis**.
3. Under Policies, select the policy whose report you want to generate.
4. Select **Generate Report**.
5. In the Privilege Analysis: Generate Report dialog box, specify a time to generate the report.

To generate the report now, select **Immediate**. To generate the report later, select **Later**, and then specify the hour, minute, second, and the time zone for the report to generate.

6. Click **OK**.

In the Privilege Analysis page, a Confirmation message notifies you that a report has been submitted. You can refresh the page until the job is complete. To view the report, select the policy name and then click **View Reports**.

#### 4.2.7.3 Accessing Privilege Analysis Reports Using Cloud Control

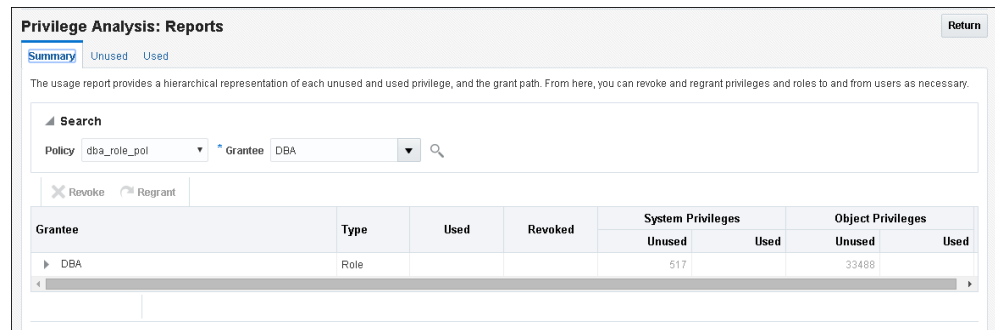
A privilege analysis report provides information about both used and unused privileges.

1. Generate the privilege analysis report.

See [Generating a Privilege Analysis Report Using Cloud Control](#) (page 4-16) for more information.

2. In the Privilege Analysis page, select the policy on which you generated a report.
3. Select **View Reports**.

The Privilege Analysis Reports page appears.



4. To view the report, do the following:

- By default, the selected report will appear, but to search for a report for another policy, use the Search region to find a different report, or to select a different grantee for the currently selected policy.
- To view unused privileges, select the **Unused** tab; to view the used privileges, select **Used**. To view a summary of both, select **Summary**.

From here, you can select roles to revoke or regrant to users as necessary. To do so, under **Grantee**, select the role and then click **Revoke** or **Regrant**.

#### 4.2.7.4 Generating a Privilege Analysis Report Using DBMS\_PRIVILEGE\_CAPTURE

The `DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT` procedure generates a report showing the results of a privilege capture.

1. Query the `NAME` and `ENABLED` columns of the `DBA_PRIV_CAPTURES` data dictionary view to find the existing privilege analysis policies and whether they are currently disabled.

The privilege analysis policy must be disabled before you can generate a privilege analysis report on it.

2. Run the `DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT` procedure using the following syntax:

```
DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT(
  name          VARCHAR2,
  run_name      VARCHAR2 DEFAULT NULL,
  dependency    BOOLEAN DEFAULT NULL);
```

In this specification:

- `name`: Specifies the name of the privilege analysis policy. The `DBA_PRIV_CAPTURES` data dictionary view lists the names of existing policies.

- `run_name`: Specifies the name for the run name for the privilege capture that must be computed. If you omit this setting, then all runs for the given privilege capture are computed.
- `dependency`: Enter Y (yes) or N (no) to specify whether the PL/SQL computation privilege usage should be included in the report.

For example, to generate a report for the privilege analysis policy `logon_users_analysis`:

```
EXEC DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT ('logon_users_analysis');
```

3. Query the used privileges from `DBA_USED_*` data dictionary views with privilege grant paths.

## 4.2.8 Dropping a Privilege Analysis Policy

You can drop a privilege analysis policy report using either Enterprise Manager Cloud Control or from SQL\*Plus, using the `DBMS_PRIVILEGE_CAPTURE` PL/SQL package.

[About Dropping a Privilege Analysis Policy](#) (page 4-18)

Before you can drop a privilege analysis policy, you must first disable it.

[Dropping a Privilege Analysis Policy Using Cloud Control](#) (page 4-18)

You can drop a privilege analysis policy by using Cloud Control.

[Dropping a Privilege Analysis Policy Using the `DBMS\_PRIVILEGE\_CAPTURE` Package](#) (page 4-18)

The `DBMS_PRIVILEGE_CAPTURE.DROP_CAPTURE` procedure drops a privilege analysis policy.

### 4.2.8.1 About Dropping a Privilege Analysis Policy

Before you can drop a privilege analysis policy, you must first disable it.

Dropping a privilege analysis policy also drops all the used and unused privilege records associated with this privilege analysis. If you created capture runs for the policy, they are dropped when you drop the policy.

### 4.2.8.2 Dropping a Privilege Analysis Policy Using Cloud Control

You can drop a privilege analysis policy by using Cloud Control.

1. Log in to Cloud Control as a user who has been granted the `CAPTURE_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. *Oracle Database 2 Day DBA* explains how to log in.
2. From the **Security** menu, select **Privilege Analysis**.
3. Under Policies, select the policy that you want to drop.
4. Select **Delete Capture**.
5. In the Confirmation dialog box, select **Yes**.

### 4.2.8.3 Dropping a Privilege Analysis Policy Using the `DBMS_PRIVILEGE_CAPTURE` Package

The `DBMS_PRIVILEGE_CAPTURE.DROP_CAPTURE` procedure drops a privilege analysis policy.

1. Query the `NAME` and `ENABLE` columns of the `DBA_PRIV_CAPTURES` data dictionary view to find the policy and to check if it is enabled or disabled.
2. If the policy is enabled, then disable it.

For example:

```
EXEC DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE ('logon_users_analysis_pol');
```

3. Run the `DBMS_PRIVILEGE_CAPTURE.DROP_CAPTURE` procedure to drop the policy.

For example:

```
EXEC DBMS_PRIVILEGE_CAPTURE.DROP_CAPTURE ('logon_users_analysis_pol');
```

If you had enabled the policy with a capture run, then the capture run is dropped as well. To individually drop a capture run, you can run the `DBMS_PRIVILEGE_CAPTURE.DELETE_RUN` procedure, but the policy must exist before you can run this statement.

## 4.3 Creating Roles and Managing Privileges Using Cloud Control

You can create new roles using privileges found in a privilege analysis report and then grant this role to users.

[Creating a Role from a Privilege Analysis Report in Cloud Control](#) (page 4-19)

You can use the report summary to find the least number of privileges an application needs, and encapsulate these privileges into a role.

[Revoking and Regranting Roles and Privileges Using Cloud Control](#) (page 4-20)

You can use Enterprise Manager Cloud Control to revoke and regrant roles and privileges to users.

[Generating a Revoke or Regrant Script Using Cloud Control](#) (page 4-20)

You can generate a script that revokes or regrants privileges from and to users, based on the results of privilege analysis reports.

### 4.3.1 Creating a Role from a Privilege Analysis Report in Cloud Control

You can use the report summary to find the least number of privileges an application needs, and encapsulate these privileges into a role.

1. Log in to Cloud Control as a user who has been granted the `CAPTURE_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. *Oracle Database 2 Day DBA* explains how to log in.
2. On the Privilege Analysis page, select the policy name, and then from **Actions** menu, click **Create Role**.
3. On the Create Role page, provide the following details, and then click **OK**:
  - Select the policy from which you would like to create a new role.
  - Enter a unique name for the new role that you want to create.
  - Select the **Used** or **Unused** check box, depending on what your role must encapsulate. The role can have used or unused system and object privileges and roles.

- Select the corresponding radio buttons for **Directly Granted System Privileges**, **Directly Granted Object Privileges**, and **Directly Granted Roles**.

For example, if you select the **Used** check box, and select:

- **All** system privileges, then all the used system privileges captured are included in the new role that you are creating.
- **None** for role, then no role that is captured in the policy will be used in the new role.
- **Customize** object privileges, then a list of available used objects privileges captured are displayed, you need to select the privileges from the list to assign to the role.

### 4.3.2 Revoking and Regranting Roles and Privileges Using Cloud Control

You can use Enterprise Manager Cloud Control to revoke and regrant roles and privileges to users.

1. If Oracle Database Vault is enabled, then ensure that you are authorized as an owner of the Oracle System Privilege and Role Management realm.

In SQL\*Plus, a user who has been granted the DV\_OWNER role can check the authorization by querying the DBA\_DV\_REALM\_AUTH data dictionary view. To grant the user authorization, use the DBMS\_MACADM.ADD\_AUTH\_TO\_REALM procedure.

2. Generate the privilege analysis report.

See [Generating a Privilege Analysis Report Using Cloud Control](#) (page 4-16) for more information.

3. In the Privilege Analysis page, select the policy on which you generated a report.
4. Select **View Reports**.
5. In the Privilege Analysis: Reports page, select the **Summary** tab.
6. Under Search, ensure that the **Policy** and **Grantee** menu options are set.
7. Under the Grantee area, expand the grantee options.

For example, for a role privilege analysis report for a role called HR\_ADMIN role, you would expand the HR\_ADMIN role to show the privileges that are associated with it.

8. Select each privilege to revoke and then click **Revoke**, or select **Regrant** to regrant the privilege to the role.

### 4.3.3 Generating a Revoke or Regrant Script Using Cloud Control

You can generate a script that revokes or regrants privileges from and to users, based on the results of privilege analysis reports.

[About Generating Revoke and Regrant Scripts](#) (page 4-21)

You can perform a bulk revoke of unused system and object privileges and roles by using scripts that you can download after you have generated the privilege analysis.

[Generating a Revoke Script](#) (page 4-21)

You can use Enterprise Manager Cloud Control to generate a script that revokes privileges from users.

[Generating a Regrant Script](#) (page 4-22)

You can use Enterprise Manager Cloud Control to generate a script that regrants privileges that have been revoked from users.

### 4.3.3.1 About Generating Revoke and Regrant Scripts

You can perform a bulk revoke of unused system and object privileges and roles by using scripts that you can download after you have generated the privilege analysis.

Later on, if you want to regrant these privileges back to the user, you can generate a regrant script. In order to generate the regrant script, you must have a corresponding revoke script.

Execute the revoke scripts in a development or test environment. Be aware that you cannot revoke privileges and roles from Oracle-supplied accounts and roles.

### 4.3.3.2 Generating a Revoke Script

You can use Enterprise Manager Cloud Control to generate a script that revokes privileges from users.

1. If Oracle Database Vault is enabled, then ensure that you are authorized as an owner of the Oracle System Privilege and Role Management realm.

In SQL\*Plus, a user who has been granted the DV\_OWNER role can check the authorization by querying the DBA\_DV\_REALM\_AUTH data dictionary view. To grant the user authorization, use the DBMS\_MACADM.ADD\_AUTH\_TO\_REALM procedure.

2. In Enterprise Manager, access the target Database home page as a user who has been granted the CAPTURE\_ADMIN role and the SELECT ANY DICTIONARY privilege.

See *Oracle Database 2 Day DBA* for more information.

3. From the **Security** menu, select **Privilege Analysis**.

4. Ensure that the reports you want have been generated.

See [Generating a Privilege Analysis Report Using Cloud Control](#) (page 4-16) for more information.

5. In the Privilege Analysis page, from the **Actions** menu, select **Revoke Scripts**.

6. On the Revoke Scripts page, click **Generate**.

The generate revoke script details wizard is displayed.

7. In the Script Details page, do the following: select a policy name from the **Policy Name** menu against which the revoke script needs to be prepared.

8. In the **Script Name** field, enter a unique name and for **Description**, a description for the script.

For example, if you want to revoke all the unused privileges, select the **All** option for all the unused privileges and roles, and click **Next**.

Based on your selection, and the available privileges, all the unused system privileges, object privileges, and roles that are going to be revoked are displayed on the respective pages.

9. For **Grantee (user/role)**, select **All** or **Customize**.
10. Select **All**, **None**, or **Customize** for the **Unused System Privileges**, **Unused Object Privileges**, and **Unused Roles** settings.
11. Click **Next**.

The next pages that appear depend on your selections of **All**, **None**, or **Customize**. If you selected **All**, the page displays a listing of the privileges. If you selected **None**, the page is bypassed. If you selected **Customize**, then you can individually select the privileges to revoke. The last page that appears is the Review page.

12. Click **Save**.

The Revoke Scripts page appears.

13. In the Revoke Scripts page, select the newly created SQL script, and then click **Download Revoke Script** to download this script, which contains `REVOKE SQL` statements for each privilege or role.

To view the script, click the **View Revoke Script** button.

14. To return to the Privilege Analysis page, click **Return**.

#### 4.3.3.3 Generating a Regrant Script

You can use Enterprise Manager Cloud Control to generate a script that regrants privileges that have been revoked from users.

1. If Oracle Database Vault is enabled, then ensure that you are authorized as an owner of the Oracle System Privilege and Role Management realm.

In SQL\*Plus, a user who has been granted the `DV_OWNER` role can check the authorization by querying the `DBA_DV_REALM_AUTH` data dictionary view. To grant the user authorization, use the `DBMS_MACADM.ADD_AUTH_TO_REALM` procedure.

2. In Enterprise Manager, access the target Database home page as a user who has been granted the `CAPTURE_ADMIN` role and the `SELECT ANY DICTIONARY` privilege.

See *Oracle Database 2 Day DBA* for more information.

3. From the **Security** menu, select **Privilege Analysis**.
4. Ensure that the reports you want have been generated.

See [Generating a Privilege Analysis Report Using Cloud Control](#) (page 4-16) for more information.

5. In the Privilege Analysis page, select the policy on which the revoke script was based.
6. From the **Actions** menu, select **Revoke Scripts**.



- In the Revoke Scripts page, select the policy name that you had created earlier, and then click **Download Regrant Script** to download this script.

You can view the scripts that are associated with the policy by selecting the **View Revoke Script** and **View Regrant Script** buttons.

## 4.4 Tutorial: Using Capture Runs to Analyze ANY Privilege Use

This tutorial demonstrates how to create capture runs to analyze the use of the READ ANY TABLE system privilege.

### Step 1: Create User Accounts (page 4-23)

You must create two users, one user to create the policy and a second user whose privilege use will be analyzed.

### Step 2: Create and Enable a Privilege Analysis Policy (page 4-24)

The user `pa_admin` must create and enable the privilege analysis policy.

### Step 3: Use the READ ANY TABLE System Privilege (page 4-25)

User `app_user` uses the READ ANY TABLE system privilege.

### Step 4: Disable the Privilege Analysis Policy (page 4-25)

You must disable the policy before you can generate a report that captures the actions of user `app_user`.

### Step 5: Generate and View a Privilege Analysis Report (page 4-25)

With the privilege analysis policy disabled, user `pa_admin` then can generate and view a privilege analysis report.

### Step 6: Create a Second Capture Run (page 4-26)

Next, you are ready to create a second capture run for the `ANY_priv_analysis_pol` privilege analysis policy.

### Step 7: Remove the Components for This Tutorial (page 4-27)

You can remove the components that you created for this tutorial if you no longer need them.

### 4.4.1 Step 1: Create User Accounts

You must create two users, one user to create the policy and a second user whose privilege use will be analyzed.

- Log into the database instance as a user who has been granted the DV\_ACCTMGR role.

For example:

```
sqlplus bea_dvacctmgr
Enter password: password
```

In a multitenant environment, you must connect to the appropriate pluggable database (PDB).

For example:

```
sqlplus bea_dvacctmgr@hrpdb
Enter password: password
```

To find the available PDBs, query the DBA\_PDBS data dictionary view. To check the current PDB, run the `show con_name` command.

If Oracle Database Vault is not enabled, then log into the database instance as a user who has the `CREATE USER` system privilege.

2. Create the following users:

```
CREATE USER pa_admin IDENTIFIED BY password;  
CREATE USER app_user IDENTIFIED BY password;
```

3. Connect as a user who has the privileges to grant roles and system privileges to other users, and who has been granted the owner authorization for the Oracle System Privilege and Role Management realm. (User `SYS` has these privileges by default.)

For example:

```
CONNECT dba_psmith -- Or, CONNECT dba_psmith@hrpdb  
Enter password: password
```

In SQL\*Plus, a user who has been granted the `DV_OWNER` role can check the authorization by querying the `DBA_DV_REALM_AUTH` data dictionary view. To grant the user authorization, use the `DBMS_MACADM.ADD_AUTH_TO_REALM` procedure.

4. Grant the following role and privilege to the users.

```
GRANT CREATE SESSION, CAPTURE_ADMIN TO pa_admin;  
GRANT CREATE SESSION, READ ANY TABLE TO app_user;
```

User `pa_admin` will create the privilege analysis policy that will analyze the `READ ANY TABLE` query that user `app_user` will perform.

## 4.4.2 Step 2: Create and Enable a Privilege Analysis Policy

The user `pa_admin` must create and enable the privilege analysis policy.

1. Connect as user `pa_admin`.

```
CONNECT pa_admin -- Or, CONNECT pa_admin@hrpdb  
Enter password: password
```

2. Create the following privilege analysis policy:

```
BEGIN  
  DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(  
    name      => 'ANY_priv_analysis_pol',  
    description => 'Analyzes system privilege use',  
    type      => DBMS_PRIVILEGE_CAPTURE.G_CONTEXT,  
    condition  => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'')='''APP_USER''';  
  END;  
  /
```

In this example:

- `type` specifies the type of capture condition that is defined by the `condition` parameter, described next. In this policy, the type is a context-based condition.
- `condition` specifies condition using a Boolean expression that must evaluate to `TRUE` for the policy to take effect. In this case, the condition checks if the session user is `app_user`.

3. Enable the policy and create a capture run for it.

```
BEGIN
  DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE (
    name      => 'ANY_priv_analysis_pol',
    run_name  => 'ANY_priv_pol_run_1');
END;
/
```

At this point, the policy is ready to start recording the actions of user `app_user`.

### 4.4.3 Step 3: Use the READ ANY TABLE System Privilege

User `app_user` uses the `READ ANY TABLE` system privilege.

1. Connect as user `app_user`.

```
CONNECT app_user -- Or, CONNECT app_user@hrpdb
Enter password: password
```

2. Query the `HR.EMPLOYEES` table.

```
SELECT FIRST_NAME, LAST_NAME, SALARY FROM HR.EMPLOYEES WHERE SALARY > 12000 ORDER
BY SALARY DESC;
```

FIRST_NAME	LAST_NAME	SALARY
Steven	King	24000
Neena	Kochhar	17000
Lex	De Haan	17000
John	Russell	14000
Karen	Partners	13500
Michael	Hartstein	13000
Shelley	Higgins	12008
Nancy	Greenberg	12008

### 4.4.4 Step 4: Disable the Privilege Analysis Policy

You must disable the policy before you can generate a report that captures the actions of user `app_user`.

1. Connect as user `pa_admin`.

```
CONNECT pa_admin -- Or, CONNECT pa_admin@hrpdb
Enter password: password
```

2. Disable the `ANY_priv_analysis_pol` privilege policy.

```
EXEC DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE ('ANY_priv_analysis_pol');
```

### 4.4.5 Step 5: Generate and View a Privilege Analysis Report

With the privilege analysis policy disabled, user `pa_admin` then can generate and view a privilege analysis report.

1. As user `pa_admin`, generate the privilege analysis results.

```
BEGIN
  DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT (
    name      => 'ANY_priv_analysis_pol',
    run_name  => 'ANY_priv_pol_run_1');
```

```
END;
/
```

The generated results are stored in the privilege analysis data dictionary views, which are described in [Privilege Analysis Policy and Report Data Dictionary Views](#) (page 4-33).

2. Enter the following commands to format the data dictionary view output:

```
col username format a10
col sys_priv format a16
col object_owner format a13
col object_name format a23
col run_name format a27
```

3. Find the system privileges that `app_user` used and the objects on which he used them during the privilege analysis period.

```
SELECT SYS_PRIV, OBJECT_OWNER, OBJECT_NAME, RUN_NAME FROM DBA_USED_PRIVS WHERE
USERNAME = 'APP_USER';
```

Output similar to the following appears. The first row shows that `app_user` used the `READ ANY TABLE` privilege on the `HR.EMPLOYEES` table.

SYS_PRIV	OBJECT_OWNER	OBJECT_NAME	RUN_NAME
	SYSTEM	PRODUCT_PRIVS	ANY_PRIV_POL_RUN_1
	SYS	DUAL	ANY_PRIV_POL_RUN_1
	SYS	DUAL	ANY_PRIV_POL_RUN_1
CREATE SESSION			ANY_PRIV_POL_RUN_1
	SYS	DBMS_APPLICATION_INFO	ANY_PRIV_POL_RUN_1
READ ANY TABLE	HR	EMPLOYEES	ANY_PRIV_POL_RUN_1

At this stage, the privilege analysis results remain available in the privilege analysis data dictionary views, even if you create additional capture runs in the future.

#### 4.4.6 Step 6: Create a Second Capture Run

Next, you are ready to create a second capture run for the `ANY_priv_analysis_pol` privilege analysis policy.

1. As user `pa_admin`, enable the `ANY_priv_analysis_pol` privilege analysis policy to use capture run `ANY_priv_pol_run_1`.

```
BEGIN
  DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE (
    name      => 'ANY_priv_analysis_pol',
    run_name  => 'ANY_priv_pol_run_2');
END;
/
```

2. Connect as user `app_user`.

```
CONNECT app_user -- Or, CONNECT app_user@hrpdb
Enter password: password
```

3. Query the `HR.JOBS` table.

```
SELECT MAX_SALARY FROM HR.JOBS WHERE MAX_SALARY > 20000;
```

4. Connect as user `pa_admin`.

```
CONNECT pa_admin -- Or, CONNECT pa_admin@hrpdb
Enter password: password
```

5. Disable the `ANY_priv_analysis_pol` privilege policy.

```
EXEC DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE ('ANY_priv_analysis_pol');
```

6. Generate a second privilege analysis report.

```
BEGIN
  DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT (
    name      => 'ANY_priv_analysis_pol',
    run_name  => 'ANY_priv_pol_run_2');
END;
/
```

7. Find the system privileges that `app_user` used and the objects on which he used them during the privilege analysis period.

```
SELECT SYS_PRIV, OBJECT_OWNER, OBJECT_NAME, RUN_NAME FROM DBA_USED_PRIVS WHERE
USERNAME = 'APP_USER' ORDER BY RUN_NAME;
```

Output similar to the following appears, which now shows the results of both of the capture runs that user `pa_admin` created.

SYS_PRIV	OBJECT_OWNER	OBJECT_NAME	RUN_NAME
READ ANY TABLE	HR	EMPLOYEES	ANY_PRIV_POL_RUN_1
	SYS	DUAL	ANY_PRIV_POL_RUN_1
CREATE SESSION			ANY_PRIV_POL_RUN_1
	SYS	DUAL	ANY_PRIV_POL_RUN_1
	SYSTEM	PRODUCT_PRIVS	ANY_PRIV_POL_RUN_1
	SYS	DBMS_APPLICATION_INFO	ANY_PRIV_POL_RUN_1
	SYS	DUAL	ANY_PRIV_POL_RUN_2
	SYS	DBMS_APPLICATION_INFO	ANY_PRIV_POL_RUN_2
READ ANY TABLE	SYSTEM	PRODUCT_PRIVS	ANY_PRIV_POL_RUN_2
	SYS	DUAL	ANY_PRIV_POL_RUN_2
	HR	JOBS	ANY_PRIV_POL_RUN_2

#### 4.4.7 Step 7: Remove the Components for This Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. As user `pa_admin`, drop the `ANY_priv_analysis_pol` privilege analysis policy and its associated capture runs.

```
EXEC DBMS_PRIVILEGE_CAPTURE.DROP_CAPTURE ('ANY_priv_analysis_pol');
```

Any capture runs that are associated with this policy are dropped automatically when you run the `DBMS_PRIVILEGE_CAPTURE.DROP_CAPTURE` procedure.

Even though in the next steps you will drop the `pa_admin` user, including any objects created in this user's schema, you must manually drop the `ANY_priv_analysis_pol` privilege analysis policy because this object resides in the `SYS` schema.

2. Connect as the user who created the user accounts. If Oracle Database Vault is enabled, then connect as the Oracle Database Vault Account Manager.

For example:

```
CONNECT bea_dvacctmgr -- Or, CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

3. Drop the users `pa_admin` and `app_user`.

```
DROP USER pa_admin;
DROP USER app_user;
```

## 4.5 Tutorial: Analyzing Privilege Use by a User Who Has the DBA Role

This tutorial demonstrates how to analyze the privilege use of a user who has the DBA role and performs database tuning operations.

### Step 1: Create User Accounts (page 4-28)

You must create two users, one to create the privilege analysis policy and a second user whose privilege use will be analyzed.

### Step 2: Create and Enable a Privilege Analysis Policy (page 4-29)

User `pa_admin` must create the and enable the privilege analysis policy.

### Step 3: Perform the Database Tuning Operations (page 4-30)

User `t_jones` uses the DBA role to perform database tuning operations.

### Step 4: Disable the Privilege Analysis Policy (page 4-30)

You must disable the policy before you can generate a report that captures the actions of user `t_jones`.

### Step 5: Generate and View Privilege Analysis Reports (page 4-31)

With the privilege analysis policy disabled, user `pa_admin` can generate and view privilege analysis reports.

### Step 6: Remove the Components for This Tutorial (page 4-32)

You can remove the components that you created for this tutorial if you no longer need them.

### 4.5.1 Step 1: Create User Accounts

You must create two users, one to create the privilege analysis policy and a second user whose privilege use will be analyzed.

1. Log into the database instance as a user who has been granted the `DV_ACCTMGR` role.

For example:

```
sqlplus bea_dvacctmgr
Enter password: password
```

In a multitenant environment, you must log into the appropriate pluggable database (PDB).

For example:

```
sqlplus bea_dvacctmgr@hrpdb
Enter password: password
```

To find the available PDBs, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

If Oracle Database Vault is not enabled, then log into the database instance as a user who has the `CREATE USER` system privilege.

**2. Create the following users:**

```
CREATE USER pa_admin IDENTIFIED BY password;
CREATE USER tjones IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace *password* with a password that is secure.

**3. Connect as a user who has the privileges to grant roles and system privileges to other users, and who has been granted the owner authorization for the Oracle System Privilege and Role Management realm. (User SYS has these privileges by default.)**

For example:

```
CONNECT dba_psmith -- Or, CONNECT dba_psmith@hrpdb
Enter password: password
```

In SQL\*Plus, a user who has been granted the DV\_OWNER role can check the authorization by querying the DBA\_DV\_REALM\_AUTH data dictionary view. To grant the user authorization, use the DBMS\_MACADM.ADD\_AUTH\_TO\_REALM procedure.

**4. Grant the following roles and privileges to the users.**

```
GRANT CREATE SESSION, CAPTURE_ADMIN TO pa_admin;
GRANT CREATE SESSION, DBA TO tjones;
```

User *pa\_admin* will create the privilege analysis policy that will analyze the database tuning operations that user *tjones* will perform.

**4.5.2 Step 2: Create and Enable a Privilege Analysis Policy**

User *pa\_admin* must create the and enable the privilege analysis policy.

**1. Connect as user *pa\_admin*.**

```
CONNECT pa_admin -- Or, CONNECT pa_admin@hrpdb
Enter password: password
```

If Oracle Database Vault is enabled, then log in as the Database Vault Account Manager, who has the DV\_ACCTMGR role. Ensure that you are the owner of the Oracle System Privilege and Role Management realm.

**2. Create the following privilege analysis policy:**

```
BEGIN
DBMS_PRIVILEGE_CAPTURE.CREATE_CAPTURE(
  name           => 'dba_tuning_priv_analysis_pol',
  description    => 'Analyzes DBA tuning privilege use',
  type           => DBMS_PRIVILEGE_CAPTURE.G_CONTEXT,
  condition      => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'')='''TJONES''';
END;
/
```

In this example:

- `type` specifies the type of capture condition that is defined by the `condition` parameter, described next. In this policy, the type is a context-based condition.

- `condition` specifies condition using a Boolean expression that must evaluate to `TRUE` for the policy to take effect. In this case, the condition checks if the session user is `tjones`.

3. Enable the policy.

```
EXEC DBMS_PRIVILEGE_CAPTURE.ENABLE_CAPTURE ('dba_tuning_priv_analysis_pol');
```

At this point, the policy is ready to start recording the actions of user `tjones`.

### 4.5.3 Step 3: Perform the Database Tuning Operations

User `tjones` uses the DBA role to perform database tuning operations.

1. Connect as user `tjones`.

```
CONNECT tjones -- Or, CONNECT tjones@hrpdb  
Enter password: password
```

2. Run the following script to create the `PLAN_TABLE` table.

```
@$ORACLE_HOME/rdbms/admin/utlxplan.sql
```

The location of this script may vary depending on your operating system. This script creates the `PLAN_TABLE` table in the `tjones` schema.

3. Run the following `EXPLAIN PLAN SQL` statement on the `HR.EMPLOYEES` table:

```
EXPLAIN PLAN  
SET STATEMENT_ID = 'Raise in Tokyo'  
INTO PLAN_TABLE  
FOR UPDATE HR.EMPLOYEES  
SET SALARY = SALARY * 1.10  
WHERE DEPARTMENT_ID =  
  (SELECT DEPARTMENT_ID FROM HR.DEPARTMENTS WHERE LOCATION_ID = 110);
```

Next, user `tjones` will analyze the `HR.EMPLOYEES` table.

4. Run either of the following scripts to create the `CHAINED_ROWS` table

```
@$ORACLE_HOME/rdbms/admin/utlchain.sql
```

Or

```
@$ORACLE_HOME/rdbms/admin/utlchn1.sql
```

5. Run the `ANALYZE TABLE` statement on the `HR.EMPLOYEES` table.

```
ANALYZE TABLE HR.EMPLOYEES LIST CHAINED ROWS INTO CHAINED_ROWS;
```

### 4.5.4 Step 4: Disable the Privilege Analysis Policy

You must disable the policy before you can generate a report that captures the actions of user `tjones`.

1. Connect as user `pa_admin`.

```
CONNECT pa_admin -- Or, CONNECT pa_admin@hrpdb  
Enter password: password
```

2. Disable the `dba_tuning_priv_analysis_pol` privilege policy.



```
EXEC DBMS_PRIVILEGE_CAPTURE.DISABLE_CAPTURE ('dba_tuning_priv_analysis_pol');
```

### 4.5.5 Step 5: Generate and View Privilege Analysis Reports

With the privilege analysis policy disabled, user `pa_admin` can generate and view privilege analysis reports.

1. As user `pa_admin`, generate the privilege analysis results.

```
EXEC DBMS_PRIVILEGE_CAPTURE.GENERATE_RESULT ('dba_tuning_priv_analysis_pol');
```

The generated results are stored in the privilege analysis data dictionary views, which are described in [Privilege Analysis Policy and Report Data Dictionary Views](#) (page 4-33).

2. Enter the following commands to format the data dictionary view output:

```
col username format a8
col sys_priv format a18
col used_role format a20
col path format a150
col obj_priv format a10
col object_owner format a10
col object_name format a10
col object_type format a10
```

3. Find the system privileges and roles that user `tjones` used during the privilege analysis period.

```
SELECT USERNAME, SYS_PRIV, USED_ROLE, PATH
FROM DBA_USED_SYSPRIVS_PATH
WHERE USERNAME = 'TJONES'
ORDER BY 1, 2, 3;
```

Output similar to the following appears:

```
USERNAME SYS_PRIV          USED_ROLE
-----
PATH
-----
TJONES  ANALYZE ANY          IMP_FULL_DATABASE
GRANT_PATH('TJONES', 'DBA')

TJONES  ANALYZE ANY          IMP_FULL_DATABASE
GRANT_PATH('TJONES', 'DBA', 'IMP_FULL_DATABASE')

TJONES  ANALYZE ANY          IMP_FULL_DATABASE
GRANT_PATH('TJONES', 'DBA', 'DATAPUMP_IMP_FULL_DATABASE', 'IMP_FULL_DATABASE')
...
```

4. Find the object privileges and roles that user `tjones` used during the privilege analysis period.

```
col username format a9
col used_role format a10
col object_name format a22
col object_type format a12

SELECT USERNAME, OBJ_PRIV, USED_ROLE,
OBJECT_OWNER, OBJECT_NAME, OBJECT_TYPE
FROM DBA_USED_OBJPRIVS
```

```
WHERE USERNAME = 'TJONES'
ORDER BY 1, 2, 3, 4, 5, 6;
```

Output similar to the following appears:

USERNAME	OBJ_PRIV	USED_ROLE	OBJECT_OWN	OBJECT_NAME	OBJECT_TYPE
TJONES	EXECUTE	PUBLIC	SYS	DBMS_APPLICATION_INFO	PACKAGE
TJONES	SELECT	PUBLIC	SYS	DUAL	TABLE
TJONES	SELECT	PUBLIC	SYS	DUAL	TABLE
TJONES	SELECT	PUBLIC	SYSTEM	PRODUCT_PRIVS	VIEW
...					

5. Find the unused system privileges for user t jones.

```
col username format a9
col sys_priv format a35

SELECT USERNAME, SYS_PRIV
FROM DBA_UNUSED_SYSPRIVS
WHERE USERNAME = 'TJONES'
ORDER BY 1, 2;
```

USERNAME	SYS_PRIV
TJONES	ADMINISTER ANY SQL TUNING SET
TJONES	ADMINISTER DATABASE TRIGGER
TJONES	ADMINISTER RESOURCE MANAGER
TJONES	ADMINISTER SQL TUNING SET
TJONES	ALTER ANY ASSEMBLY
TJONES	ON COMMIT REFRESH
...	

## 4.5.6 Step 6: Remove the Components for This Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. As user pa\_admin, drop the dba\_tuning\_priv\_analysis\_pol privilege analysis policy.

```
EXEC DBMS_PRIVILEGE_CAPTURE.DROP_CAPTURE ('dba_tuning_priv_analysis_pol');
```

Even though in the next steps you will drop the pa\_admin user, including any objects created in this user's schema, you must manually drop the dba\_tuning\_priv\_analysis\_pol privilege analysis policy because this object resides in the SYS schema.

2. Connect as the user who created the user accounts. If Oracle Database Vault is enabled, then connect as the Oracle Database Vault Account Manager.

For example:

```
CONNECT bea_dvacctmgr -- Or, CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

3. Drop the users pa\_admin and t jones.

```
DROP USER pa_admin;
DROP USER tjones CASCADE;
```

## 4.6 Privilege Analysis Policy and Report Data Dictionary Views

Oracle Database provides data dictionary views that show information about analyzed privileges.

[Table 4-1](#) (page 4-33) lists these data dictionary views.

**Table 4-1 Data Dictionary Views That Display Privilege Analysis Information**

View	Description
DBA_PRIV_CAPTURES	Lists information about existing privilege analysis policies
DBA_USED_PRIVS	Lists the privileges and capture runs that have been used for reported privilege analysis policies
DBA_UNUSED_GRANTS	Lists the privilege grants that have not been used
DBA_UNUSED_PRIVS	Lists the privileges and capture runs that have not been used for reported privilege analysis policies
DBA_USED_OBJPRIVS	Lists the object privileges and capture runs that have been used for reported privilege analysis policies. It does not include the object grant paths.
DBA_UNUSED_OBJPRIVS	Lists the object privileges and capture runs that have not been used for reported privilege analysis policies. It does not include the object privilege grant paths.
DBA_USED_OBJPRIVS_PATH	Lists the object privileges and capture runs that have been used for reported privilege analysis policies. It includes the object privilege grant paths.
DBA_UNUSED_OBJPRIVS_PATH	Lists the object privileges and capture runs that have not been used for reported privilege analysis policies. It includes the object privilege grant paths.
DBA_USED_SYSPRIVS	Lists the system privileges and capture runs that have been used for reported privilege analysis policies. It does not include the system privilege grant paths.
DBA_UNUSED_SYSPRIVS	Lists the system privileges and capture runs that have not been used for reported privilege analysis policies. It does not include the system privilege grant paths.
DBA_USED_SYSPRIVS_PATH	Lists the system privileges and capture runs that have been used for reported privilege analysis policies. It includes the system privilege grant paths.

**Table 4-1 (Cont.) Data Dictionary Views That Display Privilege Analysis Information**

<b>View</b>	<b>Description</b>
DBA_UNUSED_SYSPRIVS_PATH	Lists the system privileges and capture runs that have not been used for reported privilege analysis policies. It includes system privilege grant paths
DBA_USED_PUBPRIVS	Lists all the privileges and capture runs for the PUBLIC role that have been used for reported privilege analysis policies
DBA_USED_USERPRIVS	Lists the user privileges and capture runs that have been used for reported privilege analysis policies. It does not include the user privilege grant paths.
DBA_UNUSED_USERPRIVS	Lists the user privileges and capture runs that have not been used for reported privilege analysis policies. It does not include the user privilege grant paths.
DBA_USED_USERPRIVS_PATH	Lists the user privileges and capture runs that have been used for reported privilege analysis policies. It includes the user privilege grant paths.
DBA_UNUSED_USERPRIVS_PATH	Lists the privileges and capture runs that have not been used for reported privilege analysis policies. It includes the user privilege grant paths.

---

**See Also:**

*Oracle Database Reference* for a detailed description of these data dictionary views

---

---

## Configuring Realms

You can create a realm around database objects to protect them, and then set authorizations to control user access to this data.

### [What Are Realms?](#) (page 5-2)

Realms enable you to protect database objects, including specific object types.

### [Default Realms](#) (page 5-5)

Oracle Database Vault provides default realms, which are regular realms, not mandatory realms.

### [Creating a Realm](#) (page 5-8)

To enable realm protection, you create the realm and configure it to include realm-secured objects, roles, and authorizations.

### [About Realm-Secured Objects](#) (page 5-12)

Realm-secured objects define the territory—a set of schema and database objects and roles—that a realm protects.

### [About Realm Authorization](#) (page 5-13)

Realm authorizations establish the set of database accounts and roles that manage or access objects protected in realms.

### [Realm Authorizations in a Multitenant Environment](#) (page 5-13)

In a multitenant environment, the rules and behavior for common realm authorizations are similar to the authorizations for other common objects.

### [Modifying the Enablement Status of a Realm](#) (page 5-14)

You can disable or enable a realm, or set the realm to use simulation mode, from Enterprise Manager Cloud Control.

### [Deleting a Realm](#) (page 5-15)

You can use Enterprise Manager Cloud Control to delete realms.

### [How Realms Work](#) (page 5-15)

When an appropriately privileged database account issues a SQL statement that affects an object within a realm, a special set of activities occur.

### [How Authorizations Work in a Realm](#) (page 5-17)

Realm authorizations prevent users from performing activities if the users do not have the correct privileges.

### [Access to Objects That Are Protected by a Realm](#) (page 5-19)

You can protect an object by a realm, but still enable access to objects that are part of this realm-protected object.

[Example of How Realms Work](#) (page 5-19)

Realms can provide protection in which two users who each have the same privileges must have separate access levels for an object.

[How Realms Affect Other Oracle Database Vault Components](#) (page 5-20)

Realms have no effect on factors, identities, or rule sets, but they do affect command rules.

[Guidelines for Designing Realms](#) (page 5-20)

Oracle provides a set of guidelines for designing realms.

[How Realms Affect Performance](#) (page 5-21)

Realms can affect database performance in a variety of situations, such as with DDL and DML operations.

[Realm Related Reports and Data Dictionary Views](#) (page 5-22)

Oracle Database Vault provides reports and data dictionary views that are useful for analyzing realms.

## 5.1 What Are Realms?

Realms enable you to protect database objects, including specific object types.

[About Realms](#) (page 5-2)

A realm is a grouping of database schemas, database objects, and database roles that must be secured for a given application.

[Mandatory Realms to Restrict User Access to Objects within a Realm](#)  
(page 5-3)

By default, users who own or have object privileges are allowed to access realm-protected objects without explicit realm authorization.

[Realms in a Multitenant Environment](#) (page 5-5)

In a multitenant environment, you can create a realm to protect common objects in the application root.

[Object Types That Realms Can Protect](#) (page 5-5)

You can create realms around all objects in a schema of certain object types.

### 5.1.1 About Realms

A realm is a grouping of database schemas, database objects, and database roles that must be secured for a given application.

Think of a realm as a zone of protection for your database objects. A schema is a logical collection of database objects such as tables, views, and packages, and a role is a collection of privileges. By arranging schemas and roles into functional groups, you can control the ability of users to use system privileges against these groups and prevent unauthorized data access by the database administrator or other powerful users with system privileges. Oracle Database Vault does not replace the discretionary access control model in the existing Oracle database. It functions as a layer on top of this model for both realms and command rules.

Oracle Database Vault provides two types of realms: regular and mandatory. A regular realm protects an entire database object (such as a schema). A mandatory realm restricts user access to objects within a realm. Mandatory realms block both object privilege-based and system privilege-based access. In other words, even an

object owner cannot access his or her own objects without proper realm authorization if the objects are protected by mandatory realms.

For databases that use Oracle Flashback Technology, then both regular and mandatory realms will enforce the same behavior for a flashback table. Users can execute a `FLASHBACK TABLE` SQL statement on a realm-protected table if the user is authorized to the realm.

For databases that use Information Lifecycle Management (ILM), a Database Vault administrator can use the `DBMS_MACADM.AUTHORIZE_MAINTENANCE_USER` and `DBMS_MACADM.UNAUTHORIZE_MAINTENANCE_USER` procedure to control who can perform ILM operations on realm-protected objects.

You can register schemas, all objects of a certain type in a schema, or individual objects within a schema into a realm. After you create a realm, you can register a set of schema objects or roles (secured objects) for realm protection and authorize a set of users or roles to access the secured objects.

For example, you can create a realm to protect all existing database schemas that are used in an accounting department. The realm prohibits any user who is not authorized to the realm to use system privileges to access the secured accounting data. When an entire schema is protected, all objects in the schema are protected, including tables, indexes, procedures and other objects.

You can run reports on realms that you create in Oracle Database Vault. You can use simulation mode during development, test, and even production phases to log only realm violations instead of blocking access. This enables you to quickly test applications using Database Vault realms.

You can configure realms by using the Oracle Database Vault Administrator pages in Oracle Enterprise Manager Cloud Control. Alternatively, you can configure realms by using the PL/SQL interfaces and packages provided by Oracle Database Vault.

#### Related Topics:

[Oracle Database Vault Realm APIs](#) (page 15-1)

The `DBMS_MACADM` PL/SQL package enables you to configure Oracle Database Vault realms.

### 5.1.2 Mandatory Realms to Restrict User Access to Objects within a Realm

By default, users who own or have object privileges are allowed to access realm-protected objects without explicit realm authorization.

You optionally can configure the realm to prevent these users' access by configuring it to be a mandatory realm. Mandatory realms block system privilege-based access as well as object privilege-based access. This means that even the object owner cannot have access if he or she is not authorized to access the realm. Users can access secured objects in the mandatory realm only if the user or role is authorized to do so.

Mandatory realms have the following additional characteristics:

- If there are multiple mandatory realms on the same object, then you must authorize the user or role on all the mandatory realms before they can access the protected object.
- If a role is protected by a mandatory realm, then no privileges can be granted to or revoked from the protected role except by the realm owner.

- You can update regular realms that you created in earlier releases to be mandatory realms. This way, you can block owner access and object-privileged users from accessing the realm-protected objects.

Mandatory realms have the following benefits:

- **Mandatory realms can block object owners and object privileged users.** In previous releases, blocking these users could only be done by defining complicated command rules.
- **Mandatory realms provide more flexible configurations for access control.** For example, suppose you want to enable a user to access an object with certain conditions, such as in a specific time range during the day. You cannot grant object privileges to that user because realms do not block object privileges. You only can grant system privileges to the user and then authorize this user to the realm with a rule, or make a command rule on the command directly. These solutions are either very expensive in terms of computational cost or undesirable because they entail the excessive granting of privileges such as system privileges to the user. With a mandatory realm, you only need to grant object privileges to the user, with a rule for specific conditions, and then authorize this user to be a realm owner or participant. Thus, with mandatory realms, Oracle Database Vault policies have more flexibility without granting users excessive privileges.
- **Mandatory realms add a layer of protection during patch upgrades.** During a patch upgrade, a database administrator may need to have direct access to a realm-protected object in order to perform a patch on the object. If there are tables that contain sensitive data, such as social security numbers, you can protect these tables from the administrator's access with mandatory realms during the patch upgrade. When patching is complete, and the database administrator no longer needs access to the objects, you can disable mandatory realm protection and then re-enable the normal application realm protection so that the application protection can return to its normal state.
- **You can use mandatory realms to secure tables during runtime.** During runtime, application data can be stored in many tables. It is better to have a single user such as a runtime schema to access these tables so that you can maintain the integrity and correctness of the data. If the application data is scattered in many different schemas, then schema owners and users with object privileges can change the data if they log into the database directly. To insure that users cannot update these tables without going through the runtime schema's procedures, you can use mandatory realms to protect the tables so that only the authorized user's procedures can access them. Because a regular realm does not block object owners and object-privileged users, you can use mandatory realms to block them. This way, only authorized users can access these tables during runtime.
- **You can freeze security settings by preventing changes to configured roles.**

**Related Topics:**

[CREATE\\_REALM Procedure](#) (page 15-5)

The `CREATE_REALM` procedure creates a realm. In a multitenant environment, you can create both common and local realms.

[UPDATE\\_REALM Procedure](#) (page 15-11)

The `UPDATE_REALM` procedure updates a realm.



### 5.1.3 Realms in a Multitenant Environment

In a multitenant environment, you can create a realm to protect common objects in the application root.

The advantage of creating a realm in the application root instead of creating a large number of objects and realms around these objects within individual pluggable databases (PDBs) is that you can create them in one place, the application root. This way, you can manage them centrally.

You cannot create a common realm in the CDB root.

A Database Vault common realm can be either a regular realm or a mandatory realm. The realm protects only objects within the application root, not local objects in a PDB. The CDB root, application root, and any affected PDBs all must be Database Vault enabled.

To configure a common realm, you must be commonly granted the DV\_OWNER or DV\_ADMIN role. To grant common authorizations for a common realm, you must be in the application root. To propagate the realm to the PDBs that are associated with the application root, you must synchronize the application root. For example, to synchronize an application called `saas_sales_app`

```
ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;
```

#### Related Topics:

[About Realm Authorization](#) (page 5-13)

Realm authorizations establish the set of database accounts and roles that manage or access objects protected in realms.

### 5.1.4 Object Types That Realms Can Protect

You can create realms around all objects in a schema of certain object types.

These object types are as follows:

Object Types C-J	Object Types L-P	Object Types R-V
CLUSTER	LIBRARY	ROLE
DIMENSION	MATERIALIZED VIEW	SEQUENCE
FUNCTION	MATERIALIZED VIEW LOG	SYNONYM
INDEX	OPERATOR	TABLE
INDEX PARTITION	PACKAGE	TRIGGER
INDEXTYPE	PROCEDURE	TYPE
JOB	PROGRAM	VIEW

## 5.2 Default Realms

Oracle Database Vault provides default realms, which are regular realms, not mandatory realms.

[Oracle Database Vault Realm](#) (page 5-6)

The Oracle Database Vault realm protects configuration and role information in the Oracle Database Vault DVSYS, DVF, and LBACSYS schemas.

[Database Vault Account Management Realm](#) (page 5-7)

The Database Vault Account Management realm defines the realm for the administrators who manage and create database accounts and database profiles.

[Oracle Enterprise Manager Realm](#) (page 5-7)

Oracle Database Vault provides a realm specifically for Oracle Enterprise Manager accounts.

[Oracle Default Schema Protection Realm](#) (page 5-7)

Oracle Default Schema Protection Realm protects roles and schemas that are used with Oracle features such as Oracle Text.

[Oracle System Privilege and Role Management Realm](#) (page 5-8)

Oracle System Privilege and Role Management Realm protects sensitive roles that are used to export and import data in an Oracle database.

[Oracle Default Component Protection Realm](#) (page 5-8)

Oracle Default Component Protection Realm protects the SYSTEM and OUTLN schemas.

## 5.2.1 Oracle Database Vault Realm

The Oracle Database Vault realm protects configuration and role information in the Oracle Database Vault DVSYS, DVF, and LBACSYS schemas.

The owners of all three of the DVSYS, DVF, and LBACSYS schemas are owners of this realm.

This realm protects the following objects:

- Entire schemas that are protected: DVSYS, DVF, LABACSYS
- Roles that are protected:

Schemas DV_A-DV_S	Schemas DV_P-L	Schemas DV_G-DV_X
DV_ADMIN	DV_MONITOR	DV_GOLDENGATE_ADMIN
DV_AUDIT_CLEANUP	DV_PATCH_ADMIN	DV_GOLDENGATE_REDO_ACCESS
DV_DATAPUMP_NETWORK_LINK	DV_PUBLIC	DV_XSTREAM_ADMIN
DV_OWNER	DV_STREAMS_ADMIN	-
DV_SECANALYST	LBAC_DBA	-

- PL/SQL package that is protected: SYS.DBMS\_RLS

**Related Topics:**

[Oracle Database Vault Schemas](#) (page 14-1)

The Oracle Database Vault schemas, `DVSY` and `DVF`, support the administration and run-time processing of Oracle Database Vault.

**5.2.2 Database Vault Account Management Realm**

The Database Vault Account Management realm defines the realm for the administrators who manage and create database accounts and database profiles.

This realm protects the `DV_ACCTMGR` and `CONNECT` roles. The owner of this realm can grant or revoke the `CREATE SESSION` privilege to or from a user.

**Related Topics:**

[DV\\_ACCTMGR Database Vault Account Manager Role](#) (page 14-19)

The `DV_ACCTMGR` role is a powerful role, used for accounts management.

**5.2.3 Oracle Enterprise Manager Realm**

Oracle Database Vault provides a realm specifically for Oracle Enterprise Manager accounts.

The Oracle Enterprise Manager realm protects Oracle Enterprise Manager accounts that are used for monitoring and management (`DBSNMP` user and the `OEM_MONITOR` role).

**5.2.4 Oracle Default Schema Protection Realm**

Oracle Default Schema Protection Realm protects roles and schemas that are used with Oracle features such as Oracle Text.

The advantage of this grouping is that Oracle Spatial schemas (`MDSYS`, `MDDATA`) are used extensively with Oracle Text (`CTXSYS`), and Oracle OLAP is an application rather than a core Oracle Database kernel feature.

**Oracle Default Schema Protection Realm Protected Roles and Schemas**

Oracle Default Schema Protection Realm protects several roles and schemas.

- Roles that are protected by default: `CTXAPP`, `OLAP_DBA`, `EJBCLIENT`, `OLAP_USER`
- Schemas that are protected by default: `CTXSYS`, `EXFSYS`, `MDDATA`, `MDSYS`
- Roles that are recommended for protection: `APEX_ADMINISTRATOR_ROLE`, `SPATIAL_CSW_ADMIN`, `WFS_USR_ROLE`, `CSW_USR_ROLE`, `SPATIAL_WFS_ADMIN`, `WM_ADMIN_ROLE`
- Schemas that are recommended for protection: `APEX_030200`, `OWBSYS`, `WMSYS`

**Oracle Default Schema Protection Realm Owners**

The `SYS`, `CTXSYS`, and `EXFSYS` users are the default owners of Oracle Default Schema Protection Realm. These users can grant the roles protected by this realm to other users, and grant permissions on its schemas to other users as well.

## 5.2.5 Oracle System Privilege and Role Management Realm

Oracle System Privilege and Role Management Realm protects sensitive roles that are used to export and import data in an Oracle database.

This realm also contains authorizations for users who must grant system privileges.

User SYS is the only default owner of this realm. Any user who is responsible for managing system privileges should be authorized as an owner to this realm. These users can grant the roles that are protected by this realm to other users.

- Roles that are protected by default:

Roles A-E	Roles G-J	Roles J-S
AQ_ADMINISTRATOR_ROLE	GATHER_SYSTEM_STATISTICS	JAVAUERPRIV
AQ_USER_ROLE	GLOBAL_AQ_USER_ROLE	LOGSTDBY_ADMINISTRATOR
DBA	HS_ADMIN_ROLE	OPTIMIZER_PROCESSING_RATE
DBA_OLS_STATUS	IMP_FULL_DATABASE	RECOVERY_CATALOG_OWNER
DELETE_CATALOG_ROLE	JAVA_ADMIN	RESOURCE
DV_REALM_OWNER	JAVADEBUGPRIV	SCHEDULER_ADMIN
DV_REALM_RESOURCE	JAVA_DEPLOY	SELECT_CATALOG_ROLE
EXECUTE_CATALOG_ROLE	JAVAIDPRIV	-
EXP_FULL_DATABASE	JAVASYSPRIV	-

- Roles that are recommended for protection: DBFS\_ROLE, HS\_ADMIN\_EXECUTE\_ROLE, HS\_ADMIN\_SELECT\_ROLE

## 5.2.6 Oracle Default Component Protection Realm

Oracle Default Component Protection Realm protects the SYSTEM and OUTLN schemas.

The authorized users of this realm are users SYS and SYSTEM.

## 5.3 Creating a Realm

To enable realm protection, you create the realm and configure it to include realm-secured objects, roles, and authorizations.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Realms**.

- In the Realms page, click **Create** to display the Create Realm page.

**Create Realm: General** Back Step 1 of 4 Next Done Cancel

Define a Realm to control access to protected objects. If you mark a realm as mandatory, objects are protected from object owners accessing the data and other users exercising system or object privileges.

\* **Name**

**Description**

**Mandatory Realm**

**Status**

**Audit Options**

- Audit Disabled
- Audit on Success
- Audit on Failure
- Audit on Success or Failure

- In the Create Realm page, enter the following settings:

- Name:** Enter a name for the realm. It can contain up to 90 characters in mixed-case. This attribute is mandatory.

Oracle suggests that you use the name of the protected application as the realm name (for example, `hr_app` for an human resources application).

- Description:** Enter a brief description of the realm. The description can contain up to 1024 characters in mixed-case. This attribute is optional.

You may want to include a description for the business objective of the given application protection and document all other security policies that compliment the realm's protection. Also document who is authorized to the realm, for what purpose, and any possible emergency authorizations.

- Mandatory Realm:** Select this check box to create the realm as a mandatory realm. See [Mandatory Realms to Restrict User Access to Objects within a Realm](#) (page 5-3) for more information about mandatory realms.
- Status:** Select either **Enabled**, **Disabled**, or **Simulation**. This attribute is mandatory.
- Audit Options:** Select one of the following:
  - **Audit Disabled:** Does not create an audit record.
  - **Audit on Success:** Creates an audit record for authorized activities.

- **Audit on Failure:** Creates an audit record when a realm violation occurs (for example, when an unauthorized user tries to modify an object that is protected by the realm).
- **Audit on Success or Failure:** Creates an audit record for any activity that occurs in the realm, including both authorized and unauthorized activities.

In a non-unified auditing environment, Oracle Database Vault writes the audit trail to the `DVSYS.AUDIT_TRAIL$` table. See [Auditing Oracle Database Vault](#) (page A-1) for more information. If you have enabled unified auditing, then this setting does not capture audit records. Instead, you must create audit policies to capture this information, as described in *Oracle Database Security Guide*. Oracle Database also provides a default policy, `ORA_DV_AUDPOL`, that audits all actions that are performed on the Oracle Database Vault `DVSYS` and `DVF` schema objects and the Oracle Label Security `LBACSYS` schema objects.

5. Click **Next** to display the Realm secured objects page.

See [About Realm-Secured Objects](#) (page 5-12) for conceptual information about the settings for this page.

6. Click the **Add** button, and in the Add Secured Object dialog box, enter the following information:

- **Object Owner:** From the list, select the name of the database schema owner. You can enter the `%` character if the object you want to secure with the realm is a role. This attribute is mandatory.
- **Object Type:** From the list, select the type of the database object, such as `TABLE`, `INDEX`, or `ROLE`. This attribute is mandatory.

You can add as many objects of any type as you want to the realm.

By default, the **Object Type** box contains the `%` wildcard character to include all object types for the specified **Object Owner**. However, it does not include roles, which do not have specific schema owners in the database and must be specified explicitly.

- **Object Name:** Enter the name of the object in the database that the realm must protect, or enter `%` to specify all objects (except roles) for the object owner that you have specified. If you enter `%`, then it can encompass all objects in the schema if `%` is also used for the **Object Type** setting. But if **Object Type** is set to **Tables**, then using `%` for the **Object Name** refers to all tables in the schema. This attribute is mandatory.

By default, the **Object Name** field contains the `%` wildcard character to encompass the entire schema specified for **Object Type** and **Object Owner**. Note that the `%` wildcard character applies to objects that do not yet exist and currently existing objects.

If you enter `%` in the **Object Name** field, then it encompasses all objects in the schema if you also enter `%` in the **Object Type** field. However, if you set **Object Type** to a specific object type, such as **Tables**, then the setting of `%` in **Object Type** refers to all objects of that type (in this case, tables) in the schema.

7. Click **Next** to display the Realm authorizations page.

See [About Realm Authorization](#) (page 5-13) for conceptual information about the settings for this page.

8. Click the **Add** button, and in the Add Authorizations dialog box, enter the following information:

- **Realm Authorization Grantee:** From the list, select the database account or role to whom you want to grant the realm authorization.

This list shows all accounts and roles in the system, not just accounts with system privileges.

- **Realm Authorization Type:** Select either of the following settings. This attribute is mandatory.
  - **Participant:** This account or role can exercise system privileges to access, manipulate, and create objects protected by the realm, provided that these privileges have been granted using the standard Oracle Database privilege grant process. A realm can have multiple participants.
  - **Owner:** This account or role has the same rights as the realm participant, plus the authorization to grant or revoke realm-secured database roles. The realm owner can grant or revoke privileges on realm-protected objects to other users. A realm can have multiple owners.
- **Realm Authorization Rule Set:** Select from the available rule sets that have been created for your site. You can select only one rule set, but the rule set can have multiple rules.

See [Creating a Rule to Add to a Rule Set](#) (page 6-8) for more information about defining rules to govern the realm authorization.

Any auditing and custom event handling associated with the rule set occurs as part of the realm authorization processing.

9. Click **Next** to display the Review page.

10. In the Review page, check the settings you have created.

For example:

**Create Realm: Review** Back Step 4 of 4 Next Finish Cancel

**Review**

**General**

Name: HR\_APP  
 Description:  
 Mandatory Realm: No  
 Status: Enabled  
 Audit Options: Audit on Failure

**Realm Secured Objects**

View ▾

Owner	Object Name	Object Type
HR	EMPLOYEES	TABLE

**Realm Authorizations**

View ▾

Realm Authorization Grantee	Realm Authorization Rule Set	Realm Authorization Type
ADAMS		Participant

**Show SQL**

▶ Show

11. Click **Finish** to complete the realm creation.

#### Related Topics:

[About Realm-Secured Objects](#) (page 5-12)

Realm-secured objects define the territory—a set of schema and database objects and roles—that a realm protects.

[About Realm Authorization](#) (page 5-13)

Realm authorizations establish the set of database accounts and roles that manage or access objects protected in realms.

[Propagating Oracle Database Vault Configurations to Other Databases](#) (page 13-2)

You can propagate Database Vault configurations (such as a realm configuration) to other Database Vault-protected databases.

## 5.4 About Realm-Secured Objects

Realm-secured objects define the territory—a set of schema and database objects and roles—that a realm protects.

You can create the following types of protections:

- Objects from multiple database accounts or schemas can be under the same realm.
- One object can belong to multiple realms.

If an object belongs to multiple realms, then Oracle Database Vault checks the realms for the proper authorization. For `SELECT`, `DDL`, and `DML` statements, as long as a user is a participant in one of the realms, and if the command rules permit it, then the commands that the user enters are allowed. For `GRANT` and



REVOKE operations of a database role in multiple realms, the person performing the GRANT or REVOKE operation must be the realm owner.

If one of the realms is a mandatory realm, then the user who wants to access the object must be a realm owner or participant in the mandatory realm. During the authorization checking process, the non-mandatory realms are ignored. If there are multiple mandatory realms that protect the object, then the user who wants to access the object must be authorized in all of the mandatory realms.

## 5.5 About Realm Authorization

Realm authorizations establish the set of database accounts and roles that manage or access objects protected in realms.

You can grant a realm authorization to an account or role to allow the use of its system privileges in the following situations:

- When the user must create or access realm-secured objects
- When a user must grant or revoke realm-secured roles

A user who has been granted realm authorization as either a realm owner or a realm participant can use its system privileges to access secured objects in the realm.

Note the following:

- Realm owners cannot add other users to their realms as owners or participants. Only users who have the DV\_OWNER or DV\_ADMIN role are allowed to add users as owners or participants to a realm.
- Users who have been granted the DV\_OWNER role can add themselves to a realm authorization.
- A realm owner, but not a realm participant, can grant or revoke realm secured roles or grant or revoke object privileges on realm secured objects to anyone.
- A user can be granted either as a realm owner or a realm participant, but not both. However, you can update the authorization types of existing realm authorizations.

Use the Edit Realm page to manage realm authorizations. You can create, edit, and remove realm authorizations.

### Related Topics:

[Realm Authorization Configuration Issues Report](#) (page 27-4)

The Realm Authorization Configuration Issues Report displays Oracle Database Vault realm configuration issues.

## 5.6 Realm Authorizations in a Multitenant Environment

In a multitenant environment, the rules and behavior for common realm authorizations are similar to the authorizations for other common objects.

### Local Authorization for a Common Realm

The local authorization for a common realm refers to the authorization a user has for the PDB that this user is accessing.

The rules for the local authorization for a common realm are as follows:

- A user who has been commonly granted the DV\_OWNER or DV\_ADMIN role can grant local authorization to common users, common roles, local users, and local roles. The common DV\_OWNER or DV\_ADMIN user can also remove local authorization from a common realm in a PDB.
- A local Database Vault administrator can authorize locally (that is, grant local authorizations to both local and common users) within the PDB. A common Database Vault administrator can also grant authorizations in each PDB. A common realm authorization can only be granted by a common Database Vault administrator in the application root.
- The common Database Vault administrator can both add or remove local authorization to and from a common realm from within the PDB.
- If a common user has only local authorization for a common realm, then this user cannot access the common realm in any other PDB than this local authorization.
- A common user or a common role can have both the local authorization and the common authorization to a common realm at the same time. Removing a common user's local authorization from a common realm does not affect the common user's common authorization. Removing a common user's common authorization from a common realm does not affect the common user's local authorization.

#### **Common Authorization for a Common Realm**

The common authorization for a common realm refers to the authorization a common user or a common role has in the application root while the authorization takes effect in every container that is Database Vault enabled.

The rules for the local authorization for a common realm are as follows:

- A user who has been commonly granted the DV\_OWNER or DV\_ADMIN role can grant common realm authorization to common users or roles in the application root. This common Database Vault administrator can perform the removal of common authorizations while in the application root.
- This common authorization applies to the containers that have been Database Vault enabled in the CDB.
- If a common user is authorized to a common realm in the application root, then this user has access to the objects protected by the common realm in the application root and any application PDBs.
- Any rule sets that are associated with a common realm must be common rule sets. The rules that are added to a common rule set that is associated with common authorization cannot involve any local objects.

#### **How the Authorization of a Realm Works in Both the Application Root and in an Individual PDB**

During the Database Vault enforcement in a container, a common realm performs the same enforcement behaviors as the same realm when it is used locally in a PDB.

## **5.7 Modifying the Enablement Status of a Realm**

You can disable or enable a realm, or set the realm to use simulation mode, from Enterprise Manager Cloud Control.

If the realm is managed by a policy, and if the policy status is set to partial, then you can modify the enablement status of the realm. If the policy is set to enabled, disabled, or simulation mode, then you cannot modify the enablement status of the realm.

1. In the Oracle Database Vault Administration page, select **Realms**.
2. In the Realms page, select the realm you want to disable or enable, and then select **Edit**.
3. In the Edit Realm page, under Status in the General section, select either **Disabled**, **Enabled**, or **Simulation**.
4. Click **Done**, and then click **Finished**.

## 5.8 Deleting a Realm

You can use Enterprise Manager Cloud Control to delete realms.

1. Locate the various references to the realm that you want to delete by querying the realm-related Oracle Database Vault data dictionary views.
2. If the Realm is part of a policy, then remove the realm from the policy.
  - a. In the Oracle Database Vault Administration page, select **Policies**.
  - b. Select the policy that contains the realm and then click **Edit**.
  - c. Expand the Realms area.
  - d. Select the realm and then click **Remove**.
  - e. Click **Next**, then **Finish**.
3. In the Administration page, under Database Vault Components, select **Realms**.
4. In the Realms page, select the realm you want to delete, and then select **Remove**.
5. In the Confirmation window, click **Yes**.

Oracle Database Vault deletes the configuration for the realm, including realm authorizations. It does not delete the rule sets used for realm authorizations.

### Related Topics:

[Oracle Database Vault Data Dictionary Views](#) (page 25-1)

You can find information about the Oracle Database Vault configuration settings by querying the Database Vault-specific data dictionary views.

## 5.9 How Realms Work

When an appropriately privileged database account issues a SQL statement that affects an object within a realm, a special set of activities occur.

These privileges include DDL, DML, EXECUTE, GRANT, REVOKE, or SELECT privileges.

1. Does the SQL statement affect objects secured by a realm?

If yes, then go to Step 2 (page 5-16). If no, then realms do not affect the SQL statement. Go to Step 7 (page 5-16). If the object affected by the command is not

secured in any realms, then realms do not affect the SQL statement being attempted.

2. Is the realm a mandatory realm or regular realm?  
If yes, then go to Step 4 (page 5-16). If it is regular realm, then go to Step 3 (page 5-16).
3. Is the database account using a system privilege to execute the SQL statement?  
If yes, then go to Step 4 (page 5-16). If no, then go to Step 6 (page 5-16). If the session has object privileges on the object in question for SELECT, EXECUTE, and DML statements only, then the realm protection is not enforced. Realms protect against the use of any system privilege on objects or roles protected by the realm.  
  
Remember that if the O7\_DICTIONARY\_ACCESSIBILITY initialization parameter has been set to TRUE, then non-SYS users have access to SYS schema objects. For better security, ensure that O7\_DICTIONARY\_ACCESSIBILITY is set to FALSE.
4. Is the database account a realm owner or realm participant?  
If yes, then go to Step 5 (page 5-16). Otherwise, a realm violation occurs and the statement is not allowed to succeed. If the command is a GRANT or REVOKE of a role that is protected by the realm, or the GRANT or REVOKE of an object privilege on an object protected by the realm, then the session must be authorized as the realm owner directly or indirectly through roles.
5. Is the realm authorization for the database account conditionally based on a rule set?  
If yes, then go to Step 6 (page 5-16). If no, then go to Step 7 (page 5-16).
6. Does the rule set evaluate to TRUE?  
If yes, then go to Step 7 (page 5-16). If no, then there is a realm violation, so the SQL statement is not allowed to succeed.
7. Does a command rule prevent the command from executing?  
If yes, then there is a command rule violation and the SQL statement fails. If no, then there is no realm or command rule violation, so the command succeeds.  
  
For example, the HR account may have the DROP ANY TABLE privilege and may be the owner of the HR realm, but a command rule can prevent HR from dropping any tables in the HR schema unless it is during its monthly maintenance window. Command rules apply to the use of the ANY system privileges and object privileges and are evaluated after the realm checks.

In addition, because a session is authorized in a realm, it does not mean the account has full control on objects protected by the realm. Realm authorization does *not* implicitly grant extra privileges to the account. The account still must have system privileges or object privileges to access the objects. For example, an account or role may have the SELECT ANY table privilege and be a participant in the HR realm. This means the account or the account granted the role could query the HR.EMPLOYEES table. Being a participant in the realm does not mean the account or role can DROP the HR.EMPLOYEES table. Oracle Database Vault does not replace the discretionary access control model in the existing Oracle database. It functions as a layer on top of this model for both realms and command rules.

Note the following:

- Protecting a table in a realm does not protect the view by default. Any view that must be protected should be added to the realm regardless of whether the view was created before or after the table was added to the realm.
- For invoker's right procedures that access realm protected objects, the invoker of the procedure must be authorized to the realm.
- Be aware that realm protection does not protect a table if access to the table has been granted to PUBLIC. For example, if `SELECT ON table_name` is granted to PUBLIC, then every user has access to `table_name` (unless the table is protected by a mandatory realm), even if this table is protected by a realm. As a best practice, revoke unnecessary privileges from PUBLIC.

## 5.10 How Authorizations Work in a Realm

Realm authorizations prevent users from performing activities if the users do not have the correct privileges.

[About Authorizations in a Realm](#) (page 5-17)

Realms protect data from access through system privileges.

[Examples of Realm Authorizations](#) (page 5-17)

You can create realms that protect objects from users who have system privileges and other powerful privileges, for example.

### 5.10.1 About Authorizations in a Realm

Realms protect data from access through system privileges.

Realms do not give additional privileges to the data owner or participants.

The realm authorization provides a run-time mechanism to check logically if a user's command should be allowed or denied to access objects specified in the command and to proceed with its execution.

System privileges are sweeping database privileges such as `CREATE ANY TABLE` and `DELETE ANY TABLE`. These privileges typically apply across schemas and bypass the need for object privileges. Data dictionary views such as `DBA_SYS_PRIVS`, `USER_SYS_PRIVS`, and `ROLE_SYS_PRIVS` list the system privileges for database accounts and roles. Database authorizations work normally for objects not protected by a realm. However, a user must be authorized as a realm owner or participant to successfully use his or her system privileges on objects secured by the realm. A realm violation prevents the use of system privileges and can be audited.

Mandatory realms block both object privileged-based access and system privilege-based access. This means that even the object owner cannot have access if he or she is not authorized to access the realm. Users can access secured objects in the mandatory realm only if the user or role is authorized to do so.

### 5.10.2 Examples of Realm Authorizations

You can create realms that protect objects from users who have system privileges and other powerful privileges, for example.

[Example: Unauthorized User Trying to Create a Table](#) (page 5-18)

The `ORA-47401` error appears when unauthorized users try to create tables.

[Example: Unauthorized User Trying to Use the DELETE ANY TABLE Privilege](#)  
(page 5-18)

An `ORA-01031: insufficient privileges` error appears for unauthorized user access.

[Example: Authorized User Performing DELETE Operation](#) (page 5-18)

Authorized users are allowed to perform the activities for which they are authorized.

### 5.10.2.1 Example: Unauthorized User Trying to Create a Table

The `ORA-47401` error appears when unauthorized users try to create tables.

[Example 5-1](#) (page 5-18) shows what happens when an unauthorized user who has the `CREATE ANY TABLE` system privilege tries to create a table in a realm where the `HR` schema is protected by a realm.

**Example 5-1 Unauthorized User Trying to Create a Table**

```
CREATE TABLE HR.demo2 (col1 NUMBER(1));
```

The following output should appear

```
ORA-47401: Realm violation for CREATE TABLE on HR.DEMO2
```

As you can see, the attempt by the unauthorized user fails. Unauthorized use of system privileges such as `SELECT ANY TABLE`, `CREATE ANY TABLE`, `DELETE ANY TABLE`, `UPDATE ANY TABLE`, `INSERT ANY TABLE`, `CREATE ANY INDEX`, and others results in failure.

### 5.10.2.2 Example: Unauthorized User Trying to Use the DELETE ANY TABLE Privilege

An `ORA-01031: insufficient privileges` error appears for unauthorized user access.

[Example 5-2](#) (page 5-18) shows what happens when an unauthorized database account tries to use his `DELETE ANY TABLE` system privilege to delete an existing record, the database session returns the following error.

**Example 5-2 Unauthorized User Trying to Use the DELETE ANY TABLE Privilege**

```
DELETE FROM HR.EMPLOYEES WHERE EMPNO = 8002;
```

The following output should appear:

```
ERROR at line 1:  
ORA-01031: insufficient privileges
```

Realms do not affect direct privileges on objects. For example, a user granted delete privileges to the `HR.EMPLOYEES` table can successfully delete records without requiring realm authorizations. Therefore, realms should minimally affect normal business application usage for database accounts.

### 5.10.2.3 Example: Authorized User Performing DELETE Operation

Authorized users are allowed to perform the activities for which they are authorized.

[Example 5-3](#) (page 5-19) shows how an authorized user can perform standard tasks allowed within the realm.

**Example 5-3 Authorized User Performing DELETE Operation**

```
DELETE FROM HR.EMPLOYEES WHERE EMPNO = 8002;
```

```
1 row deleted.
```

## 5.11 Access to Objects That Are Protected by a Realm

You can protect an object by a realm, but still enable access to objects that are part of this realm-protected object.

For example, suppose you create a realm around a specific table. However, you want users to be able to create an index on this table. You can accomplish this as follows, depending on the following scenarios.

- **The user does not have the CREATE ANY INDEX privilege.** As the realm owner of the table, grant the `CREATE INDEX ON table` privilege to the user who must create the index.
- **The user has the CREATE ANY INDEX privilege.** In this case, create another realm and make all index types as the secured objects and grant that user participant authorization to the realm. (Remember that having the `CREATE ANY INDEX` privilege alone is not sufficient for a non-realm participant to create an index in a realm-protected table.)
- **You want all of your database administrators to be able to create an index and they have the CREATE ANY INDEX privilege.** In your data protection realm, specify all object types to be protected *except* the index types. This permits all of your administrators to create indexes for the protected table.

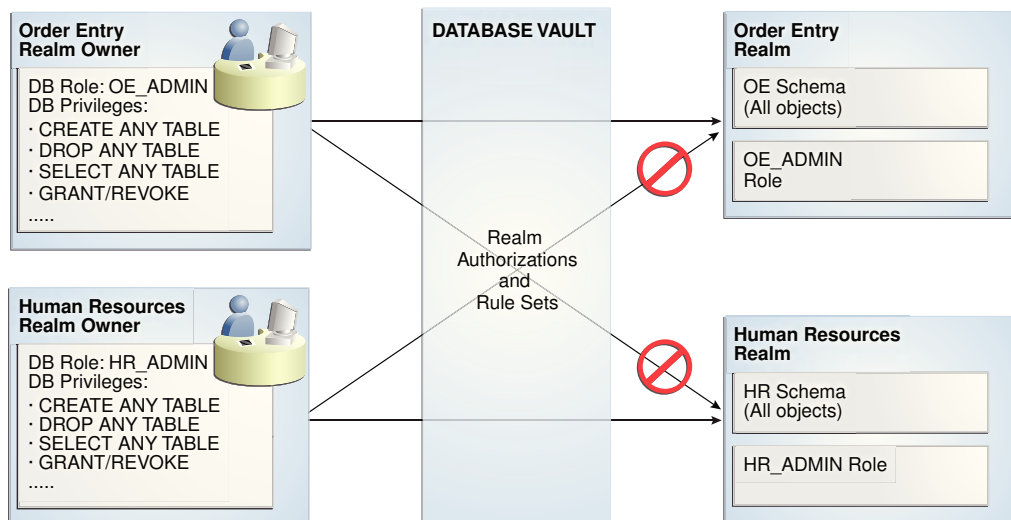
## 5.12 Example of How Realms Work

Realms can provide protection in which two users who each have the same privileges must have separate access levels for an object.

[Figure 5-1](#) (page 5-20) illustrates how data within a realm is protected.

In this scenario, two users, each in charge of a different realm, have the same system privileges. The owner of a realm can be either a database account or a database role. As such, each of the two roles, `OE_ADMIN` and `HR_ADMIN`, can be protected by a realm as a secured object *and* be configured as the owner of a realm.

Further, only a realm owner, such as `OE_ADMIN`, can grant or revoke database roles that are protected by the realm. The realm owner cannot manage roles protected by other realms such as the `DBA` role created by `SYS` in the Oracle System Privilege and Role Management realm. Any unauthorized attempt to use a system privilege to access realm-protected objects raises a realm violation, which can be audited. The powers of each realm owner are limited within the realm itself. For example, `OE_ADMIN` has no access to the Human Resources realm, and `HR_ADMIN` has no access to the Order Entry realm.

**Figure 5-1 How Authorizations Work for Realms and Realm Owners****Related Topics:**

[Quick Start Tutorial: Securing a Schema from DBA Access](#) (page 3-11)

This tutorial shows how to create a realm around the HR schema.

## 5.13 How Realms Affect Other Oracle Database Vault Components

Realms have no effect on factors, identities, or rule sets, but they do affect command rules.

With command rules, Oracle Database Vault evaluates the realm authorization first when processing SQL statements.

[How Realms Work](#) (page 5-15) explains the steps that Oracle Database Vault takes to process SQL statements that affect objects in a realm. [How Command Rules Work](#) (page 7-11) describes how command rules are processed.

## 5.14 Guidelines for Designing Realms

Oracle provides a set of guidelines for designing realms.

- Create realms based on the schemas and roles that form a database application. Define database roles with the minimum and specific roles and system privileges required to maintain the application objects and grant the role to named accounts. You then can add the role as an authorized member of the realm. For object-level privileges on objects protected by the realm and required by an application, create a role and grant these minimum and specific object-level privileges to the role, and then grant named accounts this role. In most cases, these types of roles do not need to be authorized in the realm unless ANY-style system privileges are already in use. A model using the principle of least privilege is ideal for any database application.
- A database object can belong to multiple realms and an account or role can be authorized in multiple realms. To provide limited access to a subset of a database schema (for example, just the EMPLOYEES table in the HR schema), or roles protected by a realm, create a new realm with just the minimum required objects and authorizations.



- If you want to add a role to a realm as a grantee, create a realm to protect the role. Doing so prevents users who have been granted the `GRANT ANY ROLE` system privilege, such as the `SYSTEM` user account, from granting the role to themselves.
- If you want to add the `SYS` user account to a realm authorization, you must add user `SYS` explicitly and not through a role (such as the `DBA` role).
- Be mindful of the privileges currently allowed to a role that you plan to add as a realm authorization.

Realm authorization of a role can be accidentally granted and not readily apparent if an account such as `SYS` or `SYSTEM` creates a role for the first time and the Oracle Database Vault administrator adds this role as a realm authorization. This is because the account that creates a role is implicitly granted the role when it is created.

- Sometimes you must temporarily relax realm protections for an administrative task. Rather than disabling the realm, have the Security Manager (`DV_ADMIN` or `DV_OWNER`) log in, add the named account to the authorized accounts for the realm, and set the authorization rule set to Enabled. Then in the enabled rule set, turn on all auditing for the rule set. You can remove the realm authorization when the administrative task is complete.
- If you want to grant `ANY` privileges to new users, Oracle recommends that you add a database administrative user to the Oracle System Privilege and Role Management realm so that this user can grant other users `ANY` privileges, if they need them. For example, using a named account to perform the `GRANT` of the `ANY` operations enables you to audit these operations, which creates an audit trail for accountability.
- If you drop a table, index, or role that has been protected by a realm and then recreate it using the same name, the realm protection is not restored. You must recreate the realm protection for the new table, index, or role. However, you can automatically enforce protection for all future tables, indexes, and roles within a specified schema. For example, to enforce protection for all future tables:
 

```
BEGIN
  DBMS_MACADM.ADD_OBJECT_TO_REALM('realm_name', 'schema_name', '%', 'TABLE');
END;
/
```
- You can test the development phase of a realm by using simulation mode, which enables the realm but writes detailed information about violations to a log file.

#### Related Topics:

[Using Simulation Mode for Logging Realm and Command Rule Activities](#)  
(page 11-1)

Simulation mode writes the activities performed on realms and command rules to a log file, which is accessible through a data dictionary view.

## 5.15 How Realms Affect Performance

Realms can affect database performance in a variety of situations, such as with DDL and DML operations.

- **DDL and DML operations on realm-protected objects do not have a measurable effect on Oracle Database.** Oracle recommends that you create the realm around

the entire schema, and then authorize specific users to perform only specific operations related to their assigned tasks. For finer-grained control, you can define realms around individual tables and authorize users to perform certain operations on them, and also have a realm around the entire schema to protect the entire application. Be aware, however, that this type of configuration may slow performance, but it does enable you to grant realm authorization to some of the objects in a schema.

- **Auditing affects performance.** To achieve the best performance, Oracle recommends that you use fine-grained auditing rather than auditing all operations.
- **Periodically check the system performance.** You can do so by running tools such as Oracle Enterprise Manager (including Oracle Enterprise Manager Cloud Control, which is installed by default with Oracle Database), Automatic Workload Repository (AWR), and TKPROF.

---



---

**See Also:**

- *Oracle Database Performance Tuning Guide* to learn how to monitor database performance
  - *Oracle Database SQL Tuning Guide* to monitor the performance of individual SQL and PL/SQL statements
- 
- 

## 5.16 Realm Related Reports and Data Dictionary Views

Oracle Database Vault provides reports and data dictionary views that are useful for analyzing realms.

[Table 5-1](#) (page 5-22) lists the Oracle Database Vault reports. See [Oracle Database Vault Reports](#) (page 27-1), for information about how to run these reports.

**Table 5-1 Reports Related to Realms**

Report	Purpose
<a href="#">Realm Audit Report</a> (page 27-5)	Audits records generated by the realm protection and realm authorization operations
<a href="#">Realm Authorization Configuration Issues Report</a> (page 27-4)	Lists authorization configuration information, such as incomplete or disabled rule sets, or nonexistent grantees or owners that may affect the realm
<a href="#">Rule Set Configuration Issues Report</a> (page 27-3)	Lists rule sets that do not have rules defined or enabled, which may affect the realms that use them
<a href="#">Object Privilege Reports</a> (page 27-7)	Lists object privileges that the realm affects
<a href="#">Privilege Management - Summary Reports</a> (page 27-12)	Provides information about grantees and owners for a realm
<a href="#">Sensitive Objects Reports</a> (page 27-10)	Lists objects that the command rule affects

Table 5-2 (page 5-23) lists data dictionary views that provide information about existing realms.

**Table 5-2 Data Dictionary Views Used for Realms**

Data Dictionary View	Description
<a href="#">DBA_DV_REALM View</a> (page 25-24)	Lists the realms created in the current database instance.
<a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25)	lists the authorization of a named database user account or database role ( <i>GRANTEE</i> ) to access realm objects in a particular realm
<a href="#">DBA_DV_REALM_OBJECT View</a> (page 25-27)	Lists the database schemas, or subsets of schemas with specific database objects contained therein, that are secured by the realms



---

## Configuring Rule Sets

Rule sets group one or more rules together; the rules determine whether a user can perform an action on an object.

### [What Are Rule Sets?](#) (page 6-2)

A rule set is a collection of one or more rules.

### [Rule Sets and Rules in a Multitenant Environment](#) (page 6-2)

In a multitenant environment, you can create a rule set and its associated rules in the application root.

### [Default Rule Sets](#) (page 6-3)

Oracle Database Vault provides a set of default rules sets that you can customize for your needs.

### [Creating a Rule Set](#) (page 6-5)

To create a rule set, you first create the rule set itself, and then you can edit the rule set to associate it with one or more rules.

### [Creating a Rule to Add to a Rule Set](#) (page 6-8)

A rule defines the behavior that you want to control; a rule set is a named collection of rules.

### [Removing Rule Set References to Oracle Database Vault Components](#) (page 6-15)

Before you remove a rule set, you should remove the rule set references to Oracle Database Vault components.

### [Deleting a Rule Set](#) (page 6-15)

You can use Enterprise Manager Cloud Control to find reference to the rule set and then delete the rule set.

### [How Rule Sets Work](#) (page 6-16)

Understanding how rule sets work helps to create more effective rule sets.

### [Tutorial: Creating an Email Alert for Security Violations](#) (page 6-17)

This tutorial demonstrates how to use the UTL\_MAIL PL/SQL package and an access control list to create an email alert for security violations.

### [Tutorial: Configuring Two-Person Integrity, or Dual Key Security](#) (page 6-24)

This tutorial demonstrates how to use Oracle Database Vault to control the authorization of two users.

### [Guidelines for Designing Rule Sets](#) (page 6-30)

Oracle provides guidelines for designing rule sets.

### [How Rule Sets Affect Performance](#) (page 6-30)

The number and complexity of rules can slow database performance.

[Rule Set and Rule Related Reports and Data Dictionary Views](#) (page 6-31)

Oracle Database Vault provides reports and data dictionary views that are useful for analyzing rule sets and the rules within them.

## 6.1 What Are Rule Sets?

A rule set is a collection of one or more rules.

You can associate the rule set with a realm authorization, factor assignment, command rule, or secure application role.

The rule set evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (*All True* or *Any True*). A rule within a rule set is a PL/SQL expression that evaluates to true or false. You can create a rule and add the rule to multiple rule sets.

You can use rule sets to accomplish the following activities:

- As a further restriction to realm authorization, to define the conditions under which realm authorization is active
- To define when to allow a command rule
- To enable a secure application role
- To define when to assign the identity of a factor

When you create a rule set, Oracle Database Vault makes it available for selection when you configure the authorization for a realm, command rule, factor, or secure application role.

### Related Topics:

[Rule Set and Rule Related Reports and Data Dictionary Views](#) (page 6-31)

Oracle Database Vault provides reports and data dictionary views that are useful for analyzing rule sets and the rules within them.

[Oracle Database Vault Rule Set APIs](#) (page 16-1)

You can use the `DBMS_MACADM` PL/SQL package and a set of Oracle Database Vault rule functions to manage rule sets.

## 6.2 Rule Sets and Rules in a Multitenant Environment

In a multitenant environment, you can create a rule set and its associated rules in the application root.

A common realm must use a common rule set when the associated realm or command rule is evaluated by Database Vault. The common rule set and its rules can only be created in the application root. After the common rule set is created, it exists in every container that is associated with the root where the common rule set is created. The common rule set can only include common rules.

To configure a common rule set and its rules, you must be commonly granted the `DV_OWNER` or `DV_ADMIN` role.

### Related Topics:

[Command Rules in a Multitenant Environment](#) (page 7-3)

In a multitenant environment, you can create common and local command rules in either the CDB root or the application root.

## 6.3 Default Rule Sets

Oracle Database Vault provides a set of default rules sets that you can customize for your needs.

You can find a full list of rule sets by querying the `DBA_DV_RULE_SET` data dictionary view. To find rules that are associated with a rule set, query the `DBA_DV_RULE_SET_RULE` data dictionary view.

The default rule sets are as follows:

- **Allow Dumping Datafile Header:** This rule set prevents the dumping of data blocks.
- **Allow Fine Grained Control for Alter System:** This rule set enables you to control the ability of users to set initialization parameters using the `ALTER SYSTEM SQL` statement.
- **Allow Fine Grained Control of System Parameters: Note:** This rule set has been deprecated.

This rule set provides a very flexible, fine-grained control over initialization parameters that manage system security, dump or destination location, backup and restore settings, optimizer settings, PL/SQL debugging, and security parameters. It affects the following initialization parameters, based on the associated rules of this rule set:

- **Are System Security Parameters Allowed rule:** Cannot set `O7_DICTIONARY_ACCESSIBILITY`
- **Are Dump or Dest Parameters Allowed rule:** Cannot set the following parameters:

Parameter B-D	Parameters D-U
<code>BACKGROUND_DUMP_DEST</code>	<code>DB_RECOVERY_FILE_DEST</code>
<code>CORE_DUMP_DEST</code>	<code>DIAGNOSTIC_DEST</code>
<code>DUMP_DATAFILE</code>	<code>LOG_ARCHIVE_MIN_SUCCEED_DEST</code>
<code>USER_DUMP_DEST</code>	<code>LOG_ARCHIVE_TRACE</code>
<code>DB_CREATE_ONLINE_LOG_DEST</code>	<code>USER_DUMP_DEST</code>

- **Are Backup Restore Parameters Allowed rule:** Cannot set `RECYCLEBIN` (but does not prevent disabling the recycle bin)
- **Are Database File Parameters Allowed rule:** Cannot set `CONTROL_FILES`
- **Are Optimizer Parameters Allowed rule:** Can set `OPTIMIZER_SECURE_VIEW_MERGING = FALSE` (but `TRUE` not allowed)
- **Are PL-SQL Parameters Allowed rule:** Can set `PLSQL_DEBUG = FALSE` (but `TRUE` not allowed), cannot set `UTL_FILE_DIR`. The `UTL_FILE_DIR` initialization parameter is deprecated. It is still supported for backward compatibility. However, Oracle recommends that you instead use directory

objects. See *Oracle Database Reference* for more information about UTL\_FILE\_DIR.

- **Are Security Parameters Allowed rule:** Cannot set the following:

#### Parameters A-A

AUDIT\_SYS\_OPERATIONS = FALSE

AUDIT\_TRAIL = NONE or FALSE

AUDIT\_SYSLOG\_LEVEL

#### Parameters O-S

OS\_ROLES = TRUE

REMOTE\_OS\_ROLES = TRUE

SQL92\_SECURITY = FALSE

See *Oracle Database Reference* for detailed information about initialization parameters.

- **Allow Sessions:** Controls the ability to create a session in the database. This rule set enables you to add rules to control database logins using the CONNECT command rule. The CONNECT command rule is useful to control or limit SYSDBA access to programs that require its use. This rule set is not populated.
- **Allow System Parameters: Note:** This rule set has been deprecated. Controls the ability to set system initialization parameters. Since Oracle Database 11g Release 2 (11.2), the Allow Fine Grained Control of System Parameters rule set has replaced this rule set, but it is still supported for backward compatibility. The Allow System Parameters rule set is not associated with any commands, but its rules are still available and can be used with any custom rule set. Oracle recommends that you use the Allow Fine Grained Control of System Parameters rule set.
- **Can Grant VPD Administration:** Controls the ability to grant the GRANT EXECUTE or REVOKE EXECUTE privileges on the Oracle Virtual Private Database DBMS\_RLS package, with the GRANT and REVOKE statements.
- **Can Maintain Accounts/Profiles:** Controls the roles that manage user accounts and profiles, through the CREATE USER, DROP USER, CREATE PROFILE, ALTER PROFILE, or DROP PROFILE statements.
- **Can Maintain Own Account:** Allows the accounts with the DV\_ACCTMGR role to manage user accounts and profiles with the ALTER USER statement. Also allows individual accounts to change their own password using the ALTER USER statement. See [DV\\_ACCTMGR Database Vault Account Manager Role](#) (page 14-19) for more information about the DV\_ACCTMGR role.
- **Disabled:** Convenience rule set to quickly disable security configurations like realms, command rules, factors, and secure application roles.
- **Enabled:** Convenience rule set to quickly enable system features.
- **Not allow to set AUDIT\_SYS\_OPERATIONS to False:** Prevents the AUDIT\_SYS\_OPERATIONS initialization parameter from being set to FALSE. If unified auditing is enabled, then the AUDIT\_SYS\_OPERATIONS parameter has no effect.
- **Not allow to set OPTIMIZER\_SECURE\_VIEW\_MERGING to True:** Prevents the OPTIMIZER\_SECURE\_VIEW\_MERGING initialization parameter from being set to TRUE.



- **Not allow to set OS\_ROLES to True:** Prevents the OS\_ROLES initialization parameter from being set to TRUE.
- **Not allow to set PLSQL\_DEBUG to True:** Prevents the PLSQL\_DEBUG initialization parameter from being set to TRUE.
- **Not allow to set REMOTE\_OS\_ROLES to True:** Prevents the REMOTE\_OS\_ROLES initialization parameter from being set to TRUE.
- **Not allow to set SQL92\_SECURITY to False:** Prevents the SQL92\_SECURITY from being set to FALSE.
- **Not allow to turn off AUDIT\_TRAIL:**  
Prevents the AUDIT\_TRAIL initialization parameter from being turned off. If unified auditing is enabled, then the AUDIT\_TRAIL parameter has no effect.

## 6.4 Creating a Rule Set

To create a rule set, you first create the rule set itself, and then you can edit the rule set to associate it with one or more rules.

You can associate a new rule with the rule set, add existing rules to the rule set, or delete a rule association from the rule set.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Rule Sets**.
3. In the Rule Sets page, click **Create** to display the Create Rule Sets page.

The screenshot displays the 'Create Rule Set: General' page in the Oracle Database Vault Administrator interface. At the top, there is a progress bar with four steps: 'General' (selected), 'Associate with Rules', 'Error Handling and Audit Options', and 'Review'. Below the progress bar, the page title is 'Create Rule Set: General' and there are navigation buttons: 'Back', 'Step 1 of 4', 'Next', 'Done', and 'Cancel'. The main content area contains a form with the following fields and options:

- Rule Set Name:** A text input field with an asterisk indicating it is required.
- Description:** A text area for providing details about the rule set.
- Static Rule Set:** A checkbox option.
- Status:** Radio buttons for 'Enabled' (selected) and 'Disabled'.
- Evaluation Options:** Radio buttons for 'All True' (selected) and 'Any True'.

4. In the General page, enter the following information:

- **Name:** Enter a name for the rule set. It can contain up to 90 characters in mixed-case. Spaces are allowed. This attribute is mandatory.

Oracle suggests that you start the name with a verb and complete it with the realm or command rule name to which the rule set is attached. For example:

```
Limit SQL*Plus access
```

- **Description:** Enter a description of the functionality for the rule set. It can have up to 1024 characters in mixed-case. This attribute is optional.

You may want to document the business requirement of the rule set. For example:

```
Rule to limit access to SQL*Plus
```

- **Static Rule Set:** You can control how often the rule set is evaluated when it is accessed during a user session. A static rule set is evaluated once when accessed for the first time in a user session. After that, the evaluated value is re-used in the user session. On the other hand, a non-static rule set is evaluated every time it is accessed.
- **Status:** Select either **Enabled** or **Disabled** to enable or disable the rule set during run time. This attribute is mandatory.
- **Evaluation Options:** If you plan to assign multiple rules to a rule set, then select one of the following settings:
  - **All True:** All rules in the rule set must evaluate to true for the rule set itself to evaluate to true.
  - **Any True:** At least one rule in the rule set must evaluate to true for the rule set itself to evaluate to true.

5. Click **Next** to display the Associate with Rules page.

6. Select one of the following options:

- **Add Existing Rule:** Double-click from the list of available rules to move them to the Selected Rules list, and then click **OK**.
- **Create Rule:** Enter a name and **WHERE** clause expression that evaluates to true or false. Click **OK**. See [Creating a Rule to Add to a Rule Set](#) (page 6-8) for more information.

7. Click **Next** to display the Error handling and Audit options page.

8. Enter the following information:

- **Error Handling:** Select either **Show Error Message** or **Do Not Show Error Message**.

An advantage of selecting **Do Not Show Error Message** and then enabling auditing is that you can track the activities of a potential intruder. The audit report reveals the activities of the intruder, yet the intruder is unaware that you are doing this because he or she does not see any error messages.

- **Fail Code:** Enter a number in the ranges of -20000 to -20999 or 20000 to 20999. The error code is displayed with the **Fail Message** (created next) when the rule set evaluates to false or one of the associated rules contains an invalid PL/SQL

expression. If you omit this setting, then Oracle Database Vault displays a generic error code.

- **Fail Message:** Enter a message, up to 80 characters in mixed-case, to associate with the fail code you specified under **Fail Code**. The error message is displayed when the rule set evaluates to false or one of the associated rules contains an invalid PL/SQL expression. If you do not specify an error message, then Oracle Database Vault displays a generic error message.
- **Custom Event Handler Option:** Select one of the following options to determine when to run the **Custom Event Handler Logic** (created next).
  - **Handler Disabled:** Does not run any custom event method.
  - **Execute On Failure:** Runs the custom event method when the rule set evaluates to false or one of the associated rules contains an invalid PL/SQL expression.
  - **Execute On Success:** Runs the custom event method when the rule set evaluates to true.

You can create a custom event method to provide special processing outside the standard Oracle Database Vault rule set auditing features. For example, you can use an event handler to initiate a workflow process or send event information to an external system.

- **Custom Event Handler Logic:** Enter a PL/SQL expression up to 255 characters in mixed-case. An expression may include any package procedure or standalone procedure. You can create your own expression or use the PL/SQL interfaces described in [Oracle Database Vault Rule Set APIs](#) (page 16-1).

Write the expression as a fully qualified procedure (such as *schema.procedure\_name*). Do not include any other form of SQL statements. If you are using application package procedures or standalone procedures, you must provide DVSYS with the EXECUTE privilege on the object. The procedure signature can be in one of the following two forms:

- PROCEDURE *my\_ruleset\_handler*(*p\_ruleset\_name* IN VARCHAR2, *p\_ruleset\_rules* IN BOOLEAN): Use this form when the name of the rule set and its return value are required in the handler processing.
- PROCEDURE *my\_ruleset\_handler*: Use this form when the name of the rule set and its return value are not required in the handler processing.

Be aware that you cannot use invoker's rights procedures as event handlers. Doing so can cause the rule set evaluation to fail unexpectedly. Only use definer's rights procedures as event handlers.

Use the following syntax:

```
myschema.my_ruleset_handler
```

- **Audit Options:** Select from the following options to generate an audit record for the rule set in a non-unified auditing environment. Oracle Database Vault writes the audit trail to the DVSYS.AUDIT\_TRAIL\$ table. (If you have enabled unified auditing, then this setting does not capture audit records. Instead, you must create unified audit policies to capture this information.)
  - **Audit Disabled:** Does not create an audit record under any circumstances.

- **Audit on Success:** Creates an audit record when the rule set evaluates to true.
- **Audit On Failure:** Creates an audit record when the rule set evaluates to false or one of the associated rules contains an invalid PL/SQL expression.
- **Audit On Success or Failure:** Creates an audit record whenever a rule set is evaluated.

9. Click **Next** to display the Review page.

10. Review the settings, and if they are satisfactory, click **Finish**.

---



---

**See Also:**

- [Auditing Oracle Database Vault](#) (page A-1) for more information about audit records in the `DVSYS.AUDIT_TRAIL$` table
  - *Oracle Database Security Guide* for information about creating unified audit policies for Database Vault
- 
- 

## 6.5 Creating a Rule to Add to a Rule Set

A rule defines the behavior that you want to control; a rule set is a named collection of rules.

### [About Creating Rules](#) (page 6-8)

You can create rules during the rule set creation process, or independently of it.

### [Default Rules](#) (page 6-9)

Default rules are rules that have commonly used behavior, such as checking if an action evaluates to true or false.

### [Creating a New Rule](#) (page 6-12)

You can create a new rule in Enterprise Manager Cloud Control.

### [Adding Existing Rules to a Rule Set](#) (page 6-14)

After you have created one or more rules, you can use Enterprise Manager Cloud Control to add to a rule set.

### [Removing a Rule from a Rule Set](#) (page 6-14)

Before you remove a rule from a rule set, you can locate the various references to it using Cloud Control.

### 6.5.1 About Creating Rules

You can create rules during the rule set creation process, or independently of it.

After you create the rule, you can associate a rule set with one or more additional rules.

If you create a new rule during the rule set creation process, the rule is automatically added to the current rule set. You also can add existing rules to the rule set.

Alternatively, you can omit adding rules to the rule set and use it as a template for rule sets you may want to create in the future.

You can add as many rules that you want to a rule set, but for better design and performance, you should keep the rule sets simple. See [Guidelines for Designing Rule Sets](#) (page 6-30) for additional advice.

The rule set evaluation depends on the evaluation of its rules using the Evaluation Options (**All True** or **Any True**). If a rule set is disabled, Oracle Database Vault evaluates the rule set to true without evaluating its rules.

#### Related Topics:

[How Rule Sets Work](#) (page 6-16)

Understanding how rule sets work helps to create more effective rule sets.

## 6.5.2 Default Rules

Default rules are rules that have commonly used behavior, such as checking if an action evaluates to true or false.

You can find a full list of rules by querying the `DBA_DV_RULE` data dictionary view. [Table 6-1](#) (page 6-9) lists the current default Oracle Database rules.

**Table 6-1 Current Default Oracle Database Vault Rules**

Rule	Description
Are Backup Restore Parameters Allowed	Note: This default rule has been deprecated. Checks if the current SQL statement attempts to turn on the <code>RECYCLEBIN</code> parameter
Are Database File Parameters Allowed	Note: This default rule has been deprecated. Checks if the current SQL statement attempts to alter control file related configuration
Are Dump Parameters Allowed	Checks if the current SQL statement attempts to alter initialization parameters related to the destination of a dump
Are Dest Parameters Allowed	Checks if the current SQL statement attempts to alter initialization parameters related to the size limit of a dump
Are Dump or Dest Parameters Allowed	Note: This default rule has been deprecated. Checks if the current SQL statement attempts to alter initialization parameters related to the size limit or destination of dump
Are Optimizer Parameters Allowed	Note: This default rule has been deprecated. Checks if the current SQL statement attempts to alter the setting for the <code>OPTIMIZER_SECURE_VIEW_MERGING</code> parameter
Are PL-SQL Parameters Allowed	Note: This default rule has been deprecated. Checks if the current SQL statement attempts to alter the following initialization parameters: <ul style="list-style-type: none"> <li>• <code>UTL_FILE_DIR</code></li> <li>• <code>PLSQL_DEBUG</code></li> </ul>

**Table 6-1 (Cont.) Current Default Oracle Database Vault Rules**

Rule	Description
Are Security Parameters Allowed	<p>Note: This default rule has been deprecated.</p> <p>Checks if there is an attempt to disable the following initialization parameters:</p> <ul style="list-style-type: none"> <li>• AUDIT_SYS_OPERATIONS</li> <li>• AUDIT_TRAIL</li> <li>• AUDIT_SYSLOG_LEVEL</li> <li>• SQL92_SECURITY</li> </ul> <p>Note that if you have enabled unified auditing, then the AUDIT_SYS_OPERATIONS, AUDIT_TRAIL, and AUDIT_SYSLOG_LEVEL parameters have no effect.</p> <p>This rule prevents any attempt to enable the following parameters:</p> <ul style="list-style-type: none"> <li>• OS_ROLES</li> <li>• REMOTE_OS_ROLES</li> </ul>
Are System Security Parameters Allowed	<p>Note: This default rule has been deprecated.</p> <p>Prevents modification of the following parameters:</p> <ul style="list-style-type: none"> <li>• O7_DICTIONARY_ACCESSIBILITY</li> <li>• DYNAMIC_RLS_POLICIES</li> <li>• _SYSTEM_TRIG_ENABLED</li> </ul>
False	Evaluates to FALSE
Is Alter DVSYS Allowed	<p>Note: This default rule has been deprecated.</p> <p>Checks if the logged-in user can execute the ALTER USER statement on other users successfully</p>
Is Database Administrator	Checks if a user has been granted the DBA role
Is Drop User Allowed	Checks if the logged in user can drop users
Is Dump of Block Allowed	Checks if the dumping of blocks is allowed
Is First Day of Month	Checks if the specified date is the first day of the month
Is Label Administrator	Checks if the user has been granted the LBAC_DBA role
Is Last Day of Month	Checks if the specified date is the last day of the month
Is _dynamic_rls_init Parameters Allowed	<p>Note: This default rule has been deprecated.</p> <p>Prevent modification of the DYNAMIC_RLS_POLICIES parameter</p>
Is Parameter Value False	Checks if a specified parameter value has been set to FALSE
Is Parameter Value None	Checks if a specified parameter value has been set to NONE
Is Parameter Value Not False	Checks if a specified parameter value has been set to <> FALSE

**Table 6-1 (Cont.) Current Default Oracle Database Vault Rules**

<b>Rule</b>	<b>Description</b>
Is Parameter Value Not None	Checks if a specified parameter value has been set to <> NONE
Is Parameter Value Not Off	Checks if a specified parameter value has been set to <> OFF
Is Parameter Value Not On	Checks if a specified parameter value has been set to <> ON
Is Parameter Value Not True	Checks if a specified parameter value has been set to <> TRUE
Is Parameter Value Off	Checks if a specified parameter value has been set to OFF
Is Parameter Value On	Checks if a specified parameter value has been set to ON
Is Parameter Value True	Checks if a specified parameter value has been set to TRUE
Is SYS or SYSTEM User	Checks if the user is SYS or SYSTEM
Is Security Administrator	Checks if a user has been granted the DV_ADMIN role
Is Security Owner	Checks if a user has been granted the DV_OWNER role
Is User Manager	Checks if a user has been granted the DV_ACCTMGR role

**Table 6-1 (Cont.) Current Default Oracle Database Vault Rules**

Rule	Description
Is _system_trig_enabled Parameters Allowed	<p>Note: This default rule has been deprecated.</p> <p>Checks if the user tries to modify the following system parameters, but in database recovery operations, this rule permits these parameters to be changed.</p> <ul style="list-style-type: none"> <li>AUDIT_SYS_OPERATIONS: Prevents users from setting it to FALSE</li> <li>AUDIT_TRAIL: Prevents users from setting it to NONE or FALSE</li> <li>AUDIT_SYSLOG_LEVEL: Blocks all operations on this parameter</li> <li>CONTROL_FILES: Blocks all operations</li> <li>OPTIMIZER_SECURE_VIEW_MERGING: Prevents users from setting it to TRUE</li> <li>OS_ROLES: Prevents users from setting it to TRUE</li> <li>PLSQL_DEBUG: Prevents users from setting it to ON</li> <li>RECYCLEBIN: Prevents users from setting it to ON</li> <li>REMOTE_OS_ROLES: Prevents users from setting it to TRUE</li> <li>SQL92_SECURITY: Prevents users from setting it to FALSE</li> <li>UTL_FILE_DIR: Blocks all operations on this parameter</li> </ul> <p>Note that if you have enabled unified auditing, then the AUDIT_SYS_OPERATIONS, AUDIT_TRAIL, and AUDIT_SYSLOG_LEVEL parameters have no effect.</p>
Is o7_dictionary_accessibility Parameters Allowed	<p>Note: This default rule has been deprecated.</p> <p>Checks if current SQL statement attempts to alter the setting of the O7_DICTIONARY_ACCESSIBILITY parameter</p>
Login User Is Object User	Checks if the logged in user is the same as the user about to be altered by the current SQL statement
No Exempt Access Policy Role	Checks if the user has been granted the EXEMPT ACCESS POLICY role or is user SYS
Not Export Session	Obsolete
True	Evaluates to TRUE

### 6.5.3 Creating a New Rule

You can create a new rule in Enterprise Manager Cloud Control.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Rules**.



3. Click the **Create** button.

4. In the Create Rule page, enter the following settings:

- **Name:** Enter a name for the rule. Use up to 90 characters in mixed-case.

Oracle suggests that you start the name with a verb and complete the name with the purpose of the rule. For example:

```
Prevent non-admin access to SQL*Plus
```

Because rules do not have a **Description** field, make the name explicit but be sure to not exceed over 90 characters.

- **Rule Expression:** Enter a PL/SQL expression that fits the following requirements:

- It is valid in a SQL WHERE clause.

- It can be a freestanding and valid PL/SQL Boolean expression such as the following:

```
TO_CHAR(SYSDATE, 'HH24') = '12'
```

- It must evaluate to a Boolean (TRUE or FALSE) value.

- It must be no more than 1024 characters long.

- It can contain existing and compiled PL/SQL functions from the current database instance. Ensure that these are fully qualified functions (such as *schema.function\_name*). Do not include any other form of SQL statements.

Be aware that you cannot use invoker's rights procedures with rule expressions. Doing so will cause the rule evaluation to fail unexpectedly. Only use definer's rights procedures with rule expressions.

If you want to use application package functions or standalone functions, you must grant the DVSYS account the EXECUTE privilege on the function. Doing so reduces the chances of errors when you add new rules.

- Ensure that the rule works. You can test the syntax by running the following statement in SQL\*Plus:

```
SELECT rule_expression FROM DUAL;
```

For example, suppose you have created the following the rule expression:

```
SYS_CONTEXT('USERENV', 'SESSION_USER') != 'TSMITH'
```

You could test this expression as follows:

```
SELECT SYS_CONTEXT('USERENV', 'SESSION_USER') FROM DUAL;
```

For the Boolean example listed earlier, you would enter the following:

```
SELECT TO_CHAR(SYSDATE, 'HH24') FROM DUAL;
```

5. Click **OK**.

### Related Topics:

[Oracle Database Vault PL/SQL Rule Set Functions](#) (page 16-14)

Oracle Database Vault provides functions to use in rule sets to inspect the SQL statement that the rule set protects.

[DBMS\\_MACADM Rule Set Procedures](#) (page 16-1)

The DBMS\_MACADM rule set procedures enable you to configure both rule sets and individual rules that go within these rule sets.

[Oracle Database Vault Utility APIs](#) (page 21-1)

Oracle Database Vault provides a set of utility APIs in the DBMS\_MACUTL PL/SQL package.

## 6.5.4 Adding Existing Rules to a Rule Set

After you have created one or more rules, you can use Enterprise Manager Cloud Control to add to a rule set.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Rule Sets**.
3. Select the rule set to which you want to add an existing rule, and then click **Edit**.
4. Click **Next** until you reach the Associate with Rules page.
5. Click **Add Existing Rule** to display the Add Existing Rules dialog box.
6. In the Add Existing Rules page, select the rules you want, and then click **Move** (or **Move All**, if you want all of them) to move them to the Selected Rules list.

You can select multiple rules by holding down the **Ctrl** key as you click each rule.

7. Click **OK**.
8. Click **Done**, then click **Finish**.

## 6.5.5 Removing a Rule from a Rule Set

Before you remove a rule from a rule set, you can locate the various references to it using Cloud Control.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Rule Sets**.

If you are not sure which rule set contains that rule that you want to remove, then select **Rules** from Database Vault Components, select the rule that you want to remove, and then select the **View** option (but not the **View** menu). The rule sets that are associated with the rule are listed in Rule Set Usages.

3. Select the rule set to which you want to add an existing rule, and then click **Edit**.

4. Click **Next** until you reach the Associate with Rules page.
5. Select the rule you want to delete and click **Remove**.
6. Click **Done**, then click **Finish**.

After you remove the rule from the rule set, the rule still exists. If you want, you can associate it with other rule sets. If you want to delete the rule, then you can do so from the Rules page.

## 6.6 Removing Rule Set References to Oracle Database Vault Components

Before you remove a rule set, you should remove the rule set references to Oracle Database Vault components.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.

2. Find the references to the rule set that you want to delete.

In the Rule Sets page, select the rule set and then click the **View** button (but not the **View** menu). In the View Rule Set page, check the Ruleset Usages area for the references to the rule set that you want to remove. Click **OK**.

3. In the Administration page, under Database Vault Components, select the component that contains the reference to the rule set (such as **Realms**).
4. Select the object, and then click **Edit**.
5. Click **Next** until you reach the authorizations page.
6. Select the authorization with the rule set and then click **Edit**, and then remove the referenced object.
7. Click **Done**, then click **Finish**.

## 6.7 Deleting a Rule Set

You can use Enterprise Manager Cloud Control to find reference to the rule set and then delete the rule set.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. Remove references to the rule set.
3. Select the rule set that you want to remove and click **Delete**.
4. In the Confirmation window, click **Yes**.

The rule set is deleted. Optionally, you can choose to remove the existing associations with rules before deleting the rule set.

**Related Topics:**

[Removing Rule Set References to Oracle Database Vault Components](#) (page 6-15)

Before you remove a rule set, you should remove the rule set references to Oracle Database Vault components.

## 6.8 How Rule Sets Work

Understanding how rule sets work helps to create more effective rule sets.

[How Oracle Database Vault Evaluates Rules](#) (page 6-16)

Oracle Database Vault evaluates the rules within a rule set as a collection of expressions.

[Nested Rules within a Rule Set](#) (page 6-16)

You can nest one or more rules within the rule set.

[Creating Rules to Apply to Everyone Except One User](#) (page 6-17)

You can also create rules to apply to everyone *except* one user (for example, a privileged user).

### 6.8.1 How Oracle Database Vault Evaluates Rules

Oracle Database Vault evaluates the rules within a rule set as a collection of expressions.

If you have set **Evaluation Options** to **All True** and if a rule evaluates to false, then the evaluation stops at that point, instead of attempting to evaluate the rest of the rules in the rule set. Similarly, if **Evaluation Options** is set to **Any True** and if a rule evaluates to true, the evaluation stops at that point. If a rule set is disabled, Oracle Database Vault evaluates it to true without evaluating its rules.

### 6.8.2 Nested Rules within a Rule Set

You can nest one or more rules within the rule set.

For example, suppose you want to create a nested rule, *Is Corporate Network During Maintenance*, that performs the following two tasks:

- It limits table modifications only when the database session originates within the corporate network.
- It restricts table modifications during the system maintenance window scheduled between 10:00 p.m. and 10:59 p.m.

The rule definition would be as follows:

```
DVF.F$NETWORK = 'Corporate' AND TO_CHAR(SYSDATE,'HH24') between '22' AND '23'
```

**Related Topics:**

[Oracle Database Vault DVF PL/SQL Factor Functions](#) (page 18-27)

Oracle Database Vault maintains the DVF schema functions when you use the DBMS\_MACADM PL/SQL package to manage the various factors.

[Configuring Factors](#) (page 8-1)

Factors enable you to base Database Vault restrictions on attributes such as a client IP address or a domain.

### 6.8.3 Creating Rules to Apply to Everyone Except One User

You can also create rules to apply to everyone *except* one user (for example, a privileged user).

- To create a rule that excludes specific users, use the `SYS_CONTEXT` function.

For example:

```
SYS_CONTEXT('USERENV','SESSION_USER') = 'SUPERADMIN_USER' OR additional_rule
```

If the current user is a privileged user, then the system evaluates the rule to true without evaluating *additional\_rule*. If the current user is not a privileged user, then the evaluation of the rule depends on the evaluation of *additional\_rule*.

## 6.9 Tutorial: Creating an Email Alert for Security Violations

This tutorial demonstrates how to use the `UTL_MAIL PL/SQL` package and an access control list to create an email alert for security violations.

### [About This Tutorial](#) (page 6-17)

In tutorial, you create an email alert that is sent when a user attempts to alter a table outside a maintenance period.

### [Step 1: Install and Configure the UTL\\_MAIL PL/SQL Package](#) (page 6-18)

The `UTL_MAIL PL/SQL` package, which you must manually install, has procedures to manage email notifications.

### [Step 2: Create an Email Security Alert PL/SQL Procedure](#) (page 6-19)

User `leo_dvowner` can use the `CREATE PROCEDURE` statement to create the email security alert.

### [Step 3: Configure an Access Control List File for Network Services](#) (page 6-20)

Before you can use `UTL_MAIL`, you must configure an access control list (ACL) to enable fine-grained access to external network services.

### [Step 4: Create a Rule Set and a Command Rule to Use the Email Security Alert](#) (page 6-21)

To create the rule set and command rule, you can use `DBMS_MACADM PL/SQL` package.

### [Step 5: Test the Email Security Alert](#) (page 6-22)

After the alert has been created, it is ready to be tested.

### [Step 6: Remove the Components for This Tutorial](#) (page 6-23)

You can remove the components that you created for this tutorial if you no longer need them.

### 6.9.1 About This Tutorial

In tutorial, you create an email alert that is sent when a user attempts to alter a table outside a maintenance period.

To do this, you must create a rule to set the maintenance period hours, attach this rule to a rule set, and then create a command rule to allow the user to alter the table. You then associate the rule set with this command rule, which then sends the email alert when the user attempts to use the `ALTER TABLE SQL` statement outside the maintenance period.

**Note:**

To complete this tutorial, you must use a database that has an SMTP server.

## 6.9.2 Step 1: Install and Configure the UTL\_MAIL PL/SQL Package

The UTL\_MAIL PL/SQL package, which you must manually install, has procedures to manage email notifications.

1. Log into the database instance as SYS using the SYSDBA administrative privilege.

```
sqlplus sys as sysdba
Enter password: password
```

2. In a multitenant environment, connect to the appropriate pluggable database (PDB).

For example:

```
CONNECT SYS@my_pdb AS SYSDBA
Enter password: password
```

To find the available PDBs, query the DBA\_PDBS data dictionary view. To check the current PDB, run the `show con_name` command.

3. Install the UTL\_MAIL package.

```
@$ORACLE_HOME/rdbms/admin/utlmail.sql
@$ORACLE_HOME/rdbms/admin/prvtmail.plb
```

The UTL\_MAIL package enables you to manage email. See *Oracle Database PL/SQL Packages and Types Reference* for more information about UTL\_MAIL. However, be aware that currently, the UTL\_MAIL PL/SQL package do not support SSL servers.

4. Check the current value of the SMTP\_OUT\_SERVER parameter, and make a note of this value so that you can restore it when you complete this tutorial.

For example:

```
SHOW PARAMETER SMTP_OUT_SERVER
```

Output similar to the following appears:

NAME	TYPE	VALUE
SMTP_OUT_SERVER	string	some_value.example.com

5. Issue the following ALTER SYSTEM statement:

```
ALTER SYSTEM SET SMTP_OUT_SERVER='imap_mail_server.example.com';
```

Replace *imap\_mail\_server.example.com* with the name of your SMTP server, which you can find in the account settings in your email tool. Enclose these settings in double quotation marks. For example:

```
ALTER SYSTEM SET SMTP_OUT_SERVER='my_imap_mail_server.example.com'
```

6. Connect as SYS using the SYSOPER privilege and then restart the database.

```
CONNECT SYS AS SYSOPER -- Or, CONNECT SYS@hrpdb AS SYSOPER
Enter password: password
```

```
SHUTDOWN IMMEDIATE
STARTUP
```

7. Ensure that the SMTP\_OUT\_SERVER parameter setting is correct.

```
CONNECT SYS AS SYSDBA -- Or, CONNECT SYS@hrpdb AS SYSDBA
Enter password: password
```

```
SHOW PARAMETER SMTP_OUT_SERVER
```

Output similar to the following appears:

NAME	TYPE	VALUE
SMTP_OUT_SERVER	string	my_imap_mail_server.example.com

### 6.9.3 Step 2: Create an Email Security Alert PL/SQL Procedure

User `leo_dvowner` can use the `CREATE PROCEDURE` statement to create the email security alert.

1. Ensure that you are connected as a user who has privileges to perform the grants described in this step, and then grant these privileges to a user who has been granted the `DV_OWNER` role. You should also be authorized as an owner of the Oracle System Privilege and Role Management realm.

(Alternatively, you can select a user who has been granted the `DV_ADMIN` role, but for this tutorial, you will select a user who has the `DV_OWNER` role.)

For example:

```
CONNECT dba_psmith -- Or, CONNECT dba_psmith@hrpdb
Enter password: password
```

```
GRANT CREATE PROCEDURE, DROP ANY PROCEDURE TO leo_dvowner;
GRANT EXECUTE ON UTL_TCP TO leo_dvowner;
GRANT EXECUTE ON UTL_SMTP TO leo_dvowner;
GRANT EXECUTE ON UTL_MAIL TO leo_dvowner;
GRANT EXECUTE ON DBMS_NETWORK_ACL_ADMIN TO leo_dvowner;
```

The `UTL_TCP`, `UTL_SMTP`, `UTL_MAIL`, and `DBMS_NETWORK_ACL_ADMIN` PL/SQL packages will be used by the email security alert that you create.

2. Connect to SQL\*Plus as the `DV_OWNER` user.

For example:

```
CONNECT leo_dvowner -- Or, CONNECT leo_dvowner@hrpdb
Enter password: password
```

3. Create the following procedure:

```
CREATE OR REPLACE PROCEDURE email_alert AS
msg varchar2(20000) := 'Realm violation occurred for the ALTER TABLE Command
Security Policy rule set. The time is: ';
BEGIN
  msg := msg||to_char(SYSDATE, 'Day DD MON, YYYY HH24:MI:SS');
  UTL_MAIL.SEND (
    sender      => 'youremail@example.com',
    recipients => 'recipientemail@example.com',
    subject     => 'Table modification attempted outside maintenance!');
```

```

        message      => msg);
END email_alert;
/

```

Replace *youremail@example.com* with your email address, and *recipientemail@example.com* with the email address of the person you want to receive the notification.

4. Grant the EXECUTE permission on this procedure to DVSYS.

```
GRANT EXECUTE ON email_alert TO DVSYS;
```

### 6.9.4 Step 3: Configure an Access Control List File for Network Services

Before you can use UTL\_MAIL, you must configure an access control list (ACL) to enable fine-grained access to external network services.

For detailed information about fine-grained access to external network services, see *Oracle Database Security Guide*.

1. As the DV\_OWNER user, in SQL\*Plus, configure the following access control setting and its privilege definitions.

```

BEGIN
  DBMS_NETWORK_ACL_ADMIN.APPEND_HOST_ACE(
    host      => 'SMTP_OUT_SERVER_setting',
    lower_port => 25,
    ace       => xs$ace_type(privilege_list => xs$name_list('smtp'),
                           principal_name => 'LEO_DVOWNER',
                           principal_type => xs_acl.ptype_db));
END;
/

```

In this example:

- *lower\_port*: Enter the port number that your email tool specifies for its outgoing server. Typically, this setting is 25. Enter this value for both the *lower\_port* and *upper\_port* settings. (Currently, the UTL\_MAIL package does not support SSL. If your mail server is an SSL server, then enter 25 for the port number, even if the mail server uses a different port number.)
- *principal\_name*: Replace LEO\_DVOWNER with the name of the DV\_OWNER user.
- *host*: For the *SMTP\_OUT\_SERVER\_setting*, enter the SMTP\_OUT\_SERVER setting that you set for the SMTP\_OUT\_SERVER parameter in [Step 1: Install and Configure the UTL\\_MAIL PL/SQL Package](#) (page 6-18). This setting should match exactly the setting that your email tool specifies for its outgoing server.

2. Commit your changes to the database.

```
COMMIT;
```

3. Test the settings that you have created so far.

```
EXEC EMAIL_ALERT;
COMMIT;
```



SQL\*Plus should display a PL/SQL procedure successfully completed message, and in a moment, depending on the speed of your email server, you should receive the email alert.

If you receive an ORA-24247: network access denied by access control list (ACL) error followed by ORA-06512: at *stringline string* errors, then check the settings in the access control list file.

### 6.9.5 Step 4: Create a Rule Set and a Command Rule to Use the Email Security Alert

To create the rule set and command rule, you can use DBMS\_MACADM PL/SQL package.

1. As the DV\_OWNER user, create the following rule set:

```
BEGIN
DBMS_MACADM.CREATE_RULE_SET(
  rule_set_name => 'ALTER TABLE Command Security Policy',
  description   => 'This rule set allows ALTER TABLE only during the
                    maintenance period.',
  enabled       => DBMS_MACUTL.G_YES,
  eval_options  => DBMS_MACUTL.G_RULESET_EVAL_ALL,
  audit_options => DBMS_MACUTL.G_RULESET_AUDIT_FAIL,
  fail_options  => DBMS_MACUTL.G_RULESET_FAIL_SILENT,
  fail_message  => '',
  fail_code     => NULL,
  handler_options => DBMS_MACUTL.G_RULESET_HANDLER_FAIL,
  handler       => 'leo_dvowner.email_alert');
END;
/
```

2. Create a rule similar to the following.

For now, set the rule expression to be during the time you test it. For example, if you want to test it between 2 p.m. and 3 p.m., create the rule as follows:

```
BEGIN
DBMS_MACADM.CREATE_RULE(
  rule_name => 'Restrict Access to Maintenance Period',
  rule_expr => 'TO_CHAR(SYSDATE, 'HH24') BETWEEN '14' AND '15''');
END;
/
```

Ensure that you use two single quotation marks instead of double quotation marks for HH24, 14, and 15.

You can check the system time on your computer by issuing the following SQL statement:

```
SELECT TO_CHAR(SYSDATE, 'HH24') FROM DUAL;
```

Output similar to the following appears:

```
TO
--
14
```

Later on, when you are satisfied that the rule works, you can update it to a time when your site typically performs maintenance work (for example, between 7 p.m. and 10 p.m), as follows:

```
BEGIN
  DBMS_MACADM.UPDATE_RULE(
    rule_name => 'Restrict Access to Maintenance Period',
    rule_expr => 'TO_CHAR(SYSDATE, 'HH24') BETWEEN '16' AND '22');
END;
/
```

3. Add the Restrict Access to Maintenance Period rule to the ALTER TABLE Command Security Policy rule set.

```
BEGIN
  DBMS_MACADM.ADD_RULE_TO_RULE_SET(
    rule_set_name => 'ALTER TABLE Command Security Policy',
    rule_name      => 'Restrict Access to Maintenance Period');
END;
/
```

4. Create the following command rule:

```
BEGIN
  DBMS_MACADM.CREATE_COMMAND_RULE(
    command          => 'ALTER TABLE',
    rule_set_name    => 'ALTER TABLE Command Security Policy',
    object_owner     => 'SCOTT',
    object_name      => '%',
    enabled          => DBMS_MACUTL.G_YES);
END;
/
```

5. Commit these updates to the database.

```
COMMIT;
```

## 6.9.6 Step 5: Test the Email Security Alert

After the alert has been created, it is ready to be tested.

1. Connect to SQL\*Plus as user SCOTT.

For example:

```
CONNECT SCOTT -- Or, CONNECT SCOTT@hrpdb
Enter password: password
```

If the SCOTT account is locked and expired, then a user with the DV\_ACCTMGR role can unlock this account and create a new password as follows:

```
ALTER USER SCOTT ACCOUNT UNLOCK IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace *password* with a password that is secure.

2. As the user SCOTT, create a test table.

```
CREATE TABLE mytest (col1 number);
```

3. Change the system time on your computer to a time when the ALTER TABLE Command Security Policy rule set takes place.

For example, if you set the test period time to between 2 p.m. and 3 p.m., do the following:

**UNIX:** Log in as root and use the `date` command to set the time. For example, assuming the date today is August 15, 2012, you would enter the following:

```
$ su root
Password: password

$ date -s "08/15/2012 14:48:00"
```

**Windows:** Double-click the clock icon, which is typically at the lower right corner of the screen. In the Date and Time Properties window, set the time to 2 p.m., and then click **OK**.

4. Try altering the `my_test` table.

```
ALTER TABLE mytest ADD (col2 number);

Table altered.
```

SCOTT should be able to alter the `mytest` table during this time.

5. Reset the system time to a time outside the Restrict Access to Maintenance Period time.
6. Log in as SCOTT and try altering the `my_test` table again.

```
CONNECT SCOTT -- Or, CONNECT SCOTT@hrpdb
Enter password: password
```

```
ALTER TABLE mytest ADD (col3 number);
```

The following output should appear:

```
ORA-47400: Command Rule violation for ALTER TABLE on SCOTT.MYTEST
```

SCOTT cannot alter the `mytest` table. In a moment, you should receive an email with the subject header `Table modification attempted outside maintenance!` and with a message similar to the following:

```
Realm violation occurred for the ALTER TABLE Command Security Policy rule set.
The time is: Wednesday 15 AUG, 2012 14:24:25
```

7. Reset the system time to the correct time.

## 6.9.7 Step 6: Remove the Components for This Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. Connect to SQL\*Plus as the `DV_OWNER` user.

```
CONNECT leo_dvowner -- Or, CONNECT leo_dvowner@hrpdb
Enter password: password
```

2. In the order shown, drop the Oracle Database Vault rule components.

```
EXEC DBMS_MACADM.DELETE_RULE_FROM_RULE_SET('ALTER TABLE Command Security Policy',
'Restrict Access to Maintenance Period');
EXEC DBMS_MACADM.DELETE_RULE('Restrict Access to Maintenance Period');
EXEC DBMS_MACADM.DELETE_COMMAND_RULE('ALTER TABLE', 'SCOTT', '%');
EXEC DBMS_MACADM.DELETE_RULE_SET('ALTER TABLE Command Security Policy');
```

3. Drop the `email_alert` PL/SQL procedure.

```
DROP PROCEDURE email_alert;
```

4. Connect as user `SCOTT` and remove the `mytest` table.

```
CONNECT SCOTT -- Or, CONNECT SCOTT@hrpdb
```

```
Enter password: password
```

```
DROP TABLE mytest;
```

5. Connect as a user who has privileges to revoke privileges from other users.

For example:

```
CONNECT dba_psmith -- Or, CONNECT dba_psmith@hrpdb
```

```
Enter password: password
```

6. Revoke the `EXECUTE` privilege on the `UTL_TCP`, `UTL_SMTP`, and `UTL_MAIL` PL/SQL packages from the `DV_OWNER` user.

For example:

```
REVOKE EXECUTE ON UTL_TCP FROM leo_dvowner;
```

```
REVOKE EXECUTE ON UTL_SMTP FROM leo_dvowner;
```

```
REVOKE EXECUTE ON UTL_MAIL FROM leo_dvowner;
```

```
REVOKE EXECUTE ON DBMS_NETWORK_ACL_ADMIN FROM leo_dvowner;
```

7. Set the `SMTP_OUT_SERVER` parameter to its original value.

For example:

```
ALTER SYSTEM SET SMTP_OUT_SERVER="some_value.example.com";
```

8. Connect as `SYS` with the `SYSOPER` administrative privilege and then restart the database.

```
CONNECT SYS AS SYSOPER -- Or, CONNECT SYS@hrpdb AS SYSOPER
```

```
Enter password: password
```

```
SHUTDOWN IMMEDIATE
```

```
STARTUP
```

## 6.10 Tutorial: Configuring Two-Person Integrity, or Dual Key Security

This tutorial demonstrates how to use Oracle Database Vault to control the authorization of two users.

[About This Tutorial](#) (page 6-25)

In this tutorial, you configure a rule set that defines two-person integrity (TPI).

[Step 1: Create Users for This Tutorial](#) (page 6-25)

You must create two users for this tutorial, `patch_boss` and `patch_user`.

[Step 2: Create a Function to Check if User `patch\_boss` Is Logged In](#) (page 6-26)

The behavior of the Database Vault settings will be determined by the function.

[Step 3: Create Rules, a Rule Set, and a Command Rule to Control User Access](#)  
(page 6-27)

Next, you must create two rules, a rule set to which you will add them, and a command rule.

[Step 4: Test the Users' Access](#) (page 6-28)

After the rules have been created, they are ready to be tested.

[Step 5: Remove the Components for This Tutorial](#) (page 6-29)

You can remove the components that you created for this tutorial if you no longer need them.

## 6.10.1 About This Tutorial

In this tutorial, you configure a rule set that defines two-person integrity (TPI).

This feature is also called dual key security, dual key connection, and two-man rule security. In this type of security, two users are required to authorize an action instead of one user.

The idea is that one user provides a safety check for the other user before that user can proceed with a task. Two-person integrity provides an additional layer of security for actions that potentially can be dangerous. This type of scenario is often used for tasks such as database patch updates, which is what this tutorial will demonstrate. One user, `patch_user` must log into perform a database patch upgrade, but the only way that he can do this is if his manager, `patch_boss` is already logged in. You will create a function, rules, a rule set, and a command rule to control `patch_user`'s ability to log in.

## 6.10.2 Step 1: Create Users for This Tutorial

You must create two users for this tutorial, `patch_boss` and `patch_user`.

- `patch_boss` acts in a supervisory role: If `patch_boss` is not logged in, then the `patch_user` user cannot log in.
- `patch_user` is the user who is assigned to perform the patch upgrade. However, for this tutorial, user `patch_user` does not actually perform a patch upgrade. He only attempts to log in.

To create the users:

1. Log into the database instance as a user who has been granted the `DV_ACCTMGR` role.

For example:

```
sqlplus bea_dvacctmgr
Enter password: password
```

In a multitenant environment, you must log in to the appropriate pluggable database (PDB). For example:

```
sqlplus bea_dvacctmgr@hrpdb
Enter password: password
```

To find the available PDBs, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

2. Create the following users and grant them the `CREATE SESSION` privilege.

```
GRANT CREATE SESSION TO patch_boss IDENTIFIED BY password;  
GRANT CREATE SESSION TO patch_user IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace *password* with a password that is secure.

3. Connect as user *SYS* with the *SYSDBA* administrative privilege.

```
CONNECT SYS AS SYSDBA -- Or, CONNECT SYS@hrpdb AS SYSDBA  
Enter password: password
```

4. Grant the following privileges to the *DV\_OWNER* or *DV\_ADMIN* user.

For example:

```
GRANT CREATE PROCEDURE TO leo_dvowner;  
GRANT SELECT ON V_$SESSION TO leo_dvowner;
```

The *V\_\$SESSION* table is the underlying table for the *V\$SESSION* dynamic view.

In a real-world scenario, you also would log in as the *DV\_OWNER* user and grant the *DV\_PATCH\_ADMIN* role to user *patch\_user* (but not to *patch\_boss*). But because you are not really going to perform a database patch upgrade in this tutorial, you do not need to grant this role to user *patch\_user*.

### 6.10.3 Step 2: Create a Function to Check if User *patch\_boss* Is Logged In

The behavior of the Database Vault settings will be determined by the function.

The function that you must create, *check\_boss\_logged\_in*, does just that: When user *patch\_user* tries to log into the database instance, it checks if user *patch\_boss* is already logged in by querying the *V\$SESSION* data dictionary view.

1. Connect as a user who has been granted the *DV\_OWNER* or *DV\_ADMIN* role.

For example:

```
CONNECT leo_dvowner -- Or, CONNECT leo_dvowner@hrpdb  
Enter password: password
```

2. Create the *check\_boss\_logged\_in* function as follows:

```
CREATE OR REPLACE FUNCTION check_boss_logged_in  
return varchar2  
authid definer as  
  
v_session_number number := 0;  
v_allow varchar2(10) := 'TRUE';  
v_deny varchar2(10) := 'FALSE';  
  
BEGIN  
  SELECT COUNT(*) INTO v_session_number  
  FROM SYS.V_$SESSION  
  WHERE USERNAME = 'PATCH_BOSS'; -- Enter the user name in capital letters.  
  
  IF v_session_number > 0  
  THEN RETURN v_allow;  
  ELSE  
  RETURN v_deny;  
  END IF;  
END check_boss_logged_in;  
/
```

3. Grant the EXECUTE privilege on the check\_boss\_logged\_in function to the DVSYS schema.

```
GRANT EXECUTE ON check_boss_logged_in to DVSYS;
```

### 6.10.4 Step 3: Create Rules, a Rule Set, and a Command Rule to Control User Access

Next, you must create two rules, a rule set to which you will add them, and a command rule.

The rule set triggers the check\_boss\_logged\_in function when user patch\_user tries to log in to the database.

1. Connect as a user who has been granted the DV\_OWNER or DV\_ADMIN role.

For example:

```
CONNECT leo_dvowner -- Or, CONNECT leo_dvowner@hrpdb
Enter password: password
```

2. Create the Check if Boss Is Logged In rule, which checks that the patch\_user user is logged in to the database. In the definition, replace leo\_dvowner with the name of the DVOWNER or DV\_ADMIN user who created the check\_boss\_logged\_in function.

If the check\_boss\_logged\_in function returns TRUE (that is, patch\_boss is logged in to another session), then patch\_user can log in.

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check if Boss Is Logged In',
    rule_expr => 'SYS_CONTEXT(''USERENV'', 'SESSION_USER') = ''PATCH_USER'' and
leo_dvowner.check_boss_logged_in = ''TRUE'' ');
END;
/
```

Enter the user name, PATCH\_USER, in upper-case letters, which is how the SESSION\_USER parameter stores it.

3. Create the Allow Connect for Other Database Users rule, which ensures that the user logged in (patch\_user) is not user patch\_boss. It also enables all other valid users to log in.

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Allow Connect for Other Database Users',
    rule_expr => 'SYS_CONTEXT(''USERENV'', 'SESSION_USER') != ''PATCH_USER''');
END;
/
COMMIT;
```

4. Create the Dual Connect for Boss and Patch rule set, and then add the two rules to it.

```
BEGIN
  DBMS_MACADM.CREATE_RULE_SET(
    rule_set_name => 'Dual Connect for Boss and Patch',
    description => 'Checks if both boss and patch users are logged in.',
    enabled => DBMS_MACUTL.G_YES,
    eval_options => 2,
    audit_options => DBMS_MACUTL.G_RULESET_AUDIT_FAIL,
```

```
        fail_options      => DBMS_MACUTL.G_RULESET_FAIL_SILENT,
        fail_message     => '',
        fail_code        => NULL,
        handler_options  => DBMS_MACUTL.G_RULESET_HANDLER_OFF,
        handler          => ''
    );
END;
/

BEGIN
    DBMS_MACADM.ADD_RULE_TO_RULE_SET(
        rule_set_name     => 'Dual Connect for Boss and Patch',
        rule_name        => 'Check if Boss Is Logged In'
    );
END;
/

BEGIN
    DBMS_MACADM.ADD_RULE_TO_RULE_SET(
        rule_set_name     => 'Dual Connect for Boss and Patch',
        rule_name        => 'Allow Connect for Other Database Users'
    );
END;
/
```

5. Create the following **CONNECT** command rule, which permits user `patch_user` to connect to the database only if `patch_boss` is already logged in.

```
BEGIN
    DBMS_MACADM.CREATE_COMMAND_RULE(
        command           => 'CONNECT',
        rule_set_name     => 'Dual Connect for Boss and Patch',
        object_owner      => '%',
        object_name       => '%',
        enabled           => DBMS_MACUTL.G_YES);
END;
/
COMMIT;
```

### 6.10.5 Step 4: Test the Users' Access

After the rules have been created, they are ready to be tested.

1. Exit SQL\*Plus.

```
EXIT
```

2. Create a second shell, for example:

```
xterm &
```

3. In the first shell, try to log in as user `patch_user`.

```
sqlplus patch_user -- Or, sqlplus patch_user@hrpdb
Enter password: password
```

```
ERROR:
ORA-47400: Command Rule violation for CONNECT on LOGON
```

```
Enter user-name:
```



User `patch_user` cannot log in until user `patch_boss` is already logged in. (Do not try the `Enter user-name` prompt yet.)

4. In the second shell and then log in as user `patch_boss`.

```
sqlplus patch_boss -- Or, sqlplus patch_boss@hrpdb
Enter password: password
Connected.
```

User `patch_boss` can log in.

5. Go back to the first shell, and then try logging in as user `patch_user` again.

```
Enter user_name: patch_user
Enter password: password
```

This time, user `patch_user` is deemed a valid user, so now he can log in.

## 6.10.6 Step 5: Remove the Components for This Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. In the session for the user `patch_boss`, exit SQL\*Plus and then close the shell.

```
EXIT
```

2. In the first shell, connect the `DV_ACCTMGR` user and remove the users you created.

```
CONNECT bea_dvacctmgr -- Or, CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

```
DROP USER patch_boss;
DROP USER patch_user;
```

3. Connect as a user `SYS` with the `SYSDBA` administrative privilege and revoke the privileges that you had granted to the `DV_OWNER` or `DV_ADMIN` user.

```
CONNECT SYS AS SYSDBA -- Or, CONNECT SYS@hrpdb AS SYSDBA
Enter password: password
```

```
REVOKE CREATE PROCEDURE FROM leo_dvowner;
REVOKE SELECT ON V_$SESSION FROM leo_dvowner;
```

4. Connect as the `DV_OWNER` or `DV_ADMIN` user and drop the rules, rule set, and command rule, in the order shown.

```
CONNECT leo_dvowner -- Or, CONNECT leo_dvowner@hrpdb
Enter password: password
```

```
DROP FUNCTION check_boss_logged_in;
EXEC DBMS_MACADM.DELETE_COMMAND_RULE('CONNECT', '%', '%');
EXEC DBMS_MACADM.DELETE_RULE_FROM_RULE_SET('Dual Connect for Boss and Patch',
'Check if Boss Is Logged In');
EXEC DBMS_MACADM.DELETE_RULE_FROM_RULE_SET('Dual Connect for Boss and Patch',
'Allow Connect for Other Database Users');
EXEC DBMS_MACADM.DELETE_RULE('Check if Boss Is Logged In');
EXEC DBMS_MACADM.DELETE_RULE('Allow Connect for Other Database Users');
EXEC DBMS_MACADM.DELETE_RULE_SET('Dual Connect for Boss and Patch');
COMMIT;
```

## 6.11 Guidelines for Designing Rule Sets

Oracle provides guidelines for designing rule sets.

- You can share rules among multiple rule sets. This lets you develop a library of reusable rule expressions. Oracle recommends that you design such rules to be discrete, single-purpose expressions.
- You can design a rule set so that its evaluation is static, that is, it is evaluated only once during a user session. Alternatively, it can be evaluated each time the rule set is accessed. If the rule set is evaluated only once, then the evaluated value is reused throughout the user session each time the rule set is accessed. Using static evaluation is useful in cases where the rule set must be accessed multiple times but the conditions on which the rule set depend do not change during that session. An example would be a `SELECT` command rule associated with a rule set when the same `SELECT` statement occurs multiple times and if the evaluated value is acceptable to use again, rather than evaluating the rule set each time the `SELECT` occurs.

To control the static evaluation of the rule set, set the `is_static` parameter of the `CREATE_RULE_SET` or `UPDATE_RULE_SET` procedures of the `DBMS_MACADM` PL/SQL package. See [DBMS\\_MACADM Rule Set Procedures](#) (page 16-1) for more information.

- Use Oracle Database Vault factors in your rule expressions to provide reusability and trust in the values used by your rule expressions. Factors can provide contextual information to use in your rules expressions.
- You can use custom event handlers to extend Oracle Database Vault security policies to integrate external systems for error handling or alerting. Using Oracle utility packages such as `UTL_TCP`, `UTL_HTTP`, `UTL_MAIL`, `UTL_SMTTP`, or `DBMS_AQ` can help you to achieve this type of integration.
- Test rule sets thoroughly for various accounts and scenarios either on a test database or on a test realm or command rule for nonsensitive data before you apply them to realms and command rules that protect sensitive data. You can test rule expressions directly with the following SQL statement:

```
SQL> SELECT SYSDATE from DUAL where rule expression
```

- You can nest rule expressions inside a single rule. This helps to achieve more complex situations where you would need a logical `AND` for a subset of rules and a logical `OR` with the rest of the rules. See the definition for the `Is Corporate Network During Maintenance` rule set under [Tutorial: Creating an Email Alert for Security Violations](#) (page 6-17) for an example.
- You cannot use invoker's rights procedures with rule expressions. Only use definer's rights procedures with rule expressions.

## 6.12 How Rule Sets Affect Performance

The number and complexity of rules can slow database performance.

Rule sets govern the performance for execution of certain operations. For example, if you have a very large number of rules in a rule set governing a `SELECT` statement, performance could degrade significantly.

If you have rule sets that require many rules, performance improves if you move all the rules to logic defined in a single PL/SQL standalone or package function. However, if a rule is used by other rule sets, there is little performance effect on your system.

If possible, consider setting the rule set to use static evaluation, assuming this is compatible with the associated command rule's usage. See [Guidelines for Designing Rule Sets](#) (page 6-30) for more information.

You can check system performance by running tools such as Oracle Enterprise Manager (including Oracle Enterprise Manager Cloud Control, which is installed by default with Oracle Database), Automatic Workload Repository (AWR), and TKPROF.

---



---

**See Also:**

- *Oracle Database Performance Tuning Guide* to learn how to monitor database performance
  - *Oracle Database SQL Tuning Guide* to monitor the performance of individual SQL and PL/SQL statements
- 
- 

## 6.13 Rule Set and Rule Related Reports and Data Dictionary Views

Oracle Database Vault provides reports and data dictionary views that are useful for analyzing rule sets and the rules within them.

[Table 6-2](#) (page 6-31) lists the Oracle Database Vault reports. See [Oracle Database Vault Reports](#) (page 27-1) for information about how to run these reports.

**Table 6-2 Reports Related to Rule Sets**

Report	Description
<a href="#">Rule Set Configuration Issues Report</a> (page 27-3)	Lists rule sets that have no rules defined or enabled
<a href="#">Secure Application Configuration Issues Report</a> (page 27-5)	Lists secure application roles that have incomplete or disabled rule sets
<a href="#">Command Rule Configuration Issues Report</a> (page 27-3)	Lists rule sets that are incomplete or disabled

[Table 6-3](#) (page 6-31) lists data dictionary views that provide information about existing rules and rule sets.

**Table 6-3 Data Dictionary Views Used for Rules and Rule Sets**

Data Dictionary View	Description
<a href="#">DBA_DV_RULE View</a> (page 25-29)	Lists the rules that have been defined
<a href="#">DBA_DV_RULE_SET View</a> (page 25-30)	Lists the rule sets that have been created
<a href="#">DBA_DV_RULE_SET_RULE View</a> (page 25-32)	Lists rules that are associated with existing rule sets



---

# Configuring Command Rules

You can create command rules or use the default command rules to protect DDL and DML statements.

## [What Are Command Rules?](#) (page 7-2)

A command rule applies Oracle Database Vault protections with an Oracle Database SQL statement, such as `ALTER SESSION`.

## [Default Command Rules](#) (page 7-7)

Oracle Database Vault provides default command rules, based on commonly used SQL statements.

## [SQL Statements That Can Be Protected by Command Rules](#) (page 7-8)

You can protect a large number of SQL statements by using command rules.

## [Creating a Command Rule](#) (page 7-9)

You can create a command rule in Oracle Database Vault Administrator.

## [Modifying the Enablement Status of a Command Rule](#) (page 7-11)

You can enable or disable a command rule in Oracle Database Vault Administrator.

## [Deleting a Command Rule](#) (page 7-11)

Before you delete a command rule, you can locate the various references to it by querying the command rule-related Oracle Database Vault views.

## [How Command Rules Work](#) (page 7-11)

Command rules follow a set of steps to check their associated components.

## [Tutorial: Using a Command Rule to Control Table Creations by a User](#) (page 7-12)

In this tutorial, you create a simple local command rule to control whether users can create tables in the `SCOTT` schema.

## [Guidelines for Designing Command Rules](#) (page 7-15)

Oracle provides guidelines for designing command rules.

## [How Command Rules Affect Performance](#) (page 7-16)

The performance of a command rule depends on the complexity of the rules in the rule set associated with the command rule.

## [Command Rule Related Reports and Data Dictionary View](#) (page 7-16)

Oracle Database Vault provides reports and a data dictionary view that are useful for analyzing command rules.

## 7.1 What Are Command Rules?

A command rule applies Oracle Database Vault protections with an Oracle Database SQL statement, such as `ALTER SESSION`.

### [About Command Rules](#) (page 7-2)

A command rule protects Oracle Database SQL statements that affect one or more database objects.

### [Command Rules in a Multitenant Environment](#) (page 7-3)

In a multitenant environment, you can create common and local command rules in either the CDB root or the application root.

### [Types of Command Rules](#) (page 7-4)

In addition to command rules for many SQL statements, you can create command rules specifically for the `CONNECT`, `ALTER SYSTEM`, and `ALTER SESSION` SQL statements.

### 7.1.1 About Command Rules

A command rule protects Oracle Database SQL statements that affect one or more database objects.

These statements can include `SELECT`, `ALTER SYSTEM`, database definition language (DDL), and data manipulation language (DML) statements.

To customize and enforce the command rule, you associate it with a rule set, which is a collection of one or more rules. The command rule is enforced at run time. Command rules affect anyone who tries to use the SQL statements it protects, regardless of the realm in which the object exists.

You can use command rules to protect a wide range of SQL statements, in addition to basic Oracle Database DDL and DML statements. For example, you can protect statements that are used with Oracle Flashback Technology.

A command rule has the following attributes, in addition to associating a command rule to a command:

- SQL statement the command rule protects
- Owner of the object the command rule affects
- Database object the command rule affects
- Whether the command rule is enabled
- An associated rule set

Command rules can be categorized as follows:

- **Command rules that have a system-wide scope.** With this type, in most cases, you can only create one command rule for each database instance.
- **Command rules that are schema specific.** An example of a schema-specific command rule is a command rule for the `DROP TABLE` statement. You can create only one `CONNECT` command rule for each schema.
- **Command rules that are object specific.** An example is creating a command rule for the `DROP TABLE` statement with a specific table included in the command rule definition.

When a user executes a statement affected by a command rule, Oracle Database Vault checks the realm authorization first. If it finds no realm violation and if the associated command rules are enabled, then Database Vault evaluates the associated rule sets. If all the rule sets evaluate to `TRUE`, then the statement is authorized for further processing. If any of the rule sets evaluate to `FALSE`, then the statement is not allowed to be executed and a command rule violation is raised.

You can define a command rule that uses factors for the `CONNECT` event to permit or deny sessions after the usual steps—user authentication process, factor initialization, and Oracle Label Security integration—are complete.

For example, you can configure a command rule that allows DDL statements such as `CREATE TABLE`, `DROP TABLE`, and `ALTER TABLE` in the `BIZAPP` schema to be authorized after business hours, but not during business hours.

You can run reports on the command rules that you create in Oracle Database Vault.

### Related Topics:

#### [Oracle Database Vault Command Rule APIs](#) (page 17-1)

The `DBMS_MACADM` PL/SQL package provides procedures for configuring command rules. .

#### [Configuring Rule Sets](#) (page 6-1)

Rule sets group one or more rules together; the rules determine whether a user can perform an action on an object.

#### [SQL Statements That Can Be Protected by Command Rules](#) (page 7-8)

You can protect a large number of SQL statements by using command rules.

## 7.1.2 Command Rules in a Multitenant Environment

In a multitenant environment, you can create common and local command rules in either the CDB root or the application root.

Common command rules can be associated only with common realms, rule sets, and rules. Local command rules can be associated only with local realm, rule sets, and rules.

To apply these command rules to the entire multitenant environment, you must execute the command rule procedures from the CDB root or application root as a common user who has been granted the `DVADM` or `DVOWNER` role. A common command rule that is created in the CDB root will be applied to all PDBs in that CDB environment. A common command rule that is created in the application root will only be applied to the PDBs that are associated with this application root. To propagate the command rule to the PDBs that are associated with the application root, you must synchronize the application root. For example, to synchronize an application called `saas_sales_app`:

```
ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;
```

You can check a user's roles by querying the `USER_ROLE_PRIVS` data dictionary view. To find information about command rules, query the `DBA_DV_COMMAND_RULE` data dictionary view.

## 7.1.3 Types of Command Rules

In addition to command rules for many SQL statements, you can create command rules specifically for the `CONNECT`, `ALTER SYSTEM`, and `ALTER SESSION SQL` statements.

### [CONNECT Command Rule](#) (page 7-4)

The `DBMS_MACADM.CREATE_CONNECT_CMD_RULE` procedure creates a user-specific `CONNECT` command rule.

### [ALTER SESSION and ALTER SYSTEM Command Rules](#) (page 7-5)

You can create different kinds of `ALTER SESSION` and `ALTER SYSTEM` command rules that provide fine-grained control for these SQL statements.

#### 7.1.3.1 CONNECT Command Rule

The `DBMS_MACADM.CREATE_CONNECT_CMD_RULE` procedure creates a user-specific `CONNECT` command rule.

This type of command rule specifies a user, an associated rule set, an enablement status, and for a multitenant environment, where to execute the `CONNECT` command rule. You can enable or disable the `CONNECT` command rule, or you can set it to use simulation mode. In simulation mode, violations to the command rule are logged in a designated log table with sufficient information to describe the error, such as the user name or SQL statement used.

In a multitenant environment, you can create the `CONNECT` command rule in either the application root or in a specific PDB. The associated rule set must be consistent with the `CONNECT` command rule: if the `CONNECT` command rule is in the application root, then the rule set and rules must also be in the application root. You run the `CONNECT` command rule procedures from the CDB root as a common user. If the `CONNECT` command rule is local to a pluggable database (PDB), then you must run the `CONNECT` command rule creation command in that PDB, and the rule set and rules must be local.

The following example shows a `CONNECT` command rule definition that creates a local, enabled `CONNECT` command rule for the HR user. The rule set that is associated with this command rule is local to the current PDB.

```
BEGIN
DBMS_MACADM.CREATE_CONNECT_COMMAND_RULE(
  rule_set_name => 'Enabled',
  user_name     => 'HR',
  enabled       => DBMS_MACUTL.G_YES,
  scope        => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/
```

#### Related Topics:

### [CREATE\\_COMMAND\\_RULE Procedure](#) (page 17-2)

The `CREATE_COMMAND_RULE` procedure creates a command rule and associates it with a rule set.



### Using Simulation Mode for Logging Realm and Command Rule Activities (page 11-1)

Simulation mode writes the activities performed on realms and command rules to a log file, which is accessible through a data dictionary view.

#### 7.1.3.2 ALTER SESSION and ALTER SYSTEM Command Rules

You can create different kinds of ALTER SESSION and ALTER SYSTEM command rules that provide fine-grained control for these SQL statements.

The procedures to create these types of command rules are as follows:

- DBMS\_MACADM.CREATE\_COMMAND\_RULE creates ALTER SESSION and ALTER SYSTEM command rules that use clauses from the corresponding SQL statement, such as ADVISE, CLOSE DATABASE LINK, COMMIT IN PROCEDURE, and SET for ALTER SESSION, or ARCHIVE\_LOG, CHECK DATAFILES, CHECKPOINT, and SET for ALTER SYSTEM.
- DBMS\_MACADM.CREATE\_SESSION\_EVENT creates a command rule that is specific to the ALTER SESSION SET EVENTS SQL statement
- DBMS\_MACADM.CREATE\_SYSTEM\_EVENT creates a command rule that is specific to the ALTER SYSTEM SET EVENTS SQL statement.

To create these command rules, you use the appropriate Database Vault procedure to specify the clause and if applicable, the parameter of the clause, in the creation statement. If the ALTER SESSION or ALTER SYSTEM command rule use the SET EVENTS setting, then you can use special parameters to specify events, components, and actions.

For example, for an ALTER SYSTEM command rule, you could specify the SECURITY clause and its RESTRICTED SESSION parameter from the ALTER SYSTEM SQL statement. To specify whether RESTRICTED SESSION is TRUE or FALSE, you must create a Database Vault rule and rule set, which can test for the validity of this sequence number.

To understand how this concept works, first create the following rule and rule set, which are designed to check if the RESTRICTED SESSION parameter is set to TRUE:

```
EXEC DBMS_MACADM.CREATE_RULE('RESTRICTED SESSION TRUE', 'UPPER(PARAMETER_VALUE) =
'TRUE');

BEGIN
  DBMS_MACADM.CREATE_RULE_SET(
    rule_set_name => 'Check RESTRICTED SESSION for TRUE',
    description   => 'Checks if restricted session is true',
    enabled       => DBMS_MACUTL.G_YES,
    eval_options  => DBMS_MACUTL.G_RULESET_EVAL_ALL,
    audit_options => DBMS_MACUTL.G_RULESET_AUDIT_FAIL +
DBMS_MACUTL.G_RULESET_AUDIT_SUCCESS,
    fail_options  => DBMS_MACUTL.G_RULESET_FAIL_SILENT,
    fail_message  => 'RESTRICTED SESSION is not TRUE',
    fail_code     => 20461,
    handler_options => DBMS_MACUTL.G_RULESET_HANDLER_FAIL,
    handler       => '',
    is_static     => false);
END;
/
EXEC DBMS_MACADM.ADD_RULE_TO_RULE_SET(Check RESTRICTED SESSION for TRUE',
'RESTRICTED SESSION TRUE');
```

With the rule and rule set in place, you are ready to create an ALTER SYSTEM command rule that will check if the RESTRICTED SESSION parameter:

```
BEGIN
DBMS_MACADM.CREATE_COMMAND_RULE(
  command          => 'ALTER SYSTEM',
  rule_set_name    => 'Check RESTRICTED SESSION for TRUE',
  object_owner     => '%',
  object_name      => '%',
  enabled          => DBMS_MACUTL.G_YES,
  clause_name      => 'SECURITY',
  parameter_name   => 'RESTRICTED SESSION',
  scope            => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/
```

In this example:

- `rule_set_name` checks whether RESTRICTED SESSION is set to TRUE or FALSE. In a multitenant environment, you must create the rule set and rule in the same location as the command rule: either in the application root or locally in a PDB.
- `object_owner` and `object_name` must always be set to % for this kind of ALTER SESSION or ALTER SYSTEM command rule.
- `enabled` enables you to enable or disable the command rule, or to use simulation mode to log violations to the command rule to a designated log table. The log data describes the error, such as the user name or SQL statement used.
- `clause_name` specifies the SECURITY clause of the ALTER SYSTEM SQL statement
- `parameter_name` specifies the RESTRICTED SESSION parameter from the SECURITY clause
- `scope` sets the command rule to be local to the current PDB. The associated rule set and rule must also be local to the current PDB. If you want to create the command rule in the application root, then as a common user, you would set `scope` to `DBMS_MACUTL.G_SCOPE_COMMON` and run the procedure (and its accompanying rule set and rule creation procedures) from the application root.

**See Also:**

- [CREATE\\_COMMAND\\_RULE Procedure](#) (page 17-2) about the DBMS\_MACADM.CREATE\_COMMAND\_RULE procedure
- [CREATE\\_SESSION\\_EVENT\\_CMD\\_RULE Procedure](#) (page 17-11) about the DVS.DBMS\_MACADM.CREATE\_SESSION\_EVENT\_CMD\_RULE procedure
- [CREATE\\_SYSTEM\\_EVENT\\_CMD\\_RULE Procedure](#) (page 17-12) for more information about the DBMS\_MACADM.CREATE\_SYSTEM\_EVENT\_CMD\_RULE procedure
- [DBA\\_DV\\_COMMAND\\_RULE View](#) (page 25-8) for information about the DBA\_DV\_COMMAND\_RULE data dictionary view
- *Oracle Database SQL Language Reference* for information about the ALTER SESSION SQL statement
- *Oracle Database SQL Language Reference* for information about the ALTER SYSTEM SQL statement

## 7.2 Default Command Rules

Oracle Database Vault provides default command rules, based on commonly used SQL statements.

[Table 7-1](#) (page 7-7) lists the default Database Vault command rules.

**Table 7-1 Default Command Rules**

SQL Statement	Rule Set Name
CREATE USER	Can Maintain Accounts/Profiles
ALTER USER	Can Maintain Own Account
DROP USER	Can Maintain Accounts/Profiles
CREATE PROFILE	Can Maintain Accounts/Profiles
ALTER PROFILE	Can Maintain Accounts/Profiles
DROP PROFILE	Can Maintain Accounts/Profiles
ALTER SYSTEM	Allow Fine Grained Control of System Parameters
CHANGE PASSWORD	Can Maintain Own Account <sup>1</sup>

<sup>1</sup> The actual SQL statement that the Can Maintain Own Account rule refers to is PASSWORD.

The following set of command rules helps you to achieve separation of duty for user management:

- ALTER PROFILE
- ALTER USER
- CREATE PROFILE

- CREATE USER
- DROP PROFILE
- DROP USER

To grant a user the ability to use these commands, you can grant the user the role that the rule set checks. For example, the CREATE USER command rule ensures that a user who tries to run a CREATE USER statement has the DV\_ACCTMGR role.

---

**Note:**

To find information about the default command rules, query the DBA\_DV\_COMMAND\_RULE data dictionary view.

---

## 7.3 SQL Statements That Can Be Protected by Command Rules

You can protect a large number of SQL statements by using command rules.

The SQL statements that you can protect are as follows:

SQL Statements A-C	SQL Statements C-D	SQL Statements D-U
ALTER CLUSTER	ANALYZE TABLE	CREATE TABLE
ALTER DIMENSION	ASSOCIATE STATISTICS	CREATE TABLESPACE
ALTER FLASHBACK ARCHIVE	AUDIT	CREATE TRIGGER
ALTER FUNCTION	CHANGE PASSWORD	CREATE TYPE
ALTER INDEX	COMMENT	CREATE TYPE BODY
ALTER INDEXTYPE	CONNECT	CREATE VIEW
ALTER JAVA	CREATE EDITION	DELETE
ALTER LIBRARY	CREATE FLASHBACK ARCHIVE	DISASSOCIATE STATISTICS
ALTER OPERATOR	CREATE USER	DROP CLUSTER
ALTER OUTLINE	CREATE CLUSTER	DROP CONTEXT
ALTER MATERIALIZED VIEW	CREATE CONTEXT	DROP DATABASE LINK
ALTER MATERIALIZED VIEW LOG	CREATE DATABASE LINK	DROP EDITION
ALTER PACKAGE	CREATE DIMENSION	DROP DIMENSION
ALTER PACKAGE BODY	CREATE DIRECTORY	DROP DIRECTORY
ALTER PLUGGABLE DATABASE	CREATE FUNCTION	DROP FLASHBACK ARCHIVE
ALTER PROCEDURE	CREATE INDEX	DROP FUNCTION
ALTER PROFILE	CREATE INDEXTYPE	FLASHBACK TABLE
ALTER RESOURCE COST	CREATE JAVA	EXECUTE

SQL Statements A-C	SQL Statements C-D	SQL Statements D-U
ALTER ROLE	CREATE LIBRARY	GRANT
ALTER ROLLBACK SEGMENT	CREATE OPERATOR	INSERT
ALTER SEQUENCE	CREATE OUTLINE	NOAUDIT
ALTER SESSION	CREATE PACKAGE	PURGE DBA_RECYCLEBIN
ALTER SYNONYM	CREATE PACKAGE BODY	PURGE INDEX
ALTER SYSTEM	CREATE PLUGGABLE DATABASE	RENAME
ALTER TABLE	CREATE PROCEDURE	PURGE RECYCLEBIN
ALTER TABLESPACE	CREATE PROFILE	PURGE TABLE
ALTER TRIGGER	CREATE ROLE	PURGE TABLESPACE
ALTER TYPE	CREATE ROLLBACK SEGMENT	REVOKE
ALTER TYPE BODY	CREATE SCHEMA	SELECT
ALTER USER	CREATE SEQUENCE	TRUNCATE CLUSTER
ALTER VIEW	CREATE MATERIALIZED VIEW	TRUNCATE TABLE
ANALYZE CLUSTER	CREATE MATERIALIZED VIEW LOG	UPDATE
ANALYZE INDEX	CREATE SYNONYM	-

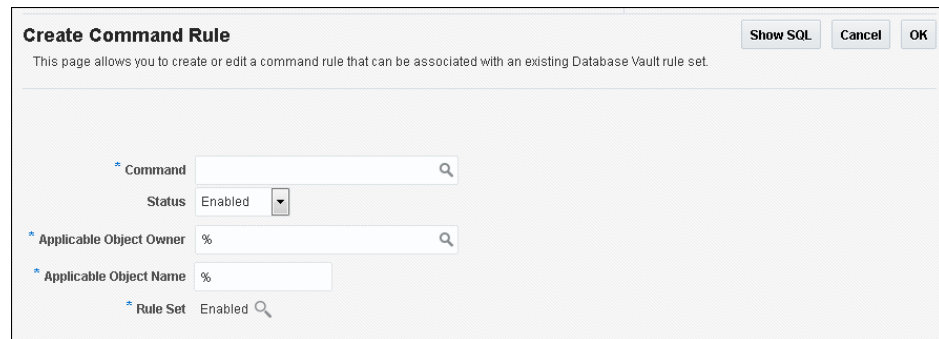
**See Also:**

[Command Rules in a Multitenant Environment](#) (page 7-3) for information about using CREATE PLUGGABLE DATABASE, ALTER PLUGGABLE DATABASE, and DROP PLUGGABLE DATABASE in a multitenant container database (CDB)

## 7.4 Creating a Command Rule

You can create a command rule in Oracle Database Vault Administrator.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Command Rules**.
3. In the Command Rules page:
  - To create a new command rule, click **Create** to display the Create Command Rule page.



4. In the Create Command Rule page, enter the following settings:

- **Command:** Select the SQL statement or operation for which you want to create a command rule. This attribute is mandatory.
- **Status:** Select either **Enabled**, **Disabled**, or **Simulation**, which will apply to the command rule during run time. This attribute is mandatory.
- **Applicable Object Owner:** From the list, select the owner of the object the command rule affects. You can use wildcard character % to select all owners. (However, you cannot use wildcard characters with text, such as EM% to select all owners whose names begin in EM.) This attribute is mandatory for all SQL statements that operate on objects within a specific schema. See [SQL Statements That Can Be Protected by Command Rules](#) (page 7-8) for a list of supported SQL statements.

Note that the `SELECT`, `INSERT`, `UPDATE`, `DELETE`, and `EXECUTE` statements are not allowed for a selection of all (%) or the `SYS` and `DVSYS` schemas.

- **Applicable Object Name:** Enter the name of the database object that the command rule affects, or specify % to select all database objects. This attribute is mandatory, if you selected an object owner from the Object Owner list.

You can run Oracle Database Vault reports on objects that the command rule affects. See the [Command Rule Related Reports and Data Dictionary View](#) (page 7-16) for more information.

- **Rule Set:** From the list, select the rule set that you want to associate with the command rule. This attribute is mandatory.

If the rule set evaluates to true, then the SQL statement succeeds. If it evaluates to false, the statement fails, and then Oracle Database Vault raises a command rule violation. (You can track rule violations by using the Command Rule Configuration Issues Report, discussed in [Oracle Database Vault Reports](#) (page 27-1).) Any auditing and custom event handling associated with the rule set occurs as a part of the command rule processing.

See [Configuring Rule Sets](#) (page 6-1), for more information about rule sets.

5. Click **OK**.

**Related Topics:**

[Propagating Oracle Database Vault Configurations to Other Databases](#)  
(page 13-2)

You can propagate Database Vault configurations (such as a realm configuration) to other Database Vault-protected databases.

## 7.5 Modifying the Enablement Status of a Command Rule

You can enable or disable a command rule in Oracle Database Vault Administrator.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Command Rules**.
3. In the Command Rules page, select the command rule that you want to enable or disable, and then select **Edit**.
4. In the Edit Command Rule page, select the status that you want from the **Status** menu:
  - **Enabled**
  - **Disabled**
  - **Simulation**
5. Click **OK**.

## 7.6 Deleting a Command Rule

Before you delete a command rule, you can locate the various references to it by querying the command rule-related Oracle Database Vault views.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Oracle Database Vault Administration page, select **Command Rules**.
3. In the Command Rules page, select the command rule that you want to remove.
4. Click **Delete**.
5. In the Confirmation window, click **Yes**.

**Related Topics:**

[Oracle Database Vault Data Dictionary Views](#) (page 25-1)

You can find information about the Oracle Database Vault configuration settings by querying the Database Vault-specific data dictionary views.

## 7.7 How Command Rules Work

Command rules follow a set of steps to check their associated components.

[How Realms Work](#) (page 5-15) describes what happens when a database account issues a `SELECT`, `DDL`, or `DML` statement that affects objects within a realm.

The following actions take place when `SELECT`, `DDL`, or `DML` statement is issued:

1. Oracle Database Vault queries all the command rules that need to be applied.  
For `SELECT`, `DDL`, and `DML` statements, multiple command rules may apply because the object owner and object name support wildcard notation.  
You can associate rule sets with both command rules and realm authorizations. Oracle Database Vault evaluates the realm authorization rule set first, and then it evaluates the rule sets that apply to the command type being evaluated.
2. For each command rule that applies, Oracle Database Vault evaluates its associated rule set.
3. If the associated rule set of any of the applicable command rules returns false or errors, Oracle Database Vault prevents the command from executing. Otherwise, the command is authorized for further processing. The configuration of the rule set with respect to auditing and event handlers dictates the auditing or custom processing that occurs.

Command rules override object privileges. That is, even the owner of an object cannot access the object if the object is protected by a command rule. You can disable either a command rule or the rule set of a command. If you disable a command rule, then the command rule does not perform the check it is designed to handle. If you disable a rule set, then the rule set always evaluates to `TRUE`. However, if you want to disable a command rule for a particular command, then you should disable the command rule because the rule set may be associated with other command rules or realm authorizations.

## 7.8 Tutorial: Using a Command Rule to Control Table Creations by a User

In this tutorial, you create a simple local command rule to control whether users can create tables in the `SCOTT` schema.

### [Step 1: Create a Table](#) (page 7-12)

First, user `SCOTT` must create a table.

### [Step 2: Create a Command Rule](#) (page 7-13)

After the table has been created in the `SCOTT` schema, you can create a command rule.

### [Step 3: Test the Command Rule](#) (page 7-14)

Next, you are ready to test the `CREATE TABLE` local command rule.

### [Step 4: Remove the Components for this Tutorial](#) (page 7-14)

You can remove the components that you created for this tutorial if you no longer need them.

### 7.8.1 Step 1: Create a Table

First, user `SCOTT` must create a table.

1. Log into the database instance as user `SCOTT`.

```
sqlplus scott
Enter password: password
```



In a multitenant environment, you must log in to the appropriate PDB. For example:

```
sqlplus scott@hrpdb
Enter password: password
```

To find the available pluggable databases (PDBs), query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

If the `SCOTT` account is locked and expired, then log in as the Database Vault Account Manager and unlock `SCOTT` and create a new password. For example:

```
sqlplus bea_dvacctmgr --Or, sqlplus bea_dvacctmgr@hrpdb
Enter password: password
```

```
ALTER USER SCOTT ACCOUNT UNLOCK IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace `password` with a password that is secure.

```
CONNECT SCOTT --Or, sqlplus SCOTT@hrpdb
Enter password: password
```

2. As user `SCOTT`, create a table.

```
CREATE TABLE t1 (num NUMBER);
```

3. Now drop the table.

```
DROP TABLE t1;
```

At this stage, user `SCOTT` can create and drop tables. Do not exit SQL\*Plus yet, and remain connected as `SCOTT`. You must use it later on when `SCOTT` tries to create another table.

## 7.8.2 Step 2: Create a Command Rule

After the table has been created in the `SCOTT` schema, you can create a command rule.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.

2. In the Oracle Database Vault Administrator Administration page, click **Command Rules**.

The Command Rules page appears.

3. Click **Create**.

The Create Command Rule page appears.

4. Enter the following settings:

- **Command:** Select **CREATE TABLE**
- **Status:** Set to **Enabled** so that the command rule is active.
- **Applicable Object Owner:** Select **SCOTT**.

- **Applicable Object Name:** Set to % so that it applies to all objects in the SCOTT schema.
- **Rule Set:** Select **Disabled** so that no one can create tables in the SCOTT schema.

5. Click **OK**.

Do not exit Database Vault Administrator

Command rules take effect immediately. Right away, user SCOTT is prevented from creating tables, even though he is still in the same user session he was in a moment ago, before you created the CREATE TABLE command rule.

### 7.8.3 Step 3: Test the Command Rule

Next, you are ready to test the CREATE TABLE local command rule.

1. In SQL\*Plus, ensure that you are logged on as user SCOTT.

```
CONNECT SCOTT --Or, CONNECT SCOTT@hrpdb
Enter password: password
```

2. Try to create a table.

```
CREATE TABLE t1 (num NUMBER);
```

The following output should appear:

```
ORA-47400: Command Rule violation for create table on SCOTT.T1
```

As you can see, SCOTT is no longer allowed to create tables, even in his own schema.

3. In Oracle Database Vault Administrator, do the following:

- a. In the Command Rules page, select the CREATE TABLE command rule and then click **Edit**.
- b. In the Edit Command Rule page, select **Enabled** from the **Rule Set** list.
- c. Click **OK**.

4. In SQL\*Plus, as user SCOTT, try creating the table again.

```
CREATE TABLE t1 (num NUMBER);
```

```
Table created.
```

Now that the CREATE TABLE command rule is set to Enabled, user SCOTT is once again permitted to create tables. (Do not exit SQL\*Plus.)

### 7.8.4 Step 4: Remove the Components for this Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. In Oracle Database Vault Administrator, remove the CREATE TABLE command rule as follows:
  - a. Return to the Command Rules page.

- b. Select the CREATE TABLE local command rule and then click **Delete**.
- c. In the Confirmation window, click **Yes**.

2. Log into the database instance as user SCOTT and remove the t1 table.

```
DROP TABLE t1;
```

3. If you no longer need the SCOTT account to be available, then connect as the Database Vault Account Manager and enter the following ALTER USER statement:

```
CONNECT bea_dvacctmgr --Or, CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

```
ALTER USER SCOTT ACCOUNT LOCK PASSWORD EXPIRE;
```

## 7.9 Guidelines for Designing Command Rules

Oracle provides guidelines for designing command rules.

- 
- Create finer-grained command rules, because they are far easier to maintain.  
For example, if you want to prevent SELECT statements from occurring on specific schema objects, then design multiple command rules to stop the SELECT statements on those specific schema objects, rather than creating a general command rule to prevent SELECT statements in the schema level.
- When designing rules for the CONNECT event, be careful to include logic that does not inadvertently lock out any required user connections. If any account has been locked out accidentally, ask a user who has been granted the DV\_ADMIN or DV\_OWNER role to log in and correct the rule that is causing the lock-out problem. The CONNECT command rule does not apply to users with the DV\_OWNER and DV\_ADMIN roles. This prevents improperly configured CONNECT command rules from causing a complete lock-out.  
  
If the account has been locked out, you can disable Oracle Database Vault, correct the rule that is causing the lock-out problem, and then reenabling Oracle Database Vault. Even when Oracle Database Vault is disabled, you still can use Database Vault Administrator and the Database Vault PL/SQL packages. See [Disabling and Enabling Oracle Database Vault](#) (page B-1), for instructions on disabling and reenabling Database Vault.
- Sometimes you must temporarily relax an enabled command rule for an administrative task. Rather than disabling the command rule, have the Security Manager (the account with the DV\_ADMIN or DV\_OWNER role) log in, set the rule set to **Enabled**, turn on **Auditing on Success or Failure** for the default rule set named Enabled, and then set the command rule back to its original rule set when the task is complete. (Be aware that in a unified auditing environment, this setting does not work. Instead, you must create a unified audit policy. *Oracle Database Security Guide* describes how to create unified audit policies for Database Vault.)
- When designing command rules, be careful to consider automated processes such as backup where these procedures may be inadvertently disabled. You can account for these tasks by creating rules that allow the command when a series of Oracle Database Vault factors is known to be true (for example, the program being used), and the account being used or the computer or network on which the client program is running.

- You can test the development phase of a command rule by using simulation mode, which enables the command rule but writes detailed information about it to a log file.

**Related Topics:**

[Using Simulation Mode for Logging Realm and Command Rule Activities](#)

(page 11-1)

Simulation mode writes the activities performed on realms and command rules to a log file, which is accessible through a data dictionary view.

## 7.10 How Command Rules Affect Performance

The performance of a command rule depends on the complexity of the rules in the rule set associated with the command rule.

For example, suppose a rule set invokes a PL/SQL function that takes 5 seconds to run. In this case, a command rule that uses that rule set would take 5 seconds to grant access for the command statement to run.

You can check the system performance by running tools such as Oracle Enterprise Manager (including Oracle Enterprise Manager Cloud Control, which is installed by default with Oracle Database), Automatic Workload Repository (AWR), and `TKPROF`.

---



---

**See Also:**

- *Oracle Database Performance Tuning Guide* to learn how to monitor database performance
  - *Oracle Database SQL Tuning Guide* to monitor the performance of individual SQL and PL/SQL statements
- 
- 

## 7.11 Command Rule Related Reports and Data Dictionary View

Oracle Database Vault provides reports and a data dictionary view that are useful for analyzing command rules.

[Table 7-2](#) (page 7-16) lists the Oracle Database Vault report. See [Oracle Database Vault Reports](#) (page 27-1), for information about how to run these reports.

**Table 7-2 Reports Related to Command Rules**

Report	Description
<a href="#">Command Rule Audit Report</a> (page 27-6)	Lists audit records generated by command rule processing operations
<a href="#">Command Rule Configuration Issues Report</a> (page 27-3)	Tracks rule violations, in addition to other configuration issues the command rule may have
<a href="#">Object Privilege Reports</a> (page 27-7)	Lists object privileges that the command rule affects
<a href="#">Sensitive Objects Reports</a> (page 27-10)	Lists objects that the command rule affects

**Table 7-2 (Cont.) Reports Related to Command Rules**

Report	Description
<a href="#">Rule Set Configuration Issues Report</a> (page 27-3)	Lists rules sets that have no rules defined or enabled, which may affect the command rules that use them

You can use the `DBA_DV_COMMAND_RULE` data dictionary view to find the SQL statements that are protected by command rules. See [DBA\\_DV\\_COMMAND\\_RULE View](#) (page 25-8) for more information.



---

# Configuring Factors

Factors enable you to base Database Vault restrictions on attributes such as a client IP address or a domain.

[What Are Factors?](#) (page 8-1)

A factor is a named variable or attribute, such as a database IP address, that Oracle Database Vault can recognize.

[Default Factors](#) (page 8-2)

Oracle Database Vault provides a set of default factors.

[Creating a Factor](#) (page 8-5)

In general, to create a factor, you first create the factor itself, and then you edit the factor to include its identity.

[Adding an Identity to a Factor](#) (page 8-14)

After you create a new factor, you optionally can add an identity to it.

[Deleting a Factor](#) (page 8-19)

Before you delete a factor, you must remove references to the factor.

[How Factors Work](#) (page 8-20)

Oracle Database Vault processes factors when a session is established.

[Tutorial: Preventing Ad Hoc Tool Access to the Database](#) (page 8-23)

This tutorial demonstrates how to use factors to prevent ad hoc tools (such as SQL\*Plus) from accessing the database.

[Tutorial: Restricting User Activities Based on Session Data](#) (page 8-28)

This tutorial shows how to restrict user activities based on their session data, such as the domain the user is using.

[Guidelines for Designing Factors](#) (page 8-36)

Oracle provides guidelines for designing factors.

[How Factors Affect Performance](#) (page 8-37)

The complexity of factors affects the performance of your Oracle database instance.

[Factor Related Reports and Data Dictionary Views](#) (page 8-37)

Oracle Database Vault provides reports and data dictionary views that display information about factors and their identities.

## 8.1 What Are Factors?

A factor is a named variable or attribute, such as a database IP address, that Oracle Database Vault can recognize.

You can use factors for activities such as authorizing database accounts to connect to the database or creating filtering logic to restrict the visibility and manageability of data.

Oracle Database Vault provides a selection of factors that lets you set controls on such components as the domain for your site, IP addresses, databases, and so on. You also can create custom factors, using your own PL/SQL retrieval methods.

Note the following:

- You can use factors in combination with rules in rule sets. The DVF factor functions are factor-specific functions that you can use in rule expressions.
- Factors have values (identities) and are further categorized by their factor types. See "Factor Type" in [Completing the General Page for Factor Creation](#) (page 8-6) for information about factor types.
- You also can integrate factors with Oracle Label Security labels.
- You can run reports on the factors that you create in Oracle Database Vault. See for more information.
- In a multitenant environment, you only can create factors in a PDB, not in the CDB root or the application root.

This chapter explains how to configure factors by using Oracle Database Vault Administrator. Alternatively, you can use the Oracle Database Vault factor APIs to configure factors.

#### **Related Topics:**

##### [Oracle Database Vault DVF PL/SQL Factor Functions](#) (page 18-27)

Oracle Database Vault maintains the DVF schema functions when you use the DBMS\_MACADM PL/SQL package to manage the various factors.

##### [Oracle Database Vault Factor APIs](#) (page 18-1)

The DBMS\_MACADM PL/SQL package has factor-related Oracle Database Vault rule procedures and functions, and DVF has functions to manage factors.

## **8.2 Default Factors**

Oracle Database Vault provides a set of default factors.

For each of these factors, there is an associated function that retrieves the value of the factor. See [Oracle Database Vault DVF PL/SQL Factor Functions](#) (page 18-27) for a listing of these functions.

You can create custom factors by using your own PL/SQL retrieval methods. A useful PL/SQL function you can use (which is used for many of the default factors) is the SYS\_CONTEXT SQL function, which retrieves data about the user session. For example, you can use the CLIENT\_PROGRAM\_NAME attribute of SYS\_CONTEXT to find the name of the program used for the database session. After you create the custom factor, you can query its values similar to the functions used to query the default factors.

See *Oracle Database SQL Language Reference* for more information about the SYS\_CONTEXT function.



You can use the default factors in your own security configurations. If you do not need them, you can remove them. (That is, they are not needed for internal use by Oracle Database Vault.)

The default factors are as follows:

- **Authentication\_Method:** Is the method of authentication. In the list that follows, the type of user is followed by the method returned:
  - Password-authenticated enterprise user, local database user, user with the SYSDBA or SYSOPER administrative privilege using the password file; proxy with user name using password: PASSWORD
  - Kerberos-authenticated enterprise user or external user (with no administrative privileges): KERBEROS
  - Kerberos-authenticated enterprise user (with administrative privileges): KERBEROS\_GLOBAL
  - Kerberos-authenticated external user (with administrative privileges): KERBEROS\_EXTERNAL
  - SSL-authenticated enterprise or external user (with no administrative privileges): SSL
  - SSL-authenticated enterprise user (with administrative privileges): SSL\_GLOBAL
  - SSL-authenticated external user (with administrative privileges): SSL\_EXTERNAL
  - Radius-authenticated external user: RADIUS
  - OS-authenticated external user, or user with the SYSDBA or SYSOPER administrative privilege: OS
  - Proxy with certificate, DN, or username without using password: NONE
  - Background process (job queue slave process): JOB
  - Parallel Query Slave process: PQ\_SLAVE

For non-administrative connections, you can use the Identification\_Type factor to distinguish between external and enterprise users when the authentication method is PASSWORD, KERBEROS, or SSL. For administrative connections, the Authentication\_Method factor is sufficient for the PASSWORD, SSL\_EXTERNAL, and SSL\_GLOBAL authentication methods.

- **Client\_IP:** Is the IP address of the machine from which the client is connected.
- **Database\_Domain:** Is the domain of the database as specified in the DB\_DOMAIN initialization parameter.
- **Database\_Hostname:** Is the host name of the computer on which the instance is running.
- **Database\_Instance:** Is the instance identification number of the current instance.
- **Database\_IP:** Is the IP address of the computer on which the instance is running.

- **Database\_Name:** Is the name of the database as specified in the `DB_NAME` initialization parameter.
- **Domain:** Is a named collection of physical, configuration, or implementation-specific factors in the run-time environment (for example, a networked IT environment or subset of it) that operates at a specific sensitivity level. You can identify a domain using factors such as host name, IP address, and database instance names of the Database Vault nodes in a secure access path to the database. Each domain can be uniquely determined using a combination of the factor identifiers that identify the domain. You can use these identifying factors and possibly additional factors to define the Maximum Security Label within the domain. This restricts data access and commands, depending on the physical factors about the Database Vault session. Example domains of interest may be Corporate Sensitive, Internal Public, Partners, and Customers.
- **Enterprise\_Identity:** Is the enterprise-wide identity for the user:
  - For enterprise users: the Oracle Internet Directory-distinguished name (DN).
  - For external users: the external identity (Kerberos principal name, Radius and DCE schema names, operating system user name, certificate DN).
  - For local users and `SYSDBA` and `SYSOPER` logins: `NULL`.

The value of the attribute differs by proxy method:

- For a proxy with DN: the Oracle Internet Directory DN of the client.
  - For a proxy with certificate: the certificate DN of the client for external users; the Oracle Internet Directory DN for global users.
  - For a proxy with user names: the Oracle Internet Directory DN if the client is an enterprise user; `NULL` if the client is a local database user.
- **Identification\_Type:** Is the way the user schema was created in the database. Specifically, it reflects the `IDENTIFIED` clause in the `CREATE USER` and `ALTER USER` syntax. In the list that follows, the syntax used during schema creation is followed by the identification type returned:
    - `IDENTIFIED BY password:` `LOCAL`
    - `IDENTIFIED EXTERNALLY:` `EXTERNAL`
    - `IDENTIFIED GLOBALLY:` `GLOBAL SHARED`
    - `IDENTIFIED GLOBALLY AS DN:` `GLOBAL PRIVATE`
  - **Lang:** Is the ISO abbreviation for the language name, a shorter form than the existing `LANGUAGE` parameter.
  - **Language:** Is the language and territory your session currently uses, along with the database character set, in the following form:

*language\_territory.characterset*

For example:

`AMERICAN_AMERICA.WE8MSWIN1252`

Refer to *Oracle Database Globalization Support Guide* for more information about languages, territories, and character sets.

- **Machine:** Is the host name for the database client that established the current session. If you must find out whether the computer was used for a client or server session, then you can compare this setting with the Database\_Hostname factor to make the determination.
- **Network\_Protocol:** Is the network protocol being used for communication, as specified in the PROTOCOL=protocol portion of the connect string.
- **Proxy\_Enterprise\_Identity:** Is the Oracle Internet Directory DN when the proxy user is an enterprise user.
- **Proxy\_User:** Is the name of the database user who opened the current session on behalf of SESSION\_USER.
- **Session\_User:** Is the database user name by which the current user is authenticated. This value remains the same throughout the session.

## 8.3 Creating a Factor

In general, to create a factor, you first create the factor itself, and then you edit the factor to include its identity.

### [Accessing the Create Factors Page](#) (page 8-5)

The Create Factors page enables you to create the factor, starting with a general definition of the factor that you want to create.

### [Completing the General Page for Factor Creation](#) (page 8-6)

In the General page, you must enter general identifying information for the factor, such as its name.

### [Configurations Page for Factor Creation](#) (page 8-7)

The Configurations page defines settings such as the factor's identification and the evaluation method.

### [Options Page of Factor Creation](#) (page 8-12)

The Options page assigns a rule set to a factor, sets error options, and for non-unified auditing, sets audit options.

### 8.3.1 Accessing the Create Factors Page

The Create Factors page enables you to create the factor, starting with a general definition of the factor that you want to create.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Factors**.
3. In the Factors page, click **Create** to display the Create Factor page.

4. Starting with the General page, enter the following information, clicking **Next** to go to each subsequent page, and then clicking **Done** and **Finish** when the factor definition is complete.
  - [Completing the General Page for Factor Creation](#) (page 8-6)
  - [Configurations Page for Factor Creation](#) (page 8-7)
  - [Options Page of Factor Creation](#) (page 8-12)
  - [Creating and Configuring a Factor Identity](#) (page 8-16)

### 8.3.2 Completing the General Page for Factor Creation

In the General page, you must enter general identifying information for the factor, such as its name.

- In the General page, enter the following information:
  - **Name:** Enter a name up to 28 characters in mixed-case, without spaces. Oracle Database Vault creates a valid Oracle identifier for the factor function to be created in the DVF schema based on the name of the factor chosen. For example, if you create a factor named `GetNetworkIP`, Oracle Database Vault creates the `DVF.F$GETNETWORKIP` function. This attribute is mandatory.  
  
Oracle suggests that you start the name with a noun and complete the name with a brief description of the derived value.  
  
[Oracle Database Vault DVF PL/SQL Factor Functions](#) (page 18-27) describes the DVF factor functions.
  - **Description:** Enter a text description of the factor. It can have up to 1024 characters in mixed-case. This attribute is optional.
  - **Factor Type:** From the list, select the type or category of the factor. This attribute is mandatory.

Factor types have a name and description and are used only to help classify factors. A factor type is the category name used to classify the factor. The default physical factor types include authentication method, host name, host IP address, instance identifiers, database account information, and others. You can create user-defined factor types, such as application name, certificate

information, and so on in addition to the installed factor types, such as time and authentication method.

You can find the factors that are associated with a particular factor type by querying the DBA\_DV\_FACTOR data dictionary view. For example:

```
SELECT NAME FROM DBA_DV_FACTOR
WHERE FACTOR_TYPE_NAME='Authentication Method';
```

The output is:

```
NAME
-----
Network_Protocol
Authentication_Method
Identification_Type
```

### 8.3.3 Configurations Page for Factor Creation

The Configurations page defines settings such as the factor's identification and the evaluation method.

#### [Setting the Factor Identification Information](#) (page 8-7)

Under Factor Identification, you must select how to resolve the identity of a factor. This attribute is mandatory.

#### [How Factor Identities Work](#) (page 8-8)

A factor identity is the actual value of a factor (for example, the IP address for a factor that uses the IP\_Address type).

#### [Setting the Evaluation Information for a Factor](#) (page 8-9)

Under Evaluation, you must select how you want the factor to be evaluated and assigned an identity.

#### [Setting the Oracle Label Security Labeling Information for a Factor](#) (page 8-9)

Under Factor Labeling, you must select how you want the factor identity to retrieve an Oracle Label Security (OLS) label.

#### [Setting the Retrieval Method for a Factor](#) (page 8-10)

Under Retrieval Method, you must enter a PL/SQL expression that retrieves the identity of a factor or a constant.

#### [How Retrieval Methods Work](#) (page 8-10)

The Retrieval Method identifies factors where the factor identification is by method or constant.

#### [Setting the Validation Method for a Factor](#) (page 8-11)

A validation method uses a PL/SQL expression to return a Boolean value to validate the identity of a factor.

#### 8.3.3.1 Setting the Factor Identification Information

Under Factor Identification, you must select how to resolve the identity of a factor. This attribute is mandatory.

- In the Configurations page, under Factor Identification, enter the following information:
  - **By Constant:** Resolves the factor identity by retrieving the constant value found in the **Retrieval Method** field.

- **By Method:** Sets the factor identity by executing the PL/SQL expression specified in the **Retrieval Method** field.

For example, suppose the expression retrieves the system date:

```
to_char(sysdate, 'yyyy-mm-dd')
```

On December 15, 2015, the **By Method** option would return the following value:

```
2015-12-15
```

- **By Factors:** Determines the factor identity by mapping the identities of the child factor to its parent factor. A parent factor is a factor whose values are resolved based on a second factor, called a child factor. To establish their relationship, you map their identities. (You do not need to specify a **Retrieval Method** expression for this option.)

See [Using Identity Mapping to Configure an Identity to Use Other Factors](#) (page 8-17) for more information about mapping identities.

### 8.3.3.2 How Factor Identities Work

A factor identity is the actual value of a factor (for example, the IP address for a factor that uses the IP\_Address type).

A factor can have several identities depending on its retrieval method or its identity mapping logic. For example, a factor such as Database\_Hostname could have multiple identities in an Oracle Real Application Clusters environment; a factor such as Client\_IP can have multiple identities in any RDBMS environment. The retrieval method for these types of factors may return different values because the retrieval method is based on the database session. Several reports allow you to track the factor identity configuration.

You can configure the assignment of a factor in the following ways:

- Assign the factor at the time a database session is established.
- Configure individual requests to retrieve the identity of the factor.

With the Oracle Label Security integration, you can label identities with an Oracle Label Security label. You can also assign an identity *trust levels*, which are numbers that indicate the magnitude of trust relative to other identities for the same factor. In general, the higher the trust level number is set, the greater the trust. Negative trust levels are not trusted.

Within a database session, a factor assigned identity is available to Oracle Database Vault and any application with a publicly accessible PL/SQL function that exists in the DVF schema (which contains functions that retrieve factor values) as follows:

```
dvf.f.$factor_name
```

This allows the identifier for a factor to be accessed globally from within the Oracle database (using PL/SQL, SQL, Oracle Virtual Private Database, triggers, and so on). For example, in SQL\*Plus:

```
CONNECT leo_dvowner
Enter password: password

SELECT DVF.F$DATABASE_IP FROM DUAL;
```

Output similar to the following appears:

```
SELECT DVF.F$DATABASE_IP FROM DUAL;
```

```
F$DATABASE_IP
```

```
-----  
192.0.2.1
```

You can also use the `GET_FACTOR` function to find the identity of a factor that is made available for public access. For example:

```
SELECT GET_FACTOR('DATABASE_IP') FROM DUAL;
```

The following output appears:

```
GET_FACTOR('DATABASE_IP')
```

```
-----  
192.0.2.1
```

### Related Topics:

[Adding an Identity to a Factor](#) (page 8-14)

After you create a new factor, you optionally can add an identity to it.

[Factor Related Reports and Data Dictionary Views](#) (page 8-37)

Oracle Database Vault provides reports and data dictionary views that display information about factors and their identities.

### 8.3.3.3 Setting the Evaluation Information for a Factor

Under Evaluation, you must select how you want the factor to be evaluated and assigned an identity.

See [How Factors Affect Performance](#) (page 8-37) for the performance effect of session factors. This attribute is mandatory.

- In the Configurations page, under Evaluation, enter the following information:
  - **For Session:** Evaluates the factor when a database session is created.
  - **By Access:** Evaluates the factor each time it is accessed (for example, referenced by an application) and when the database session is first created.
  - **On Startup:** Evaluates the factor when the database session starts.

### 8.3.3.4 Setting the Oracle Label Security Labeling Information for a Factor

Under Factor Labeling, you must select how you want the factor identity to retrieve an Oracle Label Security (OLS) label.

This setting applies if you plan to use the Oracle Label Security integration. This attribute is mandatory if you want to use an OLS label.

- In the Configurations page, under Factor Labeling, enter the following information:
  - **By Self:** Labels the identities for the factor directly from the labels associated with an Oracle Label Security policy.
  - **By Factors:** If there are multiple child factor labels, then Oracle Database Vault merges the labels by using the Oracle Label Security algorithm that is associated with the applicable Oracle Label Security policy. For each

applicable Oracle Label Security policy, a factor identity can have an assigned label.

#### Related Topics:

[Integrating Oracle Database Vault with Oracle Label Security](#) (page 12-5)

You can integrate Oracle Database Vault with Oracle Label Security, and check the integration with reports and data dictionary views.

#### 8.3.3.5 Setting the Retrieval Method for a Factor

Under Retrieval Method, you must enter a PL/SQL expression that retrieves the identity of a factor or a constant.

- In the Configurations page, under Retrieval Method, enter a PL/SQL retrieval method. It can use up to 255 characters in mixed-case.

The following retrieval method sets a value of the DB\_NAME factor by retrieving the database name (DB\_NAME) from the USERENV namespace in a user's session.

```
UPPER(SYS_CONTEXT('USERENV','DB_NAME'))
```

#### 8.3.3.6 How Retrieval Methods Work

The Retrieval Method identifies factors where the factor identification is by method or constant.

If the factor identification is by factors, Oracle Database Vault identifies it by its identity mappings. You can create your own PL/SQL retrieval methods, or use the functions supplied with Oracle Database Vault. See the following sections for factor-specific and general utility functions that you can use to build the retrieval method:

- [Oracle Database Vault DVF PL/SQL Factor Functions](#) (page 18-27)
- [DBMS\\_MACADM Factor Procedures and Functions](#) (page 18-1)
- [Oracle Database Vault Utility APIs](#) (page 21-1)

See also the default factors provided with Oracle Database Vault for examples of retrieval methods. [Default Factors](#) (page 8-2) describes these factors.

The **Retrieval Method** field is mandatory if you have selected the following settings under Factor Identification:

- **By Method:** Enter a method in the Retrieval Method field.
- **By Constant:** Enter a constant in the Retrieval Method field.

The value returned as the factor identity must be a VARCHAR2 string or otherwise convertible to one.

You can include any package function or standalone function in the expression. Ensure that the expression is a fully qualified function, such as *schema.function\_name*. Do not include complete SQL statements. If you are using application packages or functions, you must provide DVSYS with the GRANT EXECUTE privilege on the object.

Write the function signature using the following format:

```
FUNCTION GET_FACTOR RETURN VARCHAR2
```



### 8.3.3.7 Setting the Validation Method for a Factor

A validation method uses a PL/SQL expression to return a Boolean value to validate the identity of a factor.

Under Validation Method, you must enter a PL/SQL expression that returns a Boolean value (TRUE or FALSE) to validate the identity of a factor being retrieved (with the GET\_FACTOR function) or the value to be assigned to a factor (with the SET\_FACTOR function).

If the method is evaluated to false for the value being retrieved or to be assigned, then the factor identity is set to null. This optional feature provides an additional level of assurance that the factor is properly retrieved and set. This field can have up to 255 characters in mixed-case.

You can include any package function or standalone function in the expression. Ensure that the expression is a fully qualified function, such as *schema.function\_name*. Do not include complete SQL statements. If you are using application packages or functions, then you must provide DVSYS with the GRANT EXECUTE privilege on the object.

- In the Configurations page, under Validation method, create a function that uses any of the following formats:

- `FUNCTION IS_VALID RETURN BOOLEAN`

In this form, you can use the `DVF.F$factor_name` function inside the function logic. This is more appropriate for factors that are evaluated by session.

- `FUNCTION IS_VALID(p_factor_value VARCHAR2) RETURN BOOLEAN`

In this form, the factor value is passed to the validation function directly. This is more appropriate for factors that are evaluated by access. It is also valid for factors evaluated by session.

#### Related Topics:

##### [DBMS\\_MACADM Factor Procedures and Functions \(page 18-1\)](#)

The DBMS\_MACADM PL/SQL package provides procedures and functions to configure factors.

##### [Oracle Database Vault Run-Time PL/SQL Procedures and Functions \(page 18-22\)](#)

Oracle Database Vault provides procedural interfaces to administer Database Vault security options and manage Database Vault security enforcements.

##### [Oracle Database Vault DVF PL/SQL Factor Functions \(page 18-27\)](#)

Oracle Database Vault maintains the DVF schema functions when you use the DBMS\_MACADM PL/SQL package to manage the various factors.

##### [Oracle Database Vault Utility APIs \(page 21-1\)](#)

Oracle Database Vault provides a set of utility APIs in the DBMS\_MACUTL PL/SQL package.

## 8.3.4 Options Page of Factor Creation

The Options page assigns a rule set to a factor, sets error options, and for non-unified auditing, sets audit options.

### [Assigning a Rule Set to a Factor](#) (page 8-12)

Under Assignment Rule Set, you select a rule set if you want to use a rule set to control setting a factor identity.

### [Setting Error Options for a Factor](#) (page 8-13)

Under Error Options, you set the processing that must occur when a factor identity cannot be resolved.

### [Setting Audit Options for a Factor](#) (page 8-13)

Under Audit Options, you can generate an audit trail if you are not using a unified audit environment.

### [How Factor Auditing Works](#) (page 8-13)

Whether you have unified auditing enabled affects how auditing is handled for factors.

### 8.3.4.1 Assigning a Rule Set to a Factor

Under Assignment Rule Set, you select a rule set if you want to use a rule set to control setting a factor identity.

For example, you can use a rule set to determine when a database session originates from a known application server or program.

- In the Options page, from the **Assignment Rule Set** menu, select a rule set from the list.

This attribute is particularly useful for situations where database applications, such as a Web application using a JDBC connection pool, must dynamically set a factor identity for the current database session. For example, a Web application may want to assign the geographic location for a database account logging in to the Web application. To do so, the Web application can use the JDBC Callable Statement, or Oracle Data Provider for .NET (ODP.NET) to execute the PL/SQL function `SET_FACTOR`, for example:

```
BEGIN
  SET_FACTOR('GEO_STATE', 'VIRGINIA');
END;
```

Then you can create an assignment rule for the `GEO_STATE` factor to allow or disallow the setting of the `GEO_STATE` factor based on other factors or rule expressions.

#### **Related Topics:**

### [Configuring Rule Sets](#) (page 6-1)

Rule sets group one or more rules together; the rules determine whether a user can perform an action on an object.

### [How Factors Are Set](#) (page 8-22)

You can assign a factor identity at any time during a database session, but only if the factor assignment rule set evaluates to true.

### 8.3.4.2 Setting Error Options for a Factor

Under Error Options, you set the processing that must occur when a factor identity cannot be resolved.

- In the Options page, under Error Options, select from the following values:
  - **Show Error Message:** Displays an error message to the database session.
  - **Do Not Show Error Message:** Does not display the error message.

An advantage of selecting **Do Not Show Error Message** and then enabling auditing is that you can track the activities of a potential intruder. The audit report reveals the activities of the intruder, yet the intruder is unaware that you are doing this because he or she does not see any error messages.

After you have created a new factor, you are ready to configure its identity. To do so, edit the factor and then add its identity.

### 8.3.4.3 Setting Audit Options for a Factor

Under Audit Options, you can generate an audit trail if you are not using a unified audit environment.

- In the Options page, under Audit Options, select from the following values:
  - **Never:** Does not audit.
  - **Always:** Always creates an audit record when a factor is evaluated. You can select from the conditions, described next.
  - **Validation False:** Creates an audit record when the validation method (if provided) returns FALSE.
  - **Retrieval Error:** Creates an audit record when the identity of a factor cannot be resolved and assigned, due to an error (such as `No data found` or `Too many rows`).
  - **Trust Level NULL:** Creates an audit record when the resolved identity of a factor has an assigned trust level of NULL.  
See [Creating and Configuring a Factor Identity](#) (page 8-16) for more information about trust levels.
  - **Trust Level Less Than Zero:** Creates an audit record when the resolved identity of a factor has an assigned trust level less than zero.
  - **Validation Error:** Creates an audit record when the validation method (if provided) returns an error.

### 8.3.4.4 How Factor Auditing Works

Whether you have unified auditing enabled affects how auditing is handled for factors.

In a non-unified auditing environment, Oracle Database Vault writes the audit trail to the `DVSYS.AUDIT_TRAIL$` table, described in [Auditing Oracle Database Vault](#) (page A-1).

If you have enabled unified auditing, then this setting does not capture audit records. Instead, you can create audit policies to capture this information, as described in *Oracle Database Security Guide*.

You can use the Factor Audit Report to display the generated audit records. (See [Factor Related Reports and Data Dictionary Views](#) (page 8-37) for more information.) In addition, you can select multiple audit options at a time. Each option is converted to a bit mask and added to determine the aggregate behavior. Note that there is little performance impact in auditing, unless the factor has errors.

## 8.4 Adding an Identity to a Factor

After you create a new factor, you optionally can add an identity to it.

### [About Factor Identities](#) (page 8-14)

An identity is the actual value of a factor, such an IP\_Address factor identity being 192.0.2.4.

### [About Trust Levels](#) (page 8-15)

Trust levels enable you to assign a numeric value to indicate the measure of trust allowed.

### [About Label Identities](#) (page 8-15)

You can assign You Oracle Label Security (OLS) labels to factor identities.

### [Creating and Configuring a Factor Identity](#) (page 8-16)

You can create and configure a factor identity in Oracle Database Vault Administrator.

### [Deleting a Factor Identity](#) (page 8-17)

If you want to delete a factor identity, you can locate references to it by querying the factor-related Oracle Database Vault views.

### [Using Identity Mapping to Configure an Identity to Use Other Factors](#) (page 8-17)

You can use identity mapping to use a group of factors to manage identity values.

### 8.4.1 About Factor Identities

An identity is the actual value of a factor, such an IP\_Address factor identity being 192.0.2.4.

A factor identity for a given database session is assigned at run time using the **Factor Identification** and **Retrieval Method** fields described in [Creating a Factor](#) (page 8-5). You can further configure the identity for the following reasons:

- To define the known identities for a factor
- To add a trust level to a factor identity
- To add an Oracle Label Security label to a factor identity
- To resolve a factor identity through its child factors, by using identity mapping

**Related Topics:**

[Tutorial: Restricting User Activities Based on Session Data](#) (page 8-28)

This tutorial shows how to restrict user activities based on their session data, such as the domain the user is using.

**8.4.2 About Trust Levels**

Trust levels enable you to assign a numeric value to indicate the measure of trust allowed.

A trust value of 1 signifies some trust. A higher value indicates a higher level of trust. A negative value or zero indicates distrust. When the factor identity returned from a factor retrieval method is not defined in the identity, Oracle Database Vault automatically assigns the identity a negative trust level.

To determine the trust level of a factor identity at run time, you can use the `GET_TRUST_LEVEL` and `GET_TRUST_LEVEL_FOR_IDENTITY` functions in the `DVSYS` schema.

For example, suppose you have created a factor named `Network`. You can create the following identities for the `Network` factor:

- `Intranet`, with a trust level of 10
- `VPN` (virtual private network), with a trust level of 5
- `Public`, with a trust level of 1

You then can create rule expressions (or custom application code) that base policy decisions on the trust level. For example, you can use the `GET_TRUST_LEVEL` function to find trust levels greater than 5:

```
GET_TRUST_LEVEL('Network') > 5
```

Or, you can use a `SELECT` statement on the `DBA_DV_IDENTITY` data dictionary view to find trust levels for the `Network` factor greater than or equal to 5:

```
SELECT VALUE, TRUST_LEVEL FROM DBA_DV_IDENTITY
WHERE TRUST_LEVEL >= 5
AND FACTOR_NAME='Network'
```

Output similar to the following appears:

```
F$NETWORK GET_TRUST_LEVEL('NETWORK')
-----
VPN                    5
INTRANET              10
```

In the preceding example, `Network` factor identity for `VPN` is trusted (value equals 5), and the identity for the `INTRANET` domain is 10, which implies a greater trust.

**Related Topics:**

[Oracle Database Vault Realm APIs](#) (page 15-1)

The `DBMS_MACADM` PL/SQL package enables you to configure Oracle Database Vault realms.

**8.4.3 About Label Identities**

You can assign You Oracle Label Security (OLS) labels to factor identities.

In brief, a label acts as an identifier for a database table row to assign privileges to the row. The **Factor Labeling** attribute for a factor determines whether a factor is labeled **By Self** or **By Factors**. If you set the **Factor Labeling** attribute to **By Self**, then you can associate OLS labels with the factor identities. If you set the **Factor Labeling** attribute to **By Factors**, then Oracle Database Vault derives the factor identity labels from the labeling of child factor identities. When there are multiple child factor identities with labels, Oracle Database Vault merges the labels using the OLS algorithm associated with the applicable factor Oracle Label Security policy.

---

**See Also:** *Oracle Label Security Administrator's Guide* for more information about labels

---

## 8.4.4 Creating and Configuring a Factor Identity

You can create and configure a factor identity in Oracle Database Vault Administrator.

1. In the Select Identities page of the Create Factor pages, select **Add New Identity**.

The Add New Identity window appears.

2. In the Identity subpage, enter the following values:
  - **Value:** Enter the value of the identity, up to 1024 characters in mixed-case. This attribute is mandatory.
  - **Trust Level:** Select one of the following trust levels:
    - **Very Trusted:** Assigns a trust level value of 10
    - **Trusted:** Assigns a trust level value of 5
    - **Somewhat Trusted:** Assigns a trust level value of 1

- **Untrusted:** Assigns a trust level value of -1
- **Trust Level Not Defined:** Assigns a trust level value of NULL (default)

See [About Trust Levels](#) (page 8-15) for detailed information about trust levels.

- **Label Identity:** Optionally, select from the list of available Oracle Label Security policies and then click the **Move** button to move them to the **Selected OLS Policies** list.

The list shows data labels from the Oracle Label Security installation for your site. For more information, refer to *Oracle Label Security Administrator's Guide*.

See [About Label Identities](#) (page 8-15) for detailed information about label identities.

3. Click **OK** to return to the Create Factors : Identities page..
4. Click **Next** to review the factor settings.
5. Click **Finish**.

### 8.4.5 Deleting a Factor Identity

If you want to delete a factor identity, you can locate references to it by querying the factor-related Oracle Database Vault views.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Factors**.
3. Select the factor whose identity you want to delete, and then click **Edit**.
4. In the Edit Factor page, click **Next** until you reach the Identities page.
5. Select the factor identity that you want to remove.
6. Click **Remove**.
7. Click **Done**, then click **Finish**.

#### Related Topics:

[Oracle Database Vault Data Dictionary Views](#) (page 25-1)

You can find information about the Oracle Database Vault configuration settings by querying the Database Vault-specific data dictionary views.

### 8.4.6 Using Identity Mapping to Configure an Identity to Use Other Factors

You can use identity mapping to use a group of factors to manage identity values.

[About Identity Mapping](#) (page 8-18)

While you are creating a factory identity, you can map it.

[Mapping an Identity to a Factor](#) (page 8-18)

You can map an identity to a factor by creating a parent-child relationship with two factors.

### 8.4.6.1 About Identity Mapping

While you are creating a factory identity, you can map it.

Identity mapping is the process of identifying a factor by using other (child) factors. This is a way to transform combinations of factors into logical identities for a factor or to transform continuous identity values (for example, temperature) or large discrete identity values (for example, IP address ranges) into logical sets. To check configuration issues in the mapping for an identity, you can run the Identity Configuration Issues report.

You can map different identities of a parent factor to different identities of the contributing factor. For example, an INTRANET identity maps to an IP address range of 192.0.2.1 to 192.0.2.24. A REMOTE identity can map to an IP address range that excludes the address range 192.0.2.1 to 192.0.2.24.

Based on identity mapping, you can create a security policy. For example, you can define a reduced set of privileges for an employee connecting over VPN (with REMOTE), as opposed to an employee connecting from within the corporate network (with INTRANET).

#### Related Topics:

[Tutorial: Restricting User Activities Based on Session Data](#) (page 8-28)

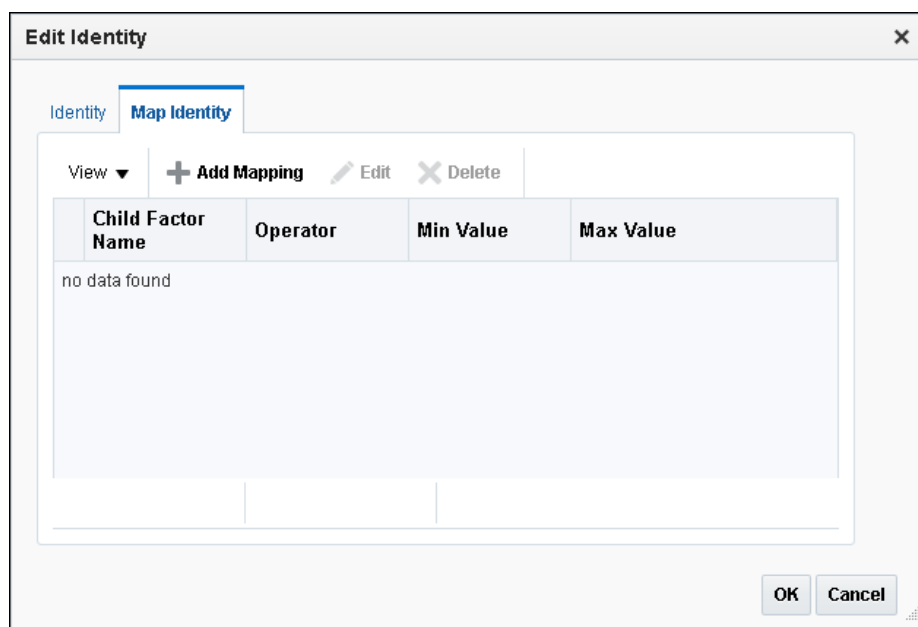
This tutorial shows how to restrict user activities based on their session data, such as the domain the user is using.

### 8.4.6.2 Mapping an Identity to a Factor

You can map an identity to a factor by creating a parent-child relationship with two factors.

1. Follow the instructions in [Creating a Factor](#) (page 8-5) to create a parent factor and set the attribute **Factor Identification** to **By Factors**.
2. In the Identities page, follow the instructions in [Creating and Configuring a Factor Identity](#) (page 8-16) to create an identity for the parent factor.
3. Map the factor-identity pair of the parent to the factor-identity pairs of its children. Use the following procedure:
  - a. In the Identities page, either select an existing identity and click **Edit**, or click **Add New Identity** to create a new identity.
  - b. In the Edit Identity window (or the Add New Identity window), ensure that at least the **Value** field is filled out in the Identity subpage.
  - c. Click the **Map Identity** tab.





- d. Click **Add Mapping**.
- e. Enter the following information:
  - Child Factor Name:** From the list, select the child factor name.
  - Operator:** Select the operator from the list.
  - Min Value:** Enter the minimum value.
  - Max Value:** Enter the maximum value.

For example, consider a scenario where the Contributing Factor to the Factor Network is set to Client\_IP, the **Operator** is set to Between, the **Min Value** is set to 192.0.2.1 and the **Max Value** is set to 192.0.2.24. This means that whenever the client IP address lies in the specified address range of 192.0.2.1 to 192.0.2.24, the parent factor evaluates to a predefined identity (for example, INTRANET).
- f. Click **OK** to exit the Add New Identity Mapping window.
- g. Click **OK** to exit the Add New Identity and Mapping window.

4. Click **Done**, and then click **Finish**.

Repeat this process to add more contributing factors for a parent factor identity. For example, you can configure the Network factor to resolve to a value ACCOUNTING-SENSITIVE, when the Program factor resolves to "Oracle General Ledger" and the Client\_IP is in between 192.0.2.1 and 192.0.2.24. So, if an authorized accounting financial application program, running on a client with IP address 192.0.2.12 accesses the database, then the Network factor is resolved to ACCOUNTING-SENSITIVE. A database session with the ACCOUNTING-SENSITIVE Network value would have more access privileges than one with the INTRANET Network value.

## 8.5 Deleting a Factor

Before you delete a factor, you must remove references to the factor.

You can find the various references to the factor and its identities by querying the factor-related Oracle Database Vault views. See [Oracle Database Vault Data Dictionary Views](#) (page 25-1), for more information.

1. Delete any references to the factor, such as rule sets, factor identities, and Oracle Label Security policy associations.

To do so, edit the factor. You can find and remove the rule set from the Options page and the Oracle Label Security policies associations and identities from the Identities page.

2. In the Oracle Database Vault Administration page, select **Factors**.
3. In the Factors page, select the factor that you want to remove.
4. Click **Delete**.
5. In the Confirmation window, click **Yes**.

## 8.6 How Factors Work

Oracle Database Vault processes factors when a session is established.

### [How Factors Are Processed When a Session Is Established](#) (page 8-20)

Oracle Database Vault evaluates the factors based on when a session begins.

### [How Factors Are Retrieved](#) (page 8-21)

You can retrieve a factor in a database session at any time by using the DVF factor function or the `GET_FACTOR` function.

### [How Factors Are Set](#) (page 8-22)

You can assign a factor identity at any time during a database session, but only if the factor assignment rule set evaluates to true.

### 8.6.1 How Factors Are Processed When a Session Is Established

Oracle Database Vault evaluates the factors based on when a session begins.

When a database session is established, the following actions occur:

1. At the start of each database session, Oracle Database Vault begins to evaluate all default and user-created factors in the database instance.

This evaluation occurs after the normal database authentication of the session and the initialization of the Oracle Label Security session information, if applicable.

2. In the factor evaluation stage, the factor initialization process executes the retrieval method for all factors that are identified by methods or constants, to resolve the factor identity for the session.

The factor error options setting has no effect on the factor initialization process.

3. If a factor has a validation method defined, Oracle Database Vault validates the identity (value) of the factor by executing this validation method. If the validation method fails or returns false, the identity of the factor is undefined (`NULL`).
4. If a factor has any identities defined for it, Oracle Database Vault resolves the trust level of the factor based on the identities defined. If an identity of the factor is defined in this list of defined identities, then Oracle Database Vault assigns the

trust level as configured; otherwise it sets it to -1. If there are no identities defined for the factor, the trust level is undefined (NULL).

5. Depending on the outcome of this factor evaluation, factor validation, and trust level resolution, Database Vault audits the details of the evaluation as dictated by the factor audit configuration.
6. When the evaluation of all factors that are identified by method or constant completes, Oracle Database Vault resolves the factors that are identified by other factors by using the identity maps that are defined for the factor configured identities.

The evaluation order of the factor-configured identities is by ASCII sort on the identity values: Oracle Database Vault uses the first alphabetically sorted identity mapping that it evaluates. For example, suppose factor TEST has identities X and Y. Furthermore, identities X and Y have identity maps that are dependent on identities for factors A, B, and C. The following mapping occurs:

- X is mapped when A=1 and B=1
- Y is mapped when A=1, B=1, and C=2

In this case, the first one evaluated is X. Y is not evaluated, but what if its C mapping meets the criteria that is needed for the TEST factor's success? You would need to reverse the mapping, that is, map Y before X so that A, B, and C can be evaluated first. To reverse the mapping, rename Y to V (or some alphabetic value that sorts before X) so that it can be correctly resolved.

This algorithm works if the ASCII sort ordering is correct and the identities map the same number factors at some level.

7. When the factor initialization completes, the Oracle Database Vault integration with Oracle Label Security occurs.

After this process completes, Oracle Database Vault checks to see if a command rule is associated with the CONNECT event. If a rule set associated with the CONNECT event, then Oracle Database Vault evaluates the rule set. If the rule set evaluates to false or results in an error, then the session is terminated. Oracle Database Vault executes any auditing or call handlers associated with the rule set before the session is terminated.

---



---

**Note:**

Be careful about associating command rules with the CONNECT event, because you can inadvertently lock out other users from of the database. In general, if you create a command rule for CONNECT, set its evaluation option of the associated rule set to Any True.

If you do inadvertently lock out users, then you should temporarily disable Oracle Database Vault, disable the CONNECT command rule, reenable Oracle Database Vault, and then fix the factor code that is causing the problem. [If the Test Fails](#) (page 8-27) provides an example of how to accomplish this.

---



---

## 8.6.2 How Factors Are Retrieved

You can retrieve a factor in a database session at any time by using the DVF factor function or the GET\_FACTOR function.

To find a listing of available factors, query the `DBA_DV_FACTOR` data dictionary view, described in [DBA\\_DV\\_FACTOR View](#) (page 25-11).

**Example 8-1** (page 8-22) shows an example of using the `GET_FACTOR` function.

**Example 8-1 Using GET\_FACTOR to Retrieve a Factor**

```
SELECT GET_FACTOR('client_ip') FROM DUAL;
```

You can use the factor values retrieved from the DVF factor function or the `GET_FACTOR` in the following ways:

- Oracle Database Vault rule expressions
- Custom application code that is available to all database sessions in an Oracle Database Vault environment

[Oracle Database Vault DVF PL/SQL Factor Functions](#) (page 18-27) describes DVF factor functions in detail.

If you had set the factor evaluation to **By Session**, then Oracle Database Vault retrieves the value from the session context established, as described under [How Factors Are Processed When a Session Is Established](#) (page 8-20).

If you had set the factor evaluation to **By Access**, then Oracle Database Vault performs Step 2 through Step 5 (or Step 6), as described under [How Factors Are Processed When a Session Is Established](#) (page 8-20), whenever the factor is retrieved.

If you had defined error options for the factor and if an error occurs, then Oracle Database Vault displays the error message.

### 8.6.3 How Factors Are Set

You can assign a factor identity at any time during a database session, but only if the factor assignment rule set evaluates to true.

You can do this in the application code by using the `SET_FACTOR` function. In Java code, you can use the JDBC class `java.sql.CallableStatement` to set this value. For example:

```
java.sql.Connection connection ;
...
java.sql.CallableStatement statement =
    connection.prepareCall("{call SET_FACTOR('FACTOR_X', ?)}");
statement.setString(1, "MyValue");
boolean result = statement.execute();
...
```

Applications that can execute Oracle PL/SQL functions can use this procedure (for example, applications written using Oracle Data Provider for .NET (ODP.NET)).

This concept is similar to the standard Oracle `DBMS_SESSION.SET_IDENTIFIER` procedure with an added feature that a rule set controls when a factor value can be set. If the rule set evaluates to true, Steps 2 (page 8-20) through 5 (page 8-21) under [How Factors Are Processed When a Session Is Established](#) (page 8-20) occur.

If you have not associated a assignment rule set for the factor or if the rule set returns false (or returns errors), then Oracle Database Vault sends an error message if you attempt to set the factor using the `SET_FACTOR` function.

## 8.7 Tutorial: Preventing Ad Hoc Tool Access to the Database

This tutorial demonstrates how to use factors to prevent ad hoc tools (such as SQL\*Plus) from accessing the database.

### [About This Tutorial](#) (page 8-23)

Many database applications contain features to explicitly control the actions of a user.

### [Step 1: Enable the HR and OE User Accounts](#) (page 8-24)

You must use the HR and OE accounts later on when you test the Oracle Database Vault components for this tutorial.

### [Step 2: Create the Factor](#) (page 8-24)

After you have ensured that the HR and OE accounts are active, you can create a factor.

### [Step 3: Create the Rule Set and Rules](#) (page 8-25)

After you have created the factor, you can create a rule set and rules to work with the factor.

### [Step 4: Create the CONNECT Command Rule](#) (page 8-26)

The CONNECT command rule controls the CONNECT SQL statement.

### [Step 5: Test the Ad Hoc Tool Access Restriction](#) (page 8-27)

You do not need to restart your SQL\*Plus session for the Oracle Database Vault changes to take effect.

### [Step 6: Remove the Components for This Tutorial](#) (page 8-28)

You can remove the components that you created for this tutorial if you no longer need them.

### 8.7.1 About This Tutorial

Many database applications contain features to explicitly control the actions of a user.

However, an ad hoc query tool, such as SQL\*Plus, may not have these controls. As a result, a user could use an ad hoc tool to perform actions in the database that he or she would normally be prevented from performing in a database application. You can use a combination of Oracle Database Vault factors, rule sets, and command rules to prevent unauthorized access to the database by ad hoc query tools.

In the following tutorial, you prevent users HR and OE from using SQL\*Plus. To accomplish this, you must create a factor to find the applications on your system and a rule and rule set to limit SQL\*Plus to these four users. Then you create a command rule for the CONNECT SQL statement, which is associated with the rule set. This factor, `Client_Prog_Name`, uses the `CLIENT_PROGRAM_NAME` attribute of the `SYS_CONTEXT` SQL function `USERENV` namespace to find the names of the applications that are used to access the current instance of Oracle Database. The `SYS_CONTEXT` SQL function provides many useful methods for finding the state of a user session. `SYS_CONTEXT` is a valuable tool for creating custom factors.

---

**See Also:**

*Oracle Database SQL Language Reference* for more information about the `SYS_CONTEXT` function.

---

## 8.7.2 Step 1: Enable the HR and OE User Accounts

You must use the HR and OE accounts later on when you test the Oracle Database Vault components for this tutorial.

1. Log into the database instance as a user who has been granted the DV\_ACCTMGR role.

For example:

```
sqlplus bea_dvacctmgr
Enter password: password
```

In a multitenant environment, you must connect to the appropriate pluggable database (PDB).

For example:

```
sqlplus bea_dvacctmgr@hrpdb
Enter password: password
```

To find the available PDBs, query the DBA\_PDBS data dictionary view. To check the current PDB, run the `show con_name` command.

2. Check the status of the HR account.

```
SELECT USERNAME, ACCOUNT_STATUS FROM DBA_USERS WHERE USERNAME = 'HR';
```

3. If the HR account is expired and locked, then enter the following statement to make it active:

```
ALTER USER HR ACCOUNT UNLOCK IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace `password` with a password that is secure.

4. Repeat these steps for the OE account.

## 8.7.3 Step 2: Create the Factor

After you have ensured that the HR and OE accounts are active, you can create a factor.

1. Connect as a user who has been granted the DV\_OWNER or DV\_ADMIN role.

For example:

```
CONNECT leo_dvowner --Or, CONNECT leo_dvowner@hrpdb
Enter password: password
```

2. Create the factor.

```
BEGIN
DBMS_MACADM.CREATE_FACTOR(
  factor_name      => 'Client_Prog_Name',
  factor_type_name => 'Application',
  description      => 'Stores client program name that connects to database',
  rule_set_name    => NULL,
  validate_expr    => NULL,
  get_expr         => 'UPPER(SYS_CONTEXT(''USERENV'', ''CLIENT_PROGRAM_NAME''))',
  identify_by      => DBMS_MACUTL.G_IDENTIFY_BY_METHOD,
  labeled_by       => DBMS_MACUTL.G_LABELED_BY_SELF,
```

```

eval_options      => DBMS_MACUTL.G_EVAL_ON_SESSION,
audit_options     => DBMS_MACUTL.G_AUDIT_ON_GET_ERROR,
fail_options      => DBMS_MACUTL.G_FAIL_SILENTLY);
END;
/

```

In this specification:

- `factor_type_name` specifies that this is an application-based factor.
- `get_expr` defines the expression for the factor. This expression calls the `SYS_CONTEXT` function, using the `USERENV` namespace and `CLIENT_PROGRAM_NAME` attribute, to find the programs that are logged into the Oracle database.
- `identify_by` identifies the factor by method.
- `labeled_by` labels the identities for the factor directly from the labels associated with an Oracle Label Security policy (default).
- `eval_options` evaluates the factor when the database session is created.
- `audit_options` audits if `get_expr` returns an error.
- `fail_silently` does not show any error messages for the factor.

### 8.7.4 Step 3: Create the Rule Set and Rules

After you have created the factor, you can create a rule set and rules to work with the factor.

1. Create the Limit SQL\*Plus Access rule set as follows:

```

BEGIN
DBMS_MACADM.CREATE_RULE_SET(
  rule_set_name      => 'Limit SQL*Plus Access',
  description        => 'Limits access to SQL*Plus for Apps Schemas',
  enabled            => DBMS_MACUTL.G_YES,
  eval_options       => DBMS_MACUTL.G_RULESET_EVAL_ANY,
  audit_options      => DBMS_MACUTL.G_RULESET_AUDIT_OFF,
  fail_options       => DBMS_MACUTL.G_RULESET_FAIL_SHOW,
  fail_message       => 'SQL*Plus access not allowed for Apps Schemas',
  fail_code          => 20461,
  handler_options    => DBMS_MACUTL.G_RULESET_HANDLER_OFF,
  handler            => NULL,
  is_static          => FALSE);
END;
/

```

In this specification:

- `fail_options` enables an error message, set by `fail_message`, and error code, set by `fail_code`, to appear if there are errors.
  - `is_static` evaluates the rule set once during the user session. After that, the value is re-used.
2. Find the exact settings for the computer on which you want to apply the policy, based on what the `CLIENT_PROGRAM_NAME` attribute will return.

```
SELECT SYS_CONTEXT('USERENV', 'CLIENT_PROGRAM_NAME') FROM DUAL;
```

The output should be similar to the following:

```
SYS_CONTEXT('USERENV','CLIENT_PROGRAM_NAME')
```

```
-----  
sqlplus@nemosity (TNS V1-V3)
```

For this tutorial, the name of the computer is `nemosity`. The (TN V1-V3) output refers to the version of the TNS connector.

### 3. Create the following rules.

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Prevent Apps Schemas Access to SQL*Plus',
    rule_expr => 'UPPER (DVF.F$CLIENT_PROG_NAME) != 'SQLPLUS@NEMOSITY (TNS V1-
V3)'' AND DVF.F$SESSION_USER IN ('HR', 'OE')');
END;
/
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Allow Non-Apps Schemas Access to SQL*Plus',
    rule_expr => 'DVF.F$SESSION_USER NOT IN ('HR', 'OE')');
END;
/
```

The rules translate to the following: "Prevent users HR and OE from logging into SQL\*Plus, but allow other users access."

### 4. Add the rules to the Limit SQL\*Plus Access rule set.

```
BEGIN
  DBMS_MACADM.ADD_RULE_TO_RULE_SET(
    rule_set_name => 'Limit SQL*Plus Access',
    rule_name      => 'Prevent Apps Schemas Access to SQL*Plus',
    rule_order     => 1);
END;
/
BEGIN
  DBMS_MACADM.ADD_RULE_TO_RULE_SET(
    rule_set_name => 'Limit SQL*Plus Access',
    rule_name      => 'Allow Non-Apps Schemas Access to SQL*Plus',
    rule_order     => 1);
END;
/
```

The `rule_order` setting is required to enable the procedure to work.

## 8.7.5 Step 4: Create the CONNECT Command Rule

The CONNECT command rule controls the CONNECT SQL statement.

This command rule also applies to logging into SQL\*Plus from the command line or other tools your site may use to access SQL\*Plus.

- Create the CONNECT command rule as follows:

```
BEGIN
  DBMS_MACADM.CREATE_COMMAND_RULE(
    command      => 'CONNECT',
    rule_set_name => 'Limit SQL*Plus Access',
    object_owner  => '%',
```



```

object_name    => '%',
enabled        => DBMS_MACUTL.G_YES);
END;
/

```

In this specification:

- `rule_set_name` associates the Limit SQL\*Plus Access rule set with the CONNECT command rule.
- `object_owner` is set to `%` so that the command rule applies to all users.
- `object_name` is set to `%` so that the command rule applies to all objects.
- `enabled` enables the command rule so that it can be used right away.

### 8.7.6 Step 5: Test the Ad Hoc Tool Access Restriction

You do not need to restart your SQL\*Plus session for the Oracle Database Vault changes to take effect.

1. In SQL\*Plus, try to connect as user HR:

```

CONNECT HR --Or, CONNECT HR@hrpdb
Enter password: password

```

The following output should appear:

```

ERROR:
ORA-47306: 20461: Limit SQL*Plus Access rule set failed

```

User HR should be prevented from using SQL\*Plus.

2. Next, try to connect as user OE:

```

CONNECT OE --Or, CONNECT OE@hrpdb
Enter password: password

```

The following output should appear:

```

ERROR:
ORA-47306: 20461: Limit SQL*Plus Access rule set failed

```

User OE also should be prevented from using SQL\*Plus.

3. Now try to connect as user SYSTEM:

```

CONNECT SYSTEM --Or, CONNECT SYSTEM@hrpdb
Enter password: password
Connected.

```

User SYSTEM should be able to log into the database instance. So should SYS, the Database Vault Owner account, and the Database Vault Account Manager account.

#### If the Test Fails

If you cannot log into the database instance as SYSTEM (or as any of the other administrative users listed in your rule expression), then you are prevented from using SQL\*Plus.

You can remedy the problem as follows:

1. Log into the database instance as a user who has been granted the DV\_OWNER or DV\_ADMIN role.

For example:

```
CONNECT dbv_owner --Or, CONNECT dbv_owner@hrpdb for a PDB
Enter password: password
```

2. Enter the following statement to drop the CONNECT command rule.

```
EXEC DBMS_MACADM.DELETE_COMMAND_RULE ('CONNECT', '%', '%');
```

Even though you have disabled Oracle Database Vault, you still can use its PL/SQL packages and Database Vault Administrator.

3. Check the policy components for any errors and then correct them. Recreate the CONNECT command rule, and then test it.

### 8.7.7 Step 6: Remove the Components for This Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. Remove the CONNECT command rule.

```
EXEC DBMS_MACADM.DELETE_COMMAND_RULE ('CONNECT', '%', '%');
```

2. Remove the Client\_Prog\_Name factor.

```
EXEC DBMS_MACADM.DELETE_FACTOR('Client_Prog_Name');
```

3. Remove the Limit SQL\*Plus Access rule set.

```
EXEC DBMS_MACADM.DELETE_RULE_SET('Limit SQL*Plus Access');
```

4. Remove the rules.

```
EXEC DBMS_MACADM.DELETE_RULE('Prevent Apps Schemas Access to SQL*Plus');
EXEC DBMS_MACADM.DELETE_RULE('Allow Non-Apps Schemas Access to SQL*Plus');
```

5. If necessary, as a user who has been granted the DBV\_ACCTMGR role, lock the HR and OE accounts.

```
CONNECT bea_dvacctmgr --Or, CONNECT amalcolumn_dbacctmgr@hrpdb
Enter password: password
```

```
ALTER USER HR ACCOUNT LOCK;
ALTER USER OE ACCOUNT LOCK;
```

## 8.8 Tutorial: Restricting User Activities Based on Session Data

This tutorial shows how to restrict user activities based on their session data, such as the domain the user is using.

[About This Tutorial](#) (page 8-29)

You can use factor identity mapping to set session-based user restrictions for database activities.

[Step 1: Create an Administrative User](#) (page 8-29)

Before you can use this tutorial, you must create an administrative user.

**Step 2: Add Identities to the Domain Factor** (page 8-30)

Next, you must add identities to the Domain factor, which is a default factor.

**Step 3: Map the Domain Factor Identities to the Client\_IP Factor** (page 8-31)

After you have added identities to the domain factory, you can map them to the Client\_IP factor.

**Step 4: Create a Rule Set to Set the Hours and Select the Factor Identity** (page 8-33)

You must create a rule set to work with the factor that you modified.

**Step 5: Create a Command Rule That Uses the Rule Set** (page 8-34)

You must create a command rule that uses the rule set that you created.

**Step 6: Test the Factor Identity Settings** (page 8-34)

Test the settings by resetting the system clock, logging in as the `mwaldron` administrative user, and then trying to create a table.

**Step 7: Remove the Components for This Tutorial** (page 8-35)

You can remove the components that you created for this tutorial if you no longer need them.

## 8.8.1 About This Tutorial

You can use factor identity mapping to set session-based user restrictions for database activities.

For example, suppose you wanted to restrict administrative access to a database using the following criteria:

- Ensure that the administrator is accessing the database from the correct IP address.
- Limit the database access to the standard business hours of the administrator.

This type of configuration is useful for restricting different types of administrators: not only local, internal administrators, but offshore and contract administrators as well.

In this tutorial, you modify the Domain factor to include identities for a secure and non-secure network access, which are based on the IP address of the computer the administrator is using. If the administrator tries to perform an action outside the standard working hours or from a different IP address, then Oracle Database Vault prevents him from doing so.

## 8.8.2 Step 1: Create an Administrative User

Before you can use this tutorial, you must create an administrative user.

1. In SQL\*Plus, log in as a user who has been granted the `DV_ACCTMGR` role, and then create the user account `mwaldron`.

For example:

```
sqlplus bea_dvacctmgr
Enter password: password
```

```
CREATE USER mwaldron IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace `password` with a password that is secure.

In a multitenant environment, you must connect to the appropriate pluggable database (PDB).

For example:

```
sqlplus bea_dvacctmgr@hrpdb
Enter password: password
```

To find the available PDBs, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

2. Connect as a user who privileges to grant the `CREATE SESSION` privilege and the `DBA` role, and then grant user `mwaldron` these privileges. This user must also be authorized as an owner of the Oracle System Privilege and Role Management realm.

For example:

```
CONNECT dba_psmith -- Or, CONNECT dba_psmith@hrpdb
Enter password: password
```

```
GRANT CREATE SESSION, DBA TO mwaldron;
```

### 8.8.3 Step 2: Add Identities to the Domain Factor

Next, you must add identities to the Domain factor, which is a default factor.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.

2. In the Administration page, under Database Vault Components, click **Factors**.

The Factors page appears.

3. Select the **Show Oracle defined Factors** check box to display the default factors.

4. Select the Domain factor and then select **Edit**.

The Domain factor will be the parent factor.

5. Click the **Next** button until you reach the Identities page.

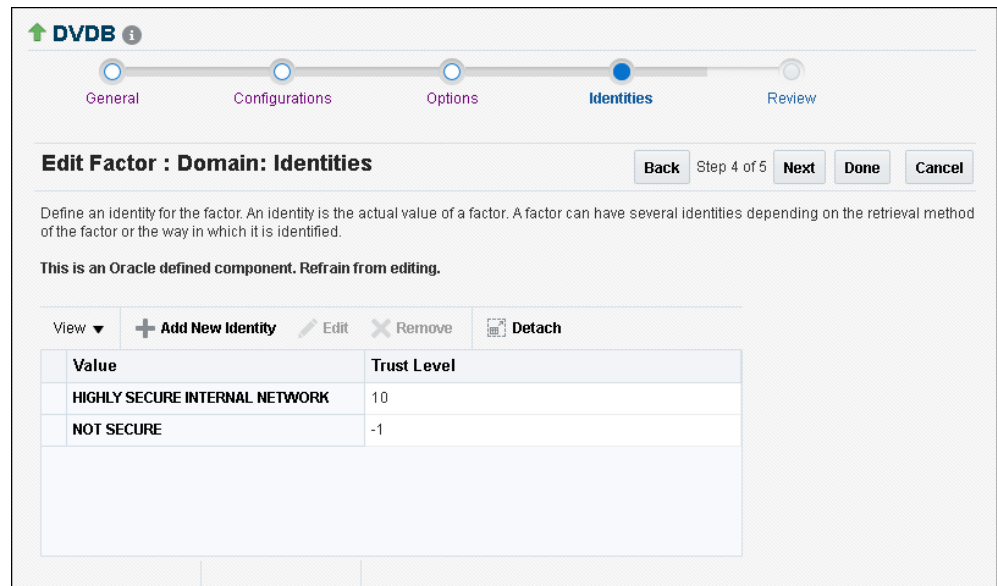
6. Select the **Add New Identity** button.

7. In the Identity tab of the Add New Identity and Mapping page, enter the following information:

- **Value:** Enter `HIGHLY SECURE INTERNAL NETWORK`
- **Trust Level:** Select **Very Trusted**

8. Click **OK**.

9. Repeat these steps to create a second identity called `NOT SECURE`, and then set its trust level to **Untrusted**.



### 8.8.4 Step 3: Map the Domain Factor Identities to the Client\_IP Factor

After you have added identities to the domain factory, you can map them to the Client\_IP factor.

The Client\_IP factor is a default factor.

1. In Identities page, select the HIGHLY SECURE INTERNAL NETWORK identity and then select **Edit**.
2. In the Add New Identity and Mapping window, select the **Map Identity** subpage.
3. Select the **Map Identity** tab, and then select **Add Mapping**.
4. In the Add New Identity Mapping page, enter the following information:
  - **Child Factor:** Select **Client\_IP** to be the child factor.
  - **Operator:** Select **Equal**.
  - **Min Value:** Enter the IP address for the Virtual Machine (for example, 192.0.2.12). (This is the computer that user mwaldron uses. For this tutorial, you can enter the IP address of your own computer. If you are using Microsoft Windows, use the IP address assigned to the Loopback Adapter.)
  - **Max Value:** Leave this field empty.
5. Click **OK**, and then click **OK** again to return to the Identities page.
6. Create the following two identity maps for the NOT SECURE identity, by editing this identity:

Child Factor	Operator	Min Value	Max Value
Client_IP	Less	192.0.2.5	(Leave blank)
Client_IP	Greater	192.0.2.20	(Leave blank)

The identity maps in the NOT SECURE identity are in a range of IP addresses outside the IP address that user `mwaldron` uses (192.0.2.12). The IP addresses here must be in any range *outside* `mwaldron`'s IP address.

This identity mapping creates the following condition: If the user logs in from the correct IP address, then Oracle Database Vault decides that the connection is secure, through the HIGHLY SECURE INTERNAL NETWORK identity. However, if the user logs in from an IP address that is less than 192.0.2.5 or greater than 192.0.2.20, then the connection is deemed not secure, through the NO SECURE identity.

7. Click **OK**.
8. Click **Done**, and then click **Finish**.
9. Test the factor identities.

First, in SQL\*Plus, connect as user `mwaldron` but do not specify a database instance.

```
CONNECT mwaldron -- Or, CONNECT mwaldron@hrpdb
Enter password: password
```

```
SELECT DVF.F$CLIENT_IP FROM DUAL;
```

The following output should appear:

```
F$CLIENT_IP
-----
```

Next:

```
SELECT DVF.F$DOMAIN FROM DUAL;
```

The following output should appear:

```
F$DOMAIN
-----
NOT SECURE
```

Because user `mwaldron` is not connecting directly to the database instance, Oracle Database Vault does not recognize the IP address from which he is connecting. In this case, Oracle Database uses the IPC protocol to perform the connection, which sets the IP value to null. Therefore, the identity for this connection is set to NOT SECURE.

Now connect to SQL\*Plus by specifying the database instance (for example, `orcl`), and then check the factor identities again:

```
CONNECT mwaldron@orcl
Enter password: password
```

```
SELECT DVF.F$CLIENT_IP FROM DUAL;
```

The following output should appear:

```
F$CLIENT_IP
-----
192.0.2.12
```

Next:

```
SELECT DVF.F$DOMAIN FROM DUAL;
```

The following output should appear:

```
F$DOMAIN
-----
HIGHLY SECURE INTERNAL NETWORK
```

Now that user `mwaldron` is connecting to the `orcl` database instance, his IP address is recognized. This is because the database uses the TCP protocol, so now the host IP value can be populated appropriately. Because the IP address is within the correct range, the factor identity is set to `HIGHLY SECURE INTERNAL NETWORK`.

### 8.8.5 Step 4: Create a Rule Set to Set the Hours and Select the Factor Identity

You must create a rule set to work with the factor that you modified.

1. In the Administration page, under Database Vault Components, select **Rule Sets**.
2. In the Rule Sets page, select **Create**.
3. In the Create Rule Set page, enter the following settings:
  - **Name:** Enter `Internal DBA Standard Working Hours`.
  - **Status:** Select **Enabled**.
  - **Evaluation Options:** Select **All True**.

Leave the remaining settings at their defaults.

4. Click **Next** to display the Associate with Rule page.
5. Select **Create Rule**.
6. In the Create Rule window, enter the following settings:
  - **Name:** `Internal DBA`
  - **Expression:** `DVF.F$SESSION_USER='MWALDRON'`  
(When you create an expression with a user name, enter the user name in upper case letters, because that is how the database stores user names.)
7. Click **OK**.
8. Use the **Create Rule** page to create the following additional rules:
  - **Name:** `Internal Network Only`  
**Rule Expression:** `DVF.F$DOMAIN='HIGHLY SECURE INTERNAL NETWORK'`
  - **Name:** `Week Day`  
**Rule Expression:** `TO_CHAR(SYSDATE, 'D') BETWEEN '2' AND '6'`
  - **Name:** `Week Working Day Hours`  
**Rule Expression:** `TO_CHAR(SYSDATE, 'HH24') BETWEEN '08' AND '19'`

9. Click **Done**, and then click **Finish**.

### 8.8.6 Step 5: Create a Command Rule That Uses the Rule Set

You must create a command rule that uses the rule set that you created.

1. In the Administration page, select **Command Rules**.
2. In the Command Rules page, select **Create**.
3. In the Create Command Rule page, enter the following settings:
  - **Command:** Select **CREATE TABLE** from the list.
  - **Status:** Select **Enabled**.
  - **Applicable Object Owner:** Ensure it is set to % (the default).
  - **Applicable Object Name:** Ensure it is set to % (the default).
  - **Evaluating Rule Set:** Select **Internal DBA Standard Working Hours** from the list.
4. Click **OK**.

### 8.8.7 Step 6: Test the Factor Identity Settings

Test the settings by resetting the system clock, logging in as the mwaldron administrative user, and then trying to create a table.

1. Set the system time to 9 p.m.

**UNIX:** Log in as root and use the `date` command to set the time. For example, assuming the date today is August 15, 2013, you would enter the following:

```
su root
Password: password

date --set="15 AUG 2013 21:00:00"
```

**Windows:** Double-click the clock icon, which is typically at the lower right corner of the screen. In the Date and Time Properties window, set the time to 9 p.m., and then click **OK**.

2. In SQL\*Plus, connect as user mwaldron and try to create a table. In the following, replace `orcl` with the name of your database instance.

```
CONNECT mwaldron@orcl
Enter password: password

CREATE TABLE TEST (num number);
```

The following output should appear:

```
ORA-47400: Command Rule violation for create table on MWALDRON.TEST
```

Because user mwaldron is create a table outside working hours, Database Vault prevents him.

3. Reset the system time back to the local time.



4. In SQL\*Plus, as user `mwaldron`, try to create the table again.

```
CREATE TABLE TEST (num number);
```

Table created.

```
DROP TABLE TEST;
```

Table dropped.

Now that user `mwaldron` is working during his local hours and from the IP address associated with the `HIGHLY SECURE INTERNAL NETWORK` identity, he can create tables.

5. Reconnect as user `mwaldron` but without adding the database instance name to the connection command, and then try to create the table again.

```
CONNECT mwaldron -- Or, CONNECT mwaldron@hrpdb
```

Enter password: *password*

```
CREATE TABLE TEST (num number);
```

The following output should appear:

```
ORA-47400: Command Rule violation for create table on MWALDRON.TEST
```

Even though user `mwaldron` is trying to create a table during the correct time, he cannot because is not directly logged in to the `orcl` database instance. Oracle Database Vault deems him to be using the `NOT SECURE` identity, and then denies him access.

### 8.8.8 Step 7: Remove the Components for This Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. Log into the database instance as the `DV_ACCTMGR` user and drop user `mwaldron`.

```
sqlplus bea_dvacctmgr -- Or, CONNECT bea_dvacctmgr@hrpdb
```

Enter password: *password*

```
DROP USER mwaldron CASCADE;
```

2. Remove the `CREATE TABLE` command rule.

Return the Administration page and select **Command Rules**. Select the `CREATE TABLE` command rule and then click **Delete**. In the Confirmation window, select **Yes**.

3. Remove the Internal DBA Standard Working Hours rule set.

Select **Rule Sets** in the Administration page. In the Rule Sets page, select the Internal DBA Standard Working Hours rule set, and then select **Delete**. In the Confirmation window, select the **Remove rules associated with the rule set** check box, and then select **Yes**.

4. Remove the rules that were associated with the Internal DBA Standard Working Hours rule set.

Select **Rules** in the Administration page. In the Rules page, select the Internal DBA, Internal Network Only, Week Day, and Week Day Working Hours rules, and then select **Delete**. Select Yes in the Confirmation window.

5. Remove the HIGHLY SECURE INTERNAL NETWORK and NOT SECURE factor identities from the Domain factor.

In the Administration page and select **Factors**. Select the Domain factor, select **Edit**. Click **Next** until you reach the Identities page. Select the HIGHLY SECURE INTERNAL NETWORK and NOT SECURE factor identities and click **Remove** to remove each one. (Hold the **Control** key down to select multiple items.) In the Confirmation window, select **Yes**. Click **Done**, and then click **Finish**.

## 8.9 Guidelines for Designing Factors

Oracle provides guidelines for designing factors.

- You can use the Oracle utility packages such as UTL\_TCP, UTL\_HTTP, DBMS\_LDAP, and DBMS\_PIPE to integrate security or other contextual information about the session from external systems.
- Do not specify a retrieval method if the factor identification is set to **Identified By Factors**. Retrieval methods are only needed if you set the factor to **By Method** or **By Constant**.
- Consider using a validation method if a factor has an assignment rule set. Doing so helps to verify that invalid identities are not submitted.
- Use the client-supplied factors such as Program, OS User, and others with caution, because the values that are supplied can only be trusted when the client software is trusted and the communications channel from the client software is known to be secure.
- Only specify an evaluation option of **By Access** if the value returned by the retrieval method could change from one invocation to the next in the same session (for example, time-based factors).
- Optimize the internal logic of a function used for the factor retrieval method using traditional SQL and PL/SQL optimization techniques. For more information about performance and optimization, see *Oracle Database SQL Tuning Guide*.
- If the discrete values returned by the retrieval method are known, be sure to define identities for each value so that you can assign trust levels for them. Trust levels add value to factors as you also can use the trust level in application logic based on factors.
- A security policy based on more factors is generally considered stronger than one based on fewer factors. You can create a new factor that is identified by other factors to store combinations of factors into logical grouping using identity maps. This also makes it easier to label the parent factor when you integrate the factors with the Oracle Label Security labels. (See [Integrating Oracle Database Vault with Oracle Label Security](#) (page 12-5) for more information.)
- It is generally easier to configure and debug a factor that is labeled **By Self** than one labeled **By Factors** when integrating the Oracle Label Security.
- You can design a database client application to pass one or more security, end-user, or environmental attributes so that they are available to an associated

database session. To do this, create a single factor for each attribute and then use an assignment rule set to control when these attributes can be assigned (for example only when using a specific Web application on specified named application server computers). Oracle Database Vault factors used in this fashion are very much like the Oracle procedure `DBMS_SESSION.SET_IDENTIFIER` but also include a capability to control when they can be set. For more information about the `DBMS_SESSION` package, see *Oracle Database PL/SQL Packages and Types Reference*.

## 8.10 How Factors Affect Performance

The complexity of factors affects the performance of your Oracle database instance.

Each factor has elements that are processed, such as its validation method, trust level, and so on. For factors that are evaluated by the session, such as `Database_Hostname` and `Proxy_User`, Oracle Database Vault performs this processing during session initialization, and then caches the results for subsequent requests for that value.

The default factors listed in [Default Factors](#) (page 8-2) are cached because they are likely candidates for a typical security policy. However, if you only use five factors (for example, in rule sets or other components), then the other factors consume resources that could otherwise be used elsewhere. In this case, you should remove the unnecessary factors by deleting them. (Oracle Database Vault does not use any of these factors internally, so you can remove them if you do not need them.)

If you have a large number of users or if your application server frequently must create and destroy connections, the resources used can affect system performance. You can delete the unnecessary factors.

You can check system performance by running tools such as Oracle Enterprise Manager (including Oracle Enterprise Manager Cloud Control, which is installed by default with Oracle Database), Automatic Workload Repository (AWR), and `TKPROF`.

---



---

### See Also:

- *Oracle Database Performance Tuning Guide* to learn how to monitor database performance
  - *Oracle Database SQL Tuning Guide* to monitor the performance of individual SQL and PL/SQL statements
- 
- 

## 8.11 Factor Related Reports and Data Dictionary Views

Oracle Database Vault provides reports and data dictionary views that display information about factors and their identities.

[Table 8-1](#) (page 8-37) lists the Oracle Database Vault reports. See [Oracle Database Vault Reports](#) (page 27-1), for information about how to run these reports.

**Table 8-1 Reports Related to Factors and Their Identities**

Report	Description
<a href="#">Factor Audit Report</a> (page 27-6)	Audits factors (for example, to find factors that failed to be evaluated)

**Table 8-1 (Cont.) Reports Related to Factors and Their Identities**

Report	Description
<a href="#">Factor Configuration Issues Report</a> (page 27-4)	Lists configuration issues, such as disabled or incomplete rule sets, or to audit issues that may affect the factor
<a href="#">Factor Without Identities Report</a> (page 27-4)	Lists factors that have had no identities assigned yet
<a href="#">Identity Configuration Issues Report</a> (page 27-4)	Lists factors that have invalid label identities or no map for the identity
<a href="#">Rule Set Configuration Issues Report</a> (page 27-3)	Lists rule sets that have no rules defined or enabled, which may affect the factors that use them

Table 8-2 (page 8-38) lists data dictionary views that provide information about existing factors and factor identities.

**Table 8-2 Data Dictionary Views Used for Factors and Factor Identities**

Data Dictionary View	Description
<a href="#">DBA_DV_FACTOR View</a> (page 25-11)	Lists the existing factors in the current database instance
<a href="#">DBA_DV_FACTOR_LINK View</a> (page 25-14)	Shows the relationships of each factor whose identity is determined by the association of child factors
<a href="#">DBA_DV_FACTOR_TYPE View</a> (page 25-13)	Lists the names and descriptions of factor types used in the system
<a href="#">DBA_DV_IDENTITY View</a> (page 25-15)	Lists the identities for each factor
<a href="#">DBA_DV_IDENTITY_MAP View</a> (page 25-15)	Lists the mappings for each factor identity

---

# Configuring Secure Application Roles for Oracle Database Vault

Secure application roles enable you to control how much access users have to an application.

## [What Are Secure Application Roles in Oracle Database Vault?](#) (page 9-1)

In Oracle Database Vault, you can create a secure application role that you enable with an Oracle Database Vault rule set.

## [Creating an Oracle Database Vault Secure Application Role](#) (page 9-2)

You can create a Database Vault secure application role in Database Vault Administrator.

## [Modifications to a Secure Application Role](#) (page 9-3)

You can modify an existing secure application role only if it has been created in Oracle Database Vault.

## [Security for Oracle Database Vault Secure Application Roles](#) (page 9-4)

Users who have database administrative privileges may try to use the `DROP ROLE` statement to delete Oracle Database Vault secure application roles.

## [Deleting an Oracle Database Vault Secure Application Role](#) (page 9-4)

You can delete Oracle Database Vault secure application roles in Oracle Database Vault Administrator.

## [How Oracle Database Vault Secure Application Roles Work](#) (page 9-4)

The process flow for an Oracle Database Vault secure application role begins after you create and set the secure application role.

## [Tutorial: Granting Access with Database Vault Secure Application Roles](#) (page 9-5)

This tutorial demonstrates how to create a secure application role to control user access to the `OE.ORDERS` table during work hours.

## [How Secure Application Roles Affect Performance](#) (page 9-10)

You can check system performance by Oracle Enterprise Manager Cloud Control.

## [Secure Application Role Related Reports and Data Dictionary View](#) (page 9-10)

Oracle Database Vault provides reports and a data dictionary view that you can use to analyze Oracle Database Vault secure application roles.

## 9.1 What Are Secure Application Roles in Oracle Database Vault?

In Oracle Database Vault, you can create a secure application role that you enable with an Oracle Database Vault rule set.

Regular Oracle Database secure application roles are enabled by custom PL/SQL procedures. You use secure application roles to prevent users from accessing data from outside an application. This forces users to work within the framework of the application privileges that have been granted to the role.

In a multitenant environment, you only can create a secure application role in a PDB, not in the CDB root or the application root.

The advantage of basing database access for a role on a rule set is that you can store database security policies in one central place, as opposed to storing them in all your applications. Basing the role on a rule set provides a consistent and flexible method to enforce the security policies that the role provides. In this way, if you must update the security policy for the application role, you do it in one place, the rule set.

Furthermore, no matter how the user connects to the database, the result is the same, because the rule set is bound to the role. All you need to do is to create the role and then associate it with a rule set. The associated rule set validates the user who is trying to enable the role.

**Related Topics:**

[Oracle Database Vault Secure Application Role APIs](#) (page 19-1)  
 The DBMS\_MACADM and DBMS\_MACSEC\_ROLES PL/SQL packages manage Database Vault secure application roles.

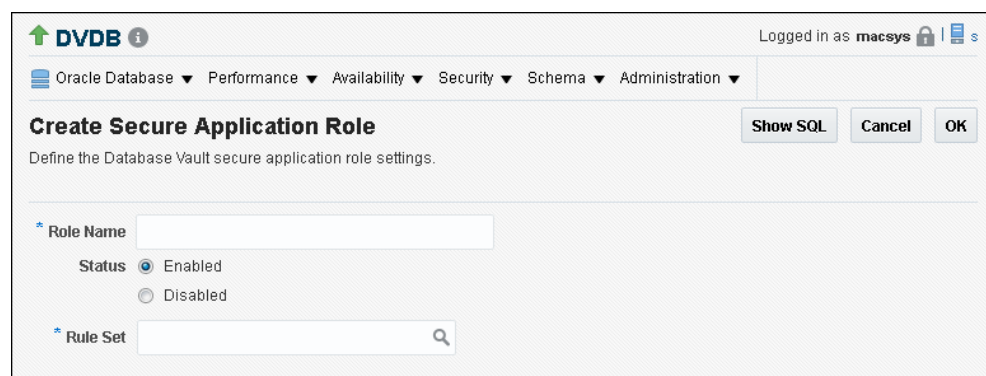
## 9.2 Creating an Oracle Database Vault Secure Application Role

You can create a Database Vault secure application role in Database Vault Administrator.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. Create a rule set that contains at least one rule to set the conditions for allowing or disallowing the user to enable the role.

When you create the underlying rule for the rule set, remember that the rule should validate the user who is trying to enable the role.

3. In the Administration page, under Database Vault Components, click **Secure Application Roles**.
4. In the Secure Application Role page, click **Create**.



5. In the Create Secure Application Role page, enter the following settings:
- **Role Name:** Enter the name using no more than 30 characters, with no spaces. Ensure that this name follows the standard Oracle naming conventions for role creation using the `CREATE ROLE` statement, described in *Oracle Database SQL Language Reference*. This attribute is mandatory.
  - **Status:** Select either **Enabled** or **Disabled** to enable or disable the secure application role during run time. This attribute is mandatory.
    - **Enabled:** Enables the role to be available for use. That is, users are allowed to call the `DBMS_MACSEC_ROLES.SET_ROLE` function to try to enable the role. Note that whether or not the role will be enabled depends on the evaluation result of the associated rule set.
    - **Disabled:** Disables the role from being available for use. The `DBMS_MACSEC_ROLES.SET_ROLE` function will not be able to enable the role.
  - **Rule Set:** From the list, select the rule set that you want to associate with the secure application role. This attribute is mandatory.
- When calling `DBMS_MACSEC_ROLES.SET_ROLE`, if the rule set evaluates to true, then Oracle Database Vault enables the role for the database session. If the rule set evaluates to false, then the role is not enabled.

6. Click **OK**.

#### Related Topics:

[Configuring Rule Sets](#) (page 6-1)

Rule sets group one or more rules together; the rules determine whether a user can perform an action on an object.

[SET\\_ROLE Procedure](#) (page 19-7)

The `SET_ROLE` procedure issues the `SET ROLE` PL/SQL statement for specified roles.

[Propagating Oracle Database Vault Configurations to Other Databases](#) (page 13-2)

You can propagate Database Vault configurations (such as a realm configuration) to other Database Vault-protected databases.

## 9.3 Modifications to a Secure Application Role

You can modify an existing secure application role only if it has been created in Oracle Database Vault.

You cannot modify secure application roles or database roles that have been created outside of Oracle Database Vault. If you want to modify an existing Oracle Database role so that it can work with Oracle Database Vault, create a new secure application role in Oracle Database Vault and then grant the existing role to the secure application role. For example, in SQL\*Plus:

```
GRANT myExistingDBrole TO myDVrole;
```

After you create a new secure application role, you must modify your code to use this new role. You can use `DBMS_MACSEC_ROLES.SET_ROLE` in your application code to accomplish this.

**Related Topics:**

[SET\\_ROLE Procedure](#) (page 19-7)

The `SET_ROLE` procedure issues the `SET ROLE` PL/SQL statement for specified roles.

## 9.4 Security for Oracle Database Vault Secure Application Roles

Users who have database administrative privileges may try to use the `DROP ROLE` statement to delete Oracle Database Vault secure application roles.

Whenever an Oracle Database Vault secure application role has been created, Database Vault adds the secure application role to the Oracle Database Vault realm. This prevents database administrator from deleting the secure application role using the `DROP ROLE` statement.

## 9.5 Deleting an Oracle Database Vault Secure Application Role

You can delete Oracle Database Vault secure application roles in Oracle Database Vault Administrator.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. If necessary, locate the various references to the secure application roles by querying the role-related Oracle Database Vault views.
3. Check and modify any applications that may be using the secure application role that you want to delete.
4. In the Administration page, under Database Vault Components, click **Secure Application Roles**.
5. In the Secure Application Roles page, select the role that you want to remove.
6. Click **Delete**.
7. In the Confirmation window, click **Yes**.

**Related Topics:**

[Oracle Database Vault Data Dictionary Views](#) (page 25-1)

You can find information about the Oracle Database Vault configuration settings by querying the Database Vault-specific data dictionary views.

## 9.6 How Oracle Database Vault Secure Application Roles Work

The process flow for an Oracle Database Vault secure application role begins after you create and set the secure application role.

1. Create or update the role either in Oracle Database Vault Administrator or by using the secure application role-specific functions in the `DBMS_MACADM` package.



See [DBMS\\_MACADM Secure Application Role Procedures](#) (page 19-1) for more information.

2. Modify your application to call the role, by using the `DBMS_MACSEC_ROLES.SET_ROLE` function.

See [SET\\_ROLE Procedure](#) (page 19-7) for more information.

3. Oracle Database Vault then evaluates the rule set associated with the secure application role.

If the rule set evaluates to true, then Oracle Database Vault enables the role for the current session. If the rule set evaluates to false, the role is not enabled. In either case, Oracle Database Vault processes the associated auditing and custom event handlers for the rule set associated with the secure application role.

## 9.7 Tutorial: Granting Access with Database Vault Secure Application Roles

This tutorial demonstrates how to create a secure application role to control user access to the `OE.ORDERS` table during work hours.

### [About This Tutorial](#) (page 9-5)

In this tutorial, you restrict the `SELECT` statement on the `ORDERS` table in the `OE` schema to a specific set of users.

### [Step 1: Create Users for This Tutorial](#) (page 9-6)

First, you must create users for the tutorial.

### [Step 2: Enable the OE User Account](#) (page 9-6)

The `OE` schema will be used for this tutorial.

### [Step 3: Create the Rule Set and Its Rules](#) (page 9-6)

The rule set and rules will restrict who can modify orders in the `OE.ORDERS` table.

### [Step 4: Create the Database Vault Secure Application Role](#) (page 9-7)

The Database Vault secure application role will be set when the rule set conditions are satisfied.

### [Step 5: Grant the SELECT Privilege to the Secure Application Role](#) (page 9-8)

The secure application role must be granted the `SELECT` privilege.

### [Step 6: Test the Database Vault Secure Application Role](#) (page 9-8)

With all the components in place, you can test the Database Vault secure application role.

### [Step 7: Remove the Components for This Tutorial](#) (page 9-9)

You can remove the components that you created for this tutorial if you no longer need them.

### 9.7.1 About This Tutorial

In this tutorial, you restrict the `SELECT` statement on the `ORDERS` table in the `OE` schema to a specific set of users.

Furthermore, these users can only perform these statements on the `OE.ORDERS` table from within the office, not from a remote connection. To accomplish this, you create an Oracle Database Vault secure application role that is enabled for the user only if the

user passes the checks enforced by the rule set that you associate with the secure application role.

## 9.7.2 Step 1: Create Users for This Tutorial

First, you must create users for the tutorial.

1. Log in to SQL\*Plus as a user who has been granted the DV\_ACCTMGR role.

For example:

```
sqlplus bea_dvacctmgr
Enter password: password
```

In a multitenant environment, you must connect to the appropriate pluggable database (PDB).

For example:

```
sqlplus bea_dvacctmgr@hrpdb
Enter password: password
```

To find the available PDBs, query the DBA\_PDBS data dictionary view. To check the current PDB, run the `show con_name` command.

2. Create the following user accounts:

```
GRANT CREATE SESSION TO eabel IDENTIFIED BY password;
GRANT CREATE SESSION TO ahutton IDENTIFIED BY password;
GRANT CREATE SESSION TO ldoran IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace `password` with a password that is secure.

## 9.7.3 Step 2: Enable the OE User Account

The OE schema will be used for this tutorial.

1. In SQL\*Plus, connect as the DV\_ACCTMGR user.

For example:

```
CONNECT bea_dvacctmgr -- Or, CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

2. Check the account status of the OE account.

```
SELECT USERNAME, ACCOUNT_STATUS FROM DBA_USERS WHERE USERNAME = 'OE';
```

3. If the OE account is locked and expired, unlock it and assign it a new password.

```
ALTER USER OE ACCOUNT UNLOCK IDENTIFIED BY password;
```

## 9.7.4 Step 3: Create the Rule Set and Its Rules

The rule set and rules will restrict who can modify orders in the OE.ORDERS table.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.

2. In the Administration page, select **Rule Sets**.

The Rule Sets page appears.

3. Click **Create**.

The Create Rule Set page appears.

4. Enter the following information:

- **Name:** Enter `Can Modify Orders`.
- **Description:** Enter Rule set to control who can modify orders in the `OE.ORDERS` table.
- **Status:** Select **Enabled**.
- **Evaluation Options:** Select **All True**.

5. Leave the remaining settings and their defaults, and then click **Next** to go to the Associate with Rules page.

6. Click **Create Rule** and in the Create Rule dialog box, enter the following settings:

- **Name:** `Check IP Address`
- **Expression:** `DVF.F$CLIENT_IP = 'your_IP_address'`

For the Check IP Address rule, replace *your\_IP\_address* with the IP address for your computer. In a real-world scenario, you would create an expression that includes all the IP addresses for the users who should be allowed access.

This rule uses the default factor `Client_IP`. If this factor has been removed, then you can use the following rule expression instead:

```
UPPER(SYS_CONTEXT('USERENV','IP_ADDRESS')) = 'your_IP_address'
```

7. Click **OK**.

8. Click **Create Rule** again and in the Create Rule dialog box, enter the following settings:

- **Name:** `Check Session User`
- **Expression:** `DVF.F$SESSION_USER IN ('EABEL','AHUTTON')`

This rule uses the default factor `Session_User`. If this factor have been removed or modified, you can use the following rule expression instead:

```
UPPER(SYS_CONTEXT('USERENV','SESSION_USER')) IN ('EABEL','AHUTTON')
```

9. Click **OK**.

10. Click **Done**, then click **Finish**.

### 9.7.5 Step 4: Create the Database Vault Secure Application Role

The Database Vault secure application role will be set when the rule set conditions are satisfied.

1. In Oracle Database Vault, return to the Administration page.

2. Under Administration, select **Secure Application Roles**.

The Secure Application Roles page appears.

3. Click **Create**.

The Create Role page appears.

4. In the **Role** box, enter `ORDERS_MGMT` to name the role.

5. Under Rule Set, select **Can Modify Orders**.

6. Click **OK**.

At this stage, the Database Vault secure application role and its associated rule set are created, though the role does not yet have any privileges.

### 9.7.6 Step 5: Grant the SELECT Privilege to the Secure Application Role

The secure application role must be granted the `SELECT` privilege.

1. In SQL\*Plus, connect as user OE.

```
CONNECT OE -- Or, CONNECT OE@hrpdb
Enter password: password
```

2. Grant the `SELECT` privilege to the `ORDERS_MGMT` Database Vault Secure application role.

```
GRANT SELECT ON ORDERS TO ORDERS_MGMT;
```

### 9.7.7 Step 6: Test the Database Vault Secure Application Role

With all the components in place, you can test the Database Vault secure application role.

1. In SQL\*Plus, connect directly to the database as user `eabel`.

```
connect eabel@orcl
Enter password: password
```

Replace `orcl` with the name of your database instance.

2. Set the `ORDERS_MGMT` role.

```
EXEC DBMS_MACSEC_ROLES.SET_ROLE('ORDERS_MGMT');
```

Typically, you would embed this call in the application that the user logs in to.

3. Select from the `OE.ORDERS` table.

```
SELECT COUNT(*) FROM OE.ORDERS;
```

The following output should appear:

```
  COUNT(*)
-----
         105
```

Because user `eabel` is logging directly into the database from the correct IP address and is listed as a valid session user, she can select from the `OE.ORDERS`

table. If user `ahutton` logs in to SQL\*Plus in the same manner, she also can select from the `OE.ORDERS` table.

4. Reconnect as user `eabel` without specifying the database instance, and then try to select from the `OE.ORDERS` table again.

```
CONNECT eabel
Enter password: password

EXEC DBMS_MACSEC_ROLES.SET_ROLE('ORDERS_MGMT');
```

The following output should appear:

```
Error at line 1:
ORA-47305: Rule Set Violation on SET ROLE (Can Modfiy Orders)
...
```

Next:

```
SELECT COUNT(*) FROM OE.ORDERS;
```

The following output should appear:

```
ERROR at line 1:
ORA-00942: table or view does not exist
```

Even though user `eabel` is a valid user, she has violated the Check IP Address rule in the rule set, so she cannot enable the `ORDERS_MGMT` role. The only way for the IP address to be recognized is to connect by specifying the database instance, as user `eabel` did in Step 1. (For an explanation about how this works, see Step 9 (page 8-32) in [Step 3: Map the Domain Factor Identities to the Client\\_IP Factor](#) (page 8-31), in [Configuring Factors](#) (page 8-1).)

5. Connect as user `ldoran`.

```
CONNECT ldoran -- Or, CONNECT ldoran@hrpdb
Enter password: password
```

6. Enter the following statements:

```
EXEC DBMS_MACSEC_ROLES.SET_ROLE('ORDERS_MGMT');
SELECT COUNT(*) FROM OE.ORDERS;
```

Because user `ldoran` is not a valid user, she cannot enable the `ORDERS_MGMT` role. Therefore, she cannot select from the `OE.ORDERS` table.

## 9.7.8 Step 7: Remove the Components for This Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. Delete the `ORDERS_MGMT` secure application role: From the Secure Application Roles page, select the `ORDERS_MGMT` secure application role, and then click **Delete**, and then **Yes** in the Confirmation dialog box.

3. Select the Rule Sets page, select the Can Modify Orders rule set, and then click **Delete**.
4. In the Confirmation dialog box, select **Yes** to remove the rule set.
5. Select the Rules page, select the Check IP Address and Check Session User rules, and then select **Delete**. Select **Yes** in the Confirmation box.

Hold the **Control** key down to select multiple rules.

6. In SQL\*Plus, connect as the Database Vault Account Manager and drop the users.

For example:

```
CONNECT bea_dvacctmgr -- Or, CONNECT bea_dvacctmgr@hrpdb
Enter password: password

DROP USER eabel;
DROP USER ahutton;
DROP USER ldoran;
```

7. If unnecessary, lock and expire the OE user account.

```
ALTER USER OE ACCOUNT LOCK PASSWORD EXPIRE;
```

## 9.8 How Secure Application Roles Affect Performance

You can check system performance by Oracle Enterprise Manager Cloud Control.

Other tools that you can use are Automatic Workload Repository (AWR) and TKPROF.

---



---

**See Also:**

- *Oracle Database Performance Tuning Guide* to learn how to monitor database performance
  - *Oracle Database SQL Tuning Guide* to monitor the performance of individual SQL and PL/SQL statements
- 
- 

## 9.9 Secure Application Role Related Reports and Data Dictionary View

Oracle Database Vault provides reports and a data dictionary view that you can use to analyze Oracle Database Vault secure application roles.

[Table 9-1](#) (page 9-10) lists the Oracle Database Vault reports. See [Oracle Database Vault Reports](#) (page 27-1) for information about how to run these reports.

**Table 9-1 Reports Related to Secure Application Roles**

Report	Description
<a href="#">Secure Application Role Audit Report</a> (page 27-6)	Lists audit records generated by the Oracle Database Vault secure application role-enabling operation.  To generate this type of audit record, enable auditing for the rule set associated with the role.

**Table 9-1 (Cont.) Reports Related to Secure Application Roles**

<b>Report</b>	<b>Description</b>
<a href="#">Secure Application Configuration Issues Report</a> (page 27-5)	Lists secure application roles that have nonexistent database roles, or incomplete or disabled rule sets
<a href="#">Rule Set Configuration Issues Report</a> (page 27-3)	Lists rule sets that have no rules defined or enabled, which may affect the secure application roles that use them
<a href="#">Powerful Database Accounts and Roles Reports</a> (page 27-13)	Provides information about powerful database accounts and roles

You can use the `DBA_DV_ROLE` data dictionary view to find the Oracle Database Vault secure application roles used in privilege management. See [DBA\\_DV\\_ROLE View](#) (page 25-28) for more information.





---

## Configuring Oracle Database Vault Policies

You can use Oracle Database Vault policies to implement frequently used realm and command rule settings.

[What Are Database Vault Policies?](#) (page 10-1)

An Oracle Database Vault policy groups local realms and command rules into a named policy that you can enable or disable as necessary.

[Default Oracle Database Vault Policies](#) (page 10-3)

Oracle Database Vault provides two default policies that you can use to better secure user accounts and system privileges.

[Creating an Oracle Database Policy](#) (page 10-4)

To create an Oracle Database Vault policy, you create a container policy that specifies the realms and command rules that encompass the policy.

[Modifying an Oracle Database Vault Policy](#) (page 10-6)

You can use Enterprise Manager Cloud Control to modify an Oracle Database Vault policy.

[Deleting an Oracle Database Vault Policy](#) (page 10-6)

You can use Enterprise Manager Cloud Control to delete Oracle Database Vault policies.

[Related Data Dictionary Views](#) (page 10-6)

Oracle Database Vault provides data dictionary views that are useful for analyzing Database Vault policies.

### 10.1 What Are Database Vault Policies?

An Oracle Database Vault policy groups local realms and command rules into a named policy that you can enable or disable as necessary.

[About Oracle Database Vault Policies](#) (page 10-1)

Oracle Database Vault policies can group realm and command rule definitions into one policy, which then can be collectively enabled or disabled.

[Oracle Database Vault Policies in a Multitenant Environment](#) (page 10-3)

Oracle Database Vault policies are only local to the pluggable database (PDB) in which they were created.

#### 10.1.1 About Oracle Database Vault Policies

Oracle Database Vault policies can group realm and command rule definitions into one policy, which then can be collectively enabled or disabled.

Database Vault policies enable you to delegate limited realm administration privileges to database users without giving them the powerful privileges that the DVADM and DVOWNER roles provide. Oracle Database Vault provides default policies.

For example, suppose you have a set of Oracle Database Vault objects that are related to a particular application, such as a realm and several command rules. You can use a Database Vault policy to group these objects into one policy. You then can designate a policy administrator to manage adding users to a realm for this application and for enabling or disabling the policy. If there is only one primary application, then it can be used for manageability where a user can enable, disable, or simulate (use simulation mode) all related objects with one command rather than issuing a command for each included Database Vault object.

How the enablement of the individual realms and command rules works depends on how you set the policy state of the policy, as follows:

- Full enabled mode (`DBMS_MACADM.G_ENABLED`) sets the policy to take precedence over the individual enablement settings of the associated realms and command rules. For example, if the associated objects of a policy are individually disabled, then they will be enabled if the policy is enabled. (Conversely, you can set `DBMS_MACADM.G_PARTIAL` to allow the embedded security objects to set their own enabled, disabled, or simulation mode.)
- Partial enabled mode (`DBMS_MACADM.G_PARTIAL`) enables the associated realms and command rules to have different status settings (`ENABLED`, `DISABLED`, and `SIMULATION`). The other policy status choices force all associated controls to the same status dictated by the policy. Setting the policy status to partial allows each realm and command rule to change status as required.
- Simulation mode (`DBMS_MACADM.G_SIMULATION`) enables the policy but writes violations to realms or command rules to a designated log table with information about the type of violation, such as a user name or the SQL statement that was used. Simulation forces every security object in the policy to be in simulation mode.
- Disabled mode (`DBMS_MACADM.G_DISABLED`) disables the policy after you create it.

In general, to create a Database Vault policy, you perform the following steps:

1. Create the necessary realms and command rules to use in the policy.
2. Create the Database Vault policy.  
You can use the `DBMS_MACADM.CREATE_POLICY` procedure to create the policy.
3. Add one or more realms to the policy.  
You can use the `DBMS_MACADM.ADD_REALM_TO_POLICY` procedure to add realms to the policy.
4. Add one or more command rules to the policy.  
You can use the `DBMS_MACADM.ADD_CMD_TO_POLICY` procedure to add command rules to the policy.
5. Add one or more database users as owners of the policy.  
You can use the `DBMS_MACADM.ADD_OWNER_TO_POLICY` procedure to add users to the policy. Afterward, grant this user the `DV_POLICY_OWNER` role. This user will be able to perform a limited set of tasks: changing the policy state, adding or

removing authorization from a realm, and having the `SELECT` privilege for a set of the `DVSYS.POLICY_OWNER*` data dictionary views. By default, the `DVOWNER` user owns the policy.

After the policy is created, it can be used right away.

This section explains how to configure policies by using the Oracle Database Vault Administrator pages in Oracle Enterprise Manager Cloud Control. To configure policies by using the PL/SQL interfaces and packages provided by Oracle Database Vault, you must use the `DBMS_MACADM` PL/SQL package.

#### Related Topics:

[Default Oracle Database Vault Policies](#) (page 10-3)

Oracle Database Vault provides two default policies that you can use to better secure user accounts and system privileges.

[Oracle Database Vault Policy APIs](#) (page 23-1)

You can use the `DBMS_MACADM` PL/SQL package to manage Oracle Database Vault policies.

[DV\\_POLICY\\_OWNER Database Vault Owner Role](#) (page 14-22)

The `DV_POLICY_OWNER` role enables database users to manage to a limited degree Oracle Database Vault policies.

## 10.1.2 Oracle Database Vault Policies in a Multitenant Environment

Oracle Database Vault policies are only local to the pluggable database (PDB) in which they were created.

That is, if you created the policy in a PDB, then only local realms and command rules can be added to it. You cannot create Database Vault policies that can have common realms or common command rules.

## 10.2 Default Oracle Database Vault Policies

Oracle Database Vault provides two default policies that you can use to better secure user accounts and system privileges.

You can use the default policies in your own security configurations. If you do not need them, then you can remove them because they are not needed for internal use by Oracle Database Vault.

The default policies are as follows:

- Oracle Account Management Controls enforces controls over user-related operations within Oracle Database Vault. It is used to prevent ad hoc user account creation, user deletions, and other user account-related operations by unauthorized privileged users. It includes the Database Vault Account Management realm and user account management command rules for SQL statements such as `CREATE USER`.
- Oracle System Protection Controls enforces controls on important database schemas, privileges, and roles that are associated with the default Oracle Database environment. It includes the realms such as Oracle Default Schema Protection Realm and command rules for the system management SQL statement `ALTER SYSTEM`.

**Related Topics:**

[DBA\\_DV\\_POLICY\\_OBJECT View](#) (page 25-21)

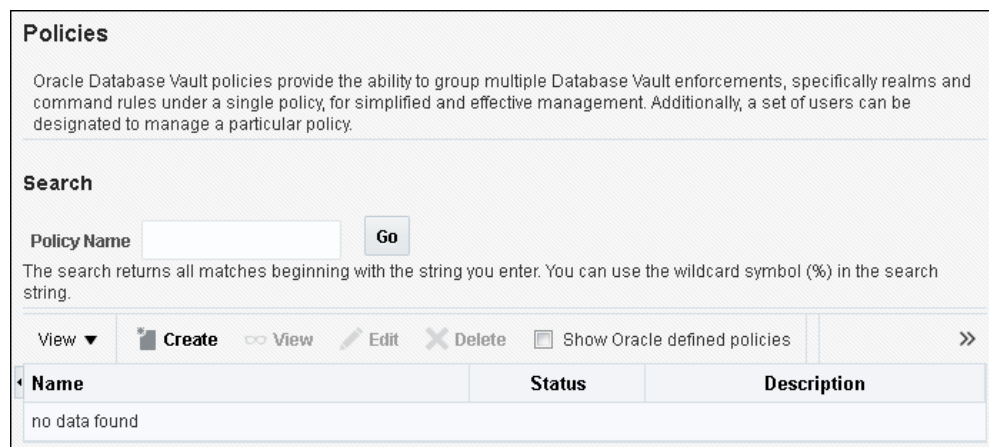
The DBA\_DV\_POLICY\_OBJECT data dictionary view lists information about the objects that are protected by Oracle Database Vault policies in the current database instance.

## 10.3 Creating an Oracle Database Policy

To create an Oracle Database Vault policy, you create a container policy that specifies the realms and command rules that encompass the policy.

You can enable the policy during creation time, or enable it later on.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. Create the realms and command rules that you want to associate with the policy, using [Creating a Realm](#) (page 5-8) and [Creating a Rule Set](#) (page 6-5).
3. In the Administration page, under Database Vault Components, click **Policies** to display the Policies page.



4. In the Policies page, click **Create** to display the Create Policy page.

**Create Policy: General** Back Step 1 of 2 Next Cancel

Define a Database Vault policy to group multiple Database Vault enforcements, specifically realms and command rules for effective management.

**Name**

**Description**

Status: Enabled

**Realms**

Specify existing realm to be added to Database Vault policy. Note that a realm can belong to at most one Database Vault policy.

View

Realm Name	Status	Mandatory Realm
no data found		

Columns Hidden 1

**Command Rules**

Specify existing command rule to be added to Database Vault policy. Note that a command rule can belong to at most one Database Vault policy.

View

Command	Object Owner	Object Name	Rule Set Name
no data found			

Columns Hidden 1

**Owners**

Specify existing database users to be added as Database Vault policy owners.

View

Username	Account Status
no data found	

5. In the Create Policy page, under General, enter the following settings:
  - **Name:** Enter a policy name, up to 128 characters.
  - **Description:** Enter a description of the policy, up to 4000 characters.
  - **Status:** Select from the following:
    - **Enabled** enables the policy after you create it.
    - **Disabled** disables the policy after you create it.
    - **Simulation** sets the policy to simulation mode. In simulation mode, any violations to realms or command rules used in the policy are logged in a designated log table with sufficient information to describe the error, such as the user name or SQL statement used.
    - **Partial** enables the enforcement state of realms or command rules associated with the policy to be changed individually.
6. Under Realms, click **Add** to select a realm to add to the policy. Then click **OK**.
7. Under Command Rules, click **Add** to select a command rule to add to the policy. Then click **OK**.
8. Under Owners, click **Add** to add an owner to the policy. Then click **OK**.
9. Click **Next**.
10. In the Review page, click **Finish**.
11. So that the Database Vault policy owner can query policy related views and execute the allowed procedures, grant this user the DV\_POLICY\_OWNER role.

For example:

```
GRANT DV_POLICY_OWNER TO psmith;
```

## 10.4 Modifying an Oracle Database Vault Policy

You can use Enterprise Manager Cloud Control to modify an Oracle Database Vault policy.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Policies**.
3. Select the row for the policy that you want to change.
4. Click **Edit**.
5. In the Edit Policy page, modify the settings as necessary.
6. Click **Next**, and then click **Finish**.

## 10.5 Deleting an Oracle Database Vault Policy

You can use Enterprise Manager Cloud Control to delete Oracle Database Vault policies.

When you delete an Oracle Database Vault policy, the underlying realms and command rules are preserved, and they retain their individual enablement status.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Administration page, under Database Vault Components, click **Policies**.
3. Select the row for the policy that you want to delete, click **Delete**, and then click **Yes** in the confirmation dialog box.

## 10.6 Related Data Dictionary Views

Oracle Database Vault provides data dictionary views that are useful for analyzing Database Vault policies.

[Table 10-1](#) (page 10-6) lists data dictionary views that provide information about existing Oracle Database Vault policies.

**Table 10-1 Data Dictionary Views Used for Oracle Database Vault Policies**

Data Dictionary View	Description
<a href="#">DBA_DV_POLICY View</a> (page 25-19)	Lists the Database Vault policies, a description, and their state
<a href="#">DBA_DV_POLICY_OBJECT View</a> (page 25-21)	Provides detailed information about the policies, such as the associated realms and command rules

**Table 10-1 (Cont.) Data Dictionary Views Used for Oracle Database Vault Policies**

Data Dictionary View	Description
<a href="#">DBA_DV_POLICY_OWNER View</a> (page 25-22)	Lists the owners of Database Vault policies
<a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25)	Enables users who have been granted the DV_POLICY_OWNER role to find information about the authorization that was granted to realms that have been associated with Database Vault policies, such as the realm name, grantee, and associated rule set.
<a href="#">DVSYS.POLICY_OWNER_COMMAND_RULE View</a> (page 25-48)	Enables users who have been granted the DV_POLICY_OWNER role to find information about the command rules that have been associated with Database Vault policies, such as the command rule name.
<a href="#">DVSYS.POLICY_OWNER_POLICY View</a> (page 25-49)	Enables users who have been granted the DV_POLICY_OWNER role to find information such as the names, descriptions, and states of existing policies in the current database instance, including policies created by other policy owners
<a href="#">DVSYS.POLICY_OWNER_POLICY View</a> (page 25-49)	Enables users who have been granted the DV_POLICY_OWNER role to find information such as the names, descriptions, and states of existing policies in the current database instance, including policies created by other policy owners
<a href="#">DVSYS.POLICY_OWNER_REALM View</a> (page 25-49)	Enables users who have been granted the DV_POLICY_OWNER role to find information about the realms that have been associated with Database Vault policies, such as the realm name, audit options, or type
<a href="#">DVSYS.POLICY_OWNER_REALM_OBJECT View</a> (page 25-52)	Enables users who have been granted the DV_POLICY_OWNER role to find information about the objects that have been added to realms that are associated with Database Vault policies, such as the realm name, grantee, and associated rule set
<a href="#">DVSYS.POLICY_OWNER_RULE View</a> (page 25-53)	Enables users who have been granted the DV_POLICY_OWNER role to find information about the rules that have been associated with rule sets in Database Vault policies, such as the rule name and its expression

**Table 10-1 (Cont.) Data Dictionary Views Used for Oracle Database Vault Policies**

Data Dictionary View	Description
<a href="#">DVSYS.POLICY_OWNER_RULE_SET View</a> (page 25-54)	Enables users who have been granted the DV_POLICY_OWNER role to find information about the rule sets that have been associated with Database Vault policies, such as the rule set name, its handler information, and whether it is enabled
<a href="#">DVSYS.POLICY_OWNER_RULE_SET_RULE View</a> (page 25-56)	Enables users who have been granted the DV_POLICY_OWNER role to find information about the rule sets that contain rules used in Database Vault policies, such as the rule set name and whether it is enabled



---

# Using Simulation Mode for Logging Realm and Command Rule Activities

Simulation mode writes the activities performed on realms and command rules to a log file, which is accessible through a data dictionary view.

[About Simulation Mode](#) (page 11-1)

Simulation mode enables you to capture a record of errors during the development phase of a realm or command rule.

[Simulation Mode Use Cases](#) (page 11-2)

Simulation mode is useful for testing a development configuration of new realms and command rules.

[Tutorial: Tracking Violations to a Realm Using Simulation Mode](#) (page 11-3)

This tutorial shows how to create a realm that uses simulation mode and then test violations to the realm.

## 11.1 About Simulation Mode

Simulation mode enables you to capture a record of errors during the development phase of a realm or command rule.

Simulation mode stores the errors that are captured in one location for easy analysis. To use simulation mode, when you create or update a realm or command rule, instead of enabling or disabling the realm or command rule, you can set it to simulation mode. The realm or command rule is still enabled, but because violations are not blocked and are instead recorded to the simulation log file, you can test it for any potential errors before you enable it for a production environment.

For example, the following creation statement for a realm enables simulation mode:

```
BEGIN
  DBMS_MACADM.CREATE_REALM(
    realm_name    => 'HR Apps',
    description   => 'Realm to protect the HR realm',
    enabled       => DBMS_MACUTL.G_SIMULATION,
    audit_options => DBMS_MACUTL.G_REALM_AUDIT_FAIL,
    realm_type    => 1,
    realm_scope   => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/
```

At this stage, SQL statements that violate realms or command rules are still able to execute, but these activities are recorded to the `DBA_DV_SIMULATION_LOG` data dictionary view. For example, the following query finds violations against the HR Apps realm:

```
SELECT USERNAME, COMMAND, SQLTEXT, VIOLATION_TYPE FROM DBA_DV_SIMULATION_LOG WHERE
REALM_NAME = 'HR APPS';
```

USERNAME	COMMAND	SQLTEXT	VIOLATION_TYPE
DGRANT	SELECT	SELECT SALARY FROM HR.EMPLOYEES;	Realm Violation

After you have completed testing the realm or command rule, a user who has been granted the DV\_ADMIN or DV\_OWNER role can clear the DBA\_DV\_SIMULATION\_LOG data dictionary view by deleting the contents of the underlying table of this view, DVSYS.SIMULATION\_LOG\$.

For example:

```
DELETE FROM DVSYS.SIMULATION_LOG$;
```

Or:

```
DELETE FROM DVSYS.SIMULATION_LOG$ WHERE COMMAND = 'SELECT';
```

## 11.2 Simulation Mode Use Cases

Simulation mode is useful for testing a development configuration of new realms and command rules.

Use cases are as follows:

- Application certification
 

When you are certifying applications, you can use simulation mode as follows in an application test environment:

  1. Put all schemas for the application into mandatory realms with simulation mode enabled.
  2. Run a full regression test.
  3. Analyze the simulation mode log by querying the DBA\_DV\_SIMULATION\_LOG data dictionary view to find who can access these schemas.
  4. Update the realms with new authorizations, and then enable the realms (that is, not using simulation mode).
  5. Re-run the regression test.
- Introduction of a new command rule
 

You can use simulation mode on a production database that has Oracle Database Vault enabled.

  1. Put the new command rule into production in simulation mode for however many weeks that are necessary.
  2. Analyze the simulation mode log by querying DBA\_DV\_SIMULATION\_LOG to determine if the command rule is working correctly.
  3. Make changes to the command rule as necessary.
  4. Enable the command rule.
- Putting a new realm into a production database in simulation mode.

This method can help to find the system context information needed to set the trusted path rules in rule sets and find authorized users for realms.

1. Create the new realm in mandatory mode and add the protected objects
2. Do not add any authorized users.
3. Run applications and development operations from the normal IP addresses that will be used.
4. Check the simulation log file for both authorized users and system context information that you can use to create trusted paths.
5. Create the trusted paths, and then add the authorized users.
6. Clear the simulation log and run the application and development operation tasks again.
7. After a period of time, review the simulation log. If all the controls were updated correctly, then the simulation log is empty. Log entries in the simulation mode indicate additional changes that you need to make to the realm and rule sets or the log entries may indicate a malicious use.

## 11.3 Tutorial: Tracking Violations to a Realm Using Simulation Mode

This tutorial shows how to create a realm that uses simulation mode and then test violations to the realm.

### [About This Tutorial](#) (page 11-4)

In this tutorial, you will create a realm around the `HR.EMPLOYEES` schema and test violations against it.

### [Step 1: Create Users for This Tutorial](#) (page 11-4)

You must create three users for this tutorial. .

### [Step 2: Create a Realm and an Oracle Database Vault Policy](#) (page 11-5)

Next, you create a realm around the `HR.EMPLOYEES` table, and then add this realm to an Oracle Database Vault policy.

### [Step 3: Test the Realm and Policy](#) (page 11-6)

User `tjones_dba` will commit a violation on the realm to test the realm and policy.

### [Step 4: Query the DBA\\_DV\\_SIMULATION\\_LOG View for Violations](#) (page 11-7)

Now you can check the simulation mode log the violations that user `tjones_dba` committed.

### [Step 5: Enable and Re-test the Realm](#) (page 11-7)

Now that you have captured the violations, user `psmith` can update the `HR.EMPLOYEES_pol` policy.

### [Step 6: Remove the Components for This Tutorial](#) (page 11-8)

You can remove the components that you created for this tutorial if you no longer need them.

### 11.3.1 About This Tutorial

In this tutorial, you will create a realm around the `HR.EMPLOYEES` schema and test violations against it.

The `HR.EMPLOYEES` schema contains confidential data such as employee salaries. To test the realm, an administrator, `tjones_dba`, will look up and modify the salary of another employee, `smavris`. The Database Vault administrator, `leo_dvowner`, will use simulation mode to track the violations to the `HR.EMPLOYEES` schema. To accomplish this, user `leo_dvowner` will create a Database Vault policy, which a delegated administrator, user `psmith`, will own. User `psmith` will then be able to make limited changes to the policy without needing the `DV_OWNER` or `DV_ADMIN` role.

### 11.3.2 Step 1: Create Users for This Tutorial

You must create three users for this tutorial. .

The users are: `psmith`, who is the Database Vault policy owner; `tjones_dba`, who commits violations on the `HR.EMPLOYEES` table; and `smavris`, whose salary is the recipient of `tjones_dba`'s violations.

1. Log into the database instance as a user who has been granted the `DV_ACCTMGR` role.

For example:

```
sqlplus bea_dvacctmgr
Enter password: password
```

In a multitenant environment, you must log in to the appropriate pluggable database (PDB). For example:

```
CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

To find the available PDBs, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

2. Create the following users and grant them the `CREATE SESSION` privilege.

```
GRANT CREATE SESSION TO psmith IDENTIFIED BY password;
GRANT CREATE SESSION TO tjones_dba IDENTIFIED BY password;
GRANT CREATE SESSION TO smavris IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace `password` with a password that is secure.

3. Connect as a user who has been granted the `DV_OWNER` role.

For example:

```
CONNECT leo_dvowner -- Or, leo_dvowner@hrpdb
Enter password: password
```

4. Grant user `psmith` the `DV_POLICY_OWNER` role, which enables `psmith` to manage Database Vault policies.

```
GRANT DV_POLICY_OWNER TO psmith;
```

5. Connect as user `SYS` with the `SYSDBA` administrative privilege.

```
CONNECT SYS AS SYSDBA -- Or, CONNECT SYS@hrpdb AS SYSDBA
Enter password: password
```

**6. Grant the DBA role to user `tjones_dba`**

```
GRANT DBA TO tjones_dba;
```

**7. Connect as the HR schema owner.**

```
CONNECT HR -- Or, HR@hrpdb
Enter password: password
```

**8. Grant the SELECT privilege on the `HR.EMPLOYEES` table to user `smavris`**

```
GRANT SELECT ON HR.EMPLOYEES TO smavris;
```

At this stage, the users have all been created and granted the appropriate privileges.

### 11.3.3 Step 2: Create a Realm and an Oracle Database Vault Policy

Next, you create a realm around the `HR.EMPLOYEES` table, and then add this realm to an Oracle Database Vault policy.

**1. Connect as a user who has been granted the `DV_OWNER` role.**

For example:

```
CONNECT leo_dvowner -- Or, leo_dvowner@hrpdb
Enter password: password
```

**2. Create the realm around `HR.EMPLOYEES` table as follows.**

These procedures create the `HR.EMPLOYEES_realm` realm, add the `HR.EMPLOYEES` table to this realm, authenticate HR as an owner, and authenticate user `psmith` as a participant.

```
BEGIN
  DBMS_MACADM.CREATE_REALM(
    realm_name    => 'HR.EMPLOYEES_realm',
    description   => 'Realm to protect HR.EMPLOYEES',
    enabled       => DBMS_MACUTL.G_SIMULATION,
    audit_options => DBMS_MACUTL.G_REALM_AUDIT_FAIL,
    realm_type    => 0);
END;
/

BEGIN
  DBMS_MACADM.ADD_OBJECT_TO_REALM(
    realm_name    => 'HR.EMPLOYEES_realm',
    object_owner  => 'HR',
    object_name   => 'EMPLOYEES',
    object_type   => 'TABLE');
END;
/
```

**3. Create the `HR.EMPLOYEES_pol` Database Vault policy and set it to be in simulation mode.**

These procedures create the `HR.EMPLOYEES_pol` policy, add the realm that was just created to the policy, and then add user `psmith` as the owner of the policy.

```

BEGIN
  DBMS_MACADM.CREATE_POLICY(
    policy_name => 'HR.EMPLOYEES_pol',
    description => 'Policy to protect HR.EMPLOYEES',
    policy_state => DBMS_MACADM.G_SIMULATION);
END;
/

BEGIN
  DBMS_MACADM.ADD_REALM_TO_POLICY(
    policy_name => 'HR.EMPLOYEES_pol',
    realm_name => 'HR.EMPLOYEES_realm');
END;
/

BEGIN
  DBMS_MACADM.ADD_OWNER_TO_POLICY(
    policy_name => 'HR.EMPLOYEES_pol',
    owner_name => 'PSMITH');
END;
/

```

At this point, the realm and policy are ready to be tested.

### 11.3.4 Step 3: Test the Realm and Policy

User `tjones_dba` will commit a violation on the realm to test the realm and policy.

1. Connect as user `tjones_dba`.

```

CONNECT tjones_dba -- Or, tjones_dba@hrpdb
Enter password: password

```

2. Query the `HR.EMPLOYEES` table for the salary of `smavris`.

```

SELECT SALARY FROM HR.EMPLOYEES WHERE EMAIL = 'SMAVRIS';

```

Output similar to the following should appear:

```

      SALARY
-----
          6500

```

3. Cut `smavris`'s salary in half.

```

UPDATE HR.EMPLOYEES
SET SALARY = SALARY / 2
WHERE EMAIL = 'SMAVRIS';

```

1 row updated.

4. Connect as user `smavris`.

```

CONNECT smavris -- Or, smavris@hrpdb

```

5. Query the salary of `smavris`.

```

SELECT SALARY FROM HR.EMPLOYEES WHERE EMAIL = 'SMAVRIS';

```

Output similar to the following should appear:

```

SALARY
-----
      3250

```

At this point, `tjones_dba`'s violations have been recorded in the `DBA_DV_SIMULATION_LOG` data dictionary view.

### 11.3.5 Step 4: Query the `DBA_DV_SIMULATION_LOG` View for Violations

Now you can check the simulation mode log the violations that user `tjones_dba` committed.

1. Connect as a user who has been granted the `DV_OWNER` role.

For example:

```

CONNECT leo_dvowner -- Or, leo_dvowner@hrpdb
Enter password: password

```

2. Query the `DBA_DV_SIMULATION_LOG` data dictionary view.

```

SELECT USERNAME, SQLTEXT, VIOLATION_TYPE FROM DBA_DV_SIMULATION_LOG WHERE
REALM_NAME = 'HR.EMPLOYEES_REALM';

```

Output similar to the following should appear:

```

USERNAME
-----
SQLTEXT
-----
VIOLATION_TYPE
-----
TJONES_DBA
SELECT SALARY FROM HR.EMPLOYEES WHERE EMAIL = 'SMAVRIS'
Realm Violation

TJONES_DBA
UPDATE HR.EMPLOYEES SET SALARY = SALARY / 2 WHERE EMAIL = 'SMAVRIS'
Realm Violation

USERNAME
-----
SQLTEXT
-----
VIOLATION_TYPE
-----

TJONES_DBA
UPDATE HR.EMPLOYEES SET SALARY = SALARY / 2 WHERE EMAIL = 'SMAVRIS'
Realm Violation

```

The output indicates that user `tjones_dba` has committed two offences: first, he looked at another employee's salary, and not only that, he cut it in half. The violation type is a realm violation. The query by `smavris` was not captured because she legitimately can look at her salary.

### 11.3.6 Step 5: Enable and Re-test the Realm

Now that you have captured the violations, user `psmith` can update the `HR.EMPLOYEES_pol` policy.

This is so that the `HR.EMPLOYEES_realm` realm can be enabled. Then you can test the violations again.

1. Connect as user `psmith`.

```
CONNECT psmith -- Or, psmith@hrpdb
Enter password: password
```

2. Update the policy so that it is enabled.

```
BEGIN
  DBMS_MACADM.UPDATE_POLICY_STATE(
    policy_name => 'HR.EMPLOYEES_pol',
    policy_state => 1);
END;
/
```

3. Connect as user `tjones_dba`.

```
CONNECT tjones_dba --Or, tjones_dba@hrpdb
```

4. Try lowering `smavris`'s salary to new depths.

```
UPDATE HR.EMPLOYEES
SET SALARY = SALARY / 2
WHERE EMAIL = 'SMAVRIS';
```

Output similar to the following should appear:

```
ERROR at line 1:
ORA-01031: insufficient privileges
```

The policy, now enabled, enables the realm to protect the `HR.EMPLOYEES` table. `smavris`'s salary can shrink no more.

### 11.3.7 Step 6: Remove the Components for This Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. Connect as a user who has been granted the `DV_OWNER` role.

For example:

```
CONNECT leo_dvowner -- Or, leo_dvowner@hrpdb
Enter password: password
```

2. Remove the `HR.EMPLOYEES_pol` Database Vault policy.

```
EXEC DBMS_MACADM.DROP_POLICY('HR.EMPLOYEES_pol');
```

You first must remove the policy before you can drop its contents.

3. Remove the `HR.EMPLOYEES_realm` realm.

```
EXEC DBMS_MACADM.DELETE_REALM('HR.EMPLOYEES_realm');
```

4. Remove the simulation mode log data that was accumulated.

Because the simulation mode log only captured information about user `tjones_dba`, you can remove only the rows that relate to this user.



```
DELETE FROM DVSYS.SIMULATION_LOG$ WHERE USERNAME = 'TJONES_DBA';
```

**5. Connect as user HR.**

```
CONNECT HR -- Or, CONNECT HR@hrpdb  
Enter password: password
```

**6. Revert smavris's salary back to its pre-violated state.**

```
UPDATE HR.EMPLOYEES  
SET SALARY = 6500  
WHERE EMAIL = 'SMAVRIS';
```

**7. Connect as a user who has been granted the DV\_ACCTMGR role.**

For example:

```
CONNECT bea_dvacctmgr -- Or, bea_dvacctmgr@hrpdb  
Enter password: password
```

**8. Remove the users psmith, smavris, and tjones\_dba.**

```
DROP USER psmith;  
DROP USER smavris;  
DROP USER tjones_dba;
```



---

## Integrating Oracle Database Vault with Other Oracle Products

You can integrate Oracle Database Vault with other Oracle products, such as Oracle Enterprise User Security.

[Integrating Oracle Database Vault with Enterprise User Security](#) (page 12-1)

You can integrate Oracle Database Vault with Oracle Enterprise User Security.

[Configuring Oracle Database Vault Accounts as Enterprise User Accounts](#) (page 12-2)

You can configure existing Oracle Database Vault user accounts as enterprise user accounts.

[Integration of Oracle Database Vault with Transparent Data Encryption](#) (page 12-4)

Transparent Data Encryption complements Oracle Database Vault in that it provides data protection when the data leaves the secure perimeter of the database.

[Attaching Factors to an Oracle Virtual Private Database](#) (page 12-5)

You can attach factors to an Oracle Virtual Private Database.

[Integrating Oracle Database Vault with Oracle Label Security](#) (page 12-5)

You can integrate Oracle Database Vault with Oracle Label Security, and check the integration with reports and data dictionary views.

[Integrating Oracle Database Vault with Oracle Data Guard](#) (page 12-15)

An Oracle Database Vault-Oracle Data Guard integration requires first, the primary database configuration, then the standby database configuration.

[Registering Oracle Internet Directory Using Oracle Database Configuration Assistant](#) (page 12-17)

You can use Oracle Internet Directory in an Oracle Database Vault-enabled database.

### 12.1 Integrating Oracle Database Vault with Enterprise User Security

You can integrate Oracle Database Vault with Oracle Enterprise User Security.

[About Integrating Oracle Database Vault with Enterprise User Security](#) (page 12-2)

Enterprise User Security centrally manages database users and authorizations in one place.

### [Configuring an Enterprise User Authorization](#) (page 12-2)

To configure an Enterprise User authorization, you must create an Oracle Database Vault rule set to control the user access.

## 12.1.1 About Integrating Oracle Database Vault with Enterprise User Security

Enterprise User Security centrally manages database users and authorizations in one place.

It is combined with Oracle Identity Management and is available in Oracle Database Enterprise Edition.

In general, to integrate Oracle Database Vault with Oracle Enterprise User Security, you configure the appropriate realms to protect the data that you want to protect in the database.

After you define the Oracle Database Vault realms as needed, you can create a rule set for the Enterprise users to allow or disallow their access.

---

---

**See Also:**

*Oracle Database Enterprise User Security Administrator's Guide* for more information about Enterprise User Security

---

---

## 12.1.2 Configuring an Enterprise User Authorization

To configure an Enterprise User authorization, you must create an Oracle Database Vault rule set to control the user access.

1. Create a rule to allow or disallow user access.

Follow the instructions in [Creating a Rule to Add to a Rule Set](#) (page 6-8) to create a new rule. In the Create Rule page, enter the following PL/SQL in the Rule Expression field:

```
SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY') = 'user_domain_name'
```

Replace *user\_domain\_name* with the domain, for example:

```
SYS_CONTEXT('USERENV','AUTHENTICATED_IDENTITY') = 'myserver.us.example.com'
```

2. Add this rule to a new rule set.

[Creating a Rule Set](#) (page 6-5) explains how to create a new rule set, including how to add an existing rule to it.

3. Add this rule set to the realm authorization for the data that you want to protect.

[About Realm Authorization](#) (page 5-13) explains how to create realm authorizations. In the Authorization Rule Set list, select the rule set that you created in Step 2 (page 12-2). Afterward, the realm authorization applies to all users.

## 12.2 Configuring Oracle Database Vault Accounts as Enterprise User Accounts

You can configure existing Oracle Database Vault user accounts as enterprise user accounts.

1. Log into the database instance as a user who has been granted the `CREATE ROLE` system privilege.

For example:

```
sqlplus system
Enter password: password
```

2. In a multitenant environment, connect to the appropriate pluggable database (PDB).

For example:

```
CONNECT SYSTEM@hrpdb
Enter password: password
```

To find the available PDBs, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

3. Create a global role for the `DV_OWNER` role and a global role for the `DV_ACCTMGR` role.

For example:

```
CREATE ROLE g_dv_owner IDENTIFIED GLOBALLY;
CREATE ROLE g_dv_acctmgr IDENTIFIED GLOBALLY;
```

4. Connect as a user who has been granted the `DV_OWNER` role.

For example:

```
CONNECT dbv_owner -- Or, CONNECT dbv_owner@hrpdb
Enter password: password
```

5. Grant the `DV_OWNER` role to the global `DV_OWNER` role.

```
GRANT DV_OWNER TO g_dv_owner;
```

6. Connect as a user who has been granted the `DV_ACCTMGR` role.

For example:

```
CONNECT dbv_acctmgr -- Or, CONNECT dbv_acctmgr@hrpdb
Enter password: password
```

7. Grant the `DV_ACCTMGR` role to the global `DV_ACCTMGR` role.

```
GRANT DV_ACCTMGR TO g_dv_acctmgr;
```

8. Connect as user `SYS` with the `SYSDBA` administrative privilege.

```
CONNECT SYS AS SYSDBA -- Or, CONNECT SYS@hrpdb AS SYSDBA
Enter password: password
```

9. Temporarily grant the `DV_ACCTMGR` user who will import the Database Vault users into OID the `CREATE TABLE` privilege and the `SELECT_CATALOG_ROLE` role.

```
GRANT CREATE TABLE, SELECT_CATALOG_ROLE TO dbv_acctmgr;
```

10. From the command line, run the User Migration Utility (UMU) to import the Database Vault accounts into Oracle Internet Directory (OID).

The following example imports the Database Vault accounts `leo_dvowner` and `bea_dvacctmgr` into OID. The `DV_ACCTMGR` user is specified for the `DBADMIN` setting.

```
$ORACLE_HOME/rdbms/bin/umu PHASE=ONE
DBADMIN=dbv_acctmgr:password
ENTADMIN=cn=jane_ent_admin,dc=example,dc=com:password
USERS= LIST
DBLOCATION=example.com:7777:orcl
DIRLOCATION=example.com:636
USERSLIST=leo_dvowner:bea_dvacctmgr
MAPSCHEMA=PRIVATE
CONTEXT=CONTEXT="c=Users, c=us"
KREALM=EXAMPLE.COM

$ORACLE_HOME/rdbms/bin/umu PHASE=TWO
DBADMIN=dbv_acctmgr:password
ENTADMIN=cn=jane_ent_admin,dc=example,dc=com:password
DBLOCATION=example.com:7777:orcl
DIRLOCATION=example.com:636
```

By default, errors are written to the `$ORACLE_HOME/network/log/umu.log` file.

- From the Oracle Internet Directory Self Service Console (`http://hostname:port/oiddas/`), grant the global `DV_OWNER` and `DV_ACCTMGR` roles (for example, `g_dv_owner` and `g_dv_acctmgr`) to the enterprise user Database Vault accounts.

See the example of creating enterprise users in *Oracle Database Enterprise User Security Administrator's Guide* for a demonstration of creating an enterprise role from a global role and then granting this role to a user.

- From SQL\*Plus, as user `SYS` with the `SYSDBA` administrative privilege, revoke the `CREATE TABLE` and `SELECT_CATALOG_ROLE` role from the `DV_ACCTMGR` user.

```
REVOKE CREATE TABLE, SELECT_CATALOG_ROLE FROM dbv_acctmgr;
```

---



---

**See Also:**

*Oracle Database Enterprise User Security Administrator's Guide* for detailed information about the User Migration Utility

---



---

## 12.3 Integration of Oracle Database Vault with Transparent Data Encryption

Transparent Data Encryption complements Oracle Database Vault in that it provides data protection when the data leaves the secure perimeter of the database.

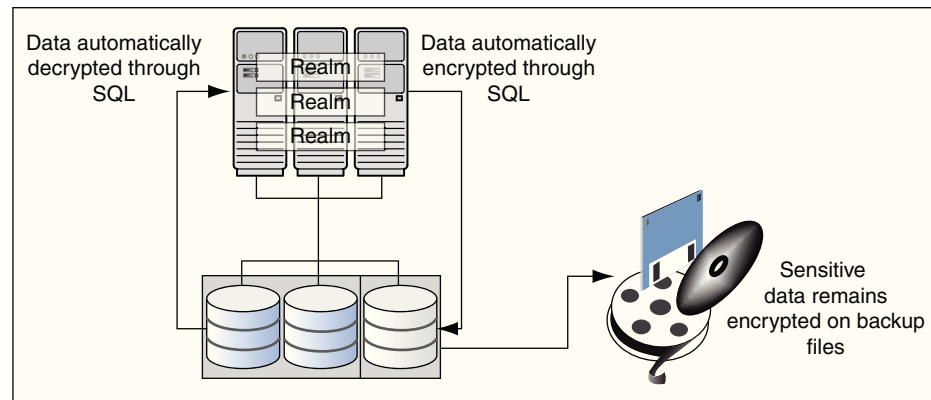
With Transparent Data Encryption, a database administrator or database security administrator can simply encrypt columns with sensitive content in application tables, or encrypt entire application tablespaces, without any modification to the application.

If a user passes the authentication and authorization checks, Transparent Data Encryption automatically encrypts and decrypts information for the user. This way, you can implement encryption without having to change your applications.

Once you have granted the Transparent Data Encryption user the appropriate privileges, then Transparent Data Encryption can be managed as usual and be used complimentary to Database Vault.

[Figure 12-1](#) (page 12-5) shows how Oracle Database Vault realms handle encrypted data.

**Figure 12-1 Encrypted Data and Oracle Database Vault**




---

**See Also:** *Oracle Database Advanced Security Guide* for detailed information about Transparent Data Encryption

---

## 12.4 Attaching Factors to an Oracle Virtual Private Database

You can attach factors to an Oracle Virtual Private Database.

1. Define a Virtual Private Database policy predicate that is a PL/SQL function or expression.
2. For each function or expression, use the `DVF.F$` PL/SQL function that is created for each factor.

---

**See Also:**

*Oracle Database Security Guide* Oracle Database Security Guide for more information about Oracle Virtual Private Database

---

## 12.5 Integrating Oracle Database Vault with Oracle Label Security

You can integrate Oracle Database Vault with Oracle Label Security, and check the integration with reports and data dictionary views.

[How Oracle Database Vault Is Integrated with Oracle Label Security](#)  
(page 12-6)

An Oracle Database Vault-Oracle Label Security integration enables you to assign an OLS label to a Database Vault factor identity.

[Requirements for Using Oracle Database Vault with Oracle Label Security](#)  
(page 12-7)

You must fulfill specific requirements in place before you use Oracle Database Vault with Oracle Label Security.

[Using Oracle Database Vault Factors with Oracle Label Security Policies](#)  
(page 12-7)

To enhance security, you can integrate Oracle Database Vault factors with Oracle Label Security policies.

[Tutorial: Integrating Oracle Database Vault with Oracle Label Security](#)  
(page 12-10)

An Oracle Database Vault-Oracle Label Security integration can grant different levels of access to two administrative users who have the same privileges.

[Related Reports and Data Dictionary Views](#) (page 12-14)

Oracle Database Vault provides reports and data dictionary views that list information about the Oracle Database Vault-Oracle Label Security integration.

## 12.5.1 How Oracle Database Vault Is Integrated with Oracle Label Security

An Oracle Database Vault-Oracle Label Security integration enables you to assign an OLS label to a Database Vault factor identity.

In Oracle Label Security, you can restrict access to records in database tables or PL/SQL programs. For example, Mary may be able to see data protected by the HIGHLY SENSITIVE label, an Oracle Label Security label on the EMPLOYEE table that includes records that should have access limited to certain managers. Another label can be PUBLIC, which allows more open access to this data.

In Oracle Database Vault, you can create a factor called Network, for the network on which the database session originates, with the following identities:

- **Intranet:** Used for when an employee is working on site within the intranet for your company.
- **Remote:** Used for when the employee is working at home from a VPN connection.

You then assign a maximum session label to both. For example:

- Assign the Intranet identity to the HIGHLY SENSITIVE Oracle Label Security label.
- Assign the Remote identity to the PUBLIC label.

This means that when Mary is working at home using her VPN connection, she has access only to the limited table data protected under the PUBLIC identity. But when she is in the office, she has access to the HIGHLY SENSITIVE data, because she is using the Intranet identity. [Tutorial: Integrating Oracle Database Vault with Oracle Label Security](#) (page 12-10) provides an example of how to accomplish this type of integration.

In a non-unified auditing environment, you can audit the integration with Oracle Label Security by using the Label Security Integration Audit Report. Oracle Database Vault writes the audit trail to the DVSYS.AUDIT\_TRAIL\$ table. If unified auditing is enabled, then you can create audit policies to capture this information, as described in *Oracle Database Security Guide*.



**See Also:**

- [Label Security Integration Audit Report](#) (page 27-6)
- [Oracle Database Vault Oracle Label Security APIs](#) (page 20-1) for information about Database Vault APIs that you can use to integrate Database Vault with Oracle Label Security
- [Related Reports and Data Dictionary Views](#) (page 12-14) for information about reports that you can run on the Oracle Database Vault and Oracle Label Security integration
- *Oracle Label Security Administrator's Guide* for more information about Oracle Label Security labels

## 12.5.2 Requirements for Using Oracle Database Vault with Oracle Label Security

You must fulfill specific requirements in place before you use Oracle Database Vault with Oracle Label Security.

- Oracle Label Security is licensed separately. Ensure that you have purchased a license to use it.
- Before you install Oracle Database Vault, you must have already installed Oracle Label Security.
- The installation process for Oracle Label Security creates the LBACSYS user account. As a user who has been granted the DV\_ACCTMGR role, unlock this account and grant it a new password. For example:

```
sqlplus bea_dvacctmgr -- Or, sqlplus bea_dvacctmgr@hrpdb for a PDB
Enter password: password
```

```
ALTER USER LBACSYS ACCOUNT UNLOCK IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace *password* with a password that is secure.

- If you plan to use the LBACSYS user account in Oracle Enterprise Manager, then log into Enterprise Manager as user SYS with the SYSDBA administrative privilege, and grant this user the SELECT ANY DICTIONARY and SELECT\_CATALOG\_ROLE system privileges.
- Ensure that you have the appropriate Oracle Label Security policies defined. For more information, see *Oracle Label Security Administrator's Guide*.
- If you plan to integrate an Oracle Label Security policy with a Database Vault policy, then ensure that the policy name for Oracle Label Security is less than 24 characters. You can check the names of Oracle Label Security policies by querying the POLICY\_NAME column of the ALL\_SA\_POLICIES data dictionary view.

## 12.5.3 Using Oracle Database Vault Factors with Oracle Label Security Policies

To enhance security, you can integrate Oracle Database Vault factors with Oracle Label Security policies.

[About Using Oracle Database Vault Factors with Oracle Label Security Policies](#) (page 12-8)

And Oracle Database Vault-Oracle Label Security integration enables you to control the maximum security clearance for a database session.

[Configuring Factors to Work with an Oracle Label Security Policy](#) (page 12-8)

You can define factors that contribute to the maximum allowable data label of an Oracle Label Security policy.

### 12.5.3.1 About Using Oracle Database Vault Factors with Oracle Label Security Policies

And Oracle Database Vault-Oracle Label Security integration enables you to control the maximum security clearance for a database session.

Oracle Database Vault controls the maximum security clearance for a database session by merging the maximum allowable data for each label in a database session by merging the labels of Oracle Database Vault factors that are associated to an Oracle Label Security policy.

In brief, a label acts as an identifier for the access privileges of a database table row. A policy is a name associated with the labels, rules, and authorizations that govern access to table rows.

---

---

**See Also:** *Oracle Label Security Administrator's Guide* for more information about row labels and policies

---

---

### 12.5.3.2 Configuring Factors to Work with an Oracle Label Security Policy

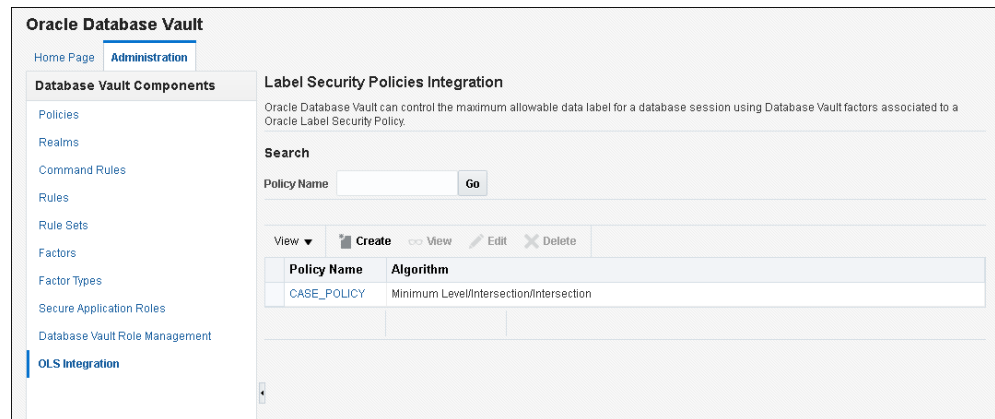
You can define factors that contribute to the maximum allowable data label of an Oracle Label Security policy.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role and the `SELECT ANY DICTIONARY` privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. Make the user `LBACSYS` account an owner of the realm that contains the schema to which a label security policy has been applied.

This enables the `LBACSYS` account to have access to all the protected data in the realm, so that it can properly classify the data.

The `LBACSYS` account is created in Oracle Label Security using the Oracle Universal Installer custom installation option. Before you can create an Oracle Label Security policy for use with Oracle Database Vault, you must make `LBACSYS` an owner for the realm you plan to use. See [About Realm Authorization](#) (page 5-13) for more information.

3. Authorize the schema owner (on which the label security policy has been applied) as either a realm participant or a realm owner.
4. In the Administration page, under Database Vault Components, click **OLS Integration**.



5. In the Label Security Policies Integration page:

- To register a new label security policy with Database Vault, click **Create**.
- To edit an existing label security policy that has been registered with Database Vault, select it from the list and then click **Edit**.

6. Enter the following settings:

- **Label Security Policy:** From the list, select the Oracle Label Security policy that you want to use.
- **Algorithm:** Optionally change the label-merging algorithm for cases when Oracle Label Security has merged two labels. In most cases, you may want to select **LII - Minimum Level/Intersection/Intersection**. This setting is the most commonly used method that Oracle Label Security administrators use when they want to merge two labels. This setting provides optimum flexibility when your applications must determine the resulting label that is required when combining two data sets that have different labels. It is also necessary for situations in which you must perform queries using joins on rows with different data labels.

If you want to use the DBMS\_MACADM package to specify a merge algorithm, see [Table 20-2](#) (page 20-2) for a full listing of possible merge algorithms.

- **Label Security Policy Factors:** In the **Available Factors** list under Label Security Policy Factors, select the factor that you want to associate with the Oracle Label Security policy. Then click **Move** to move the factor to the **Selected Factors** list. You can select multiple factors by holding down the **Ctrl** key as you click each factor that you want to select.

7. Click **OK**.

The policy is listed in the Label Security Policies Integration page.

8. Label the factor identities using the labels for the policy.

[Adding an Identity to a Factor](#) (page 8-14) provides detailed information.

---

---

**Note:**

If you do not associate an Oracle Label Security policy with factors, then Oracle Database Vault maintains the default Oracle Label Security behavior for the policy.

---

---

## 12.5.4 Tutorial: Integrating Oracle Database Vault with Oracle Label Security

An Oracle Database Vault-Oracle Label Security integration can grant different levels of access to two administrative users who have the same privileges.

[About This Tutorial](#) (page 12-10)

You can use Oracle Database Vault factors with Oracle Label Security and Oracle Virtual Private Database (VPD) to restrict sensitive data access.

[Step 1: Create Users for This Tutorial](#) (page 12-10)

You must create two administrative users for this tutorial.

[Step 2: Create the Oracle Label Security Policy](#) (page 12-11)

Next, you can create the Oracle Label Security policy and grant users the appropriate privileges for it.

[Step 3: Create Oracle Database Vault Rules to Control the OLS Authorization](#) (page 12-12)

After you create the Oracle Label Security policy, you can create Database Vault rules to work with it.

[Step 4: Update the ALTER SYSTEM Command Rule to Use the Rule Set](#) (page 12-12)

Before the rule set can be used, you must update the ALTER SYSTEM command rule, which is a default command rule.

[Step 5: Test the Authorizations](#) (page 12-13)

With all the components in place, you are ready to test the authorization.

[Step 6: Remove the Components for This Tutorial](#) (page 12-13)

You can remove the components that you created for this tutorial if you no longer need them.

### 12.5.4.1 About This Tutorial

You can use Oracle Database Vault factors with Oracle Label Security and Oracle Virtual Private Database (VPD) to restrict sensitive data access.

You can restrict this data so that it is only exposed to a database session when the correct combination of factors exists, defined by the security administrator, for any given database session.

### 12.5.4.2 Step 1: Create Users for This Tutorial

You must create two administrative users for this tutorial.

1. Log into the database instance as a user who has been granted the DV\_ACCTMGR role.

For example:

```
sqlplus bea_dvacctmgr
Enter password: password
```

In a multitenant environment, you must connect to the appropriate pluggable database (PDB).

For example:

```
sqlplus bea_dvacctmgr@hrpdb
Enter password: password
```

To find the available PDBs, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

## 2. Create the following local users:

```
GRANT CREATE SESSION TO mdale IDENTIFIED BY password CONTAINER = CURRENT;
GRANT CREATE SESSION TO jsmith IDENTIFIED BY password CONTAINER = CURRENT;
```

Follow the guidelines in *Oracle Database Security Guide* to replace `password` with a password that is secure.

## 3. Connect as a user who can grant system privileges and who has been granted the owner authorization for the Oracle System Privilege and Role Management realm, and then grant administrative privileges to users `mdale` and `jsmith`.

```
CONNECT dba_psmith -- Or, CONNECT dba_psmith@hrpdb
Enter password: password
```

```
GRANT DBA TO mdale, jsmith;
```

At this stage, users `mdale` and `jsmith` have identical administrative privileges.

### 12.5.4.3 Step 2: Create the Oracle Label Security Policy

Next, you can create the Oracle Label Security policy and grant users the appropriate privileges for it.

#### 1. In SQL\*Plus, connect as the Oracle Label Security administrator, `LBACSYS`.

```
CONNECT LBACSYS -- Or, CONNECT LBACSYS@hrpdb
Enter password: password
```

If user `LBACSYS` is locked and expired, connect as the Database Vault Account Manager, unlock and unexpire the `LBACSYS` account, and then log back in as `LBACSYS`.

For example:

```
CONNECT bea_dvacctmgr -- Or, CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

```
ALTER USER LBACSYS ACCOUNT UNLOCK IDENTIFIED BY password;
```

```
CONNECT LBACSYS
Enter password: password
```

#### 2. Create a new Oracle Label Security policy:

```
EXEC SA_SYSDBA.CREATE_POLICY('PRIVACY', 'PRIVACY_COLUMN', 'NO_CONTROL');
```

#### 3. Create the following levels for the `PRIVACY` policy:

```
EXEC SA_COMPONENTS.CREATE_LEVEL('PRIVACY',2000,'S','SENSITIVE');
EXEC SA_COMPONENTS.CREATE_LEVEL('PRIVACY',1000,'C','CONFIDENTIAL');
```

4. Create the PII compartment.

```
EXEC SA_COMPONENTS.CREATE_COMPARTMENT('PRIVACY',100,'PII','PERS_INFO');
```

5. Grant users `mdale` and `jsmith` the following labels:

```
EXEC SA_USER_ADMIN.SET_USER_LABELS('PRIVACY','mdale','S:PII');
EXEC SA_USER_ADMIN.SET_USER_LABELS('PRIVACY','jsmith','C');
```

User `mdale` is granted the more sensitive label, Sensitive, which includes the PII compartment. User `jsmith` gets the Confidential label, which is less sensitive.

### 12.5.4.4 Step 3: Create Oracle Database Vault Rules to Control the OLS Authorization

After you create the Oracle Label Security policy, you can create Database Vault rules to work with it.

1. Connect to SQL\*Plus as the Database Vault Owner.

For example:

```
CONNECT leo_dvowner -- Or, CONNECT leo_dvowner@hrpdb
Enter password: password
```

2. Create the following rule set:

```
EXEC DBMS_MACADM.CREATE_RULE_SET('PII Rule Set', 'Protect PII data from
privileged users', 'Y',1,0,2,NULL,NULL,0,NULL);
```

3. Create a rule for the PII Rule Set.

```
EXEC DBMS_MACADM.CREATE_RULE('Check OLS Factor',
'dominates(sa_utl.numeric_label('PRIVACY'),
char_to_label('PRIVACY','S:PII')) = '1');
```

Ensure that you use single quotes, as shown in this example, and not double quotes.

4. Add the Check OLS Factor rule to the PII Rule Set.

```
EXEC DBMS_MACADM.ADD_RULE_TO_RULE_SET('PII Rule Set', 'Check OLS Factor');
```

### 12.5.4.5 Step 4: Update the ALTER SYSTEM Command Rule to Use the Rule Set

Before the rule set can be used, you must update the ALTER SYSTEM command rule, which is a default command rule.

1. As the Database Vault Owner, check the current value of the ALTER SYSTEM command rule, which is one of the default command rules when you install Oracle Database Vault.

```
SELECT * FROM DBA_DV_COMMAND_RULE WHERE COMMAND = 'ALTER SYSTEM';
```

2. Make a note of these settings so that you can revert them to their original values later on.

In a default installation, the ALTER SYSTEM command rule uses the Allow Fine Grained Control of System Parameters rule set, and is enabled.

3. Update the ALTER SYSTEM command rule to be associated with the PII Rule Set.

```
EXEC DBMS_MACADM.UPDATE_COMMAND_RULE('ALTER SYSTEM', 'PII Rule Set', '%', '%',
'Y');
```

This command adds the PII Rule Set to the ALTER SYSTEM command rule, applies it to all object owners and object names, and enables the command rule.

#### 12.5.4.6 Step 5: Test the Authorizations

With all the components in place, you are ready to test the authorization.

1. In SQL\*Plus, log on as user mdale.

```
CONNECT mdale -- Or, CONNECT mdale@hrpdb
Enter password: password
```

2. Check the current setting for the AUDIT\_TRAIL initialization parameter.

```
SHOW PARAMETER AUDIT_TRAIL
```

NAME	TYPE	VALUE
audit_trail	string	DB

Make a note of this setting, so that you can revert it to its original setting later on.

3. As user mdale, use the ALTER SYSTEM statement to modify the CPU\_COUNT parameter.

```
ALTER SYSTEM SET CPU_COUNT = 4;
System altered.
```

Because user mdale was assigned the Sensitive label with the PII compartment, he can use the ALTER SYSTEM statement to modify the AUDIT\_TRAIL system parameter.

4. Set the CPU\_COUNT parameter back to its original value.

For example:

```
ALTER SYSTEM SET CPU_COUNT = 2;
```

5. Log in as user jsmith and then issue the same ALTER SYSTEM statement:

```
CONNECT jsmith -- Or, CONNECT jsmith@hrpdb
Enter password: password
```

```
ALTER SYSTEM SET CPU_COUNT = 14;
```

The following output should appear:

```
ERROR at line 1:
ORA-01031: insufficient privileges
```

Because user jsmith was assigned only the Confidential label, he cannot perform the ALTER SYSTEM statement.

#### 12.5.4.7 Step 6: Remove the Components for This Tutorial

You can remove the components that you created for this tutorial if you no longer need them.

1. Connect as the Oracle Label Security administrator and remove the label policy and its components.

```
CONNECT LBACSYS -- Or, CONNECT LBACSYS@hrpdb
Enter password: password
```

```
EXEC SA_SYSDBA.DROP_POLICY('PRIVACY', TRUE);
```

2. Connect as the Oracle Database Vault Owner and issue the following commands in the order shown, to set the ALTER SYSTEM command rule back to its previous setting and remove the rule set.

For example:

```
CONNECT leo_dvowner
Enter password: password
```

```
EXEC DBMS_MACADM.UPDATE_COMMAND_RULE('ALTER SYSTEM', 'Allow System
Parameters','%','%', 'Y');
EXEC DBMS_MACADM.DELETE_RULE_FROM_RULE_SET('PII Rule Set', 'Check OLS Factor');
EXEC DBMS_MACADM.DELETE_RULE('Check OLS Factor');
EXEC DBMS_MACADM.DELETE_RULE_SET('PII Rule Set');
COMMIT;
```

3. Connect as the Database Vault Account Manager and remove users mdale and jsmith.

```
CONNECT bea_dvacctmgr -- Or, CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

```
DROP USER mdale;
DROP USER jsmith;
```

## 12.5.5 Related Reports and Data Dictionary Views

Oracle Database Vault provides reports and data dictionary views that list information about the Oracle Database Vault-Oracle Label Security integration.

[Table 12-1](#) (page 12-14) lists the Oracle Database Vault reports. See [Oracle Database Vault Reports](#) (page 27-1), for information about how to run these reports.

**Table 12-1 Reports Related to Database Vault and Oracle Label Security Integration**

Report	Description
<a href="#">Factor Configuration Issues Report</a> (page 27-4)	Lists factors in which the Oracle Label Security policy does not exist.
<a href="#">Identity Configuration Issues Report</a> (page 27-4)	Lists invalid label identities (the Oracle Label Security label for this identity has been removed and no longer exists).
<a href="#">Security Policy Exemption Report</a> (page 27-14)	Lists accounts and roles that have the EXEMPT ACCESS POLICY system privilege granted to them. Accounts that have this privilege can bypass all Virtual Private Database policy filters and any Oracle Label Security policies that use Oracle Virtual Private Database indirectly.

[Table 12-2](#) (page 12-15) lists data dictionary views that provide information about existing Oracle Label Security policies used with Oracle Database Vault.



**Table 12-2 Data Dictionary Views Used for Oracle Label Security**

Data Dictionary View	Description
<a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17)	Lists the Oracle Label Security policies defined
<a href="#">DBA_DV_MAC_POLICY_FACTOR View</a> (page 25-17)	Lists the factors that are associated with Oracle Label Security policies
<a href="#">DBA_DV_POLICY_LABEL View</a> (page 25-20)	Lists the Oracle Label Security label for each factor identifier in the <code>DBA_DV_IDENTITY</code> view for each policy

## 12.6 Integrating Oracle Database Vault with Oracle Data Guard

An Oracle Database Vault-Oracle Data Guard integration requires first, the primary database configuration, then the standby database configuration.

### Step 1: Configure the Primary Database (page 12-15)

You must run the DGMGRL and DBCA utilities, and then the `ALTER SYSTEM` statement, to configure the primary database.

### Step 2: Configure the Standby Database (page 12-16)

You can perform the standby database configuration within the database to be used for the standby database.

### 12.6.1 Step 1: Configure the Primary Database

You must run the DGMGRL and DBCA utilities, and then the `ALTER SYSTEM` statement, to configure the primary database.

1. For Linux and UNIX systems, ensure there is an `/etc/oratab` entry for the database on the node in which you are installing Oracle Database Vault.
2. If you are using Data Guard Broker, then from the command prompt, disable the configuration as follows:

```
dgmgrl sys
Enter password: password

DGMGRL> disable configuration;
```

3. Run Database Configuration Assistant (DBCA) and configure the database options to add Oracle Database Vault to the primary database.
  - a. From the command line, enter the following command to start DBCA:

```
dbca
```
  - b. Select the correct database type (**Cluster** or **Single Instance**) and click **Next**.
  - c. In the Database Operation page, select **Configure Database Options** and click **Next**.
  - d. Select the appropriate database and click **Next**.
  - e. Select **Oracle Label Security**, which then enables you to select **Oracle Database Vault** and click **Next**.

- f. Enter the name of the Database Vault owner (required) and the Database Vault account manager (recommended).  
Passwords must have at least one alphabetic character, one number, and one special character.
- g. Click **Next**.
- h. Choose appropriate connection mode and click **Next**.
- i. Click **OK** to restart the database.
- j. Click **OK** on **Configure Additional Components**.

At this point, the installation on the primary site is complete.

4. Log into the database instance as user `SYS` with the `SYSDBA` administrative privilege.

```
sqlplus sys as sysdba
Enter password: password
```

5. Run the following `ALTER SYSTEM` statements:

```
ALTER SYSTEM SET AUDIT_SYS_OPERATIONS=TRUE SCOPE=SPFILE;
ALTER SYSTEM SET OS_ROLES=FALSE SCOPE=SPFILE;
ALTER SYSTEM SET RECYCLEBIN='OFF' SCOPE=SPFILE;
ALTER SYSTEM SET REMOTE_LOGIN_PASSWORDFILE='EXCLUSIVE' SCOPE=SPFILE;
ALTER SYSTEM SET SQL92_SECURITY=TRUE SCOPE=SPFILE;
ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE SCOPE=SPFILE;
ALTER SYSTEM SET REMOTE_OS_ROLES=FALSE SCOPE=SPFILE;
```

6. Run the `ALTER SYSTEM` statement on each database instance to set the parameters as shown in Step 5 (page 12-16).
7. Restart each database instance.

```
CONNECT SYS AS SYSOPER
Enter password: password
```

```
SHUTDOWN IMMEDIATE
STARTUP
```

## 12.6.2 Step 2: Configure the Standby Database

You can perform the standby database configuration within the database to be used for the standby database.

1. Log into the database instance as user `SYS` with the `SYSDBA` administrative privilege.

```
sqlplus sys as sysdba
Enter password: password
```

2. In a multitenant environment, connect to the appropriate PDB.

For example:

```
CONNECT bea_dvacctmgr@hrpdb
Enter password: password
```

To find the available PDBs, query the `DBA_PDBS` data dictionary view. To check the current PDB, run the `show con_name` command.

**3. Mount a standby database instance.**

```
ALTER DATABASE MOUNT STANDBY DATABASE;
```

**4. Run the following ALTER SYSTEM statements:**

```
ALTER SYSTEM SET AUDIT_SYS_OPERATIONS=TRUE SCOPE=SPFILE;
ALTER SYSTEM SET OS_ROLES=FALSE SCOPE=SPFILE;
ALTER SYSTEM SET RECYCLEBIN='OFF' SCOPE=SPFILE;
ALTER SYSTEM SET REMOTE_LOGIN_PASSWORDFILE='EXCLUSIVE' SCOPE=SPFILE;
ALTER SYSTEM SET SQL92_SECURITY=TRUE SCOPE=SPFILE;
ALTER SYSTEM SET REMOTE_OS_AUTHENT=FALSE SCOPE=SPFILE;
ALTER SYSTEM SET REMOTE_OS_ROLES=FALSE SCOPE=SPFILE;
```

**5. Restart or mount the database instance.**

For example:

```
SHUTDOWN IMMEDIATE
STARTUP
```

**6. Mount the next standby instance.****7. Restart the managed recovery as follows:**

```
ALTER DATABASE RECOVER MANAGED STANDBY DATABASE;
```

**8. If you are using Data Guard Broker, then from the command line, re-enable the configuration.**

```
dgmgrl sys
Enter password: password

DGMGRL> enable configuration;
```

This command applies the changes to the physical standby database made by the Oracle Database Vault installation on the primary database.

**9. Repeat the physical standby installation process on each physical standby database. For example, if there are three physical standby databases, then run these procedures on each standby database.**

## 12.7 Registering Oracle Internet Directory Using Oracle Database Configuration Asssitant

You can use Oracle Internet Directory in an Oracle Database Vault-enabled database.

However, if you want to register Oracle Internet Directory (OID) using Oracle Database Configuration Assistant (DBCA), then you must first disable Oracle Database Vault.

**Related Topics:**

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.



---

# DBA Operations in an Oracle Database Vault Environment

Database administrators can perform operations in an Oracle Database Vault environment, such as using Database Vault with products such as Oracle Data Pump.

[Using Oracle Database Vault with Oracle Enterprise Manager](#) (page 13-2)

Oracle Database Vault administrators can perform tasks in Oracle Enterprise Manager Cloud Control such as propagating policies to other databases.

[Using Oracle Data Pump with Oracle Database Vault](#) (page 13-5)

Database administrators can authorize Oracle Data Pump users to work in a Database Vault environment.

[Using Oracle Scheduler with Oracle Database Vault](#) (page 13-14)

Users who are responsible for scheduling database jobs must have Oracle Database Vault-specific authorization.

[Using Information Lifecycle Management with Oracle Database Vault](#) (page 13-16)

Users who perform Information Lifecycle Management operations on an Oracle Database Vault-enabled database must be granted authorization to perform these operations.

[Oracle Recovery Manager and Oracle Database Vault](#) (page 13-18)

You can use Recovery Manager (RMAN) in an Oracle Database Vault environment.

[Privileges for Using Oracle Streams with Oracle Database Vault](#) (page 13-19)

If you want to use Oracle Streams in an Oracle Database Vault environment, then you must have the correct privileges.

[Privileges for Using XStream with Oracle Database Vault](#) (page 13-19)

If you want to use XStream in an Oracle Database Vault environment, then you must have the appropriate privileges.

[Privileges for Using Oracle GoldenGate in with Oracle Database Vault](#) (page 13-20)

If you want to use Oracle GoldenGate in an Oracle Database Vault environment, then you must have the appropriate privileges.

[Using Data Masking in an Oracle Database Vault Environment](#) (page 13-21)

You must have the correct authorization to perform data masking in an Oracle Database Vault environment.

[Plugging a Database Vault-Enabled PDB to a CDB](#) (page 13-23)

You can plug a legacy Database Vault-enabled PDB to a multitenant container database (CDB).

[Using the ORADEBUG Utility with Oracle Database Vault](#) (page 13-26)

The ORADEBUG utility is used primarily by Oracle Support to diagnose problems that may arise with an Oracle database.

## 13.1 Using Oracle Database Vault with Oracle Enterprise Manager

Oracle Database Vault administrators can perform tasks in Oracle Enterprise Manager Cloud Control such as propagating polices to other databases.

[Propagating Oracle Database Vault Configurations to Other Databases](#)  
(page 13-2)

You can propagate Database Vault configurations (such as a realm configuration) to other Database Vault-protected databases.

[Enterprise Manager Cloud Control Alerts for Oracle Database Vault Policies](#)  
(page 13-4)

To view Oracle Database Vault alerts, you must be granted the DV\_OWNER, DV\_ADMIN, or DV\_SECANALYST role.

[Oracle Database Vault-Specific Reports in Enterprise Manager Cloud Control](#)  
(page 13-4)

From the Database Vault home page, you can find information about violations.

[Changing the DBSNMP Account Password in a Database Vault Environment](#)  
(page 13-5)

Before you can change the password for the DBSNMP user account, you must revoke the DV\_MONITOR role from this account.

### 13.1.1 Propagating Oracle Database Vault Configurations to Other Databases

You can propagate Database Vault configurations (such as a realm configuration) to other Database Vault-protected databases.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the DV\_OWNER or DV\_ADMIN role and the SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.

2. In the Database Vault home page, under Database Vault Policy Propagation, select **Database Vault Policy Propagation**.

The Available Policies area in the Policy Propagation subpage lists a summary of the Oracle Database Vault configurations that were created for the current database: that is, configurations that were created for realms, command rules, rule sets, and secure application roles. It does not list the Oracle Database Vault policies that were introduced in Oracle Database release 12c (12.2). From here, you can propagate these configurations to another database.

3. Under Available Policies, select each configuration that you want to propagate to another database.

**Database Vault Policy Propagation**

This page enables the propagation of Database Vault policies like realms, command rules, secure application roles, factors and rule sets from a source database to multiple destination databases. You can also backup your Database Vault policies to a file by clicking on Show SQL then on Save SQL. Cancel Show SQL OK

**Available Policies**

The following is the list of all the available Database Vault policies. Select the policies that need to be propagated to the destination databases.

Select All | Select None | Expand All | Collapse All

Select	Name	Status
	▼ Policies	
	▷ Realms	
	▷ Command Rules	
	▷ Secure Application Roles	
	▷ Rule Sets	

**Destination Databases**

Select the databases to which these policies need to be applied. Database vault administrator credentials are required for each of the destination databases to successfully propagate the policies.

The table below shows the list of database targets to which these database policies will be applied.

Add Remove

Select	Database Name	Database Type	Database Vault Administrator User Name	Database Vault Administrator Password
	Add destination databases.			

**Propagate Options**

Restore on failure.  
If policy propagation encounters errors, the original Database Vault policies on the destination are restored.

Skip propagation if user defined policies exist.  
If there are already existing user defined policies, policy propagation would not be attempted.

Propagate Enterprise Manager metric thresholds for Database Vault metrics.  
Database vault related metric thresholds, configured on this database will be propagated to destination databases.

Cancel Show SQL OK

4. Under Destination Databases, click the **Add** button.
5. Under Search and Select: Database Vault Enabled Destination Databases, search for the destination databases, and then select each database to which you want to propagate the configurations. Then click the **Select** button.
6. Under Destination Databases, do the following:
  - a. Under Apply credentials across destination database(s), enter the user name and password of the administrator of the Database Vault database that contains the configurations you want to propagate.  
This feature applies the Database Vault administrator's user name and password to all of the selected destination databases.
  - b. Select each database to which you want to propagate the configurations.
  - c. Enter the Database Vault administrator user name and password for each database.
  - d. Click the **Apply** button.
7. In the Propagate Options page, select from the following options.  
Any changes made to the seeded realms, command rules, rule sets, and so on will not be propagated to the destination databases. Only custom-created data are propagated.
  - **Restore on failure:** If the propagation operations encounters errors, then the propagation is rolled back. That is, the original policies on the destination database are restored. If you do not select this option, then the policy propagation on the destination database continues and ignores any errors.
  - **Skip propagation if user defined policies exist:** If the destination databases already have the user-defined configurations, then the propagation operation

is not attempted. If you do not select this option, then regardless of whether user-defined policies exist on the destination database, all the existing configurations are cleared, and the configurations from the source database are applied to the destination database.

- **Propagate Enterprise Manager metric thresholds for database vault metrics:** If the source database has Oracle Database Vault metric thresholds set, then these thresholds are also propagated to the destination databases. If you do not select this option, then only configurations are propagated and not the Oracle Database Vault thresholds.

8. Click the **OK** button.
9. In the Confirmation window, click **OK**.

A message indicating success or failure appears. If the propagation succeeds, then the configurations are active right away in their destination databases.

### 13.1.2 Enterprise Manager Cloud Control Alerts for Oracle Database Vault Policies

To view Oracle Database Vault alerts, you must be granted the `DV_OWNER`, `DV_ADMIN`, or `DV_SECANALYST` role.

The alerts are as follows:

- **Database Vault Attempted Realm Violations.** This alert helps the Oracle Database Vault security analyst (`DV_SECANALYST` role) to monitor violation attempts on the Database Vault database. This user can select the realms to be affected by the alert and filter these realms based on the different types of attempts by using error codes. You can enable this metric from the Metrics and Policy Settings page. By default, the attempted realm violations are collected every 24 hours.
- **Database Vault Attempted Command Rule Violations.** The functionality for this alert is the same as for Database Vault Attempted Realm Violations, except that it focuses on violations on command rules.
- **Database Vault Realm Configuration Issues.** This metric tracks and raises an alert if users misconfigure realms. This metric is enabled when you install Oracle Database vault, and by default it collects data every one hour.
- **Database Vault Command Rule Configuration Issues.** This functionality for this alert is that same as Database Vault Realm Configuration Issues, except that it focuses on configuration changes to command rules.
- **Database Vault Policy Changes.** This metric raises an alert on any change to any Database Vault policy, such as policies for realms and command rules. It provides a detailed policy changes report.

### 13.1.3 Oracle Database Vault-Specific Reports in Enterprise Manager Cloud Control

From the Database Vault home page, you can find information about violations.

These violations are as follows:

- Top five attempted violations on realm and command rule
- Top five attempted violations by database users and client host



- Time series-based graphical reports on attempted violations for more detailed analysis

To have full access to the Database Vault reports, you must log into Database Vault Administrator as a user who has been granted the DV\_OWNER, DV\_ADMIN, or DV\_SECANALYST role.

#### Related Topics:

[Oracle Database Vault Reports](#) (page 27-1)

Oracle Database Vault provides reports that track activities, such as the Database Vault configuration settings.

### 13.1.4 Changing the DBSNMP Account Password in a Database Vault Environment

Before you can change the password for the DBSNMP user account, you must revoke the DV\_MONITOR role from this account.

In an Oracle Database Vault environment, the DBSNMP user account is granted the DV\_MONITOR role. (The DBSNMP user can change his or her own password directly, without having to have the DV\_MONITOR role revoked first.)

1. Log into the database instance using an account that has been granted the DV\_OWNER role.
2. Revoke the DV\_MONITOR role from the DBSNMP user account.
3. Connect as a user who has been granted the DV\_ACCTMGR role and then change the DBSNMP user account password.
4. Connect as the DV\_OWNER user and then grant the DV\_MONITOR role back to the DBSNMP user account.

## 13.2 Using Oracle Data Pump with Oracle Database Vault

Database administrators can authorize Oracle Data Pump users to work in a Database Vault environment.

[About Using Oracle Data Pump with Oracle Database Vault](#) (page 13-6)

Database administrators who use Oracle Data Pump in an Database Vault environment must have Database Vault-specific authorization to export and import data.

[Authorizing Users for Data Pump Regular Export and Import Operations](#) (page 13-6)

You can use different authorization types for administrators who perform Oracle Data Pump export and import operations in a Database Vault environment.

[Authorizing Users for Data Pump Transportable Export and Import Operations](#) (page 13-9)

You can grant authorization levels for users who must perform Oracle Data Pump transportable operations.

[Guidelines for Exporting or Importing Data in a Database Vault Environment](#) (page 13-13)

After you grant the Oracle Data Pump database administrator the proper authorization, this can perform any export or import operations that are necessary.

## 13.2.1 About Using Oracle Data Pump with Oracle Database Vault

Database administrators who use Oracle Data Pump in an Database Vault environment must have Database Vault-specific authorization to export and import data.

They must have these privileges in addition to the standard Oracle Data Pump privileges. If these users want to perform Oracle Data Pump transportable tablespace operations, then they must have special authorization. You can check a user's authorizations for using Data Pump in an Oracle Database Vault environment by querying the `DBA_DV_DATAPUMP_AUTH` data dictionary view.

---

---

**See Also:**

- *Oracle Database Utilities* for detailed information about Oracle Data Pump
  - *Oracle Database Administrator's Guide* for more information about transportable tablespaces
  - [DBA\\_DV\\_DATAPUMP\\_AUTH View](#) (page 25-10)
- 
- 

## 13.2.2 Authorizing Users for Data Pump Regular Export and Import Operations

You can use different authorization types for administrators who perform Oracle Data Pump export and import operations in a Database Vault environment.

[About Authorizing Users for Oracle Data Pump Regular Operations](#)  
(page 13-6)

Users who have Oracle Data Pump authorization can perform regular Oracle Data Pump operations in a Database Vault environment.

[Levels of Database Vault Authorization for Oracle Data Pump Regular Operations](#) (page 13-7)

Oracle Database Vault provides several levels of authorization required for Oracle Data Pump regular operations in a Database Vault environment.

[Authorizing Users for Oracle Data Pump Regular Operations in Database Vault](#)  
(page 13-7)

You can authorize a database administrator to use Data Pump for regular operations in an Oracle Database Vault environment.

[Revoking Oracle Data Pump Authorization from Users](#) (page 13-8)

You can revoke authorization from the database administrator who is using Oracle Data Pump for regular operations.

### 13.2.2.1 About Authorizing Users for Oracle Data Pump Regular Operations

Users who have Oracle Data Pump authorization can perform regular Oracle Data Pump operations in a Database Vault environment.

Full level Data Pump authorization enables these users to perform transportable export and import operations as well.

---

**See Also:** [Authorizing Users for Data Pump Transportable Export and Import Operations](#) (page 13-9) if you want the user only to perform transportable export and import operations

---

### 13.2.2.2 Levels of Database Vault Authorization for Oracle Data Pump Regular Operations

Oracle Database Vault provides several levels of authorization required for Oracle Data Pump regular operations in a Database Vault environment.

[Table 13-1](#) (page 13-7) describes these levels.

**Table 13-1 Levels of Authorization for Oracle Data Pump Regular Operations**

Scenario	Authorization Required
A database administrator wants to import data into another schema.	You must grant this user the <code>BECOME USER</code> system privilege and the <code>IMP_FULL_DATABASE</code> role. <sup>1</sup> To find the privileges a user has been granted, query the <code>USER_SYS_PRIVS</code> data dictionary view.
A database administrator wants to export or import data in a schema that has no Database Vault protection.	You only need to grant this user the standard Oracle Data Pump privileges, which are the <code>EXP_FULL_DATABASE</code> and <code>IMP_FULL_DATABASE</code> roles. If the user wants to import data, grant this user the <code>BECOME USER</code> system privilege.
A database administrator wants to export or import data in a protected schema.	In addition to the <code>EXP_FULL_DATABASE</code> and <code>IMP_FULL_DATABASE</code> roles, you must grant this user Database Vault-specific authorization by using the <code>DBMS_MACADM.AUTHORIZE_DATAPUMP_USER</code> procedure. This authorization applies to both the <code>EXPDP</code> and <code>IMPDP</code> utilities. Later on, you can revoke this authorization by using the <code>DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER</code> procedure. If the user wants to import data, also grant this user the <code>BECOME USER</code> system privilege.
A database administrator wants to export or import the contents of an entire database.	In addition to the <code>EXP_FULL_DATABASE</code> and <code>IMP_FULL_DATABASE</code> roles and the authorization granted by the <code>DBMS_MACADM.AUTHORIZE_DATAPUMP_USER</code> procedure, you must grant this user the <code>DV_OWNER</code> role. If the user wants to import data, grant this user the <code>BECOME USER</code> system privilege.

<sup>1</sup> The `BECOME USER` privilege is part of the `IMP_FULL_DATABASE` role by default, but in an Oracle Database Vault environment, this privilege is revoked.

### 13.2.2.3 Authorizing Users for Oracle Data Pump Regular Operations in Database Vault

You can authorize a database administrator to use Data Pump for regular operations in an Oracle Database Vault environment.

1. Log into the database instance as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role.
2. Ensure that the user to whom you want to grant authorization has been granted the `EXP_FULL_DATABASE` and `IMP_FULL_DATABASE` roles, which are required for using Oracle Data Pump.

```
SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE LIKE '%FULL%';
```

3. Grant this user Oracle Database Vault authorization for Oracle Data Pump regular operations.

For example, to authorize the Data Pump user DP\_MGR to export and import objects for the database table EMPLOYEES:

```
EXEC DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DP_MGR', 'HR', 'EMPLOYEES');
```

To restrict DP\_MGR's activities to a specific schema, you would enter the following procedure:

```
EXEC DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DP_MGR', 'HR');
```

To authorize the Data Pump user DP\_MGR to export and import objects for the entire database, enter the following:

```
EXEC DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DP_MGR');
```

After you run the DBMS\_MACADM.AUTHORIZE\_DATAPUMP\_USER procedure, you can check the user's authorization by querying the DBA\_DV\_DATAPUMP\_AUTH data dictionary view.

4. If the user must export the entire database, then grant the user the DV\_OWNER role.

```
GRANT DV_OWNER TO DP_MGR;
```

### Related Topics:

#### [AUTHORIZE\\_DATAPUMP\\_USER Procedure](#) (page 22-3)

The AUTHORIZE\_DATAPUMP\_USER procedure authorizes a user to perform Oracle Data Pump operations when Oracle Database Vault is enabled.

#### [DBA\\_DV\\_DATAPUMP\\_AUTH View](#) (page 25-10)

The DBA\_DV\_DATAPUMP\_AUTH data dictionary view lists the authorizations for using Oracle Data Pump in an Oracle Database Vault environment.

### 13.2.2.4 Revoking Oracle Data Pump Authorization from Users

You can revoke authorization from the database administrator who is using Oracle Data Pump for regular operations.

1. If you granted the user the DV\_OWNER role, then optionally revoke this role.

```
REVOKE DV_OWNER FROM DP_MGR;
```

2. Query the DBA\_DV\_DATAPUMP\_AUTH data dictionary view to find the users who have been granted Oracle Data Pump authorizations.

```
SELECT GRANTEE, SCHEMA, OBJECT FROM DBA_DV_DATAPUMP_AUTH;
```

3. Use the information you gathered from the preceding step to build the DBMS\_MACADM.UNAUTHORIZE\_DATAPUMP\_USER command.

For example:

```
EXEC DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('DP_MGR', 'HR', 'EMPLOYEES');
```

Ensure that this unauthorization complements the original authorization action. In other words, if you originally gave DP\_MGR authorization over the entire database, then the following commands will not work:

```
EXEC DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('DP_MGR', 'HR');
```

```
EXEC DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('DP_MGR', 'HR', 'EMPLOYEES');
```

### Related Topics:

#### [UNAUTHORIZE\\_DATAPUMP\\_USER Procedure](#) (page 22-8)

The UNAUTHORIZE\_DATAPUMP\_USER procedure revokes the authorization that was granted by the AUTHORIZE\_DATAPUMP\_USER procedure.

#### [DBA\\_DV\\_DATAPUMP\\_AUTH View](#) (page 25-10)

The DBA\_DV\_DATAPUMP\_AUTH data dictionary view lists the authorizations for using Oracle Data Pump in an Oracle Database Vault environment.

## 13.2.3 Authorizing Users for Data Pump Transportable Export and Import Operations

You can grant authorization levels for users who must perform Oracle Data Pump transportable operations.

#### [About Authorizing Users for Oracle Data Pump Transportable Operations](#) (page 13-9)

You can grant users different levels of transportable operation authorization.

#### [Levels of Database Vault Authorization for Data Pump Transportable Operations](#) (page 13-10)

Oracle Database Vault provides levels of authorization required for users who must perform export and import transportable operations in a Database Vault environment.

#### [Authorizing Users for Data Pump Transportable Operations in Database Vault](#) (page 13-11)

You can authorize users to perform Oracle Data Pump transportable export or import operations in a Database Vault environment.

#### [Revoking Transportable Tablespace Authorization from Users](#) (page 13-12)

You can revoke authorization from the database administrator who is using Data Pump.

### 13.2.3.1 About Authorizing Users for Oracle Data Pump Transportable Operations

You can grant users different levels of transportable operation authorization.

If you want users to only have the authorization to perform transportable export and import operations, then you must grant users the correct authorization, based on their tasks.

---

**See Also:** [Authorizing Users for Data Pump Regular Export and Import Operations](#) (page 13-6) if your users must have Oracle Data Pump authorization to perform regular operations in a Database Vault environment

---

### 13.2.3.2 Levels of Database Vault Authorization for Data Pump Transportable Operations

Oracle Database Vault provides levels of authorization required for users who must perform export and import transportable operations in a Database Vault environment.

Table 13-2 (page 13-10) describes these levels.

**Table 13-2 Levels of Authorization for Oracle Data Pump Transportable Operations**

Scenario	Authorization Required
A database administrator wants to transportable export a tablespace or table that has no Database Vault protection.	You only need to grant this user the standard Oracle Data Pump privileges, which are the <code>EXP_FULL_DATABASE</code> and <code>IMP_FULL_DATABASE</code> roles.
A database administrator wants to transportable export a tablespace where there is Database Vault protection (for example, realm or command rule for a table object residing on that tablespace).	In addition to the <code>EXP_FULL_DATABASE</code> and <code>IMP_FULL_DATABASE</code> roles, you must grant this user Database Vault-specific transportable tablespace authorization by using the <code>DBMS_MACADM.AUTHORIZE_TTS_USER</code> procedure. Later on, you can revoke this authorization by using the <code>DBMS_MACADM.UNAUTHORIZE_TTS_USER</code> procedure. Remember that users who have been granted full database level Oracle Data Pump authorization (through the <code>DBMS_MACADM.AUTHORIZE_DATAPUMP_USER</code> procedure) can perform these operations as well.
A database administrator wants to transportable export a table within a tablespace where there is Database Vault protection (for example, a realm or command rule for a table object residing on the tablespace that contains the table to be exported).	In addition to the <code>EXP_FULL_DATABASE</code> and <code>IMP_FULL_DATABASE</code> roles, you must grant this user Database Vault-specific transportable tablespace authorization for the tablespace that contains the table to be exported by using the <code>DBMS_MACADM.AUTHORIZE_TTS_USER</code> procedure. Remember that users who have been granted full database level Oracle Data Pump authorization (from the <code>DBMS_MACADM.AUTHORIZE_DATAPUMP_USER</code> procedure) can perform these operations as well.
A database administrator wants to transportable export the contents of an entire database.	In addition to the <code>DV_OWNER</code> , <code>EXP_FULL_DATABASE</code> , and <code>IMP_FULL_DATABASE</code> roles, you must grant this user Database Vault-specific full database level Oracle Data Pump authorization by using the <code>DBMS_MACADM.AUTHORIZE_DATAPUMP_USER</code> procedure. You do not need to run the <code>DBMS_MACADM.AUTHORIZE_TTS_USER</code> procedure for this user.
A database administrator wants to use a network link to transportable import a tablespace or a table that has no Database Vault protection.	In addition to the <code>EXP_FULL_DATABASE</code> and <code>IMP_FULL_DATABASE</code> roles for both the database administrator and the connecting user, you must grant the connecting user specified in the network link the <code>DV_DATAPUMP_NETWORK_LINK</code> role.

**Table 13-2 (Cont.) Levels of Authorization for Oracle Data Pump Transportable Operations**

Scenario	Authorization Required
A database administrator wants to use a network link to transportable import a tablespace where there is Database Vault protection (for example, realm or command rule for a table object residing on that tablespace)	<p>In addition to the <code>EXP_FULL_DATABASE</code> and <code>IMP_FULL_DATABASE</code> roles, you must grant the connecting user specified in the network link the Database Vault-specific transportable tablespace authorization for that tablespace by using the <code>DBMS_MACADM.AUTHORIZE_TTS_USER</code> procedure. You must also grant the connecting user the <code>DV_DATAPUMP_NETWORK_LINK</code> role.</p> <p>Remember that users who have been granted Database Vault-specific full database level Oracle Data Pump authorization (through the <code>DBMS_MACADM.AUTHORIZE_DATAPUMP_USER</code> procedure) can perform these operations.</p>
A database administrator wants to use a network link to import a table within a transportable tablespace where there is Database Vault protection (for example, realm or command rule for a table object residing on the tablespace that contains the table to be exported)	<p>In addition to the <code>EXP_FULL_DATABASE</code> and <code>IMP_FULL_DATABASE</code> roles, you must grant the connecting user the Database Vault-specific transportable tablespace authorization for the tablespace that contains the table to be exported by using the <code>DBMS_MACADM.AUTHORIZE_TTS_USER</code> procedure. You also must grant the connecting user specified in the network link the <code>DV_DATAPUMP_NETWORK_LINK</code> role.</p> <p>Remember that users who have been granted Database Vault-specific full database level Oracle Data Pump authorization (through the <code>DBMS_MACADM.AUTHORIZE_DATAPUMP_USER</code> procedure) can perform the operations.</p>
A database administrator wants to use a network link to transportable import the contents of an entire database.	<p>In addition to the <code>DV_OWNER</code> role, you must grant the connecting user Database Vault-specific full database level Oracle Data Pump authorization by using the <code>DBMS_MACADM.AUTHORIZE_DATAPUMP_USER</code> procedure. You do not need to run the <code>DBMS_MACADM.AUTHORIZE_TTS_USER</code> procedure for this user. You must also grant the connecting user who is specified in the network link the <code>DV_DATAPUMP_NETWORK_LINK</code> role.</p>

### 13.2.3.3 Authorizing Users for Data Pump Transportable Operations in Database Vault

You can authorize users to perform Oracle Data Pump transportable export or import operations in a Database Vault environment.

1. Log into the database instance as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role.
2. Ensure that the user to whom you want to grant authorization has been granted the `EXP_FULL_DATABASE` and `IMP_FULL_DATABASE` roles, which are required for using Oracle Data Pump.

```
SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS
WHERE GRANTED_ROLE LIKE '%FULL%';
```

3. If the user wants to transportable export or use a network link to transportable import the contents of an entire database, then grant the full database level Oracle Data Pump authorization by using the `DBMS_MACADM.AUTHORIZE_DATAPUMP_USER` procedure. Otherwise, bypass this step.

For example:

```
EXEC DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DP_MGR');
```

4. If the user must have Database Vault-specific transportable tablespace authorization only, then grant this user this authorization.

For example:

```
EXEC DBMS_MACADM.AUTHORIZE_TTS_USER('DP_MGR', 'HR_TS');
```

5. If the user who wants to perform a transportable import operation wants to use a network link to perform the operation, then grant this user the DV\_DATAPUMP\_NETWORK\_LINK role.

For example:

```
GRANT DV_DATAPUMP_NETWORK_LINK TO DP_MGR;
```

6. If the user wants to transportable export or use a network link to transportable import the entire database, then grant this user the DV\_OWNER role.

```
GRANT DV_OWNER TO DP_MGR;
```

#### Related Topics:

##### [AUTHORIZE\\_TTS\\_USER Procedure](#) (page 22-7)

The AUTHORIZE\_TTS\_USER procedure authorizes a user to perform Oracle Data Pump transportable tablespace operations for a tablespace when Oracle Database Vault is enabled.

##### [AUTHORIZE\\_DATAPUMP\\_USER Procedure](#) (page 22-3)

The AUTHORIZE\_DATAPUMP\_USER procedure authorizes a user to perform Oracle Data Pump operations when Oracle Database Vault is enabled.

##### [DV\\_DATAPUMP\\_NETWORK\\_LINK Data Pump Network Link Role](#)

(page 14-14)

The DV\_DATAPUMP\_NETWORK\_LINK role is used for Data Pump import operations.

#### 13.2.3.4 Revoking Transportable Tablespace Authorization from Users

You can revoke authorization from the database administrator who is using Data Pump.

1. If you granted the user the DV\_OWNER role, then optionally revoke this role.

```
REVOKE DV_OWNER FROM DP_MGR;
```

2. Query the DBA\_DV\_TTS\_AUTH data dictionary view to find the users who have been granted Oracle Data Pump authorizations.

```
SELECT GRANTEE, TSNAME FROM DBA_DV_TTS_AUTH;
```

3. Use the information you gathered from the preceding step to build the DBMS\_MACADM.UNAUTHORIZE\_TTS\_USER statement.

For example:

```
EXEC DBMS_MACADM.UNAUTHORIZE_TTS_USER('DP_MGR', 'HR_TS');
```



4. If the user had transportable exported or used a network link to transportable import the contents of an entire database, then revoke the full database level Oracle Data Pump authorization.

For example:

```
EXEC DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('DP_MGR');
```

5. If the user who had performed a transportable import operation used a network link to perform the operation, then revoke the DV\_DATAPUMP\_NETWORK\_LINK role from this user.

For example:

```
REVOKE DV_DATAPUMP_NETWORK_LINK FROM DP_MGR;
```

#### Related Topics:

##### [UNAUTHORIZE\\_TTS\\_USER Procedure](#) (page 22-13)

The UNAUTHORIZE\_TTS\_USER procedure removes from authorization users who had previously been granted the authorization to perform Oracle Data Pump transportable tablespace operations.

##### [UNAUTHORIZE\\_DATAPUMP\\_USER Procedure](#) (page 22-8)

The UNAUTHORIZE\_DATAPUMP\_USER procedure revokes the authorization that was granted by the AUTHORIZE\_DATAPUMP\_USER procedure.

##### [DV\\_DATAPUMP\\_NETWORK\\_LINK Data Pump Network Link Role](#) (page 14-14)

The DV\_DATAPUMP\_NETWORK\_LINK role is used for Data Pump import operations.

## 13.2.4 Guidelines for Exporting or Importing Data in a Database Vault Environment

After you grant the Oracle Data Pump database administrator the proper authorization, this can perform any export or import operations that are necessary.

Before this user begins work, he or she should follow these guidelines:

- **Create a full backup of the database datafiles.** This way, if you or other users do not like the newly-imported data, then you easily can revert the database to its previous state. This guideline is especially useful if an intruder had managed to modify Oracle Data Pump exported data to use his or her own policies.
- **Decide how to handle exporting and importing multiple schemas or tables.** You cannot specify multiple schemas or tables in the DBMS\_MACADM.AUTHORIZE\_DATAPUMP\_USER procedure, but you can use either of the following methods to accomplish this task:
  - Run the DBMS\_MACADM.AUTHORIZE\_DATAPUMP\_USER procedure for each schema or table, and then specify the list of these objects in the SCHEMAS or TABLES parameter of the EXPDP and IMPDP utilities.
  - Perform a full database export or import operation. If so, see the next guideline.

- **When performing an export or import operation for an entire database, set the EXPDP or IMPDP FULL option to Y.** Remember that this setting will capture the DVSYS schema, so ensure that the user has been granted the DV\_OWNER role.

Note the following:

- You cannot use the legacy EXP and IMP utilities with the direct path option (`direct=y`) if Oracle Database Vault is enabled.
- Users who have been granted Database Vault-specific Oracle Data Pump authorization through the `DBMS_MACADM.AUTHORIZE_DATAPUMP_USER` procedure or transportable tablespace authorization through the `DBMS_MACADM.AUTHORIZE_TTS_USER` procedure can export and import database objects, but they cannot perform other activities, such as SELECT queries on schema tables to which they normally do not have access. Similarly, users are not permitted to perform Data Pump operations on objects outside the designated data objects.
- You must grant the DV\_OWNER role to users who want to export or import an entire database, because a full database export requires access to the DVSYS schema, which stores the Oracle Database Vault policies. However, you cannot export the DVSYS schema itself. Data Pump only exports the protection definitions. The target database must have the DVSYS schema in it and Database Vault enabled before you can begin the import process.) Conversely, for a Data Pump import operation to apply the imported policies to the target database, it internally uses the `DBMS_MACADM` PL/SQL package, which in turn requires the Data Pump user to have the DV\_OWNER role.

---

**See Also:** *Oracle Database Utilities* for detailed information about Oracle Data Pump

---

## 13.3 Using Oracle Scheduler with Oracle Database Vault

Users who are responsible for scheduling database jobs must have Oracle Database Vault-specific authorization.

[About Using Oracle Scheduler with Oracle Database Vault](#) (page 13-14)

The level of authorization that you must grant depends on schema in which the administrator wants to perform a task.

[Granting a Job Scheduling Administrator Authorization for Database Vault](#) (page 13-15)

You can authorize a user to schedule database jobs in a Database Vault environment.

[Revoking Authorization from Job Scheduling Administrators](#) (page 13-16)

You can revoke authorization from a user for scheduling database jobs.

### 13.3.1 About Using Oracle Scheduler with Oracle Database Vault

The level of authorization that you must grant depends on schema in which the administrator wants to perform a task.

Possible scenarios are as follows:

- **An administrator wants to schedule a job in his or her own schema.** An administrator who has been granted privileges to schedule database jobs can

continue to do so without any Oracle Database Vault-specific authorizations, unless this schema is protected by a realm. In that case, ensure that this user is authorized to access the realm.

- **An administrator wants to run a job in another schema, but this job does not access any Oracle Database Vault realm or command rule protected object.** In this case, this user only needs job related system privileges, not the Oracle Database Vault privileges.
- **An administrator wants to run a job under the schema of another user, including any schema in the database or a remote database.** If this job accesses an Oracle Database Vault realm or command rule protected object, then you must grant this user Database Vault-specific authorization by using the `DBMS_MACADM.AUTHORIZE_SCHEDULER_USER` procedure. This authorization applies to both background and foreground jobs. For background jobs, the authorization applies to the last user who created or modified the job. In addition, ensure that the schema owner (the protected schema in which the job is created) authorized to the realm.

Later on, you can revoke this authorization by using the `DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER` procedure. If the schema is not protected by a realm, then you do not need to run the `DBMS_MACADM.AUTHORIZE_SCHEDULER_USER` procedure for the user.

#### Related Topics:

[About Realm Authorization](#) (page 5-13)

Realm authorizations establish the set of database accounts and roles that manage or access objects protected in realms.

### 13.3.2 Granting a Job Scheduling Administrator Authorization for Database Vault

You can authorize a user to schedule database jobs in a Database Vault environment.

1. Log into the database instance as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role.

Only a user who has been granted either of these roles can grant the necessary authorization.

2. Ensure that the user to whom you want to grant authorization has been granted system privileges to schedule database jobs.

These privileges include any of the following: `CREATE JOB`, `CREATE ANY JOB`, `CREATE EXTERNAL JOB`, `EXECUTE ANY PROGRAM`, `EXECUTE ANY CLASS`, `MANAGE SCHEDULER`. The `DBA` and `SCHEDULER_ADMIN` roles provide these privileges; however, when Oracle Database Vault is enabled, the privileges are revoked from these roles.

For example:

```
SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS
WHERE PRIVILEGE IN ('CREATE JOB', 'CREATE ANY JOB');
```

3. Grant this user Oracle Database Vault authorization.

For example, to authorize the user `job_mgr` to schedule jobs for any schema in the database:

```
EXEC DBMS_MACADM.AUTHORIZE_SCHEDULER_USER('JOB_MGR');
```

Optionally, you can restrict `job_mgr`'s activities to a specific schema, as follows:

```
EXEC DBMS_MACADM.AUTHORIZE_SCHEDULER_USER('JOB_MGR', 'HR');
```

4. Ensure that the user has been authorized by querying the `DBA_DV_JOB_AUTH` data dictionary view as follows:

```
SELECT GRANTEE, SCHEMA FROM DBA_DV_JOB_AUTH WHERE GRANTEE = 'user_name';
```

#### Related Topics:

[AUTHORIZE\\_SCHEDULER\\_USER Procedure](#) (page 22-7)

The `AUTHORIZE_SCHEDULER_USER` procedure grants a user authorization to schedule database jobs when Oracle Database Vault is enabled.

[DBA\\_DV\\_JOB\\_AUTH View](#) (page 25-16)

The `DBA_DV_JOB_AUTH` data dictionary view lists the authorizations for using Oracle Scheduler in an Oracle Database Vault environment.

### 13.3.3 Revoking Authorization from Job Scheduling Administrators

You can revoke authorization from a user for scheduling database jobs.

1. Query the `DBA_DV_JOB_AUTH` data dictionary view to find the user's authorization.

```
SELECT GRANTEE, SCHEMA FROM DBA_DV_JOB_AUTH WHERE GRANTEE='username';
```

2. Use the information you gathered from the preceding step to build the `DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER` command.

For example:

```
EXEC DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER('JOB_MGR');
```

Ensure that this unauthorization complements the original authorization action. In other words, if you originally gave `job_mgr` authorization over the entire database, then the following command will not work:

```
EXEC DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER('JOB_MGR', 'HR');
```

#### Related Topics:

[UNAUTHORIZE\\_SCHEDULER\\_USER Procedure](#) (page 22-12)

The `UNAUTHORIZE_SCHEDULER_USER` procedure revokes the authorization that was granted by the `AUTHORIZE_SCHEDULER_USER` procedure.

## 13.4 Using Information Lifecycle Management with Oracle Database Vault

Users who perform Information Lifecycle Management operations on an Oracle Database Vault-enabled database must be granted authorization to perform these operations.

[About Using Information Lifecycle Management with Oracle Database Vault](#) (page 13-17)

You can grant authorization to and from users who are responsible for performing Information Lifecycle Management (ILM) operations on Oracle Database Vault realm- and command rule-protected objects.

[Authorizing Users for ILM Operations in Database Vault](#) (page 13-17)

You can authorize a user to perform Information Lifecycle Management (ILM) operations in an Oracle Database Vault environment.

[Revoking Information Lifecycle Management Authorization from Users](#) (page 13-18)

You can revoke authorization from users so that they cannot perform Information Lifecycle Management (ILM) operations in an Oracle Database Vault environment.

### 13.4.1 About Using Information Lifecycle Management with Oracle Database Vault

You can grant authorization to and from users who are responsible for performing Information Lifecycle Management (ILM) operations on Oracle Database Vault realm- and command rule-protected objects.

You must first authorize users before they can perform the following SQL statements for ILM operations in a Database Vault-enabled database:

- ALTER TABLE
  - ILM
  - FLASHBACK ARCHIVE
  - NO FLASHBACK ARCHIVE
- ALTER TABLESPACE
  - FLASHBACK MODE

### 13.4.2 Authorizing Users for ILM Operations in Database Vault

You can authorize a user to perform Information Lifecycle Management (ILM) operations in an Oracle Database Vault environment.

1. Log into the database instance as a user who has been granted the DV\_OWNER or DV\_ADMIN role.

Only a user who has been granted either of these roles can grant the necessary authorization.

2. Use the DBMS\_MACADM.AUTHORIZE\_MAINTENANCE\_USER to authorize the user.

For example, to grant a user authorization to perform ILM operations on the HR.EMPLOYEES table:

```
EXEC DBMS_MACADM.AUTHORIZE_MAINTENANCE_USER ('PSMITH', 'HR', 'EMPLOYEES',
'TABLE', 'ILM');
```

If you wanted to grant user `psmith` ILM authorizations for the entire database, you would enter a procedure similar to the following:

```
EXEC DBMS_MACADM.AUTHORIZE_MAINTENANCE_USER ('PSMITH', '%', '%', '%', '%');
```

3. Ensure that the user has been authorized by querying the DBA\_DV\_MAINTENANCE\_AUTH data dictionary view.

**Related Topics:**[AUTHORIZE\\_MAINTENANCE\\_USER Procedure](#) (page 22-5)

The `AUTHORIZE_MAINTENANCE_USER` procedure grants a user authorization to perform Information Lifecycle Management (ILM) operations in an Oracle Database Vault environment.

[DBA\\_DV\\_MAINTENANCE\\_AUTH View](#) (page 25-18)

The `DBA_DV_MAINTENANCE_AUTH` data dictionary view provides information about the configuration of Oracle Database Vault authorizations to use Information Life Management (ILM) features.

### 13.4.3 Revoking Information Lifecycle Management Authorization from Users

You can revoke authorization from users so that they cannot perform Information Lifecycle Management (ILM) operations in an Oracle Database Vault environment.

1. Log into the database instance as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role.

Only a user who has been granted either of these roles can grant the necessary authorization.

2. Query the `DBA_DV_MAINTENANCE_AUTH` data dictionary view to find the kind of authorization that was granted to the ILM user.
3. Use the `DBMS_MACADM.UNAUTHORIZE_MAINTENANCE_USER` to revoke the authorization from the user.

For example:

```
EXEC DBMS_MACADM.UNAUTHORIZE_MAINTENANCE_USER ('PSMITH', 'HR', '%', 'TABLE', 'ILM');
```

**Related Topics:**[DBA\\_DV\\_MAINTENANCE\\_AUTH View](#) (page 25-18)

The `DBA_DV_MAINTENANCE_AUTH` data dictionary view provides information about the configuration of Oracle Database Vault authorizations to use Information Life Management (ILM) features.

[UNAUTHORIZE\\_MAINTENANCE\\_USER Procedure](#) (page 22-10)

The `UNAUTHORIZE_MAINTENANCE_USER` procedure revokes privileges from users who have been granted authorization to perform Information Lifecycle Management (ILM) operations in an Oracle Database Vault environment.

## 13.5 Oracle Recovery Manager and Oracle Database Vault

You can use Recovery Manager (RMAN) in an Oracle Database Vault environment.

The functionality of RMAN with Oracle Database Vault is the same as its functionality in a standard Oracle Database environment.

---

**See Also:**

- *Oracle Database Backup and Recovery User's Guide*
  - *Oracle Database Backup and Recovery Reference*
- 

## 13.6 Privileges for Using Oracle Streams with Oracle Database Vault

If you want to use Oracle Streams in an Oracle Database Vault environment, then you must have the correct privileges.

The privileges that you must have are as follows:

- You must be granted the `DV_STREAMS_ADMIN` role in order to configure the Oracle Streams capture process.
- Before you can apply changes to any tables that are protected by a realm, you must be authorized to have access to that realm. For example:

```
EXEC DBMS_MACADM.ADD_AUTH_TO_REALM('realm_name','username');
```

**Related Topics:**

[DV\\_STREAMS\\_ADMIN Oracle Streams Configuration Role](#) (page 14-15)

The `DV_STREAMS_ADMIN` role is used with Oracle Streams.

[ADD\\_AUTH\\_TO\\_REALM Procedure](#) (page 15-2)

The `ADD_AUTH_TO_REALM` procedure authorizes a user or role to access a realm as an owner or a participant. In a multitenant environment, you can authenticate both common and local realms.

## 13.7 Privileges for Using XStream with Oracle Database Vault

If you want to use XStream in an Oracle Database Vault environment, then you must have the appropriate privileges.

These privileges are as follows:

- You must be granted the `DV_XSTREAM_ADMIN` role in order to configure the XStream.
- Before you can apply changes to any tables that are protected by a realm, you must be authorized to have access to that realm. For example:

```
EXEC DBMS_MACADM.ADD_AUTH_TO_REALM('realm_name','username');
```

**Related Topics:**

[DV\\_XSTREAM\\_ADMIN XStream Administrative Role](#) (page 14-16)

The `DV_XSTREAM_ADMIN` role is used for Oracle XStream.

[ADD\\_AUTH\\_TO\\_REALM Procedure](#) (page 15-2)

The `ADD_AUTH_TO_REALM` procedure authorizes a user or role to access a realm as an owner or a participant. In a multitenant environment, you can authenticate both common and local realms.

## 13.8 Privileges for Using Oracle GoldenGate in with Oracle Database Vault

If you want to use Oracle GoldenGate in an Oracle Database Vault environment, then you must have the appropriate privileges.

These privileges are as follows:

- The user must be granted the `DV_GOLDENGATE_ADMIN` role in order to configure the Oracle GoldenGate.
- The user must be granted the `DV_GOLDENGATE_REDO_ACCESS` role if the user must use the Oracle GoldenGate `TRANLOGOPTIONS DBLOGREADER` method to access redo logs.

For example, to grant the `DV_GOLDENGATE_ADMIN` and `DV_GOLDENGATE_REDO_ACCESS` roles to a user named `gg_admin`:

```
GRANT DV_GOLDENGATE_ADMIN, DV_GOLDENGATE_REDO_ACCESS TO gg_admin;
```

- The user must be granted the `DV_ACCTMGR` role before this user can create users on the replicated side.
- Before users can apply changes to any tables that are protected by a realm, they must be authorized to have access to that realm. For example:

```
EXEC DBMS_MACADM.ADD_AUTH_TO_REALM('realm_name','username');
```

- The `SYS` user must be authorized to perform Data Definition Language (DDL) operations in the `SYSTEM` schema, as follows:
- The user must be granted authorization to the Oracle Default Component Protection Realm. For example, to grant this realm authorization to a user named `gg_admin`:

```
EXECUTE DVSYS.DBMS_MACADM.AUTHORIZE_DDL('SYS', 'SYSTEM');
```

```
BEGIN
DVSYS.DBMS_MACADM.ADD_AUTH_TO_REALM(
  REALM_NAME => 'Oracle Default Component Protection Realm',
  GRANTEE    => 'gg_admin',
  AUTH_OPTIONS => 1);
END;
```

### Related Topics:

[DV\\_GOLDENGATE\\_ADMIN GoldenGate Administrative Role](#) (page 14-17)

The `DV_GOLDENGATE_ADMIN` role is used with Oracle GoldenGate.

[DV\\_GOLDENGATE\\_REDO\\_ACCESS GoldenGate Redo Log Role](#) (page 14-18)

The `DV_GOLDENGATE_REDO_ACCESS` role is used with Oracle GoldenGate.

[ADD\\_AUTH\\_TO\\_REALM Procedure](#) (page 15-2)

The `ADD_AUTH_TO_REALM` procedure authorizes a user or role to access a realm as an owner or a participant. In a multitenant environment, you can authenticate both common and local realms.



## 13.9 Using Data Masking in an Oracle Database Vault Environment

You must have the correct authorization to perform data masking in an Oracle Database Vault environment.

[About Data Masking in an Oracle Database Vault Enabled Database](#)  
(page 13-21)

In an Oracle Database Vault-enabled database, only users who have Database Vault authorizations can mask data in Database Vault-protected database objects.

[Adding Data Masking Users to the Data Dictionary Realm Authorizations](#)  
(page 13-21)

You can add data masking users to the Oracle Default Component Protection realm to give them data dictionary realm authorizations.

[Giving Users Access to Tables or Schemas That They Want to Mask](#) (page 13-22)

To give users access to tables or schemas that they want to mask, you must authorize them for the appropriate realm.

[Creating a Command Rule to Control Data Masking Privileges](#) (page 13-22)

You must have privileges to manage tables, packages, and triggers before you can use data masking in an Oracle Database Vault environment.

---



---

### See Also:

*Oracle Database Testing Guide* for more information about data masking

---



---

### 13.9.1 About Data Masking in an Oracle Database Vault Enabled Database

In an Oracle Database Vault-enabled database, only users who have Database Vault authorizations can mask data in Database Vault-protected database objects.

In a non-Database Vault environment, users who have been granted the `SELECT_CATALOG_ROLE` and `DBA` roles can perform data masking. However, with Database Vault, users must have additional privileges. This section describes three ways that you can use to enable users to mask data in Database Vault-protected objects.

If users do not have the correct privileges, then the following errors can occur while creating the masking definition or when the job is executing:

ORA-47400: Command Rule violation for string on string

ORA-47401: Realm violation for string on string.

ORA-47408: Realm violation for the EXECUTE command

ORA-47409: Command Rule violation for the EXECUTE command

ORA-01301: insufficient privileges

### 13.9.2 Adding Data Masking Users to the Data Dictionary Realm Authorizations

You can add data masking users to the Oracle Default Component Protection realm to give them data dictionary realm authorizations.

The Oracle Data Dictionary controls access to the Oracle Database catalog schemas, such as `SYS` and `SYSTEM`. (See [Default Realms](#) (page 5-5) for a full list of these schemas.) It also controls the ability to grant system privileges and database administrator roles. If you add users to the Oracle Default Component Protection realm, and assuming these users already have the privileges associated with the Oracle Data Dictionary, then these users will have these same privileges in a Database Vault environment. Therefore, if you do add a user to this realm, ensure that this user is a trusted user.

- To add a user to the Oracle Default Component Protection realm, use the `DBMS_MACADM.ADD_AUTH_TO_REALM` procedure.

For example:

```
BEGIN
  DBMS_MACADM.ADD_AUTH_TO_REALM(
    realm_name => 'Oracle Default Component Protection Realm',
    grantee    => 'DBA_JSMITH',
    auth_options => DBMS_MACUTL.G_REALM_AUTH_PARTICIPANT);
END;
/
```

### 13.9.3 Giving Users Access to Tables or Schemas That They Want to Mask

To give users access to tables or schemas that they want to mask, you must authorize them for the appropriate realm.

If the table or schema of a table that is to be data masked is in a realm, then you must add the user responsible for data masking to the realm authorization as a participant or owner. If the table or schema has dependent objects that are in other realm-protected tables, then you must grant the user participant or owner authorization for those realms as well.

- To authorize users for data masking to a realm that protects the objects they want to data mask, use the `DBMS_MACADM.ADD_AUTH_TO_REALM` procedure.

The following example shows how to grant user `DBA_JSMITH` authorization for the `HR.EMPLOYEES` table, which is protected by a realm called Business Apps Realm:

```
BEGIN
  DBMS_MACADM.ADD_AUTH_TO_REALM(
    realm_name => 'Business Apps Realm',
    grantee    => 'DBA_JSMITH',
    auth_options => DBMS_MACUTL.G_REALM_AUTH_PARTICIPANT);
END;
/
```

### 13.9.4 Creating a Command Rule to Control Data Masking Privileges

You must have privileges to manage tables, packages, and triggers before you can use data masking in an Oracle Database Vault environment.

For data masking, users must have the `CREATE TABLE`, `SELECT TABLE`, `ALTER TABLE`, and `DROP TABLE` privileges for the masking objects and if there are any dependent objects to be created, the user must have the appropriate privileges such as `CREATE PACKAGE`, `CREATE TRIGGER`, and so on.

You can create command rules to control data masking privileges at a granular level. To do so, create a command rule that can either prevent or allow the user access to objects that must have to be data masked. For example, you can create a command

rule called Allow Data Masking that checks if the user is in a list of users who are responsible for data masking. If the user logging in is one of these users, then the command rule evaluates to true and the user is permitted to create the data mask for the protected object.

To create a command rule that controls data masking privileges:

1. Create the rule set rule.

For example:

```
BEGIN
DBMS_MACADM.CREATE_RULE(
  rule_name => 'Is HDRISCOLL or DBA_JSMITH User',
  rule_expr => 'USER IN(''HDRISCOLL'', ''DBA_JSMITH'')';
END;
/
```

2. Create a rule set and then add the rule to it:

```
BEGIN
DBMS_MACADM.CREATE_RULE_SET(
  rule_set_name => 'Allow Data Masking',
  description   => 'Allows users HDRISCOLL and DBA_JSMITH access',
  enabled       => 'Y',
  eval_options  => 1,
  audit_options => 1,
  fail_options  => 1,
  fail_message  => 'You do not have access to this object.',
  fail_code     => 20461,
  handler_options => 0,
  is_static     => TRUE);
END;
/
BEGIN
DBMS_MACADM.ADD_RULE_TO_RULE_SET(
  rule_set_name => 'Allow Data Masking',
  rule_name     => 'Is HDRISCOLL or DBA_JSMITH User'),
  rule_order    => 1);
END;
/
```

3. Create a command rule and then add this rule to it:

```
BEGIN
DBMS_MACADM.CREATE_COMMAND_RULE(
  command       => 'CREATE TABLE',
  rule_set_name => 'Allow Data Masking',
  object_owner  => 'HR',
  object_name   => 'EMPLOYEES',
  enabled       => DBMS_MACUTL.G_YES);
END;
/
```

## 13.10 Plugging a Database Vault-Enabled PDB to a CDB

You can plug a legacy Database Vault-enabled PDB to a multitenant container database (CDB).

1. Connect to the root as a user who has been granted the DV\_OWNER role.

For example:

```
sqlplus c##sec_admin
Enter password: password
```

- Grant the DV\_PATCH\_ADMIN role to user SYS with CONTAINER = CURRENT.

```
GRANT DV_PATCH_ADMIN TO SYS CONTAINER = CURRENT;
```

- In the root, connect as user SYS with the SYSOPER system privilege.

For example:

```
CONNECT SYS AS SYSOPER -- Or, CONNECT SYS@hrpdb AS SYSOPER
Enter password: password
```

- Restart the database in read-only mode.

For example:

```
SHUTDOWN IMMEDIATE
STARTUP MOUNT
ALTER DATABASE OPEN READ ONLY
```

- Connect to the Database Vault-enabled database as a user who has the DV\_OWNER role.

For example:

```
CONNECT sec_admin@dv_db
```

- Grant the DV\_PATCH\_ADMIN role to user SYS on this database.

```
GRANT DV_PATCH_ADMIN TO SYS;
```

- Optionally, run the DBMS\_PDB.CHECK\_PLUG\_COMPATIBILITY function to determine whether the unplugged PDB is compatible with the CDB.

When you run the function, set the following parameters:

- `pdb_descr_file`: Set this parameter to the full path to the XML file that will contain a description of the PDB.
- `store_report`: Set this parameter to indicate whether you want to generate a report if the PDB is not compatible with the CDB. Set it to `TRUE` to generate a report or `FALSE` to not generate a report. A generated report is stored in the `PDB_PLUG_IN_VIOLATIONS` temporary table and is generated only if the PDB is not compatible with the CDB.

For example, to determine whether a PDB described by the `/disk1/usr/dv_db_pdb.xml` file is compatible with the current CDB, run the following PL/SQL block:

```
SET SERVEROUTPUT ON
DECLARE
  compatible CONSTANT VARCHAR2(3) :=
    CASE DBMS_PDB.CHECK_PLUG_COMPATIBILITY(
      pdb_descr_file => '/disk1/usr/dv_db_pdb.xml',
      store_report   => TRUE)
    WHEN TRUE THEN 'YES'
    ELSE 'NO'
  END;
BEGIN
  DBMS_OUTPUT.PUT_LINE(compatible);
```

```
END;
/
```

If the output is YES, then the PDB is compatible, and you can continue with the next step.

If the output is NO, then the PDB is not compatible. You can check the PDB\_PLUG\_IN\_VIOLATIONS temporary table to see why it is not compatible.

**8. Create an XML file that describes the PDB.**

For example:

```
BEGIN
  DBMS_PDB.DESCRIBE(
    pdb_descr_file => '/disk1/oracle/dv_db.xml');
END;
/
```

**9. Run the CREATE PLUGGABLE DATABASE statement, and specify the XML file in the USING clause. Specify other clauses when they are required.**

For example:

```
CREATE PLUGGABLE DATABASE dv_db_pdb AS CLONE USING 'dv_db.xml' NOCOPY;
```

**10. Connect to the PDB that you just created as user SYS with the SYSDBA administrative privilege.**

```
CONNECT SYS@dv_db_pdb AS SYSDBA
```

**11. Execute the noncdb\_to\_pdb.sql script.**

```
@$ORACLE_HOME/rdbms/admin/noncdb_to_pdb.sql
```

**12. Open this PDB in a read-write restricted mode.**

```
ALTER PLUGGABLE DATABASE dv_db_pdb OPEN READ WRITE RESTRICTED;
```

**13. Run the following procedure to synchronize the PDB:**

```
EXECUTE DBMS_PDB.SYNC_PDB;
```

**14. Connect to the root as a user who has been granted the DV\_OWNER role.**

```
sqlplus c##sec_admin
Enter password: password
```

**15. Revoke the DV\_PATCH\_ADMIN role from user SYS with CONTAINER = CURRENT.**

```
REVOKE DV_PATCH_ADMIN FROM SYS CONTAINER = CURRENT;
```

**16. Connect to the legacy Database Vault-enabled database as user SYS with the SYSOPER system privilege.**

```
CONNECT SYS@dv_db_pdb AS SYSOPER
```

**17. Restart this database.**

For example:

```
SHUTDOWN IMMEDIATE
STARUP
```

18. Revoke the DV\_PATCH\_ADMIN role from user SYS.

```
REVOKE DV_PATCH_ADMIN FROM SYS;
```

## 13.11 Using the ORADEBUG Utility with Oracle Database Vault

The ORADEBUG utility is used primarily by Oracle Support to diagnose problems that may arise with an Oracle database.

You can control whether users can run the ORADEBUG utility in an Oracle Database Vault-enabled environment.

1. Log into the database instance as a user who has been granted the DV\_OWNER or DV\_ADMIN role.
2. If necessary, find out if ORADEBUG is already disabled or enabled.

```
SELECT * FROM DBA_DV_ORADEBUG;
```

3. Run one of the following procedures:

- To disable the use of ORADEBUG:

```
EXEC DBMS_MACADM.DISABLE_ORADEBUG;
```

- To enable the use of ORADEBUG:

```
EXEC DBMS_MACADM.ENABLE_ORADEBUG;
```

### Related Topics:

#### [DBA\\_DV\\_ORADEBUG View](#) (page 25-18)

The DBA\_DV\_ORADEBUG data dictionary view indicates whether users can use the ORADEBUG utility in an Oracle Database Vault environment.

#### [DISABLE\\_ORADEBUG Procedure](#) (page 22-15)

The DISABLE\_ORADEBUG procedure disables the use of the ORADEBUG utility in an Oracle Database Vault environment.

#### [ENABLE\\_ORADEBUG Procedure](#) (page 22-17)

The ENABLE\_ORADEBUG procedure enables the use of the ORADEBUG utility in an Oracle Database Vault environment.

---

# Oracle Database Vault Schemas, Roles, and Accounts

Oracle Database Vault provides schemas that contain Database Vault objects, roles that provide separation of duty for specific tasks, and default user accounts.

[Oracle Database Vault Schemas](#) (page 14-1)

The Oracle Database Vault schemas, *DVSY*S and *DVF*, support the administration and run-time processing of Oracle Database Vault.

[Oracle Database Vault Roles](#) (page 14-3)

Oracle Database Vault provides default roles that are based on specific user tasks and adhere to separation of duty concepts.

[Oracle Database Vault Accounts Created During Registration](#) (page 14-23)

You must create accounts for the Oracle Database Vault Owner and Oracle Database Vault Account Manager during the registration process.

[Backup Oracle Database Vault Accounts](#) (page 14-25)

As a best practice, you should maintain backup accounts for the *DV\_OWNER* and *DV\_ACCTMGR* roles.

## 14.1 Oracle Database Vault Schemas

The Oracle Database Vault schemas, *DVSY*S and *DVF*, support the administration and run-time processing of Oracle Database Vault.

[DVSY](#)S Schema (page 14-1)

The *DVSY*S schema contains Oracle Database Vault database objects.

[DVF](#) Schema (page 14-2)

The *DVF* schema is the owner of the Oracle Database Vault *DBMS\_MACSEC\_FUNCTION* PL/SQL package.

### 14.1.1 DVSY

S Schema

The *DVSY*S schema contains Oracle Database Vault database objects.

These objects store Oracle Database Vault configuration information and support the administration and run-time processing of Oracle Database Vault.

In a default installation, the *DVSY*S schema is locked. The *DVSY*S schema also owns the *AUDIT\_TRAIL*\$ table.

In a multitenant environment, the *DVSY*S schema is considered a common schema, which means that the objects within *DVSY*S (tables, views, PL/SQL packages, and so on) are automatically available to any child pluggable databases (PDBs). In addition, the *DVSY*S schema account cannot switch to other containers using the *ALTER SESSION* statement.

Oracle Database Vault secures the `DVSYS` schema by using a protected schema design. A protected schema design guards the schema against improper use of system privileges (for example, `SELECT ANY TABLE`, `CREATE ANY VIEW`, or `DROP ANY`).

Oracle Database Vault protects and secures the `DVSYS` schema in the following ways:

- The `DVSYS` protected schema and its administrative roles cannot be dropped. By default, the `DVSYS` account is locked.
- By default, users cannot directly log into the `DVSYS` account. To control the ability of users to directly log into this account, you can run the `DBMS_MACADM.DISABLE_DV_DICTIONARY_ACCTS` procedure to prevent users from logging in and the `DBMS_MACADM.ENABLE_DV_DICTIONARY_ACCTS` procedure to allow users to log in.
- Statements such as `CREATE USER`, `ALTER USER`, `DROP USER`, `CREATE PROFILE`, `ALTER PROFILE`, and `DROP PROFILE` can only be issued by a user with the `DV_ACCTMGR` role. A user logged in with the `SYSDBA` administrative privilege can issue these statements only if it is allowed to do so by modifying the Can Maintain Accounts/Profiles rule set.
- The powerful `ANY` system privileges for database definition language (DDL) and data manipulation language (DML) commands are blocked in the protected schema. This means that the objects in the `DVSYS` schema must be created by the schema account itself. Also, access to the schema objects must be authorized through object privilege grants.
- Object privileges in the `DVSYS` schema can only be granted to Database Vault administrative roles in the schema. This means that users can access the protected schema only through predefined administrative roles.
- Only the protected schema account `DVSYS` can issue `ALTER ROLE` statements on Database Vault predefined administrative roles of the schema. [Oracle Database Vault Roles](#) (page 14-3) describes Oracle Database Vault predefined administrative roles in detail.
- The `SYS.DBMS_SYS_SQL.PARSE_AS_USER` procedure cannot be used to run SQL statements on behalf of the protected schema `DVSYS`.

---

---

**Note:**

Database users can grant additional object privileges and roles to the Oracle Database Vault administrative roles (`DV_ADMIN` and `DV_OWNER`, for example) provided they have sufficient privileges to do so.

---

---

## 14.1.2 DVF Schema

The `DVF` schema is the owner of the Oracle Database Vault `DBMS_MACSEC_FUNCTION` PL/SQL package.

This package contains the functions that retrieve factor identities. After you install Oracle Database Vault, the installation process locks the `DVF` account to better secure it. When you create a new factor, Oracle Database Vault creates a new retrieval function for the factor and saves it in this schema.

In a multitenant environment, the `DVF` user cannot switch to other containers using the `ALTER SESSION` statement.



By default, users cannot directly log into the DVF account. To control the ability of users to directly log into this account, you can run the `DBMS_MACADM.DISABLE_DV_DICTIONARY_ACCTS` procedure to prevent users from logging in and the `DBMS_MACADM.ENABLE_DV_DICTIONARY_ACCTS` procedure to allow users to log in.

## 14.2 Oracle Database Vault Roles

Oracle Database Vault provides default roles that are based on specific user tasks and adhere to separation of duty concepts.

### [About Oracle Database Vault Roles](#) (page 14-4)

Oracle Database Vault provides a set of roles that are required for managing Oracle Database Vault.

### [Privileges of Oracle Database Vault Roles](#) (page 14-6)

The Oracle Database Vault roles are designed to provide the maximum benefits of separation of duty.

### [Granting Oracle Database Vault Roles to Users](#) (page 14-8)

You can use Enterprise Manager Cloud Control to grant Oracle Database Vault roles to users.

### [DV\\_OWNER Database Vault Owner Role](#) (page 14-9)

The `DV_OWNER` role enables you to manage the Oracle Database Vault roles and its configuration.

### [DV\\_ADMIN Database Vault Configuration Administrator Role](#) (page 14-11)

The `DV_ADMIN` role controls the Oracle Database Vault PL/SQL packages.

### [DV\\_MONITOR Database Vault Monitoring Role](#) (page 14-12)

The `DV_MONITOR` role is used for monitoring Oracle Database Vault.

### [DV\\_SECANALYST Database Vault Security Analyst Role](#) (page 14-13)

The `DV_SECANALYST` role enables users to analyze activities.

### [DV\\_AUDIT\\_CLEANUP Audit Trail Cleanup Role](#) (page 14-13)

The `DV_AUDIT_CLEANUP` role is used for purge operations.

### [DV\\_DATAPUMP\\_NETWORK\\_LINK Data Pump Network Link Role](#) (page 14-14)

The `DV_DATAPUMP_NETWORK_LINK` role is used for Data Pump import operations.

### [DV\\_STREAMS\\_ADMIN Oracle Streams Configuration Role](#) (page 14-15)

The `DV_STREAMS_ADMIN` role is used with Oracle Streams.

### [DV\\_XSTREAM\\_ADMIN XStream Administrative Role](#) (page 14-16)

The `DV_XSTREAM_ADMIN` role is used for Oracle XStream.

### [DV\\_GOLDENGATE\\_ADMIN GoldenGate Administrative Role](#) (page 14-17)

The `DV_GOLDENGATE_ADMIN` role is used with Oracle GoldenGate.

### [DV\\_GOLDENGATE\\_REDO\\_ACCESS GoldenGate Redo Log Role](#) (page 14-18)

The `DV_GOLDENGATE_REDO_ACCESS` role is used with Oracle GoldenGate.

### [DV\\_PATCH\\_ADMIN Database Vault Database Patch Role](#) (page 14-18)

The `DV_PATCH_ADMIN` role is used for patching operations.

[DV\\_ACCTMGR Database Vault Account Manager Role](#) (page 14-19)

The DV\_ACCTMGR role is a powerful role, used for accounts management.

[DV\\_REALM\\_OWNER Database Vault Realm DBA Role](#) (page 14-21)

The DV\_REALM\_OWNER role is used for realm management.

[DV\\_REALM\\_RESOURCE Database Vault Application Resource Owner Role](#) (page 14-21)

The DV\_REALM\_RESOURCE role is use for the management of realm resources.

[DV\\_POLICY\\_OWNER Database Vault Owner Role](#) (page 14-22)

The DV\_POLICY\_OWNER role enables database users to manage to a limited degree Oracle Database Vault policies.

[DV\\_PUBLIC Database Vault PUBLIC Role](#) (page 14-23)

The DV\_PUBLIC role is no longer used.

## 14.2.1 About Oracle Database Vault Roles

Oracle Database Vault provides a set of roles that are required for managing Oracle Database Vault.

[Figure 14-1](#) (page 14-5) illustrates how these roles are designed to implement the first level of separation of duties within the database. How you use these roles depends on the requirements that your company has in place.

**Figure 14-1 How Oracle Database Vault Roles Are Categorized**

<b>Security administrative roles</b>	DV_OWNER DV_ADMIN DV_MONITOR DV_SECANALYST DV_PATCH_ADMIN DV_DATAPUMP_NETWORK_LINK	DV_STREAMS_ADMIN DV_XSTREAM_ADMIN DV_GOLDENGATE_ADMIN DV_GOLDENGATE_REDO_ACCESS DV_AUDIT_CLEANUP
<b>Account management responsibility role</b>	DV_ACCTMGR	
<b>Resource management roles</b>	DV_REALM_OWNER (for application management and granted to realm owners) DV_REALM_RESOURCE (for application access and granted to realm participants) DV_POLICY_OWNER	
<b>All responsibilities</b>	DV_PUBLIC (granted by default to all database users to give access to the Oracle Database Vault public functions)	

**Note:**

You can grant additional object privileges and roles to the Oracle Database Vault roles to extend their scope of privileges. For example, a user logged in with the `SYSDBA` administrative privilege can grant object privileges to an Oracle Database Vault role as long as the object is not in the `DVSYs` schema or realm.

**See Also:**

- [Separation of Duty Guidelines](#) (page D-1)
- [Managing Oracle Database Administrative Accounts](#) (page D-5)
- *Oracle Database Security Guide*

## 14.2.2 Privileges of Oracle Database Vault Roles

The Oracle Database Vault roles are designed to provide the maximum benefits of separation of duty.

The DV\_PATCH\_ADMIN, DV\_STREAMS\_ADMIN, DV\_XSTREAM, DV\_GOLDENGATE\_ADMIN, and DV\_GOLDENGATE\_REDO\_ACCESS roles are not included in the following table because they have no system privileges.

Table 14-1 (page 14-6) summarizes the privileges available with Oracle Database Vault roles.

**Table 14-1 Privileges of Oracle Database Vault Roles**

Privilege	DV_O WNER	DV_A DMIN	DV_MO NITOR	DV_SECAN ALYST	DV_ACC TMGR	DV_RE ALM_O WNER	DV_REAL M_RESO URCE	DV_PU BLIC	DV_PO LIC_Y_ OWNE R	DV_AUD IT_CLE ANUP
DVSYSSchema, EXECUTE	Yes <sup>1</sup>	Yes <sup>2</sup>	No	No	No	No	No	No	Yes, on some DBMS_MACADM procedures	No
DVSYSSchema, SELECT	Yes	Yes	Yes	Yes, on some Database Vault views <sup>3</sup>	No	No	No	No <sup>4</sup>	Yes, on some Database Vault views <sup>5</sup>	Yes, on some Database Vault tables and views <sup>6</sup>
DVSYSSchema, DELETE	Yes, on some Database Vault tables and views <sup>7</sup>	No	No	No	No	No	No	No	No	Yes, on some Database Vault tables and views <sup>8</sup>
DVSYSSchema, grant privileges on objects	No	No	No	No	No	No	No	No	No	No
DVFSchema, EXECUTE	Yes	No	No	No	No	No	No	No	No	No

**Table 14-1 (Cont.) Privileges of Oracle Database Vault Roles**

Privilege	DV_O WNER	DV_A DMIN	DV_MO NITOR	DV_SECAN ALYST	DV_ACC TMGR	DV_RE ALM_O WNER	DV_REAL M_RESO URCE	DV_PU BLIC	DV_PO LICY_ OWNE R	DV_AUD IT_CLE ANUP
DVF schema, SELECT	Yes	No	No	Yes	No	No	No	No	No	No
Monitor Database Vault	Yes	Yes	Yes	Yes	No	No	No	No	No	No
Run Database Vault reports	Yes	Yes	No	Yes	No	No	No	No	No	No
SYS schema, SELECT	Yes	No	Yes	Yes, on the same system views as DV_OWNER and DV_ADMIN	No	No	No	No	No	No
SYSMAN schema, SELECT	Yes, portio ns of	No	No	Yes, portions of	No	No	No	No	No	No
CREATE, ALTER, DROP user account s and profiles <sup>9</sup>	No	No	No	No	Yes	No	No	No	No	No
Manage objects in schemas that define a realm <sup>10</sup>	No	No	No	No	No	Yes <sup>11</sup>	No	No	No	No
RESOUR CE role privileg es <sup>12</sup>	No	No	No	No	No	No	Yes	No	No	No

<sup>1</sup> Includes the EXECUTE privilege on all Oracle Database Vault PL/SQL packages.

<sup>2</sup> Includes the EXECUTE privilege on all Oracle Database Vault PL/SQL packages.

<sup>3</sup> DV\_SECANALYST can query DVSYS schema objects through Oracle Database Vault-supplied views only.

<sup>4</sup> DV\_PUBLIC can query DVSYS schema objects through Oracle Database Vault-supplied views only.

<sup>5</sup> POLICY\_OWNER\* views only

<sup>6</sup> DV\_AUDIT\_CLEANUP can perform SELECT statements on the AUDIT\_TRAIL\$ table and the DV\$ENFORCEMENT\_AUDIT, and DV\$CONFIGURATION\_AUDIT views.

- 7 DV\_AUDIT\_CLEANUP can perform DELETE statements on the AUDIT\_TRAIL,\$ table and the DV \$ENFORCEMENT\_AUDIT, and DV\$CONFIGURATION\_AUDIT views.
- 8 DV\_AUDIT\_CLEANUP can perform DELETE statements on the AUDIT\_TRAIL,\$ table and the DV \$ENFORCEMENT\_AUDIT, and DV\$CONFIGURATION\_AUDIT views.
- 9 This privilege does not include the ability to drop or alter the DVSYS account, nor change the DVSYS password.
- 1 This privilege includes ANY privileges, such as CREATE ANY, ALTER ANY, and DROP ANY.
- 0
- 1 The user with this role also must be the realm participant or owner to exercise his or her system privileges.
- 1
- 1 The RESOURCE role provides the following system privileges: CREATE CLUSTER, CREATE INDEXTYPE, CREATE OPERATOR, CREATE PROCEDURE, CREATE SEQUENCE, CREATE TABLE, CREATE TRIGGER, CREATE TYPE.
- 2

### 14.2.3 Granting Oracle Database Vault Roles to Users

You can use Enterprise Manager Cloud Control to grant Oracle Database Vault roles to users.

1. From Cloud Control, log into Oracle Database Vault Administrator as a user who has been granted the DV\_OWNER role and the SELECT ANY DICTIONARY privilege..

[Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.

Refer to the role descriptions to find the requirements for who can grant roles to other users.

2. In the Administration page, under Database Vault Components, click **Database Vault Role Management**.

The Database Vault Role Management page appears.

**Database Vault Role Management**

This page displays users or roles granted with Database Vault roles.

**Search**

Grantee

The search returns all matches beginning with the string you enter. You can use the wildcard symbol (%) in the search string.

View ▼

Grantee	Grantee Type	DV_OWNER	DV_ADMIN	DV_MONITOR	DV_S
DBSNMP	USER			✓	
MACAUTH	USER				
MACSYS	USER	✓	✓	✓	
SYS	USER				

3. Do one of the following:
  - To add a new user or role for a grant, click the Add button to display the Add Authorization dialog box. Enter the grantee in the **Grantee** field, and then select the roles for the grant. Then click **OK**.

- To grant different roles or modify role grants for a user or role listed in the Database Vault Role Management page, select the user or role, click **Edit**, and then modify the role grants as necessary. Then click **OK**.

#### 14.2.4 DV\_OWNER Database Vault Owner Role

The DV\_OWNER role enables you to manage the Oracle Database Vault roles and its configuration.

In *Oracle Database Vault Administrator's Guide*, the example account that uses this role is `leo_dvowner`.

##### Privileges Associated with the DV\_OWNER Role

The DV\_OWNER role has the administrative capabilities that the DV\_ADMIN role provides, and the reporting capabilities the DV\_SECANALYST role provides.

This role also provides privileges for monitoring Oracle Database Vault. It is created when you install Oracle Database Vault, and has the most privileges on the DVSYS schema. In addition to DV\_ADMIN role, the DV\_OWNER role has the GRANT ANY ROLE, ADMINISTER DATABASE TRIGGER, and ALTER ANY TRIGGER privileges.

To find the full list of system and object privileges associated with the DV\_OWNER role, you can log into the database instance and enter the following queries:

```
SELECT TABLE_NAME, OWNER, PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE = 'DV_OWNER';
SELECT PRIVILEGE FROM DBA_SYS_PRIVS WHERE GRANTEE = 'DV_OWNER';
```

When you install and register Oracle Database Vault, the DV\_OWNER account is created. The user who is granted this role is also granted the ADMIN option and can grant any Oracle Database Vault roles (except DV\_ACCTMGR) to any account. Users granted this role also can run Oracle Database Vault reports and monitor Oracle Database Vault.

**Tip:**

Oracle strongly recommends that you create separate, named account for the DV\_OWNER user. This way, if the user is no longer available (for example, he or she left the company), then you can easily recreate this user account and then grant this user the DV\_OWNER role.

**How Are GRANT and REVOKE Operations Affected by DV\_OWNER?**

Anyone with the DV\_OWNER role can grant the DV\_OWNER and DV\_ADMIN roles to another user.

The account granted this role can revoke any granted Database Vault role from another account. Accounts such as SYS or SYSTEM, with the GRANT ANY ROLE system privilege alone (directly granted or indirectly granted using a role) do not have the right to grant or revoke the DV\_OWNER role to or from any other database account. Note also that a user with the DV\_OWNER role cannot grant or revoke the DV\_ACCTMGR role.

**Managing Password Changes for Users Who Have the DV\_OWNER Role**

Before you can change the password for another user who has been granted the DV\_OWNER role, you must revoke the DV\_OWNER role from that user account.

However, be cautious about revoking the DV\_OWNER role. At least one user on your site must have this role granted. If another DV\_OWNER user has been granted this role and needs to have his or her password changed, then you can temporarily revoke DV\_OWNER from that user. Note also that if you have been granted the DV\_OWNER role, then you can change your own password without having to revoke the role from yourself.

To change the DV\_OWNER user password:

1. Log into the database instance using an account that has been granted the DV\_OWNER role.
2. Revoke the DV\_OWNER role from the user account whose password needs to change.
3. Connect as a user who has been granted the DV\_ACCTMGR role and then change the password for this user.
4. Connect as the DV\_OWNER user and then grant the DV\_OWNER role back to the user whose password you changed.

**DV\_OWNER Status When Oracle Database Vault Security Is Disabled**

The protection of all Oracle Database Vault roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the GRANT ANY ROLE system privilege can perform GRANT and REVOKE operations on protected Database Vault roles.

**Related Topics:**

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.



## 14.2.5 DV\_ADMIN Database Vault Configuration Administrator Role

The DV\_ADMIN role controls the Oracle Database Vault PL/SQL packages.

These packages are the underlying interface for the Database Vault Administrator user interface in Oracle Enterprise Manager Cloud Control.

### Privileges Associated with the DV\_ADMIN Role

The DV\_ADMIN role has the EXECUTE privilege on the DVSYS packages (DBMS\_MACADM, DBMS\_MACSECROLES, and DBMS\_MACUTL).

DV\_ADMIN also has the capabilities provided by the DV\_SECANALYST role, which allow the user to run Oracle Database Vault reports and monitor Oracle Database Vault. During installation, the DV\_ADMIN role is granted to the DV\_OWNER role with the ADMIN OPTION.

In addition, the DV\_ADMIN role provides the SELECT privilege on the DBA\_DV\_POLICY, DBA\_DV\_POLICY\_OWNER, and DBA\_DV\_POLICY\_OBJECT data dictionary views. The DV\_ADMIN role also has the REGISTER SESSION system privilege.

To find the full list of system and object privileges associated with the DV\_ADMIN role, log into the database instance with sufficient privileges and then enter the following queries:

```
SELECT TABLE_NAME, OWNER, PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE = 'DV_ADMIN';
SELECT PRIVILEGE FROM DBA_SYS_PRIVS WHERE GRANTEE = 'DV_ADMIN';
```

### How Are GRANT and REVOKE Operations Affected by DV\_ADMIN?

Accounts such as SYS or SYSTEM, with the GRANT ANY ROLE system privilege alone do not have the rights to grant or revoke DV\_ADMIN from any other database account.

The user with the DV\_OWNER role can grant or revoke this role to and from any database account.

### Managing Password Changes for Users Who Have the DV\_ADMIN Role

Before you can change the password for a user who has been granted the DV\_ADMIN role, you must revoke the DV\_ADMIN role from this account.

If you have been granted the DV\_ADMIN role, then you can change your own password without having to revoke the role from yourself.

To change the DV\_ADMIN user password:

1. Log into the database instance using an account that has been granted the DV\_OWNER role.
2. Revoke the DV\_ADMIN role from the user account whose password needs to change.
3. Connect as a user who has been granted the DV\_ACCTMGR role and then change the password for this user.
4. Connect as the DV\_OWNER user and then grant the DV\_ADMIN role back to the user whose password you changed.

### DV\_ADMIN Status When Oracle Database Vault Security Is Disabled

The protection of all Oracle Database Vault roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the `GRANT ANY ROLE` system privilege can perform `GRANT` and `REVOKE` operations on protected Database Vault roles.

**Related Topics:**

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

## 14.2.6 DV\_MONITOR Database Vault Monitoring Role

The `DV_MONITOR` role is used for monitoring Oracle Database Vault.

The `DV_MONITOR` role enables the Oracle Enterprise Manager Cloud Control agent to monitor Oracle Database Vault for attempted violations and configuration issues with realm or command rule definitions.

This role enables Cloud Control to read and propagate realm definitions and command rule definitions between databases.

**Privileges Associated with the DV\_MONITOR Role**

There are no system privileges associated with the `DV_MONITOR` role, but it does have the `SELECT` privilege on `SYS` and `DVSYS` objects.

In addition, the `DV_MONITOR` role provides the `SELECT` privilege on the `DBA_DV_POLICY`, `DBA_DV_POLICY_OWNER`, and `DBA_DV_POLICY_OBJECT` data dictionary views.

To find the full list of `DV_MONITOR` object privileges, log into the database instance with sufficient (such as `DV_OWNER`) privileges and then enter the following query:

```
SELECT TABLE_NAME, OWNER, PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE = 'DV_MONITOR';
```

**How Are GRANT and REVOKE Operations Affected by DV\_MONITOR?**

By default, the `DV_MONITOR` role is granted to the `DV_OWNER` role and the `DBSNMP` user.

Only a user who has been granted the `DV_OWNER` role can grant or revoke the `DV_MONITOR` role to another user.

**DV\_MONITOR Status When Oracle Database Vault Security Is Disabled**

The protection of all Oracle Database Vault roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the `GRANT ANY ROLE` system privilege can perform `GRANT` and `REVOKE` operations on protected Database Vault roles.

**Related Topics:**

[Monitoring Oracle Database Vault](#) (page 26-1)

You can monitor Oracle Database Vault by checking for violations to the Database Vault configurations and by tracking changes to policies.

[Auditing Oracle Database Vault](#) (page A-1)

You can audit activities in Oracle Database Vault, such as changes to policy configurations.

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

## 14.2.7 DV\_SECANALYST Database Vault Security Analyst Role

The DV\_SECANALYST role enables users to analyze activities.

Use the DV\_SECANALYST role to run Oracle Database Vault reports and monitor Oracle Database Vault.

This role is also used for database-related reports. In addition, this role enables you to check the DVSYS configuration by querying the DVSYS views described in [Oracle Database Vault Data Dictionary Views](#) (page 25-1).

### Privileges Associated with the DV\_SECANALYST Role

There are no system privileges associated with the DV\_SECANALYST role, but it does have the SELECT privilege for some DVSYS schema objects and portions of the SYS and SYSMAN schema objects for reporting on DVSYS- and DVF-related entities.

In addition, the DV\_SECANALYST role provides the SELECT privilege on the DBA\_DV\_POLICY, DBA\_DV\_POLICY\_OWNER, and DBA\_DV\_POLICY\_OBJECT data dictionary views.

To find the full list of DV\_SECANALYST object privileges, log into the database instance with sufficient privileges and then enter the following query:

```
SELECT TABLE_NAME, OWNER, PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE =
'DV_SECANALYST' ;
```

### How Are GRANT and REVOKE Operations Affected by DV\_SECANALYST?

Any account, such as SYS or SYSTEM, with the GRANT ANY ROLE system privilege alone does not have the rights to grant this role to or revoke this role from any other database account.

Only the user with the DV\_OWNER role can grant or revoke this role to and from another user.

### DV\_SECANALYST Status When Oracle Database Vault Security Is Disabled

The protection of all Oracle Database Vault roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the GRANT ANY ROLE system privilege can perform GRANT and REVOKE operations on protected Database Vault roles.

### Related Topics:

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

## 14.2.8 DV\_AUDIT\_CLEANUP Audit Trail Cleanup Role

The DV\_AUDIT\_CLEANUP role is used for purge operations.

---

**Note:**

This feature has been updated in Oracle Database 12c release 1 (12.1.0.2).

---

Grant the `DV_AUDIT_CLEANUP` role to any user who is responsible for purging the Database Vault audit trail in a non-unified auditing environment.

[Archiving and Purging the Oracle Database Vault Audit Trail](#) (page A-6) explains how to use this role to complete a purge operation.

**Privileges Associated with the `DV_AUDIT_CLEANUP` Role**

The `DV_AUDIT_CLEANUP` role has `SELECT` and `DELETE` privileges for three Database Vault-related auditing views.

- `SELECT` and `DELETE` on the `DVSYS.AUDIT_TRAIL$` table
- `SELECT` and `DELETE` on the `DVSYS.DV$ENFORCEMENT_AUDIT` view
- `SELECT` and `DELETE` on the `DVSYS.DV$CONFIGURATION_AUDIT` view

**How Are `GRANT` and `REVOKE` Operations Affected by `DV_AUDIT_CLEANUP`?**

By default, this role is granted to the `DV_OWNER` role with the `ADMIN OPTION`.

Only a user who has been granted the `DV_OWNER` role can grant or revoke the `DV_AUDIT_CLEANUP` role to another user.

**`DV_AUDIT_CLEANUP` Status When Oracle Database Vault Security Is Disabled**

The protection of all Oracle Database Vault roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the `GRANT ANY ROLE` system privilege can perform `GRANT` and `REVOKE` operations on protected Database Vault roles.

**Related Topics:**

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

## 14.2.9 `DV_DATAPUMP_NETWORK_LINK` Data Pump Network Link Role

The `DV_DATAPUMP_NETWORK_LINK` role is used for Data Pump import operations.

Grant the `DV_DATAPUMP_NETWORK_LINK` role to any user who is responsible for conducting the `NETWORK_LINK` transportable Data Pump import operation in an Oracle Database Vault environment.

This role enables the management of the Oracle Data Pump `NETWORK_LINK` transportable import processes to be tightly controlled by Database Vault, but does not change or restrict the way you would normally conduct Oracle Data Pump operations.

**Privileges Associated with the `DV_DATAPUMP_NETWORK_LINK` Role**

There are no system privileges associated with the `DV_DATAPUMP_NETWORK_LINK` role, but it does have the `EXECUTE` privilege on `DVSYS` objects.

To find the full list of DV\_DATAPUMP\_NETWORK\_LINK object privileges, log into the database instance with sufficient privileges and then enter the following query:

```
SELECT TABLE_NAME, OWNER, PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE =
'DV_DATAPUMP_NETWORK_LINK' ;
```

Be aware that the DV\_DATAPUMP\_NETWORK\_LINK role does not provide a sufficient set of database privileges to conduct NETWORK\_LINK transportable Data Pump import operation. Rather, the DV\_DATAPUMP\_NETWORK\_LINK role is an additional requirement (that is, in addition to the privileges that Oracle Data Pump currently requires) for database administrators to conduct NETWORK\_LINK transportable Data Pump import operations in an Oracle Database Vault environment.

### **How Are GRANT and REVOKE Operations Affected by DV\_DATAPUMP\_NETWORK\_LINK?**

Only users who have been granted the DV\_OWNER role can grant or revoke the DV\_DATAPUMP\_NETWORK\_LINK role to or from other users.

### **DV\_DATAPUMP\_NETWORK\_LINK Status When Oracle Database Vault Security Is Disabled**

The protection of all Oracle Database roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the GRANT ANY ROLE system privilege can perform GRANT and REVOKE operations on protected Database Vault roles.

#### **Related Topics:**

[Using Oracle Data Pump with Oracle Database Vault](#) (page 13-5)

Database administrators can authorize Oracle Data Pump users to work in a Database Vault environment.

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

## **14.2.10 DV\_STREAMS\_ADMIN Oracle Streams Configuration Role**

The DV\_STREAMS\_ADMIN role is used with Oracle Streams.

Grant the DV\_STREAMS\_ADMIN role to any user who is responsible for configuring Oracle Streams in an Oracle Database Vault environment.

This enables the management of Oracle Streams processes to be tightly controlled by Database Vault, but does not change or restrict the way an administrator would normally configure Oracle Streams.

### **Privileges Associated with the DV\_STREAMS\_ADMIN Role**

There are no system privileges associated with the DV\_STREAMS\_ADMIN role, but it does have the SELECT privilege on DVSYS objects.

To find the full list of DV\_STREAMS\_ADMIN object privileges, log into the database instance with sufficient privileges and then enter the following query:

```
SELECT TABLE_NAME, OWNER, PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE =
'DV_STREAMS_ADMIN' ;
```

Be aware that the `DV_STREAMS_ADMIN` role does not provide a sufficient set of database privileges for configuring Oracle Streams. Rather, the `DV_STREAMS_ADMIN` role is an additional requirement (that is, in addition to the privileges that Oracle Streams currently requires) for database administrators to configure Oracle Streams in an Oracle Database Vault environment.

#### **How Are GRANT and REVOKE Operations Affected by DV\_STREAMS\_ADMIN?**

Only users who have been granted the `DV_OWNER` role can grant or revoke the `DV_STREAMS_ADMIN` role to or from other users.

#### **DV\_STREAMS\_ADMIN Status When Oracle Database Vault Security Is Disabled**

The protection of all Oracle Database roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the `GRANT ANY ROLE` system privilege can perform `GRANT` and `REVOKE` operations on protected Database Vault roles.

#### **Related Topics:**

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

### **14.2.11 DV\_XSTREAM\_ADMIN XStream Administrative Role**

The `DV_XSTREAM_ADMIN` role is used for Oracle XStream.

Grant the `DV_XSTREAM_ADMIN` role to any user who is responsible for configuring Oracle XStream in an Oracle Database Vault environment.

This enables the management of XStream processes to be tightly controlled by Database Vault, but does not change or restrict the way an administrator would normally configure XStream.

#### **Privileges Associated with the DV\_XSTREAM\_ADMIN Role**

There are no privileges associated with the `DV_XSTREAM_ADMIN` role.

Be aware that the `DV_XSTREAM_ADMIN` role does not provide a sufficient set of database privileges for configuring XStream. Rather, the `DV_XSTREAM_ADMIN` role is an additional requirement (that is, in addition to the privileges that XStream currently requires) for database administrators to configure XStream in an Oracle Database Vault environment.

#### **How Are GRANT and REVOKE Operations Affected by DV\_XSTREAM\_ADMIN?**

Only users who have been granted the `DV_OWNER` role can grant or revoke the `DV_XSTREAM_ADMIN` role to or from other users.

#### **DV\_XSTREAM\_ADMIN Status When Oracle Database Vault Security Is Disabled**

The protection of all Oracle Database roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the `GRANT ANY ROLE` system privilege can perform `GRANT` and `REVOKE` operations on protected Database Vault roles.

**Related Topics:**[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

[Privileges for Using XStream with Oracle Database Vault](#) (page 13-19)

If you want to use XStream in an Oracle Database Vault environment, then you must have the appropriate privileges.

**14.2.12 DV\_GOLDENGATE\_ADMIN GoldenGate Administrative Role**

The DV\_GOLDENGATE\_ADMIN role is used with Oracle GoldenGate.

Grant this to any user who is responsible for configuring Oracle GoldenGate in an Oracle Database Vault environment.

This enables the management of Oracle GoldenGate processes to be tightly controlled by Database Vault, but does not change or restrict the way an administrator would normally configure Oracle GoldenGate.

**Privileges Associated with the DV\_GOLDENGATE\_ADMIN Role**

There are no privileges associated with the DV\_GOLDENGATE\_ADMIN role.

Be aware that the DV\_GOLDENGATE\_ADMIN role does not provide a sufficient set of database privileges for configuring Oracle GoldenGate. Rather, the DV\_GOLDENGATE\_ADMIN role is an additional requirement (that is, in addition to the privileges that Oracle GoldenGate currently requires) for database administrators to configure Oracle GoldenGate in an Oracle Database Vault environment.

**How Are GRANT and REVOKE Operations Affected by DV\_GOLDENGATE\_ADMIN?**

Only users who have been granted the DV\_OWNER role can grant or revoke the DV\_GOLDENGATE\_ADMIN role to or from other users.

**DV\_GOLDENGATE\_ADMIN Status When Oracle Database Vault Security Is Disabled**

The protection of all Oracle Database roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the GRANT ANY ROLE system privilege can perform GRANT and REVOKE operations on protected Database Vault roles.

**Related Topics:**[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

[Privileges for Using Oracle GoldenGate in with Oracle Database Vault](#) (page 13-20)

If you want to use Oracle GoldenGate in an Oracle Database Vault environment, then you must have the appropriate privileges.

### 14.2.13 DV\_GOLDENGATE\_REDO\_ACCESS GoldenGate Redo Log Role

The DV\_GOLDENGATE\_REDO\_ACCESS role is used with Oracle GoldenGate.

Grant the DV\_GOLDENGATE\_REDO\_ACCESS role to any user who is responsible for using the Oracle GoldenGate `TRANLOGOPTIONS DBLOGREADER` method to access redo logs in an Oracle Database Vault environment.

This enables the management of Oracle GoldenGate processes to be tightly controlled by Database Vault, but does not change or restrict the way an administrator would normally configure Oracle GoldenGate.

#### Privileges Associated with the DV\_GOLDENGATE\_REDO\_ACCESS Role

There are no privileges associated with the DV\_GOLDENGATE\_REDO\_ACCESS role.

Be aware that the DV\_GOLDENGATE\_REDO\_ACCESS role does not provide a sufficient set of database privileges for configuring Oracle GoldenGate. Rather, the DV\_GOLDENGATE\_REDO\_ACCESS role is an additional requirement (that is, in addition to the privileges that Oracle GoldenGate currently requires) for database administrators to configure Oracle Streams in an Oracle Database Vault environment.

#### How Are GRANT and REVOKE Operations Affected by DV\_GOLDENGATE\_REDO\_ACCESS?

You cannot grant the DV\_GOLDENGATE\_REDO\_ACCESS role with `ADMIN OPTION`.

Only users who have been granted the DV\_OWNER role can grant or revoke the DV\_GOLDENGATE\_REDO\_ACCESS role to or from other users.

#### DV\_GOLDENGATE\_REDO\_ACCESS Status When Oracle Database Vault Security Is Disabled

The protection of all Oracle Database roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the `GRANT ANY ROLE` system privilege can perform `GRANT` and `REVOKE` operations on protected Database Vault roles.

#### Related Topics:

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

[Privileges for Using Oracle GoldenGate in with Oracle Database Vault](#) (page 13-20)

If you want to use Oracle GoldenGate in an Oracle Database Vault environment, then you must have the appropriate privileges.

### 14.2.14 DV\_PATCH\_ADMIN Database Vault Database Patch Role

The DV\_PATCH\_ADMIN role is used for patching operations.

In order to generate all Database Vault-related audit records in accordance with the audit policies specified in the Database Vault metadata as well as Database Vault unified audit policies, execute the

`DBMS_MACADM.ENABLE_DV_PATCH_ADMIN_AUDIT` procedure as a user who has been granted the DV\_ADMIN role before using the DV\_PATCH\_ADMIN role.



Temporarily grant the DV\_PATCH\_ADMIN role to any database administrator who is responsible for performing database patching. Before this administrator performs the patch operation, run the DBMS\_MACADM.ENABLE\_DV\_PATCH\_ADMIN\_AUDIT procedure. This procedure enables realm, command rule, and rule set auditing of the actions by users who have been granted the DV\_PATCH\_ADMIN role, in accordance with the existing audit configuration. If you have mixed-mode auditing, then this user's actions are written to the AUDIT\_TRAIL\$ table. If you have pure unified auditing enabled, then you should create a unified audit policy to capture this user's actions.

After the patch operation is complete, do not immediately disable the auditing of users who are responsible for performing database patch operations. This way, you can track the actions of the DV\_PATCH\_ADMIN role users. For backwards compatibility, this type of auditing is disabled by default.

### Privileges Associated with the DV\_PATCH\_ADMIN Role

The DV\_PATCH\_ADMIN role does not provide access to any secured data.

The DV\_PATCH\_ADMIN role is a special Database Vault role that does not have any object or system privilege. It is designed to allow the database administrator or the user SYS to patch Database Vault enabled databases (for example, applying a database patch without disabling Database Vault). It also enables the database administrator to create users, because some patches may require the need to create new schemas.

### How Are GRANT and REVOKE Operations Affected by DV\_PATCH\_ADMIN?

Only a user who has the DV\_OWNER role can grant or revoke the DV\_PATCH\_ADMIN role to and from another user.

### DV\_PATCH\_ADMIN Status When Oracle Database Vault Security Is Disabled

The protection of all Oracle Database roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the GRANT ANY ROLE system privilege can perform GRANT and REVOKE operations on protected Database Vault roles.

---

#### See Also:

- *Oracle Database Security Guide* for information about creating unified audit policies
  - [Disabling and Enabling Oracle Database Vault](#) (page B-1)
- 

## 14.2.15 DV\_ACCTMGR Database Vault Account Manager Role

The DV\_ACCTMGR role is a powerful role, used for accounts management.

Use the DV\_ACCTMGR role to create and maintain database accounts and database profiles. In this manual, the example DV\_ACCTMGR role is assigned to a user named bea\_dvacctmgr.

### Privileges Associated with the DV\_ACCTMGR Role

A user who has been granted this role can use the CREATE, ALTER, and DROP statements for user accounts or profiles, including users who have been granted the DV\_SECANALYST, DV\_AUDIT\_CLEANUP, and DV\_MONITOR roles.

This user also can grant the `CREATE SESSION` privilege to other users. However, a person who has been granted the `DV_ACCTMGR` role cannot perform the following operations:

- `ALTER` or `DROP` statements on the `DVSYS` account
- `ALTER` or `DROP` statements on users who have been granted the `DV_ADMIN` or `DV_OWNER` role
- Change passwords for users who have been granted the `DV_ADMIN` or `DV_OWNER` role

A common user who has been granted the `DV_ACCTMGR` role in the CDB root can alter a common user or a common profile in the CDB root even if the common `DV_ACCTMGR` user does not have the `SET CONTAINER` privilege or the `DV_ACCTMGR` role in any PDB.

To find the full list of system and object privileges associated with the `DV_ACCTMGR` role, log into the database instance with sufficient privileges and then enter the following queries:

```
SELECT TABLE_NAME, OWNER, PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE = 'DV_ACCTMGR';
SELECT PRIVILEGE FROM DBA_SYS_PRIVS WHERE GRANTEE = 'DV_ACCTMGR';
```

---



---

#### Tips:

- If you want the `DV_ACCTMGR` user to be able to grant or revoke the `ANY` privileges for other users, then log in as user `SYS` with the `SYSDBA` privilege and grant this user the `GRANT ANY PRIVILEGE` and `REVOKE ANY PRIVILEGE` privileges. Then add this user to the Oracle System Privilege and Role Management Realm as an owner.
  - Oracle strongly recommends that you create a separate, named account for the `DV_ACCTMGR` user. This way, if this user forgets his or her password, you can log in as the original `DV_ACCTMGR` account and reset the user's password. Otherwise, you must disable Oracle Database Vault, log in as `SYS` or `SYSTEM` to recreate the password, and then re-enable Database Vault.
- 
- 

#### How Are `GRANT` and `REVOKE` Operations Affected by `DV_ACCTMGR`?

Any account, such as `SYS` or `SYSTEM`, with the `GRANT ANY ROLE` system privilege alone does not have the rights to grant this role to or revoke this role from any other database account.

The account with the `DV_ACCTMGR` role and the `ADMIN OPTION` can grant this role to any given database account and revoke this role from another account.

#### `DV_ACCTMGR` Status When Oracle Database Vault Security Is Disabled

The protection of all Oracle Database roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the `GRANT ANY ROLE` system privilege can perform `GRANT` and `REVOKE` operations on protected Database Vault roles.

**Related Topics:**

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

**14.2.16 DV\_REALM\_OWNER Database Vault Realm DBA Role**

The DV\_REALM\_OWNER role is used for realm management.

Use the DV\_REALM\_OWNER role to manage database objects in multiple schemas that define a realm.

Grant this role to the database account who is responsible for managing one or more schema database accounts within a realm and the roles associated with the realm.

**Privileges Associated with the DV\_REALM\_OWNER Role**

A user who has been granted this role can use powerful system privileges like CREATE ANY, ALTER ANY, and DROP ANY within the realm.

However, before this user can exercise these privileges, you must make this user either a participant or an owner for the realm. See [About Realm Authorization](#) (page 5-13) for instructions.

There are no object privileges granted to the DV\_REALM\_OWNER role, but it does have some system privileges. To find the full list of DV\_REALM\_OWNER system privileges, log into the database instance with sufficient privileges and enter the following query:

```
SELECT PRIVILEGE FROM DBA_SYS_PRIVS WHERE GRANTEE = 'DV_REALM_OWNER';
```

**How Are GRANT and REVOKE Operations Affected by DV\_REALM\_OWNER?**

The realm owner of the Oracle System Privilege and Role Management realm, such as SYS, can grant this role to any given database account or role.

Note that though this role has powerful system privileges, it does not have any Oracle Database Vault roles such as the DV\_OWNER or DV\_ADMIN roles.

If you want to attach this role to a specific realm, then you must assign it to an account or business-related role, then authorize that account or role in the realm.

**DV\_REALM\_OWNER Status When Oracle Database Vault Security Is Disabled**

The protection of all Oracle Database roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the GRANT ANY ROLE system privilege can perform GRANT and REVOKE operations on protected Database Vault roles.

**Related Topics:**

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

**14.2.17 DV\_REALM\_RESOURCE Database Vault Application Resource Owner Role**

The DV\_REALM\_RESOURCE role is use for the management of realm resources.

Use the `DV_REALM_RESOURCE` role for operations such as creating tables, views, triggers, synonyms, and other objects that a realm would typically use.

### **Privileges Associated with the `DV_REALM_RESOURCE` Role**

The `DV_REALM_RESOURCE` role provides the same system privileges as the Oracle `RESOURCE` role. In addition, both `CREATE SYNONYM` and `CREATE VIEW` are granted to this role.

There are no object privileges granted to the `DV_REALM_RESOURCE` role, but it does have some system privileges. To find the full list of `DV_REALM_RESOURCE` system privileges, log into the database instance with sufficient privileges and enter the following query:

```
SELECT PRIVILEGE FROM DBA_SYS_PRIVS WHERE GRANTEE = 'DV_REALM_RESOURCE';
```

Though this role has powerful system privileges, it does not have any Oracle Database Vault roles such as the `DV_OWNER` or `DV_ADMIN` roles.

### **How Are `GRANT` and `REVOKE` Operations Affected by `DV_REALM_RESOURCE`?**

You can grant the `DV_REALM_RESOURCE` role to a database account that owns database tables, objects, triggers, views, procedures, and so on that are used to support any database application.

This is a role designed for a schema type database account. The realm owner of the Oracle System Privilege and Role Management realm, such as `SYS`, can grant this role to any database account or role.

### **`DV_REALM_RESOURCE` Status When Oracle Database Vault Security Is Disabled**

The protection of all Oracle Database roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the `GRANT ANY ROLE` system privilege can perform `GRANT` and `REVOKE` operations on protected Database Vault roles.

#### **Related Topics:**

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

## **14.2.18 `DV_POLICY_OWNER` Database Vault Owner Role**

The `DV_POLICY_OWNER` role enables database users to manage to a limited degree Oracle Database Vault policies.

### **Privileges Associated with the `DV_POLICY_OWNER` Role**

The `DV_POLICY_OWNER` role provides non-Database Vault administrative users the sufficient privileges to enable or disable a Database Vault policy, add or remove authorization to or from a realm, and use the `SELECT` privilege for the following database views:

- `DVSYS.POLICY_OWNER_COMMAND_RULE`
- `DVSYS.POLICY_OWNER_POLICY`

- `DVSYS.POLICY_OWNER_REALM`
- `DVSYS.POLICY_OWNER_REALM_AUTH`
- `DVSYS.POLICY_OWNER_REALM_OBJECT`
- `DVSYS.POLICY_OWNER_RULE_SET`
- `DVSYS.POLICY_OWNER_RULE`
- `DVSYS.POLICY_OWNER_RULE_SET_RULE`

Only the `DV_POLICY_OWNER` can query these views. Even users who have the `DV_OWNER` and `DV_ADMIN` roles cannot query these views.

The `DV_POLICY_OWNER` role does not have any system privileges. To find the full list of object privileges that are associated with the `DV_POLICY_OWNER` role, you can log into the database instance enter the following query:

```
SELECT TABLE_NAME, OWNER, PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE =
'DV_POLICY_OWNER' ;
```

### How Are GRANT and REVOKE Operations Affected by DV\_POLICY\_OWNER?

Users who have been granted `DV_POLICY_OWNER` role cannot grant or revoke this role to or from other users.

### DV\_POLICY\_OWNER Status When Oracle Database Vault Security Is Disabled

The protection of all Oracle Database Vault roles is enforced only if Oracle Database Vault is enabled.

If Oracle Database Vault is disabled, then any account with the `GRANT ANY ROLE` system privilege can perform `GRANT` and `REVOKE` operations on protected Database Vault roles.

### Related Topics:

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

## 14.2.19 DV\_PUBLIC Database Vault PUBLIC Role

The `DV_PUBLIC` role is no longer used.

The `DV_PUBLIC` role is still created during installation, but it is not granted any roles or privileges. All privileges that were granted to `DV_PUBLIC` in previous releases are now granted directly to the `PUBLIC` role.

## 14.3 Oracle Database Vault Accounts Created During Registration

You must create accounts for the Oracle Database Vault Owner and Oracle Database Vault Account Manager during the registration process.

You must supply an account name and password for the Oracle Database Vault Owner accounts during installation. Creating an Oracle Database Vault Account Manager is optional but strongly recommended for better separation of duty.

The Oracle Database Vault Owner account is granted the `DV_OWNER` role. This account can manage Oracle Database Vault roles and configuration.

The Oracle Database Vault Account Manager account is granted the DV\_ACCTMGR role. This account is used to manage database user accounts to facilitate separation of duties.

If you choose not to create the Oracle Database Vault Account Manager account during installation, then both the DV\_OWNER and DV\_ACCTMGR roles are granted to the Oracle Database Vault Owner user account.

[Table 14-2](#) (page 14-24) lists the Oracle Database Vault database accounts that are needed in addition to the accounts that you create during installation.

**Table 14-2 Database Accounts Used by Oracle Database Vault**

Database Account	Roles and Privileges	Description
DVSYSD	Several system and object privileges are provided to support Oracle Database Vault. The ability to create a session with this account is revoked at the end of the installation, and the account is locked.	Owner of Oracle Database Vault schema and related objects
DVF	A limited set of system privileges are provided to support Oracle Database Vault. The ability to create a session with this account is revoked at the end of the installation, and the account is locked.	Owner of the Oracle Database Vault functions that are created to retrieve factor identities
LBACSYS	This account is created when you install Oracle Label Security by using the Oracle Universal Installer custom installation option. (It is not created when you install Oracle Database Vault.) Do not drop or re-create this account.  If you plan to integrate a factor with an Oracle Label Security policy, you must assign this user as the owner of the realm that uses this factor. See <a href="#">Using Oracle Database Vault Factors with Oracle Label Security Policies</a> (page 12-7) for more information.	Owner of the Oracle Label Security schema

You can create different database accounts to implement the separation of duties requirements for Oracle Database Vault. [Table 14-3](#) (page 14-25) lists some model database accounts that can act as a guide. (The accounts listed in [Table 14-3](#) (page 14-25) serve as a guide to implementing Oracle Database Vault roles. These are not actual accounts that are created during installation.)

**Table 14-3 Model Oracle Database Vault Database Accounts**

Database Account	Roles and Privileges	Description
EBROWN	DV_OWNER (with DV_ADMIN and DV_SECANALYST)	Account that is the realm owner for the Oracle Database Vault realm. This account can: <ul style="list-style-type: none"> <li>Execute DVSYS packages</li> <li>Grant privileges on the DVSYS schema objects</li> <li>Select objects in the DVSYS schema</li> <li>Monitor Oracle Database Vault activity</li> <li>Run reports on the Oracle Database Vault configuration</li> </ul>
JGODFREY	DV_ACCTMGR	Account for administration of database accounts and profiles. This account can: <ul style="list-style-type: none"> <li>Create, alter, and drop users</li> <li>Create, alter, and drop profiles</li> <li>Grant and revoke the CREATE SESSION privilege</li> <li>Grant and revoke the DV_ACCTMGR role, but only if this account was created during the Database Vault installation (this account is created with the ADMIN option)</li> <li>Grant and revoke the CONNECT role</li> </ul> <p><b>Note:</b> This account cannot create roles, or grant the RESOURCE or DBA roles.</p>
RLAYTON	DV_ADMIN (with DV_SECANALYST)	Account to serve as the access control administrator. This account can: <ul style="list-style-type: none"> <li>Execute DVSYS packages</li> <li>Monitor Oracle Database Vault activity</li> <li>Run reports on the Oracle Database Vault configuration</li> </ul> <p><b>Note:</b> This account cannot directly update the DVSYS tables.</p>
PSMYTHE	DV_SECANALYST	Account for running Oracle Database Vault reports

**Related Topics:**

[Configuring Oracle Database Vault Accounts as Enterprise User Accounts](#) (page 12-2)

You can configure existing Oracle Database Vault user accounts as enterprise user accounts.

[Backup Oracle Database Vault Accounts](#) (page 14-25)

As a best practice, you should maintain backup accounts for the DV\_OWNER and DV\_ACCTMGR roles.

## 14.4 Backup Oracle Database Vault Accounts

As a best practice, you should maintain backup accounts for the DV\_OWNER and DV\_ACCTMGR roles.

The Oracle Database Vault registration process entails creating both day-to-day and backup accounts for the `DV_OWNER` and `DV_ACCTMGR` roles. You should keep and maintain these accounts as a safety measure in case a user who has been granted one of these roles forgets his or her password or leaves the organization. Then you can log in to the backup account to recover the password or grant the role to a new account. These should be only used as a backup account kept safe in a privileged account management system or an organization break-glass (or emergency password recovery) system.

Because of the strong separation of duty that Oracle Database Vault implements, loss of access to the `DV_OWNER` account will force you to rebuild the database. The `SYS` account cannot override the `DV_OWNER` account

**Related Topics:**

[Resetting Oracle Database Vault Account Passwords](#) (page E-12)

Backup accounts can help you reset lost passwords for users who have been granted the `DV_OWNER` and `DV_ACCTMGR` roles.



---

## Oracle Database Vault Realm APIs

The DBMS\_MACADM PL/SQL package enables you to configure Oracle Database Vault realms.

Only users who have been granted the DV\_OWNER or DV\_ADMIN role can use these procedures. For constants that you can use with these procedures, see [Table 21-1](#) (page 21-2) for more information.

### [ADD\\_AUTH\\_TO\\_REALM Procedure](#) (page 15-2)

The ADD\_AUTH\_TO\_REALM procedure authorizes a user or role to access a realm as an owner or a participant. In a multitenant environment, you can authenticate both common and local realms.

### [ADD\\_OBJECT\\_TO\\_REALM Procedure](#) (page 15-4)

The ADD\_OBJECT\_TO\_REALM procedure registers a set of objects for realm protection.

### [CREATE\\_REALM Procedure](#) (page 15-5)

The CREATE\_REALM procedure creates a realm. In a multitenant environment, you can create both common and local realms.

### [DELETE\\_AUTH\\_FROM\\_REALM Procedure](#) (page 15-8)

The DELETE\_AUTH\_FROM\_REALM procedure removes the authorization of a user or role to access a realm.

### [DELETE\\_OBJECT\\_FROM\\_REALM Procedure](#) (page 15-9)

The DELETE\_OBJECT\_FROM\_REALM procedure removes a set of objects from realm protection.

### [DELETE\\_REALM Procedure](#) (page 15-9)

The DELETE\_REALM procedure deletes a realm, including its related configuration information that specifies who is authorized and what objects are protected.

### [DELETE\\_REALM\\_CASCADE Procedure](#) (page 15-10)

The DELETE\_REALM\_CASCADE procedure deletes a realm, including its related Database Vault configuration information that specifies who is authorized and the objects that are protected.

### [RENAME\\_REALM Procedure](#) (page 15-11)

The RENAME\_REALM procedure renames a realm; the name change takes effect everywhere the realm is used.

### [UPDATE\\_REALM Procedure](#) (page 15-11)

The UPDATE\_REALM procedure updates a realm.

### [UPDATE\\_REALM\\_AUTH Procedure](#) (page 15-13)

The UPDATE\_REALM\_AUTH procedure updates the authorization of a user or role to access a realm.

## 15.1 ADD\_AUTH\_TO\_REALM Procedure

The `ADD_AUTH_TO_REALM` procedure authorizes a user or role to access a realm as an owner or a participant. In a multitenant environment, you can authenticate both common and local realms.

For detailed information about realm authorization, see [About Realm Authorization](#) (page 5-13).

Optionally, you can specify a rule set that must be checked before allowing the authorization to be enabled.

### Syntax

```
DBMS_MACADM.ADD_AUTH_TO_REALM(
  realm_name      IN VARCHAR2,
  grantee         IN VARCHAR2,
  rule_set_name   IN VARCHAR2,
  auth_options    IN NUMBER
  auth_scope      IN NUMBER DEFAULT);
```

### Parameters

**Table 15-1 ADD\_AUTH\_TO\_REALM Parameters**

Parameter	Description
<code>realm_name</code>	<p>Realm name.</p> <p>To find the existing realms in the current database instance, query the <code>DBA_DV_REALM</code> view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24).</p>
<code>grantee</code>	<p>User or role name to authorize as an owner or a participant.</p> <p>To find the existing users and roles in the current database instance, query the <code>DBA_USERS</code> and <code>DBA_ROLES</code> views, described in <i>Oracle Database Reference</i>.</p> <p>To find the authorization of a particular user or role, query the <code>DVA_DV_REALM_AUTH</code> view, described in <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</p> <p>To find existing secure application roles used in privilege management, query the <code>DBA_DV_ROLE</code> view. Both are described in <a href="#">Oracle Database Vault Data Dictionary Views</a> (page 25-1).</p>
<code>rule_set_name</code>	<p>Optional. The rule set to check during runtime. The realm authorization is enabled only if the rule set evaluates to <code>TRUE</code>.</p> <p>To find the available rule sets, query the <code>DBA_DV_RULE_SET</code> view, described in <a href="#">DBA_DV_RULE_SET_RULE View</a> (page 25-32).</p>

**Table 15-1 (Cont.) ADD\_AUTH\_TO\_REALM Parameters**

Parameter	Description
auth_options	<p>Optional. Specify one of the following options to authorize the realm:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_REALM_AUTH_PARTICIPANT: Participant. This account or role provides system or direct privileges to access, manipulate, and create objects protected by the realm, provided these rights have been granted using the standard Oracle Database privilege grant process. (Default)</li> <li>DBMS_MACUTL.G_REALM_AUTH_OWNER: Owner. This account or role has the same authorization as the realm participant, plus the authorization to grant or revoke realm-secured roles and privileges on realm-protected objects.</li> </ul> <p>See <a href="#">About Realm Authorization</a> (page 5-13) for more information on participants and owners.</p>
auth_scope	<p>For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) to authorize the realm locally in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) to authorize the realm in the application root</li> </ul>

### Examples

The following example authorizes user SYSADM as a participant in the Performance Statistics Realm. Because the default is to authorize the user as a participant, the auth\_options parameter can be omitted.

```
BEGIN
  DBMS_MACADM.ADD_AUTH_TO_REALM(
    realm_name => 'Performance Statistics Realm',
    grantee    => 'SYSADM');
END;
/
```

This example sets user SYSADM as the owner of the Performance Statistics Realm.

```
BEGIN
  DBMS_MACADM.ADD_AUTH_TO_REALM(
    realm_name  => 'Performance Statistics Realm',
    grantee     => 'SYSADM',
    auth_options => DBMS_MACUTL.G_REALM_AUTH_OWNER);
END;
/
```

The next example triggers the Check Conf Access rule set before allowing user SYSADM to act as the owner of the Performance Statistics Realm.

```
BEGIN
  DBMS_MACADM.ADD_AUTH_TO_REALM(
    realm_name    => 'Performance Statistics Realm',
    grantee       => 'SYSADM',
    rule_set_name => 'Check Conf Access',
    auth_options  => DBMS_MACUTL.G_REALM_AUTH_OWNER);
```

```
END;
/
```

This example shows how to commonly grant the common user C##HR\_ADMIN access to the common realm HR Statistics Realm. The user running this procedure must be in the CDB root, and the rule set must be a common rule set residing in the application root.

```
BEGIN
DBMS_MACADM.ADD_AUTH_TO_REALM(
  realm_name    => 'HR Statistics Realm',
  grantee       => 'C##HR_ADMIN',
  rule_set_name => 'Check Access',
  auth_options  => DBMS_MACUTL.G_REALM_AUTH_OWNER,
  auth_scope    => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

This example shows how to locally grant the common user C##HR\_CLERK access to the common realm HR Statistics Realm. The user running this procedure must be in the same PDB in which the authorization applies. To find the existing PDBs query the DBA\_PDBS data dictionary view. The rule set must be a local rule set.

```
BEGIN
DBMS_MACADM.ADD_AUTH_TO_REALM(
  realm_name    => 'HR Statistics Realm',
  grantee       => 'C##HR_CLERK',
  rule_set_name => 'Check Access',
  auth_options  => DBMS_MACUTL.G_REALM_AUTH_OWNER,
  auth_scope    => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/
```

## 15.2 ADD\_OBJECT\_TO\_REALM Procedure

The ADD\_OBJECT\_TO\_REALM procedure registers a set of objects for realm protection.

### Syntax

```
DBMS_MACADM.ADD_OBJECT_TO_REALM(
  realm_name    IN VARCHAR2,
  object_owner  IN VARCHAR2,
  object_name   IN VARCHAR2,
  object_type   IN VARCHAR2);
```

### Parameters

**Table 15-2 ADD\_OBJECT\_TO\_REALM Parameters**

Parameter	Description
realm_name	Realm name. To find the existing realms in the current database instance, query the DBA_DV_REALM view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24).

**Table 15-2 (Cont.) ADD\_OBJECT\_TO\_REALM Parameters**

Parameter	Description
object_owner	<p>The owner of the object that is being added to the realm. If you add a role to a realm, the object owner of the role is shown as % (for all), because roles do not have owners.</p> <p>To find the available users, query the DBA_USERS view, described in <i>Oracle Database Reference</i>.</p> <p>To find the authorization of a particular user or role, query the DVA_DV_REALM_AUTH view, described in <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</p>
object_name	<p>Object name. (The wildcard % is allowed. See "Object Name" under <a href="#">About Realm-Secured Objects</a> (page 5-12) for exceptions to the wildcard %.) You can also use the DBMS_MACUTL.G_ALL_OBJECT constant.</p> <p>To find the available objects, query the ALL_OBJECTS view, described in <i>Oracle Database Reference</i>.</p> <p>To find objects that are secured by existing realms, query the DBA_DV_REALM_OBJECT view, described in <a href="#">DBA_DV_REALM_OBJECT View</a> (page 25-27).</p>
object_type	<p>Object type, such as TABLE, INDEX, or ROLE. (The wildcard % is allowed. See "Object Types" under <a href="#">About Realm-Secured Objects</a> (page 5-12) for exceptions to the wildcard %.)</p> <p>You can also use the DBMS_MACUTL.G_ALL_OBJECT constant.</p>

**Example**

```

BEGIN
  DBMS_MACADM.ADD_OBJECT_TO_REALM(
    realm_name => 'Performance Statistics Realm',
    object_owner => '%',
    object_name => 'GATHER_SYSTEM_STATISTICS',
    object_type => 'ROLE');
END;
/

```

**15.3 CREATE\_REALM Procedure**

The CREATE\_REALM procedure creates a realm. In a multitenant environment, you can create both common and local realms.

After you create the realm, use the following procedures to complete the realm definition:

- ADD\_OBJECT\_TO\_REALM procedure registers one or more objects for the realm.
- ADD\_AUTH\_TO\_REALM procedure authorizes users or roles for the realm.

**Syntax**

```

DBMS_MACADM.CREATE_REALM(
  realm_name  IN VARCHAR2,
  description IN VARCHAR2,

```

```

enabled          IN VARCHAR2,
audit_options    IN NUMBER,
realm_type       IN NUMBER DEFAULT,
realm_scope      IN NUMBER DEFAULT);

```

## Parameters

**Table 15-3 CREATE\_REALM Parameters**

Parameter	Description
realm_name	<p>Realm name, up to 128 characters in mixed-case.</p> <p>To find the existing realms in the current database instance, query the DBA_DV_REALM view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24).</p>
description	Description of the purpose of the realm, up to 1024 characters in mixed-case.
enabled	<p>Specify one of the following options to set the status of the realm:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_YES or 'y' to enable realm checking (default)</li> <li>DBMS_MACUTL.G_NO or 'n' to disable all realm checking, including the capture of violations in the simulation log</li> <li>DBMS_MACUTL.G_SIMULATION or 's' to enable SQL statements to execute but capture violations in the simulation log</li> </ul>
audit_options	<p>Specify one of the following options to audit the realm:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_REALM_AUDIT_OFF: Disables auditing for the realm (default)</li> <li>DBMS_MACUTL.G_REALM_AUDIT_FAIL: Creates an audit record when a realm violation occurs (for example, when an unauthorized user tries to modify an object that is protected by the realm)</li> <li>DBMS_MACUTL.G_REALM_AUDIT_SUCCESS: Creates an audit record for authorized activities on objects protected by the realm</li> <li>DBMS_MACUTL.G_REALM_AUDIT_FAIL + DBMS_MACUTL.G_REALM_AUDIT_SUCCESS: Creates an audit record for both authorized and unauthorized activities on objects protected by the realm</li> </ul>
realm_type	<p>Specify one of the following options:</p> <ul style="list-style-type: none"> <li>0: Disables mandatory realm checking.</li> <li>1: Enables mandatory realm checking for realm objects. Only realm owners or realm participants will have access to objects in a realm. Object owners and object-privileged users who are not realm owners or participants will have no access.</li> </ul> <p>See also <a href="#">Mandatory Realms to Restrict User Access to Objects within a Realm</a> (page 5-3) for more information about mandatory realms.</p>

**Table 15-3 (Cont.) CREATE\_REALM Parameters**

Parameter	Description
realm_scope	<p>For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows:</p> <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the realm must be local in the current PDB.</li> <li>• DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the realm must be in the application root. This setting duplicates the realm in all of the associated PDBs.</li> </ul> <p>If you create the common realm in an application root and want it visible to the associated PDBs, then you must synchronize the application. For example:</p> <pre>ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;</pre>

### Examples

The following example shows how to create a realm that is enabled, has auditing set to track both failed and successful access, and uses mandatory realm checking.

```
BEGIN
  DBMS_MACADM.CREATE_REALM(
    realm_name    => 'Performance Statistics Realm',
    description   => 'Realm to measure performance',
    enabled       => DBMS_MACUTL.G_YES,
    audit_options => DBMS_MACUTL.G_REALM_AUDIT_FAIL +
DBMS_MACUTL.G_REALM_AUDIT_SUCCESS,
    realm_type    => 1);
END;
/
```

This example shows how to create a variation of the preceding example, but as a common realm located in the application root. The user who creates this realm must be a common user and must execute the procedure in the CDB root.

```
BEGIN
  DBMS_MACADM.CREATE_REALM(
    realm_name    => 'Performance Statistics Realm',
    description   => 'Realm to measure performance',
    enabled       => DBMS_MACUTL.G_YES,
    audit_options => DBMS_MACUTL.G_REALM_AUDIT_FAIL +
DBMS_MACUTL.G_REALM_AUDIT_SUCCESS,
    realm_type    => 1,
    realm_scope   => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

This example shows how to create a local version n of the preceding example. The user who creates this realm must be in the PDB in which the realm will reside. To find existing PDBs, query the DBA\_PDBS data dictionary view.

```
BEGIN
  DBMS_MACADM.CREATE_REALM(
    realm_name    => 'Performance Statistics Realm',
    description   => 'Realm to measure performance',
    enabled       => DBMS_MACUTL.G_YES,
    audit_options => DBMS_MACUTL.G_REALM_AUDIT_FAIL +
```

```

DBMS_MACUTL.G_REALM_AUDIT_SUCCESS,
  realm_type    => 1,
  realm_scope   => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/

```

---



---

**See Also:**

[Example 21-1](#) (page 21-6)

---



---

## 15.4 DELETE\_AUTH\_FROM\_REALM Procedure

The `DELETE_AUTH_FROM_REALM` procedure removes the authorization of a user or role to access a realm.

### Syntax

```

DBMS_MACADM.DELETE_AUTH_FROM_REALM(
  realm_name    IN VARCHAR2,
  grantee       IN VARCHAR2,
  auth_scope    IN NUMBER DEFAULT);

```

### Parameters

**Table 15-4** *DELETE\_AUTH\_FROM\_REALM Parameters*

Parameter	Description
<code>realm_name</code>	<p>Realm name.</p> <p>To find the existing realms in the current database instance, query the <code>DBA_DV_REALM</code> view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24)</p>
<code>grantee</code>	<p>User or role name.</p> <p>To find the authorization of a particular user or role, query the <code>DVA_DV_REALM_AUTH</code> view, described in <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</p>
<code>auth_scope</code>	<p>For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows:</p> <ul style="list-style-type: none"> <li>• <code>DBMS_MACUTL.G_SCOPE_LOCAL</code> (or 1) if the realm was authorized locally in the current PDB</li> <li>• <code>DBMS_MACUTL.G_SCOPE_COMMON</code> (or 2 if the realm was authorized in the application root</li> </ul>

### Example

```

BEGIN
DBMS_MACADM.DELETE_AUTH_FROM_REALM(
  realm_name => 'Performance Statistics Realm',
  grantee    => 'PSMITH',
  auth_scope => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/

```



## 15.5 DELETE\_OBJECT\_FROM\_REALM Procedure

The `DELETE_OBJECT_FROM_REALM` procedure removes a set of objects from realm protection.

### Syntax

```
DBMS_MACADM.DELETE_OBJECT_FROM_REALM(
  realm_name   IN VARCHAR2,
  object_owner IN VARCHAR2,
  object_name  IN VARCHAR2,
  object_type  IN VARCHAR2);
```

### Parameters

**Table 15-5** *DELETE\_OBJECT\_FROM\_REALM Parameters*

Parameter	Description
<code>realm_name</code>	<p>Realm name.</p> <p>To find the existing realms in the current database instance, query the <code>DBA_DV_REALM</code> view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24).</p>
<code>object_owner</code>	<p>The owner of the object that was added to the realm.</p> <p>To find the available users, query the <code>DBA_USERS</code> view, described in <i>Oracle Database Reference</i>.</p>
<code>object_name</code>	<p>Object name. (The wildcard % is allowed. See "Object Name" under <a href="#">About Realm-Secured Objects</a> (page 5-12) for exceptions to the wildcard %.) You can also use the <code>DBMS_MACUTL.G_ALL_OBJECT</code> constant.</p> <p>To find objects that are secured by existing realms, query the <code>DBA_DV_REALM_OBJECT</code> view, described in <a href="#">DBA_DV_REALM_OBJECT View</a> (page 25-27).</p>
<code>object_type</code>	<p>Object type, such as <code>TABLE</code>, <code>INDEX</code>, or <code>ROLE</code>. (The wildcard % is allowed. See "Object Types" under <a href="#">About Realm-Secured Objects</a> (page 5-12) for exceptions to the wildcard %.)</p> <p>You can also use the <code>DBMS_MACUTL.G_ALL_OBJECT</code> constant.</p>

### Example

```
BEGIN
  DBMS_MACADM.DELETE_OBJECT_FROM_REALM(
    realm_name => 'Performance Statistics Realm',
    object_owner => 'SYS',
    object_name => 'GATHER_SYSTEM_STATISTICS',
    object_type => 'ROLE');
END;
/
```

## 15.6 DELETE\_REALM Procedure

The `DELETE_REALM` procedure deletes a realm, including its related configuration information that specifies who is authorized and what objects are protected.

This procedure does not delete the actual database objects or users.

To find users who are authorized for the realm, query the `DBA_DV_REALM_AUTH` view. To find the objects that are protected by the realm, query the `DBA_DV_REALM_OBJECT` view. These views are described in [Oracle Database Vault Data Dictionary Views](#) (page 25-1).

### Syntax

```
DBMS_MACADM.DELETE_REALM(
    realm_name IN VARCHAR2);
```

### Parameters

**Table 15-6** *DELETE\_REALM Parameter*

Parameter	Description
<code>realm_name</code>	<p>Realm name.</p> <p>To find the existing realms in the current database instance, query the <code>DBA_DV_REALM</code> view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24).</p>

### Example

```
EXEC DBMS_MACADM.DELETE_REALM('Performance Statistics Realm');
```

## 15.7 DELETE\_REALM\_CASCADE Procedure

The `DELETE_REALM_CASCADE` procedure deletes a realm, including its related Database Vault configuration information that specifies who is authorized and the objects that are protected.

The `DBA_DV_REALM_AUTH` view lists who is authorized in the realm and the `DBA_DV_REALM_OBJECT` view lists the protected objects.

It does not delete the actual database objects or users. This procedure works the same as the `DELETE_REALM` procedure. (In previous releases, these procedures were different, but now they are the same. Both are retained for earlier compatibility.) To find a listing of the realm-related objects, query the `DBA_DV_REALM` view. To find its authorizations, query `DBA_DV_REALM_AUTH`. Both are described under [Oracle Database Vault Data Dictionary Views](#) (page 25-1).

### Syntax

```
DBMS_MACADM.DELETE_REALM_CASCADE(
    realm_name IN VARCHAR2);
```

### Parameters

**Table 15-7** *DELETE\_REALM\_CASCADE Parameter*

Parameter	Description
<code>realm_name</code>	<p>Realm name.</p> <p>To find the existing realms in the current database instance, query the <code>DBA_DV_REALM</code> view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24).</p>

**Example**

```
EXEC DBMS_MACADM.DELETE_REALM_CASCADE('Performance Statistics Realm');
```

**15.8 RENAME\_REALM Procedure**

The `RENAME_REALM` procedure renames a realm; the name change takes effect everywhere the realm is used.

**Syntax**

```
DBMS_MACADM.RENAME_REALM(
  realm_name  IN VARCHAR2,
  new_name    IN VARCHAR2);
```

**Parameters****Table 15-8 RENAME\_REALM Parameters**

Parameter	Description
<code>realm_name</code>	Current realm name. To find the existing realms in the current database instance, query the <code>DBA_DV_REALM</code> view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24).
<code>new_name</code>	New realm name, up to 128 characters in mixed-case.

**Example**

```
BEGIN
  DBMS_MACADM.RENAME_REALM(
    realm_name => 'Performance Statistics Realm',
    new_name   => 'Sector 2 Performance Statistics Realm');
END;
/
```

**15.9 UPDATE\_REALM Procedure**

The `UPDATE_REALM` procedure updates a realm.

To find information about the current settings for a realm, query the `DVSYSDV$REALM` view, described in [DVSYS.DV\\$REALM View](#) (page 25-46).

**Syntax**

```
DBMS_MACADM.UPDATE_REALM(
  realm_name    IN VARCHAR2,
  description   IN VARCHAR2,
  enabled       IN VARCHAR2,
  audit_options IN NUMBER DEFAULT NULL,
  realm_type    IN NUMBER DEFAULT NULL);
```

## Parameters

**Table 15-9 UPDATE\_REALM Parameters**

Parameter	Description
realm_name	<p>Realm name.</p> <p>To find the existing realms in the current database instance, query the DBA_DV_REALM view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24).</p>
description	<p>Description of the purpose of the realm, up to 1024 characters in mixed-case.</p>
enabled	<p>Specify one of the following options to set the status of the realm:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_YES or 'y' to enable realm checking</li> <li>DBMS_MACUTL.G_NO or 'n' to disable all realm checking, including the capture of violations in the simulation log</li> <li>DBMS_MACUTL.G_SIMULATION or 's' to enable SQL statements to execute but capture violations in the simulation log</li> </ul> <p>The default for enabled is the previously set value, which you can find by querying the DBA_DV_REALM data dictionary view.</p>
audit_options	<p>Specify one of the following options to audit the realm:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_REALM_AUDIT_OFF: Disables auditing for the realm</li> <li>DBMS_MACUTL.G_REALM_AUDIT_FAIL: Creates an audit record when a realm violation occurs (for example, when an unauthorized user tries to modify an object that is protected by the realm)</li> <li>DBMS_MACUTL.G_REALM_AUDIT_SUCCESS: Creates an audit record for authorized activities on objects protected by the realm.</li> <li>DBMS_MACUTL.G_REALM_AUDIT_FAIL + DBMS_MACUTL.G_REALM_AUDIT_SUCCESS: Creates an audit record for both authorized and unauthorized activities on objects protected by the realm</li> </ul> <p>The default for audit_options is the previously set value, which you can find by querying the DBA_DV_REALM data dictionary view.</p>
realm_type	<p>If you do not specify the realm_type parameter, then Oracle Database Vault does not update the current realm_type setting.</p> <p>Specify one of the following options:</p> <ul style="list-style-type: none"> <li>0: Sets the realm to be a regular realm, which does not have mandatory realm checking.</li> <li>1: Enables mandatory realm checking for realm objects. Only realm owners or realm participants will have access to objects in a realm. Object owners and object-privileged users who are not realm owners or participants will have no access.</li> </ul> <p>See also <a href="#">Mandatory Realms to Restrict User Access to Objects within a Realm</a> (page 5-3) for more information about mandatory realms.</p>

## Example

```
BEGIN
  DBMS_MACADM.UPDATE_REALM(
    realm_name    => 'Sector 2 Performance Statistics Realm',
    description   => 'Realm to measure performance for Sector 2 applications',
    enabled       => DBMS_MACUTL.G_YES,
    audit_options => DBMS_MACUTL.G_REALM_AUDIT_FAIL + G_REALM_AUDIT_SUCCESS);
```

```

END,
  realm_type    => 1);
/

```

## 15.10 UPDATE\_REALM\_AUTH Procedure

The UPDATE\_REALM\_AUTH procedure updates the authorization of a user or role to access a realm.

### Syntax

```

DBMS_MACADM.UPDATE_REALM_AUTH(
  realm_name     IN VARCHAR2,
  grantee        IN VARCHAR2,
  rule_set_name  IN VARCHAR2,
  auth_options   IN NUMBER,
  auth_scope     IN NUMBER DEFAULT);

```

### Parameters

**Table 15-10 UPDATE\_REALM\_AUTH Parameters**

Parameter	Description
realm_name	<p>Realm name.</p> <p>To find the existing realms in the current database instance, query the DBA_DV_REALM view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24).</p>
grantee	<p>User or role name.</p> <p>To find the available users and roles in the current database instance, query the DBA_USERS and DBA_ROLES views, described in <i>Oracle Database Reference</i>.</p> <p>To find the authorization of a particular user or role, query the DVA_DV_REALM_AUTH view, described in <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</p> <p>To find existing secure application roles used in privilege management, query the DBA_DV_ROLE view, described in <a href="#">DBA_DV_ROLE View</a> (page 25-28).</p>
rule_set_name	<p>Optional. A rule set to check during runtime. The realm authorization is enabled only if the rule set evaluates to TRUE.</p> <p>To find the available rule sets, query the DBA_DV_RULE_SET view. To find rules that are associated with the rule sets, query the DBA_DB_RULE_SET_RULE view. Both are described in <a href="#">Oracle Database Vault Data Dictionary Views</a> (page 25-1).</p>

**Table 15-10 (Cont.) UPDATE\_REALM\_AUTH Parameters**

Parameter	Description
auth_options	<p>Optional. Specify one of the following options to authorize the realm:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_REALM_AUTH_PARTICIPANT: Participant. This account or role provides system or direct privileges to access, manipulate, and create objects protected by the realm, provided these rights have been granted using the standard Oracle Database privilege grant process.</li> <li>DBMS_MACUTL.G_REALM_AUTH_OWNER: Owner. This account or role has the same authorization as the realm participant, plus the authorization to grant or revoke realm-secured roles and privileges on realm-protected objects. A realm can have multiple owners.</li> </ul> <p>The default for auth_options value is the previously set value, which you can find by querying the DBA_DV_REALM_AUTH data dictionary view.</p>
realm_auth	<p>For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the realm is authorized locally in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the realm is authorized in the application root</li> </ul>

**Example**

```

BEGIN
  DBMS_MACADM.UPDATE_REALM_AUTH(
    realm_name    => 'Sector 2 Performance Statistics Realm',
    grantee       => 'SYSADM',
    rule_set_name => 'Check Conf Access',
    auth_options  => DBMS_MACUTL.G_REALM_AUTH_OWNER);
END;
/

```

---

## Oracle Database Vault Rule Set APIs

You can use the `DBMS_MACADM` PL/SQL package and a set of Oracle Database Vault rule functions to manage rule sets.

### [DBMS\\_MACADM Rule Set Procedures](#) (page 16-1)

The `DBMS_MACADM` rule set procedures enable you to configure both rule sets and individual rules that go within these rule sets.

### [Oracle Database Vault PL/SQL Rule Set Functions](#) (page 16-14)

Oracle Database Vault provides functions to use in rule sets to inspect the SQL statement that the rule set protects.

## 16.1 DBMS\_MACADM Rule Set Procedures

The `DBMS_MACADM` rule set procedures enable you to configure both rule sets and individual rules that go within these rule sets.

Only users who have been granted the `DV_OWNER` or `DV_ADMIN` role can use these procedures.

### [ADD\\_RULE\\_TO\\_RULE\\_SET Procedure](#) (page 16-2)

The `ADD_RULE_TO_RULE_SET` procedure adds rule to a rule set; you can enable having the rule checked when the rule set is evaluated.

### [CREATE\\_RULE Procedure](#) (page 16-3)

The `CREATE_RULE` procedure creates a rule, which afterwards, can be added to a rule set.

### [CREATE\\_RULE\\_SET Procedure](#) (page 16-5)

The `CREATE_RULE_SET` procedure creates a rule set.

### [DELETE\\_RULE Procedure](#) (page 16-8)

The `DELETE_RULE` procedure deletes a rule.

### [DELETE\\_RULE\\_FROM\\_RULE\\_SET Procedure](#) (page 16-8)

The `DELETE_RULE_FROM_RULE_SET` procedure deletes a rule from a rule set.

### [DELETE\\_RULE\\_SET Procedure](#) (page 16-9)

The `DELETE_RULE_SET` procedure deletes a rule set.

### [RENAME\\_RULE Procedure](#) (page 16-9)

The `RENAME_RULE` procedure renames a rule and causes the name change to take effect everywhere the rule is used

### [RENAME\\_RULE\\_SET Procedure](#) (page 16-10)

The `RENAME_RULE_SET` procedure renames a rule set and causes the name change to take effect everywhere the rule set is used.

[UPDATE\\_RULE Procedure](#) (page 16-11)

The UPDATE\_RULE procedure updates a rule.

[UPDATE\\_RULE\\_SET Procedure](#) (page 16-12)

The UPDATE\_RULE\_SET procedure updates a rule set.

**Related Topics:**[Configuring Rule Sets](#) (page 6-1)

Rule sets group one or more rules together; the rules determine whether a user can perform an action on an object.

[Oracle Database Vault Utility APIs](#) (page 21-1)

Oracle Database Vault provides a set of utility APIs in the DBMS\_MACUTL PL/SQL package.

## 16.1.1 ADD\_RULE\_TO\_RULE\_SET Procedure

The ADD\_RULE\_TO\_RULE\_SET procedure adds rule to a rule set; you can enable having the rule checked when the rule set is evaluated.

**Syntax**

```
DBMS_MACADM.ADD_RULE_TO_RULE_SET(
  rule_set_name  IN VARCHAR2,
  rule_name      IN VARCHAR2,
  rule_order     IN NUMBER,
  enabled        IN VARCHAR2,
  scope          IN NUMBER DEFAULT);
```

**Parameters****Table 16-1 ADD\_RULE\_TO\_RULE\_SET Parameters**

Parameter	Description
rule_set_name	Rule set name. To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).
rule_name	Rule to add to the rule set. To find existing rules, query the DBA_DV_RULE view, described in <a href="#">DBA_DV_RULE View</a> (page 25-29). To find rules that have been associated with rule sets, use DBA_DV_RULE_SET_RULE, described in <a href="#">DBA_DV_RULE View</a> (page 25-29).
rule_order	Does not apply to this release, but you must include a value for the ADD_RULE_TO_RULE_SET procedure to work. Enter 1.
enabled	Optional. Determines whether the rule should be checked when the rule set is evaluated. Possible values are: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_YES (default). Enables the rule to be checked during the rule set evaluation.</li> <li>DBMS_MACUTL.G_NO Prevents the rule from being checked during the rule set evaluation.</li> </ul> See <a href="#">Table 21-1</a> (page 21-2) for more information.



**Table 16-1 (Cont.) ADD\_RULE\_TO\_RULE\_SET Parameters**

Parameter	Description
scope	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the rule and rule set are local in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the rule and rule set are in the application root</li> </ul>

### Examples

The following example adds a rule to a rule set, and by omitting the `enabled` parameter, automatically enables the rule to be checked when the rule set is evaluated.

```
BEGIN
  DBMS_MACADM.ADD_RULE_TO_RULE_SET(
    rule_set_name => 'Limit_DBA_Access',
    rule_name      => 'Restrict DROP TABLE operations',
    rule_order     => 1);
END;
/
```

This example adds the rule to the rule set but disables rule checking.

```
BEGIN
  DBMS_MACADM.ADD_RULE_TO_RULE_SET(
    rule_set_name => 'Limit_DBA_Access',
    rule_name      => 'Check UPDATE operations',
    rule_order     => 1,
    enabled        => DBMS_MACUTL.G_NO);
END;
/
```

## 16.1.2 CREATE\_RULE Procedure

The `CREATE_RULE` procedure creates a rule, which afterwards, can be added to a rule set.

In a multitenant environment, you can create both common and local rules.

### Syntax

```
DBMS_MACADM.CREATE_RULE(
  rule_name  IN VARCHAR2,
  rule_expr  IN VARCHAR2
  scope      IN NUMBER DEFAULT);
```

## Parameters

**Table 16-2 CREATE\_RULE Parameters**

Parameter	Description
rule_name	<p>Rule name, up to 128 characters in mixed-case. Spaces are allowed.</p> <p>To find existing rules in the current database instance, query the DBA_DV_RULE view, described in <a href="#">DBA_DV_RULE View</a> (page 25-29).</p> <p>To find rules that have been associated with rule sets, query DBA_DV_RULE_SET_RULE, described in <a href="#">DBA_DV_RULE_SET_RULE View</a> (page 25-32).</p>
rule_expr	<p>PL/SQL BOOLEAN expression.</p> <p>If the expression contains quotation marks, do not use double quotation marks. Instead, use two single quotation marks. Enclose the entire expression within single quotation marks. For example:</p> <pre>'TO_CHAR(SYSDATE, 'HH24') = '12''</pre> <p>See <a href="#">Creating a New Rule</a> (page 6-12) for more information on rule expressions.</p>
scope	<p>For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows:</p> <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the rule is local in the current PDB</li> <li>• DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the rule is in the application root</li> </ul>

## Examples

The following example shows how to create a local rule expression that checks if the current session user is SYSADM. The user running this procedure must be in the same PDB in which the rule and its rule set reside. To find the existing PDBs, query the DBA\_PDBS data dictionary view. The rule and rule set must be local.

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check UPDATE operations',
    rule_expr => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') = ''SYSADM''',
    scope     => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/
```

This example shows a multitenant environment common version of the preceding example. The user running this procedure must be in the CDB root, and the rule and its associated rule set must be common. The rule will reside in the application root.

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check UPDATE operations',
    rule_expr => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') = ''SYSADM''',
    scope     => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

This example shows how to create a rule expression that uses the public standalone function OLS\_LABEL\_DOMINATES to find if the session label of the hr\_ols\_pol

Oracle Label Security policy dominates or is equal to the hs label. The value 0 indicates if it is false. (To check if it is equal, you would specify 1.)

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check OLS Factor',
    rule_expr => 'OLS_LABEL_DOMINATES(''hr_ols_pol'', ''hs'') = 1');
END;
/
```

## 16.1.3 CREATE\_RULE\_SET Procedure

The CREATE\_RULE\_SET procedure creates a rule set.

After you create a rule set, you can use the CREATE\_RULE and ADD\_RULE\_TO\_RULE\_SET procedures to create and add rules to the rule set.

### Syntax

```
DBMS_MACADM.CREATE_RULE_SET(
  rule_set_name    IN VARCHAR2,
  description      IN VARCHAR2,
  enabled          IN VARCHAR2,
  eval_options     IN NUMBER,
  audit_options   IN NUMBER,
  fail_options     IN NUMBER,
  fail_message     IN VARCHAR2,
  fail_code        IN NUMBER,
  handler_options  IN NUMBER,
  handler          IN VARCHAR2,
  is_static        IN BOOLEAN DEFAULT,
  scope           IN NUMBER DEFAULT);
```

### Parameters

**Table 16-3 CREATE\_RULE\_SET Parameters**

Parameter	Description
rule_set_name	Rule set name, up to 128 characters in mixed-case. Spaces are allowed. To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).
description	Description of the purpose of the rule set, up to 1024 characters in mixed-case.
enabled	DBMS_MACUTL.G_YES (Yes) enables the rule set; DBMS_MACUTL.G_NO (No) disables it. The default is DBMS_MACUTL.G_YES.
eval_options	If you plan to assign multiple rules to the rule set, enter one of the following settings: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_RULESET_EVAL_ALL: All rules in the rule set must evaluate to true for the rule set itself to evaluate to true (default).</li> <li>DBMS_MACUTL.G_RULESET_EVAL_ANY: At least one rule in the rule set must evaluate to true for the rule set itself to evaluate to true.</li> </ul>

**Table 16-3 (Cont.) CREATE\_RULE\_SET Parameters**

Parameter	Description
audit_options	Select one of the following settings: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_RULESET_AUDIT_OFF: Disables auditing for the rule set (default)</li> <li>DBMS_MACUTL.G_RULESET_AUDIT_FAIL: Creates an audit record when a rule set violation occurs</li> <li>DBMS_MACUTL.G_RULESET_AUDIT_SUCCESS: Creates an audit record for a successful rule set evaluation</li> <li>DBMS_MACUTL.G_RULESET_AUDIT_FAIL + DBMS_MACUTL.G_RULESET_AUDIT_SUCCESS: Creates an audit record for both successful and failed rule set evaluations</li> </ul>
fail_options	Options for reporting errors: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_RULESET_FAIL_SHOW: Shows an error message (default)</li> <li>DBMS_MACUTL.G_RULESET_FAIL_SILENT: Does not show an error message</li> </ul>
fail_message	Enter an error message for failure, up to 80 characters in mixed-case, to associate with the fail code you specify for fail_code.
fail_code	Enter a number in the range of -20000 to -20999 or 20000 to 20999 to associate with the fail_message parameter.
handler_options	Select one of the following settings: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_RULESET_HANDLER_OFF: Disables error handling (default)</li> <li>DBMS_MACUTL.G_RULESET_HANDLER_FAIL: Calls handler on rule set failure</li> <li>DBMS_MACUTL.G_RULESET_HANDLER_SUCCESS: Calls handler on rule set success</li> </ul>
handler	Name of the PL/SQL function or procedure that defines the custom event handler logic.
is_static	Optional. Determines how often a rule set is evaluated when it is accessed. The default is FALSE. <ul style="list-style-type: none"> <li>TRUE: The rule set is evaluated once during the user session. After that, the value is re-used.</li> <li>FALSE: The rule set is evaluated every time.</li> </ul>
scope	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the rule set is to be local in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the rule set is to be in the application root</li> </ul>

### Examples

The following example creates a rule set that is enabled, is set so that at least one rule must evaluate to true for the rule set itself to evaluate to true, and audits both failed and successful attempts. It does not show error messages but uses the fail code 20461 to track failures. It also uses a handler to send email alerts to the appropriate users if there are violations to the rule set.

```

BEGIN
  DBMS_MACADM.CREATE_RULE_SET(
    rule_set_name    => 'Limit_DBA_Access',
    description      => 'DBA access through predefined processes',
    enabled          => DBMS_MACUTL.G_YES,
    eval_options     => DBMS_MACUTL.G_RULESET_EVAL_ANY,
    audit_options    => DBMS_MACUTL.G_RULESET_AUDIT_FAIL +
DBMS_MACUTL.G_RULESET_AUDIT_SUCCESS,
    fail_options     => DBMS_MACUTL.G_RULESET_FAIL_SILENT,
    fail_message     => '',
    fail_code        => 20461,
    handler_options  => DBMS_MACUTL.G_RULESET_HANDLER_FAIL,
    handler          => 'dbavowner.email_alert',
    is_static        => TRUE);
END;
/

```

This rule set uses no fail messages or fail codes, nor does it use any handlers. This rule set will be in the application root of a multitenant environment, so the user running this procedure must be in the application root. Any rules or command rules that are associated with this rule set must be common.

```

BEGIN
  DBMS_MACADM.CREATE_RULE_SET(
    rule_set_name    => 'Check_HR_Access',
    description      => 'Checks for failed access attempts to the HR schema',
    enabled          => DBMS_MACUTL.G_YES,
    eval_options     => DBMS_MACUTL.G_RULESET_EVAL_ANY,
    audit_options    => DBMS_MACUTL.G_RULESET_AUDIT_FAIL,
    fail_options     => DBMS_MACUTL.G_RULESET_FAIL_SILENT,
    fail_message     => '',
    fail_code        => '',
    handler_options  => DBMS_MACUTL.G_RULESET_HANDLER_OFF,
    handler          => '',
    is_static        => TRUE,
    scope            => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/

```

This rule set is a local version of the preceding rule set. The user who creates this rule set must be in the PDB in which this rule set will reside. To find the existing PDBs, query the DBA\_PDBS data dictionary view. Any rules or command rules that are associated with this rule set must be local.

```

BEGIN
  DBMS_MACADM.CREATE_RULE_SET(
    rule_set_name    => 'Check_HR_Access',
    description      => 'Checks for failed access attempts to the HR schema',
    enabled          => DBMS_MACUTL.G_YES,
    eval_options     => DBMS_MACUTL.G_RULESET_EVAL_ANY,
    audit_options    => DBMS_MACUTL.G_RULESET_AUDIT_FAIL,
    fail_options     => DBMS_MACUTL.G_RULESET_FAIL_SILENT,
    fail_message     => '',
    fail_code        => '',
    handler_options  => DBMS_MACUTL.G_RULESET_HANDLER_OFF,
    handler          => '',
    is_static        => TRUE,
    scope            => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/

```

**See Also:**[Example 21-2](#) (page 21-6)

## 16.1.4 DELETE\_RULE Procedure

The DELETE\_RULE procedure deletes a rule.

**Syntax**

```
DBMS_MACADM.DELETE_RULE(  
  rule_name IN VARCHAR2);
```

**Parameter****Table 16-4** DELETE\_RULE Parameter

Parameter	Description
rule_name	Rule name.  To find existing rules in the current database instance, query the DBA_DV_RULE view, described in <a href="#">DBA_DV_RULE View</a> (page 25-29). To find rules that have been associated with rule sets, query DBA_DV_RULE_SET_RULE, described in <a href="#">DBA_DV_RULE_SET_RULE View</a> (page 25-32).

**Example**

```
EXEC DBMS_MACADM.DELETE_RULE('Check UPDATE operations');
```

## 16.1.5 DELETE\_RULE\_FROM\_RULE\_SET Procedure

The DELETE\_RULE\_FROM\_RULE\_SET procedure deletes a rule from a rule set.

**Syntax**

```
DBMS_MACADM.DELETE_RULE_FROM_RULE_SET(  
  rule_set_name IN VARCHAR2,  
  rule_name      IN VARCHAR2);
```

**Parameters****Table 16-5** DELETE\_RULE\_FROM\_RULE\_SET Parameters

Parameter	Description
rule_set_name	Rule set name.  To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).

**Table 16-5 (Cont.) DELETE\_RULE\_FROM\_RULE\_SET Parameters**

Parameter	Description
rule_name	Rule to remove from the rule set. To find existing rules in the current database instance, query the DBA_DV_RULE view, described in <a href="#">DBA_DV_RULE View</a> (page 25-29). To find rules that have been associated with rule sets, query DBA_DV_RULE_SET_RULE, described in <a href="#">DBA_DV_RULE_SET_RULE View</a> (page 25-32).

**Example**

```
BEGIN
  DBMS_MACADM.DELETE_RULE_FROM_RULE_SET(
    rule_set_name => 'Limit_DBA_Access',
    rule_name      => 'Check UPDATE operations');
END;
/
```

**16.1.6 DELETE\_RULE\_SET Procedure**

The DELETE\_RULE\_SET procedure deletes a rule set.

**Syntax**

```
DBMS_MACADM.DELETE_RULE_SET(
  rule_set_name IN VARCHAR2);
```

**Parameters****Table 16-6 DELETE\_RULE\_SET Parameter**

Parameter	Description
rule_set_name	Rule set name. To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).

**Example**

```
EXEC DBMS_MACADM.DELETE_RULE_SET('Limit_DBA_Access');
```

**16.1.7 RENAME\_RULE Procedure**

The RENAME\_RULE procedure renames a rule and causes the name change to take effect everywhere the rule is used

**Syntax**

```
DBMS_MACADM.RENAME_RULE(
  rule_name  IN VARCHAR2,
  new_name   IN VARCHAR2,
  scope      IN NUMBER DEFAULT);
```

## Parameters

**Table 16-7** *RENAME\_RULE Parameters*

Parameter	Description
rule_name	Current rule name. To find existing rules in the current database instance, query the DBA_DV_RULE view, described in <a href="#">DBA_DV_RULE View</a> (page 25-29). To find rules that have been associated with rule sets, query DBA_DV_RULE_SET_RULE, described in <a href="#">DBA_DV_RULE_SET_RULE View</a> (page 25-32).
new_name	New rule name, up to 128 characters in mixed-case.
scope	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the rule is local in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the rule is in the application root</li> </ul>

## Example

```
BEGIN
  DBMS_MACADM.RENAME_RULE(
    rule_name => 'Check UPDATE operations',
    new_name  => 'Check Sector 2 Processes');
END;
/
```

## 16.1.8 RENAME\_RULE\_SET Procedure

The RENAME\_RULE\_SET procedure renames a rule set and causes the name change to take effect everywhere the rule set is used.

### Syntax

```
DBMS_MACADM.RENAME_RULE_SET(
  rule_set_name IN VARCHAR2,
  new_name      IN VARCHAR2,
  scope         IN NUMBER DEFAULT);
```

## Parameters

**Table 16-8** *RENAME\_RULE\_SET Parameters*

Parameter	Description
rule_set_name	Current rule set name. To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).
new_name	New rule set name, up to 128 characters in mixed-case. Spaces are allowed.



**Table 16-8 (Cont.) RENAME\_RULE\_SET Parameters**

Parameter	Description
scope	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the rule set is local in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the rule set is in the application root</li> </ul>

**Example**

```
BEGIN
  DBMS_MACADM.RENAME_RULE_SET(
    rule_set_name => 'Limit_DBA_Access',
    new_name      => 'Limit Sector 2 Access');
END;
/
```

**16.1.9 UPDATE\_RULE Procedure**

The UPDATE\_RULE procedure updates a rule.

**Syntax**

```
DBMS_MACADM.UPDATE_RULE(
  rule_name  IN VARCHAR2,
  rule_expr  IN VARCHAR2);
```

**Parameters****Table 16-9 UPDATE\_RULE Parameters**

Parameter	Description
rule_name	Rule name. To find existing rules in the current database instance, query the DBA_DV_RULE view, described in <a href="#">DBA_DV_RULE View</a> (page 25-29). To find rules that have been associated with rule sets, query DBA_DV_RULE_SET_RULE, described in <a href="#">DBA_DV_RULE_SET_RULE View</a> (page 25-32).
rule_expr	PL/SQL BOOLEAN expression. If the expression contains quotation marks, do not use double quotation marks. Instead, use two single quotation marks. Enclose the entire expression within single quotation marks. For example:  <code>'TO_CHAR(SYSDATE, 'HH24') = '12''</code>  See <a href="#">Creating a New Rule</a> (page 6-12) for more information on rule expressions. To find existing rule expressions, query the DBA_DV_RULE view.

**Example**

```

BEGIN
  DBMS_MACADM.UPDATE_RULE(
    rule_name => 'Check UPDATE operations',
    rule_expr => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') = ''SYSADM'' AND
      (
        UPPER(SYS_CONTEXT(''USERENV'', ''MODULE'')) LIKE ''APPSRV%' OR
        UPPER(SYS_CONTEXT(''USERENV'', ''MODULE'')) LIKE ''DBAPP%' )'
      );
END;
/

```

**16.1.10 UPDATE\_RULE\_SET Procedure**

The UPDATE\_RULE\_SET procedure updates a rule set.

**Syntax**

```

DBMS_MACADM.UPDATE_RULE_SET(
  rule_set_name      IN VARCHAR2,
  description        IN VARCHAR2,
  enabled            IN VARCHAR2,
  eval_options       IN NUMBER,
  audit_options      IN NUMBER,
  fail_options       IN NUMBER,
  fail_message       IN VARCHAR2,
  fail_code          IN NUMBER,
  handler_options    IN NUMBER,
  handler            IN VARCHAR2,
  is_static          IN BOOLEAN DEFAULT);

```

**Parameters****Table 16-10 UPDATE\_RULE\_SET Parameters**

Parameter	Description
rule_set_name	Rule set name. To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).
description	Description of the purpose of the rule set, up to 1024 characters in mixed-case.
enabled	DBMS_MACUTL.G_YES (Yes) enables rule set checking; DBMS_MACUTL.G_NO (No) disables it. The default for the enabled setting is the previously set value, which you can find by querying the DBA_DV_RULE_SET data dictionary view.

**Table 16-10 (Cont.) UPDATE\_RULE\_SET Parameters**

Parameter	Description
eval_options	<p>If you plan to assign multiple rules to the rule set, enter one of the following settings:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_RULESET_EVAL_ALL: All rules in the rule set must evaluate to true for the rule set itself to evaluate to true.</li> <li>DBMS_MACUTL.G_RULESET_EVAL_ANY: At least one rule in the rule set must evaluate to true for the rule set itself to evaluate to true.</li> </ul> <p>The default for eval_options is the previously set value, which you can find by querying the DBA_DV_RULE_SET data dictionary view.</p>
audit_options	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_RULESET_AUDIT_OFF: Disables auditing for the rule set</li> <li>DBMS_MACUTL.G_RULESET_AUDIT_FAIL: Creates an audit record when a rule set violation occurs</li> <li>DBMS_MACUTL.G_RULESET_AUDIT_SUCCESS: Creates an audit record for a successful rule set evaluation</li> <li>DBMS_MACUTL.G_RULESET_AUDIT_FAIL + DBMS_MACUTL.G_RULESET_AUDIT_SUCCESS: Creates an audit record for both successful and failed rule set evaluations</li> </ul> <p>The default for audit_options is the previously set value, which you can find by querying the DBA_DV_RULE_SET data dictionary view.</p>
fail_options	<p>Options for reporting errors:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_RULESET_FAIL_SHOW: Shows an error message.</li> <li>DBMS_MACUTL.G_RULESET_FAIL_SILENT: Does not show an error message.</li> </ul> <p>The default for fail_options is the previously set value, which you can find by querying the DBA_DV_RULE_SET data dictionary view.</p>
fail_message	<p>Error message for failure, up to 80 characters in mixed-case, to associate with the fail code you specify for fail_code.</p>
fail_code	<p>Enter a number in the range of -20000 to -20999 or 20000 to 20999 to associate with the fail_message parameter.</p>
handler_options	<p>Select one of the following settings:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_RULESET_HANDLER_OFF: Disables error handling.</li> <li>DBMS_MACUTL.G_RULESET_HANDLER_FAIL: Call handler on rule set failure.</li> <li>DBMS_MACUTL.G_RULESET_HANDLER_SUCCESS: Call handler on rule set success.</li> </ul> <p>The default for handler_options is the previously set value, which you can find by querying the DBA_DV_RULE_SET data dictionary view.</p>
handler	<p>Name of the PL/SQL function or procedure that defines the custom event handler logic.</p>

**Table 16-10 (Cont.) UPDATE\_RULE\_SET Parameters**

Parameter	Description
<code>is_static</code>	Optional. Determines how often a rule set is evaluated when it is accessed by a SQL statement. The default is <code>FALSE</code> . <ul style="list-style-type: none"> <li><code>TRUE</code>: The rule set is evaluated once during the user session. After that, the value is re-used.</li> <li><code>FALSE</code>: The rule set evaluated each time a SQL statement accesses it.</li> </ul>

**Example**

```

BEGIN
  DBMS_MACADM.UPDATE_RULE_SET(
    rule_set_name => 'Limit_DBA_Access',
    description   => 'DBA access through predefined processes',
    enabled       => DBMS_MACUTL.G_YES,
    eval_options  => DBMS_MACUTL.G_RULESET_EVAL_ANY,
    audit_options => DBMS_MACUTL.G_RULESET_AUDIT_FAIL,
    fail_options  => DBMS_MACUTL.G_RULESET_FAIL_SHOW,
    fail_message  => 'Access denied!',
    fail_code     => 20900,
    handler_options => DBMS_MACUTL.G_RULESET_HANDLER_OFF,
    handler       => '',
    is_static     =  TRUE);
END;
/

```

## 16.2 Oracle Database Vault PL/SQL Rule Set Functions

Oracle Database Vault provides functions to use in rule sets to inspect the SQL statement that the rule set protects.

**DV\_SYSEVENT Function** (page 16-15)

The `DV_SYSEVENT` function returns the system event firing the rule set. .

**DV\_LOGIN\_USER Function** (page 16-15)

The `DV_LOGIN_USER` function returns the login user name, in `VARCHAR2` data type.

**DV\_INSTANCE\_NUM Function** (page 16-15)

The `DV_INSTANCE_NUM` function returns the database instance number, in `NUMBER` data type.

**DV\_DATABASE\_NAME Function** (page 16-16)

The `DV_DATABASE_NAME` function returns the database name, in `VARCHAR2` data type.

**DV\_DICT\_OBJ\_TYPE Function** (page 16-16)

The `DV_DICT_OBJ_TYPE` function returns the type of the dictionary object on which the database operation occurred.

**DV\_DICT\_OBJ\_OWNER Function** (page 16-17)

The `DV_DICT_OBJ_OWNER` function returns the name of the owner of the dictionary object on which the database operation occurred.

**DV\_DICT\_OBJ\_NAME Function** (page 16-17)

The DV\_DICT\_OBJ\_NAME function returns the name of the dictionary object on which the database operation occurred.

**DV\_SQL\_TEXT Function** (page 16-18)

The DV\_SQL\_TEXT function returns the first 4000 characters of SQL text of the database statement used in the operation.

**16.2.1 DV\_SYSEVENT Function**

The DV\_SYSEVENT function returns the system event firing the rule set. .

The event name is the same as that in the syntax of the SQL statement (for example, INSERT, CREATE.) The return type is VARCHAR2.

**Syntax**

```
DV_SYSEVENT ()
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Get System Event Firing the Maintenance Rule Set',
    rule_expr => 'DV_SYSEVENT = ''CREATE''');
END;
/
```

**16.2.2 DV\_LOGIN\_USER Function**

The DV\_LOGIN\_USER function returns the login user name, in VARCHAR2 data type.

**Syntax**

```
DV_LOGIN_USER ()
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check System Login User Name',
    rule_expr => 'DV_LOGIN_USER = ''SEBASTIAN''');
END;
/
```

**16.2.3 DV\_INSTANCE\_NUM Function**

The DV\_INSTANCE\_NUM function returns the database instance number, in NUMBER data type.

**Syntax**

```
DV_INSTANCE_NUM ()  
RETURN NUMBER;
```

**Parameters**

None

**Example**

```
BEGIN  
  DBMS_MACADM.CREATE_RULE(  
    rule_name => 'Check Database Instance Number',  
    rule_expr => 'DV_INSTANCE_NUM BETWEEN 6 AND 9');  
END;  
/
```

## 16.2.4 DV\_DATABASE\_NAME Function

The DV\_DATABASE\_NAME function returns the database name, in VARCHAR2 data type.

**Syntax**

```
DV_DATABASE_NAME ()  
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```
BEGIN  
  DBMS_MACADM.CREATE_RULE(  
    rule_name => 'Check Database Name',  
    rule_expr => 'DV_DATABASE_NAME = ''ORCL''');  
END;  
/
```

## 16.2.5 DV\_DICT\_OBJ\_TYPE Function

The DV\_DICT\_OBJ\_TYPE function returns the type of the dictionary object on which the database operation occurred.

For example, dictionary objects it returns are table, procedure, or view. The return type is VARCHAR2.

**Syntax**

```
DV_DICT_OBJ_TYPE ()  
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```

BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Dictionary Object Type',
    rule_expr => 'DV_DICT_OBJ_TYPE IN (''TABLE'', ''VIEW'')');
END;
/

```

**16.2.6 DV\_DICT\_OBJ\_OWNER Function**

The `DV_DICT_OBJ_OWNER` function returns the name of the owner of the dictionary object on which the database operation occurred.

The return type is `VARCHAR2`.

**Syntax**

```

DV_DICT_OBJ_OWNER ()
RETURN VARCHAR2;

```

**Parameters**

None

**Example**

```

BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Dictionary Object Owner',
    rule_expr => 'DV_DICT_OBJ_OWNER = ''JSMITH''');
END;
/

```

**16.2.7 DV\_DICT\_OBJ\_NAME Function**

The `DV_DICT_OBJ_NAME` function returns the name of the dictionary object on which the database operation occurred.

The return type is `VARCHAR2`.

**Syntax**

```

DV_DICT_OBJ_NAME ()
RETURN VARCHAR2;

```

**Parameters**

None

**Example**

```

BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Dictionary Object Name',
    rule_expr => 'DV_DICT_OBJ_NAME = ''SALES''');
END;
/

```

## 16.2.8 DV\_SQL\_TEXT Function

The DV\_SQL\_TEXT function returns the first 4000 characters of SQL text of the database statement used in the operation.

The return type is VARCHAR2.

### Syntax

```
DV_SQL_TEXT ()  
RETURN VARCHAR2;
```

### Parameters

None

### Example

```
BEGIN  
  DBMS_MACADM.CREATE_RULE(  
    rule_name => 'Check SQL Text',  
    rule_expr => 'DV_SQL_TEXT = ''SELECT SALARY FROM HR.EMPLOYEES''');  
END;  
/
```



---

## Oracle Database Vault Command Rule APIs

The DBMS\_MACADM PL/SQL package provides procedures for configuring command rules. .

Only users who have been granted the DV\_OWNER or DV\_ADMIN role can use these procedures.

### [CREATE\\_COMMAND\\_RULE Procedure](#) (page 17-2)

The CREATE\_COMMAND\_RULE procedure creates a command rule and associates it with a rule set.

### [CREATE\\_CONNECT\\_COMMAND\\_RULE Procedure](#) (page 17-9)

The CREATE\_CONNECT\_COMMAND\_RULE procedure creates a CONNECT command rule that you can associate with a user and a rule set.

### [CREATE\\_SESSION\\_EVENT\\_CMD\\_RULE Procedure](#) (page 17-11)

The CREATE\_SESSION\_EVENT\_CMD\_RULE procedure creates a command rule that you can associate with session events, based on the ALTER SESSION statement.

### [CREATE\\_SYSTEM\\_EVENT\\_CMD\\_RULE Procedure](#) (page 17-12)

The CREATE\_SYSTEM\_EVENT\_CMD\_RULE procedure creates a command rule that you can associate with system events, based on the ALTER SYSTEM statement.

### [DELETE\\_COMMAND\\_RULE Procedure](#) (page 17-14)

The DELETE\_COMMAND\_RULE procedure drops a command rule declaration.

### [DELETE\\_CONNECT\\_COMMAND\\_RULE Procedure](#) (page 17-16)

The DELETE\_CONNECT\_COMMAND\_RULE procedure deletes a CONNECT command rule that had been created with the CREATE\_CONNECT\_COMMAND\_RULE procedure.

### [DELETE\\_SESSION\\_EVENT\\_CMD\\_RULE Procedure](#) (page 17-17)

The DELETE\_SESSION\_EVENT\_CMD\_RULE procedure deletes a session command rule that was associated with events.

### [DELETE\\_SYSTEM\\_EVENT\\_CMD\\_RULE Procedure](#) (page 17-17)

The DELETE\_SYSTEM\_EVENT\_CMD\_RULE procedure deletes a system command rule that was associated with events.

### [UPDATE\\_COMMAND\\_RULE Procedure](#) (page 17-18)

The UPDATE\_COMMAND\_RULE procedure updates a command rule declaration.

**[UPDATE\\_CONNECT\\_COMMAND\\_RULE Procedure](#)** (page 17-21)

The `UPDATE_CONNECT_COMMAND_RULE` procedure updates a `CONNECT` command rule that had been created with the `CREATE_CONNECT_COMMAND_RULE` procedure.

**[UPDATE\\_SESSION\\_EVENT\\_CMD\\_RULE Procedure](#)** (page 17-22)

The `UPDATE_SESSION_EVENT_CMD_RULE` procedure updates a session event command rule, based on the `ALTER SESSION` statement.

**[UPDATE\\_SYSTEM\\_EVENT\\_CMD\\_RULE Procedure](#)** (page 17-24)

The `UPDATE_SYSTEM_EVENT_CMD_RULE` procedure updates a system event command rule, based on the `ALTER SYSTEM` statement.

**Related Topics:****[Configuring Command Rules](#)** (page 7-1)

You can create command rules or use the default command rules to protect DDL and DML statements.

**[Oracle Database Vault Utility APIs](#)** (page 21-1)

Oracle Database Vault provides a set of utility APIs in the `DBMS_MACUTL` PL/SQL package.

## 17.1 CREATE\_COMMAND\_RULE Procedure

The `CREATE_COMMAND_RULE` procedure creates a command rule and associates it with a rule set.

Optionally, you can use it to enable the command rule for rule checking with a rule set. In a multitenant environment, you can create both common and local command rules.

**Syntax**

```
DBMS_MACADM.CREATE_COMMAND_RULE(  
  command           IN VARCHAR2,  
  rule_set_name     IN VARCHAR2,  
  object_owner      IN VARCHAR2,  
  object_name       IN VARCHAR2,  
  enabled           IN VARCHAR2,  
  privilege_scope   IN NUMBER,  
  clause_name       IN VARCHAR2,  
  parameter_name    IN VARCHAR2,  
  event_name        IN VARCHAR2,  
  component_name    IN VARCHAR2,  
  action_name       IN VARCHAR2,  
  scope             IN NUMBER DEFAULT);
```

## Parameters

**Table 17-1 CREATE\_COMMAND\_RULE Parameters**

Parameter	Description
command	<p>SQL statement to protect.</p> <p>See also the following:</p> <ul style="list-style-type: none"> <li>• <a href="#">Default Command Rules</a> (page 7-7) for information about default command rules</li> <li>• <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8) for a listing of existing command rules</li> <li>• <a href="#">SQL Statements That Can Be Protected by Command Rules</a> (page 7-8) for a listing of available SQL statements that you can use</li> </ul>
rule_set_name	<p>Name of rule set to associate with this command rule.</p> <p>To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).</p>
object_owner	<p>Database schema to which this command rule will apply. The wildcard % is allowed, except for the SELECT, INSERT, UPDATE, DELETE, and EXECUTE statements.</p> <p>To find the available users, query the DBA_USERS view, described in <i>Oracle Database Reference</i>.</p> <p>See also "Object Owner" in <a href="#">Creating a Command Rule</a> (page 7-9) for more information.</p>
object_name	<p>Object to be protected by the command rule. (The wildcard % is allowed. See "Object Name" in <a href="#">Creating a Command Rule</a> (page 7-9) for more information about objects protected by command rules.)</p> <p>To find the available objects, query the ALL_OBJECTS view, described in <i>Oracle Database Reference</i>.</p>
enabled	<p>Specify one of the following options to set the status of the command rule:</p> <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_YES or 'y' (Yes) to enable the command rule (default)</li> <li>• DBMS_MACUTL.G_NO or 'n' to disable the command rule, including the capture of violations in the simulation log</li> <li>• DBMS_MACUTL.G_SIMULATION or 's' to enable SQL statements to execute but capture violations in the simulation log</li> </ul>
privilege_scope	<p>Obsolete parameter</p>
clause_name	<p>A clause from the SQL statement that was used to create the command rule. For example, a command rule for the ALTER SESSION SQL statement could have the SET clause as the clause_name parameter.</p> <p>Applies only to command rules for ALTER SYSTEM and ALTER SESSION.</p>
parameter_name	<p>A parameter from the clause_name parameter. For example, for an ALTER SESSION command rule, you could set parameter_name to EVENTS if the clause_name is SET.</p> <p>Applies only to command rules for ALTER SYSTEM and ALTER SESSION.</p>

**Table 17-1 (Cont.) CREATE\_COMMAND\_RULE Parameters**

Parameter	Description
event_name	An event that the command rule defines. For example, suppose an ALTER SESSION command rule uses SET for the clause_name and EVENTS as the parameter_name. The event_name could be set to TRACE if you want to track trace events.  Applies only to ALTER SYSTEM and ALTER SESSION command rules that have the parameter parameter set to EVENTS.
component_name	A component of the event_name setting. For example, for a TRACE event, the component_name could be GCS.  Applies only to ALTER SYSTEM and ALTER SESSION command rules that have the parameter parameter set to EVENTS.
action_name	An action of the component_name setting.  Applies only to ALTER SYSTEM and ALTER SESSION command rules that have the parameter parameter set to EVENTS.
scope	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the command rule is local in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the command rule is in the application root</li> </ul> If you create the common command rule in an application root and want it visible to the associated PDBs, then you must synchronize the application. For example:  ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;

## ALTER SYSTEM Command Rule Settings

Table 17-2 (page 17-4) describes the ALTER SYSTEM command rule settings.

**Table 17-2 ALTER SYSTEM Command Rule Settings**

clause_name	parameter_name — Parameter Value
ARCHIVE LOG	<ul style="list-style-type: none"> <li>ALL — <i>sequence_number</i></li> <li>CHANGE — <i>change_number</i></li> <li>CURRENT — N/A</li> <li>GROUP — <i>group_number</i></li> <li>LOGFILE — <i>log_file_name</i></li> <li>NEXT — N/A</li> <li>SEQUENCE — N/A</li> </ul>
CHECK DATAFILES	N/A — global or local
CHECKPOINT	N/A — global or local
COPY LOGFILE	N/A — N/A
DISTRIBUTED RECOVERY	N/A — enable or disable

**Table 17-2 (Cont.) ALTER SYSTEM Command Rule Settings**

<b>clause_name</b>	<b>parameter_name — Parameter Value</b>
DUMP	<ul style="list-style-type: none"> <li>• DATAFILE — N/A</li> <li>• FLASHBACK — N/A</li> <li>• LOGFILE — N/A</li> <li>• REDO — N/A</li> <li>• TEMPFILE — N/A</li> <li>• UNDO — N/A</li> </ul>
END SESSION	DISCONNECT SESSION — N/A KILL SESSION — N/A
FLUSH	BUFFER_CACHE — N/A GLOBAL_CONTEXT — N/A REDO — <i>target_db_name</i> SHARED_POOL — N/A
QUIESCE	QUIESCE RESTRICTED — N/A UNQUIESCE — N/A
REFRESH	LDAP_REGISTRATION — N/A
REGISTER	N/A — N/A
RESET	<i>initialization_parameter_name</i> — N/A
RESUME	N/A — N/A
SECURITY	RESTRICTED_SESSION — enable or disable SET_ENCRYPTION_KEY — N/A SET_ENCRYPTION_WALLET — open or close
SET	EVENTS — <i>event_string</i> GLOBAL_TOPIC_ENABLED — true or false <i>initialization_parameter_name</i> — <i>parameter_value</i> LDAP_REGISTRATION_ENABLED — true or false LDAP_REG_SYNC_INTERVAL — Number SINGLETASK_DEBUG — N/A USE_STORED_OUTLINES — true, false, or <i>category_name</i>
SHUTDOWN DISPATCHER	N/A — <i>dispatcher_name</i>
SWITCH LOGFILE	N/A — all or none
SUSPEND	N/A — N/A
TX RECOVERY	N/A — enable or disable

**ALTER SESSION Command Rule Settings**

Table 17-3 (page 17-6) describes the ALTER SESSION command rule settings.

**Table 17-3 ALTER SESSION Command Rule Settings**

<b>clause_name</b>	<b>parameter_name — Parameter Value</b>
ADVISE	N/A — COMMIT, ROLLBACK, or NOTHING
CLOSE DATABASE LINK	N/A — <i>database_link</i>
COMMIT IN PROCEDURE	N/A — ENABLE or DISABLE
GUARD	N/A — ENABLE or DISABLE
ILM	ROW ACCESS TRACKING — N/A ROW MODIFICATION TRACKING — N/A
LOGICAL REPLICATION	N/A — N/A
PARALLEL DML	N/A — ENABLE, DISABLE, or FORCE
PARALLEL DDL	N/A — ENABLE, DISABLE, or FORCE
PARALLEL QUERY	N/A — ENABLE, DISABLE, or FORCE
RESUMABLE	N/A — ENABLE or DISABLE
SYNC WITH PRIMARY	N/A — N/A
SET	APPLICATION ACTION — <i>action_name</i> APPLICATION MODULE — <i>module_name</i> CONSTRAINTS — IMMEDIATE, DEFERRED, or DEFAULT CONTAINER — <i>container_name</i> CURRENT SCHEMA — <i>schema_name</i> EDITION — <i>edition_name</i> ERROR ON OVERLAP TIME — TRUE or FALSE EVENTS — <i>event_string</i> FLAGGER — OFF, FULL, INTERMEDIATE, ENTRY <i>initialization_parameter_name</i> — <i>parameter_name</i> INSTANCE — <i>instance_number</i> ISOLATION_LEVEL — SERIALIZABLE or READ COMMITTED ROW_ARCHIVAL_VISABILITY — ACTIVE or ALL SQL_TRANSFORMATION_PROFILE — <i>profile_name</i> STANDBY_MAX_DATA_DELAY — NONE <i>number</i> TIME_ZONE — LOCAL, DBTIMEZONE, or <i>other_value</i> USE_PRIVATE_OUTLINES — TRUE, FALSE, or <i>category_name</i> USE_STORED_OUTLINES — TRUE, FALSE, or <i>category_name</i>

## Examples

The following example shows how to create a simple command rule for the SELECT statement on the OE.ORDERS table. This command rule uses no command rules.

```
BEGIN
  DBMS_MACADM.CREATE_COMMAND_RULE(
    command      => 'SELECT',
    object_owner  => 'OE',
    object_name   => 'ORDERS',
    enabled       => DBMS_MACUTL.G_YES);
END;
/
```

## ALTER SESSION Command Rule Using the SET Clause

The following example shows how to create an ALTER SESSION command rule that uses the SET clause with the ERROR\_ON\_OVERLAP\_TIME parameter.

```
BEGIN
  DBMS_MACADM.CREATE_COMMAND_RULE(
    command      => 'ALTER SESSION',
    rule_set_name => 'Test ERROR_ON_OVERLAP_TIME for FALSE',
    object_owner  => '%',
    object_name   => '%',
    enabled       => DBMS_MACUTL.G_YES,
    clause_name   => 'SET',
    parameter_name => 'ERROR_ON_OVERLAP_TIME',
    scope         => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

In this example:

- **rule\_set\_name:** The ALTER SESSION SQL statement ERROR\_ON\_OVERLAP\_TIME session parameter must be set to either TRUE or FALSE. You can create a rule set that checks if this setting. For example, for the rule:

```
EXEC DBMS_MACADM.CREATE_RULE('RULE_TRUE', 'UPPER(PARAMETER_VALUE) = ''TRUE''');
```

The rule set that is used with this rule can be similar to the following:

```
BEGIN
  DBMS_MACADM.CREATE_RULE_SET(
    rule_set_name  => 'Test ERROR_ON_OVERLAP_TIME',
    description    => 'Checks if the ERROR_ON_OVERLAP_TIME setting is TRUE or
FALSE',
    enabled        => DBMS_MACUTL.G_YES,
    eval_options   => DBMS_MACUTL.G_RULESET_EVAL_ALL,
    audit_options  => DBMS_MACUTL.G_RULESET_AUDIT_FAIL +
DBMS_MACUTL.G_RULESET_AUDIT_SUCCESS,
    fail_options   => DBMS_MACUTL.G_RULESET_FAIL_SILENT,
    fail_message   => 'false error on overlaptime',
    fail_code      => 20461,
    handler_options => DBMS_MACUTL.G_RULESET_HANDLER_FAIL,
    handler        => '',
    is_static      => false);
END;
/
EXEC DBMS_MACADM.ADD_RULE_TO_RULE_SET('Test ERROR_ON_OVERLAP_TIME', 'RULE_TRUE');
```

- `object_owner` and `object_name` must be set to `%` for `ALTER SESSION` and `ALTER SYSTEM` command rules.
- `enabled` uses the `DBMS_MACUTL.G_YES` constant to enable the command rule when it is created.
- `clause_name` sets the `ALTER SESSION` command rule to use the `SET` clause of the `ALTER SESSION PL/SQL` statement.
- `parameter_name` is set to the `ERROR_ON_OVERLAP_TIME` parameter of the `SET` clause.
- `scope` uses the `DBMS_MACUTL.G_SCOPE_COMMON` constant to set the command rule to be a common command rule. This command rule will be in the application root of a multitenant environment, so the user running this procedure must be in the CDB root. Any rules or rule sets that are associated with this command rule must be common.

If you were creating the command rule locally, you would set `scope` to `DBMS_MACUTL.G_SCOPE_LOCAL`. In that case, the user who runs this procedure must be in the PDB in which the command rule will reside. To find the existing PDBs, you can query the `DBA_PDBS` data dictionary view. Any rules or rule sets that are associated with this command rule must be local.

### ALTER SYSTEM Command Rule Using the CHECKPOINT Clause

This example shows how to create an `ALTER SYSTEM` command rule that uses the `CHECKPOINT` clause. To have the command rule test for the `CHECKPOINT` setting, you must create a rule set and rule, similar to the `ALTER SESSION` command rule in the previous example. In this example, the `parameter` setting is not specified because the `CHECKPOINT` setting does not have parameters.

```
BEGIN
DBMS_MACADM.CREATE_COMMAND_RULE(
  command      => 'ALTER SYSTEM',
  rule_set_name => 'Test CHECKPOINT Setting',
  object_owner  => '%',
  object_name   => '%',
  enabled       => DBMS_MACUTL.G_YES,
  clause_name   => 'CHECKPOINT',
  parameter_name => '',
  scope        => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/
```

### ALTER SESSION Command Rule Using the SET Clause

The following `ALTER SESSION` command rule uses the `SET` clause to specify an `event_name` and `component_name`. You can only use the `event_name`, `component_name`, and `action_name` parameters if the `clause_name` parameter specifies `SET`.

```
BEGIN
DBMS_MACADM.CREATE_COMMAND_RULE(
  command      => 'ALTER SESSION',
  rule_set_name => 'Check Trace Events',
  object_owner  => '%',
  object_name   => '%',
  enabled       => DBMS_MACUTL.G_YES,
  clause_name   => 'SET',
  parameter_name => 'EVENTS',
```



```

event_name      => 'TRACE',
component_name  => 'GCS',
scope           => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/

```

See also [ALTER SESSION and ALTER SYSTEM Command Rules](#) (page 7-5) for conceptual information about this topic.

## 17.2 CREATE\_CONNECT\_COMMAND\_RULE Procedure

The `CREATE_CONNECT_COMMAND_RULE` procedure creates a `CONNECT` command rule that you can associate with a user and a rule set.

In a multitenant environment, you can create both common and local command rules.

### Syntax

```

DBMS_MACADM.CREATE_CONNECT_COMMAND_RULE(
  user_name      IN VARCHAR2,
  rule_set_name  IN VARCHAR2,
  enabled        IN VARCHAR2,
  scope         IN NUMBER DEFAULT);

```

### Parameters

**Table 17-4 CREATE\_CONNECT\_COMMAND\_RULE Parameters**

Parameter	Description
<code>user_name</code>	<p>User to whom the <code>CONNECT</code> command rule will apply. If you enter the <code>%</code> wildcard, then the <code>CONNECT</code> command rule will be applied to every database user.</p> <p>In a multitenant environment, if you execute this procedure in the root, then specifying <code>%</code> applies to all common users. If you run the procedure in a PDB, then it applies to all local and common users who have access to this PDB. If there are two command rules, one common and one local, and they both apply to the same object, then both must evaluate successfully for the operation to succeed.</p> <p>In a multitenant environment, ensure that this user is common if the <code>CONNECT</code> command rule is common, and local or common if the <code>CONNECT</code> command rule is local.</p> <p>To find existing database users in the current instance, query the <code>DBA_USERS</code> view, described in <i>Oracle Database Reference</i>.</p>
<code>rule_set_name</code>	<p>Name of rule set to associate with this command rule. In a multitenant environment, ensure that this rule set is common if the <code>CONNECT</code> command rule is common, and local if the <code>CONNECT</code> command rule is local.</p> <p>To find existing rule sets in the current database instance, query the <code>DBA_DV_RULE_SET</code> view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).</p>

**Table 17-4 (Cont.) CREATE\_CONNECT\_COMMAND\_RULE Parameters**

Parameter	Description
enabled	<p>Specify one of the following options to set the status of the command rule:</p> <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_YES or 'y' (Yes) to enable the command rule (default)</li> <li>• DBMS_MACUTL.G_NO or 'n' to disable the command rule, including the capture of violations in the simulation log</li> <li>• DBMS_MACUTL.G_SIMULATION or 's' to enable SQL statements to execute but capture violations in the simulation log</li> </ul>
scope	<p>For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows:</p> <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the command rule is local in the current PDB</li> <li>• DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the command rule is in the application root</li> </ul> <p>If you create the common CONNECT command rule in an application root and want it visible to the associated PDBs, then you must synchronize the application. For example:</p> <pre>ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;</pre>

## Examples

The following example shows how to create a common CONNECT command rule in a multitenant environment. This command rule will be in the CDB root, so the user who runs this procedure must be in the CDB root. Any user names or rule sets that are associated with this command rule must be common.

```
BEGIN
  DBMS_MACADM.CREATE_CONNECT_COMMAND_RULE(
    rule_set_name => 'Allow Sessions',
    user_name     => 'C##HR_ADMIN',
    enabled       => DBMS_MACUTL.G_SIMULATION,
    scope         => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

This example is a local version of the preceding example. The user who runs this procedure must be in the PDB in which the local CONNECT command rule will reside. To find the existing PDBs, query the DBA\_PDBS data dictionary view. Any rule sets that are associated with this command rule must be local. The user can be either common or local.

```
BEGIN
  DBMS_MACADM.CREATE_CONNECT_COMMAND_RULE(
    rule_set_name => 'Allow Sessions',
    user_name     => 'PSMITH',
    enabled       => DBMS_MACUTL.G_SIMULATION,
    scope         => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/
```

## 17.3 CREATE\_SESSION\_EVENT\_CMD\_RULE Procedure

The `CREATE_SESSION_EVENT_CMD_RULE` procedure creates a command rule that you can associate with session events, based on the `ALTER SESSION` statement.

In a multitenant environment, you can create both session event common and local command rules.

### Syntax

```
DBMS_MACADM.CREATE_SESSION_EVENT_CMD_RULE(
  rule_set_name  IN VARCHAR2,
  enabled        IN VARCHAR2,
  event_name     IN VARCHAR2 DEFAULT,
  component_name IN VARCHAR2 DEFAULT,
  action_name    IN VARCHAR2 DEFAULT,
  scope          IN NUMBER DEFAULT);
```

### Parameters

**Table 17-5 CREATE\_SESSION\_EVENT\_CMD\_RULE Parameters**

Parameter	Description
<code>rule_set_name</code>	<p>Name of the rule set to associate with the command rule. In a multitenant environment, ensure that this rule set is common if the session event command rule is common, and local if the command rule is local.</p> <p>To find existing rule sets in the current database instance, query the <code>DBA_DV_RULE_SET</code> view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).</p>
<code>enabled</code>	<p>Specify one of the following options to set the status of the command rule:</p> <ul style="list-style-type: none"> <li><code>DBMS_MACUTL.G_YES</code> or <code>'y'</code> (Yes) to enable the command rule (default)</li> <li><code>DBMS_MACUTL.G_NO</code> or <code>'n'</code> to disable the command rule, including the capture of violations in the simulation log</li> <li><code>DBMS_MACUTL.G_SIMULATION</code> or <code>'s'</code> to enable SQL statements to execute but capture violations in the simulation log</li> </ul>
<code>event_name</code>	<p>An event that the command rule defines. This setting enables the command rule to correspond with an <code>ALTER SESSION SET EVENTS event_name</code> statement. For example, to track trace events, you would set <code>event_name</code> to <code>TRACE</code>.</p>
<code>component_name</code>	<p>A component of the <code>event_name</code> setting. Example settings are <code>DV</code>, <code>OLS</code>, or <code>GCS</code>.</p> <p>You can find valid component names by issuing <code>ORADEBUG DOC COMPONENT RDBMS</code> as user <code>SYS</code>. The output displays parent and child components, which you can use for the <code>component_name</code> setting. For example, both <code>XS</code> (parent) and <code>XSESSION</code> (child of <code>XS</code>) are valid component names. If you select the parent component, then the command rule applies to it and the child components.</p>

**Table 17-5 (Cont.) CREATE\_SESSION\_EVENT\_CMD\_RULE Parameters**

Parameter	Description
action_name	An action of the component_name setting
scope	<p>For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the command rule is local in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the command rule is in the application root</li> </ul> <p>If you create the common command rule in an application root and want it visible to the associated PDBs, then you must synchronize the application. For example:</p> <pre>ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;</pre>

### Examples

The following example shows how to create a common session event command rule in a multitenant environment. This command rule will be in the application root, so the user running this procedure must be in the CDB root. Any user names or rule sets that are associated with this command rule must be common.

```
BEGIN
DBMS_MACADM.CREATE_SESSION_EVENT_CMD_RULE(
  rule_set_name => 'Allow Sessions',
  event_name    => 'TRACE',
  component_name => 'DV',
  action_name   => 'CURSORTRACE',
  enabled       => DBMS_MACUTL.G_SIMULATION,
  scope        => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

This example shows how to create a session event for the 47998 trace event.

```
BEGIN
DBMS_MACADM.CREATE_SESSION_EVENT_CMD_RULE(
  rule_set_name => 'Allow Sessions',
  event_name    => '47998',
  enabled       => 'y',
  scope        => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/
```

## 17.4 CREATE\_SYSTEM\_EVENT\_CMD\_RULE Procedure

The CREATE\_SYSTEM\_EVENT\_CMD\_RULE procedure creates a command rule that you can associate with system events, based on the ALTER SYSTEM statement.

In a multitenant environment, you can create both ALTER SYSTEM common and local command rules.

## Syntax

```
DBMS_MACADM.CREATE_SYSTEM_EVENT_CMD_RULE(
  rule_set_name  IN VARCHAR2,
  enabled        IN VARCHAR2,
  event_name     IN VARCHAR2 DEFAULT,
  component_name IN VARCHAR2 DEFAULT,
  action_name    IN VARCHAR2 DEFAULT,
  scope          IN NUMBER DEFAULT);
```

## Parameters

**Table 17-6 CREATE\_SYSTEM\_EVENT\_CMD\_RULE Parameters**

Parameter	Description
rule_set_name	<p>Name of the rule set to associate with the command rule. In a multitenant environment, ensure that this rule set is common if the system event command rule is common, and local if the command rule is local.</p> <p>To find existing rule sets in the current database instance, query the <code>DBA_DV_RULE_SET</code> view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).</p>
event_name	<p>An event that the command rule defines. This setting enables the command rule to correspond to an <code>ALTER SYSTEM SET EVENTS event_name</code> statement. For example, to track trace events, you would set <code>event_name</code> to <code>TRACE</code>.</p>
component_name	<p>A component of the <code>event_name</code> setting. Example settings are <code>DV</code>, <code>OLS</code>, or <code>GCS</code>.</p> <p>You can find valid component names by issuing <code>ORADEBUG DOC COMPONENT RDBMS</code> as user <code>SYS</code>. The output displays parent and child components, which you can use for the <code>component_name</code> setting. For example, both <code>XS</code> (parent) and <code>XSESSION</code> (child of <code>XS</code>) are valid component names. If you select the parent component, then the command rule applies to it and the child components.</p>
action_name	<p>An action of the <code>component_name</code> setting</p>
enabled	<p>Specify one of the following options to set the status of the command rule:</p> <ul style="list-style-type: none"> <li>• <code>DBMS_MACUTL.G_YES</code> or <code>'y'</code> to enable the command rule (default)</li> <li>• <code>DBMS_MACUTL.G_NO</code> or <code>'n'</code> to disable the command rule, including the capture of violations in the simulation log</li> <li>• <code>DBMS_MACUTL.G_SIMULATION</code> or <code>'s'</code> to enable SQL statements to execute but capture violations in the simulation log</li> </ul>

**Table 17-6 (Cont.) CREATE\_SYSTEM\_EVENT\_CMD\_RULE Parameters**

Parameter	Description
scope	<p>For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the command rule is local in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the command rule is in the application root</li> </ul> <p>If you create the common command rule in an application root and want it visible to the associated PDBs, then you must synchronize the application. For example:</p> <pre>ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;</pre>

**Example**

The following example shows how to create a common system event command rule in a multitenant environment. This command rule will be in the application root, so the user running this procedure must be in the CDB root. Any user names or rule sets that are associated with this command rule must be common.

```
BEGIN
DBMS_MACADM.CREATE_SYSTEM_EVENT_CMD_RULE(
  rule_set_name => 'Enabled',
  event_name    => 'TRACE',
  component_name => 'GSIPC',
  action_name   => 'HEAPDUMP',
  enabled       => DBMS_MACUTL.G_YES,
  scope         => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

**17.5 DELETE\_COMMAND\_RULE Procedure**

The DELETE\_COMMAND\_RULE procedure drops a command rule declaration.

**Syntax**

```
DBMS_MACADM.DELETE_COMMAND_RULE(
  command          IN VARCHAR2,
  object_owner     IN VARCHAR2,
  object_name      IN VARCHAR2,
  clause_name      IN VARCHAR2,
  parameter_name  IN VARCHAR2 DEFAULT,
  event_name       IN VARCHAR2 DEFAULT,
  component_name   IN VARCHAR2 DEFAULT,
  action_name      IN VARCHAR2 DEFAULT,
  scope           IN NUMBER DEFAULT);
```

## Parameters

**Table 17-7 DELETE\_COMMAND\_RULE Parameters**

Parameter	Description
command	SQL statement the command rule protects. To find available command rules, query the <code>DBA_DV_COMMAND_RULE</code> view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
object_owner	Database schema to which this command rule applies. To find the available users in the current database instance, query the <code>DBA_USERS</code> view, described in <i>Oracle Database Reference</i> .
object_name	Object name. The wildcard % is allowed. To find the available objects in the current database instance, query the <code>ALL_OBJECTS</code> view, described in <i>Oracle Database Reference</i> .
clause_name	A clause from the SQL statement that was used to create the command rule. Applies only to command rules for <code>ALTER SYSTEM</code> and <code>ALTER SESSION</code> .
parameter_name	A parameter from the <code>clause_name</code> parameter. Applies only to command rules for <code>ALTER SYSTEM</code> and <code>ALTER SESSION</code> .
event_name	An event that the command rule defines. Applies only to command rules for <code>ALTER SYSTEM</code> and <code>ALTER SESSION</code> .
component_name	A component of the <code>event_name</code> setting. Applies only to command rules for <code>ALTER SYSTEM</code> and <code>ALTER SESSION</code> .
action_name	An action of the <code>component_name</code> setting. Applies only to command rules for <code>ALTER SYSTEM</code> and <code>ALTER SESSION</code> .
scope	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li>• <code>DBMS_MACUTL.G.SCOPE_LOCAL</code> (or 1) if the command rule is local in the current PDB</li> <li>• <code>DBMS_MACUTL.G.SCOPE_COMMON</code> (or 2) if the command rule is in the application root</li> </ul>

## Example

The following example shows how to delete an `ALTER SESSION` command rule. When you specify the parameters, ensure that they match exactly the parameters that were used the last time the command rule was updated. To find the current settings of the command rule, query the `DBA_DV_COMMAND_RULE` view, described in [DBA\\_DV\\_COMMAND\\_RULE View](#) (page 25-8).

```
BEGIN
DBMS_MACADM.DELETE_COMMAND_RULE(
  command      => 'ALTER SESSION',
  object_owner => '%',
```

```

object_name    => '%',
clause_name    => 'SET',
parameter_name => 'EVENTS',
event_name     => 'TRACE',
component_name => 'GCS',
scope          => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/

```

This example shows how to delete a SELECT command rule.

```

BEGIN
DBMS_MACADM.DELETE_COMMAND_RULE(
  command       => 'SELECT',
  object_owner  => 'HR',
  object_name   => 'EMPLOYEES',
  scope         => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/

```

## 17.6 DELETE\_CONNECT\_COMMAND\_RULE Procedure

The `DELETE_CONNECT_COMMAND_RULE` procedure deletes a `CONNECT` command rule that had been created with the `CREATE_CONNECT_COMMAND_RULE` procedure.

### Syntax

```

DBMS_MACADM.DELETE_CONNECT_COMMAND_RULE(
  user_name     IN VARCHAR2,
  scope         IN NUMBER DEFAULT);

```

### Parameters

**Table 17-8** *DELETE\_CONNECT\_COMMAND\_RULE Parameters*

Parameter	Description
<code>user_name</code>	User to whom the <code>CONNECT</code> command rule applied. To find this user, query the <code>OBJECT_OWNER</code> field of the <code>DBA_DV_COMMAND_RULE</code> view.
<code>scope</code>	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li><code>DBMS_MACUTL.G_SCOPE_LOCAL</code> (or 1) if the command rule is local in the current PDB</li> <li><code>DBMS_MACUTL.G_SCOPE_COMMON</code> (or 2) if the command rule is in the application root</li> </ul>

### Example

```

BEGIN
DBMS_MACADM.DELETE_CONNECT_COMMAND_RULE(
  user_name     => 'PSMITH',
  scope         => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/

```



## 17.7 DELETE\_SESSION\_EVENT\_CMD\_RULE Procedure

The `DELETE_SESSION_EVENT_CMD_RULE` procedure deletes a session command rule that was associated with events.

### Syntax

```
DBMS_MACADM.DELETE_SESSION_EVENT_CMD_RULE(
  event_name      IN VARCHAR2 DEFAULT,
  component_name  IN VARCHAR2 DEFAULT,
  action_name     IN VARCHAR2 DEFAULT,
  scope           IN NUMBER DEFAULT);
```

### Parameters

**Table 17-9** *DELETE\_SESSION\_EVENT\_CMD\_RULE Parameters*

Parameter	Description
<code>event_name</code>	An event that the session event command rule defines. <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8) for a information about existing command rules
<code>component_name</code>	A component of the <code>event_name</code> setting
<code>action_name</code>	An action of the <code>component_name</code> setting
<code>scope</code>	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li><code>DBMS_MACUTL.G_SCOPE_LOCAL</code> (or 1) if the command rule is local in the current PDB</li> <li><code>DBMS_MACUTL.G_SCOPE_COMMON</code> (or 2) if the command rule is in the application root</li> </ul>

### Example

The following example shows how to delete a common session event command rule in the application root a multitenant environment. The user running this procedure must be a common user in the CDB root. When you specify the parameters, ensure that they match exactly the parameters that were used the last time the command rule was updated. To find the current settings of the command rule, query the `DBA_DV_COMMAND_RULE` view, described in [DBA\\_DV\\_COMMAND\\_RULE View](#) (page 25-8)

```
BEGIN
DBMS_MACADM.DELETE_SESSION_EVENT_CMD_RULE(
  event_name      => '47999',
  scope           => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

## 17.8 DELETE\_SYSTEM\_EVENT\_CMD\_RULE Procedure

The `DELETE_SYSTEM_EVENT_CMD_RULE` procedure deletes a system command rule that was associated with events.

**Syntax**

```
DBMS_MACADM.DELETE_SYSTEM_EVENT_CMD_RULE(
  event_name      IN VARCHAR2 DEFAULT,
  component_name  IN VARCHAR2 DEFAULT,
  action_name     IN VARCHAR2 DEFAULT,
  scope          IN NUMBER DEFAULT);
```

**Parameters****Table 17-10 DELETE\_SYSTEM\_EVENT\_CMD\_RULE Parameters**

Parameter	Description
event_name	An event that the system event command rule defines. See <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8) for a information about existing command rules.
component_name	A component of the event_name setting
action_name	An action of the component_name setting
scope	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the command rule is local in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the command rule is in the application root</li> </ul>

**Examples**

The following example shows how to delete a common system event command rule in the application root of a multitenant environment. The user running this procedure must be a common user in the CDB root. When you specify the parameters, ensure that they match exactly the parameters that were used the last time the command rule was updated. To find the current settings of the command rule, query the [DBA\\_DV\\_COMMAND\\_RULE view](#), described in [DBA\\_DV\\_COMMAND\\_RULE View](#) (page 25-8)

```
BEGIN
  DBMS_MACADM.DELETE_SYSTEM_EVENT_CMD_RULE(
    event_name      => 'TRACE',
    component_name  => 'DV',
    action_name     => '',
    scope          => DBMS_MACUTL.G_SCOPE_COMMON);
END;
```

**17.9 UPDATE\_COMMAND\_RULE Procedure**

The `UPDATE_COMMAND_RULE` procedure updates a command rule declaration.

In a multitenant environment, you can update both common and local command rules.

## Syntax

```
DBMS_MACADM.UPDATE_COMMAND_RULE(
  command          IN VARCHAR2,
  rule_set_name    IN VARCHAR2,
  object_owner     IN VARCHAR2,
  object_name      IN VARCHAR2,
  enabled          IN VARCHAR2,
  privilege_scope  IN NUMBER,
  clause_name      IN VARCHAR2,
  parameter_name   IN VARCHAR2 DEFAULT,
  event_name       IN VARCHAR2 DEFAULT,
  component_name   IN VARCHAR2 DEFAULT,
  action_name      IN VARCHAR2 DEFAULT,
  scope           IN NUMBER DEFAULT);
```

## Parameters

**Table 17-11 UPDATE\_COMMAND\_RULE Parameters**

Parameter	Description
command	<p>Command rule to update</p> <p>See also the following:</p> <ul style="list-style-type: none"> <li><a href="#">SQL Statements That Can Be Protected by Command Rules</a> (page 7-8) for a listing of available SQL statements that you can use</li> <li><a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8) for a information about existing command rules</li> </ul>
rule_set_name	<p>Name of rule set to associate with this command rule.</p> <p>To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">Oracle Database Vault Data Dictionary Views</a> (page 25-1).</p>
object_owner	<p>Database schema to which this command rule applies.</p> <p>To find the available users, query the DBA_USERS view, described in <i>Oracle Database Reference</i>. See also "Object Owner" in <a href="#">Creating a Command Rule</a> (page 7-9) for more information.</p>
object_name	<p>Object name. (The wildcard % is allowed. See "Object Name" in <a href="#">Creating a Command Rule</a> (page 7-9) for more information about objects protected by command rules.)</p> <p>To find the available objects, query the ALL_OBJECTS view, described in <i>Oracle Database Reference</i>.</p>
enabled	<p>Specify one of the following options to set the status of the command rule:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_YES or 'y' to enable the command rule (default)</li> <li>DBMS_MACUTL.G_NO or 'n' to disable the command rule, including the capture of violations in the simulation log</li> <li>DBMS_MACUTL.G_SIMULATION or 's' to enable SQL statements to execute but capture violations in the simulation log</li> </ul>
privilege_scope	Obsolete parameter

**Table 17-11 (Cont.) UPDATE\_COMMAND\_RULE Parameters**

Parameter	Description
<code>clause_name</code>	A clause from the SQL statement that was used to create the command rule. For example, a command rule for the <code>ALTER SESSION SQL</code> statement could have the <code>SET</code> clause as the <code>clause_name</code> parameter.  Applies only to command rules for <code>ALTER SYSTEM</code> and <code>ALTER SESSION</code> .
<code>parameter_name</code>	A parameter from the <code>clause_name</code> parameter. For example, for an <code>ALTER SESSION</code> command rule, you could set <code>parameter_name</code> to <code>EVENTS</code> if the <code>clause_name</code> is <code>SET</code> .  Applies only to command rules for <code>ALTER SYSTEM</code> and <code>ALTER SESSION</code> .
<code>event_name</code>	An event that the command rule defines. For example, for an <code>ALTER SESSION</code> command rule that uses <code>SET</code> for the <code>clause_name</code> and <code>EVENTS</code> as the <code>parameter_name</code> , then the <code>event_name</code> could be set to <code>TRACE</code> .  Applies only to <code>ALTER SYSTEM</code> and <code>ALTER SESSION</code> command rules that have the <code>parameter</code> parameter set to <code>events</code> .
<code>component_name</code>	A component of the <code>event_name</code> setting. For example, for a <code>TRACE</code> event, the <code>component_name</code> could be <code>GCS</code> .  Applies only to <code>ALTER SYSTEM</code> and <code>ALTER SESSION</code> command rules that have the <code>parameter</code> parameter set to <code>events</code> .
<code>action_name</code>	An action of the <code>component_name</code> setting. For example, if <code>component_name</code> is set to <code>GCS</code> , then the <code>action_name</code> setting could be <code>DISK HIGH</code> .  Applies only to <code>ALTER SYSTEM</code> and <code>ALTER SESSION</code> command rules that have the <code>parameter</code> parameter set to <code>events</code> .
<code>scope</code>	For a multitenant environment, determines how to execute this procedure. The default is <code>local</code> . Options are as follows: <ul style="list-style-type: none"> <li><code>DBMS_MACUTL.G_SCOPE_LOCAL</code> (or 1) if the command rule is local in the current PDB</li> <li><code>DBMS_MACUTL.G_SCOPE_COMMON</code> (or 2) if the command rule is in the application root</li> </ul> If you update the common command rule in an application root and want it visible to the associated PDBs, then you must synchronize the application. For example: <pre>ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;</pre>

## Examples

The following example shows how to create a simple command rule that protects the `HR.EMPLOYEES` schema.

```
BEGIN
DBMS_MACADM.UPDATE_COMMAND_RULE(
  command      => 'SELECT',
  rule_set_name => 'Enabled',
  object_owner  => 'HR',
  object_name   => 'EMPLOYEES',
  enabled       => DBMS_MACUTL.G_SIMULATION,
```

```

scope          => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/

```

This example shows how to update a more complex command rule, which is based on the ALTER SESSION SQL statement.

```

BEGIN
DBMS_MACADM.UPDATE_COMMAND_RULE(
  command       => 'ALTER SESSION',
  rule_set_name => 'Enabled',
  object_owner  => '%',
  object_name   => '%',
  enabled       => 's',
  clause_name   => 'SET',
  parameter_name => 'EVENTS',
  event_name    => 'TRACE',
  component_name => 'GCS',
  scope         => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/

```

## 17.10 UPDATE\_CONNECT\_COMMAND\_RULE Procedure

The UPDATE\_CONNECT\_COMMAND\_RULE procedure updates a CONNECT command rule that had been created with the CREATE\_CONNECT\_COMMAND\_RULE procedure.

### Syntax

```

DBMS_MACADM.CREATE_UPDATE_CONNECT_COMMAND_RULE (
  user_name      IN VARCHAR2,
  rule_set_name  IN VARCHAR2,
  enabled        IN VARCHAR2,
  scope          IN NUMBER DEFAULT);

```

### Parameters

**Table 17-12 UPDATE\_CONNECT\_COMMAND\_RULE Parameters**

Parameter	Description
user_name	<p>User to whom the CONNECT command rule will apply. If you enter the % wildcard, then the CONNECT command rule will be applied to every database user.</p> <p>In a multitenant environment, if you execute this procedure in the root, then specifying % applies to all common users. If you run the procedure in a PDB, then it applies to all local and common users who have access to this PDB. If there are two command rules, one common and one local, and they both apply to the same object, then both must evaluate successfully for the operation to succeed.</p> <p>In a multitenant environment, ensure that this user is common if the CONNECT command rule is common, and local or common if the CONNECT command rule is local.</p> <p>To find existing command rules, query the DBA_DV_COMMAND_RULE view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8).</p> <p>To find existing database users in the current instance, query the DBA_USERS view, described in <i>Oracle Database Reference</i>.</p>

**Table 17-12 (Cont.) UPDATE\_CONNECT\_COMMAND\_RULE Parameters**

Parameter	Description
rule_set_name	<p>Name of rule set to associate with this command rule. In a multitenant environment, ensure that this rule set is common if the CONNECT command rule is common, and local if the CONNECT command rule is local.</p> <p>To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).</p>
enabled	<p>Specify one of the following options to set the status of the command rule:</p> <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_YES or 'y' to enable the command rule (default)</li> <li>• DBMS_MACUTL.G_NO or 'n' to disable the command rule, including the capture of violations in the simulation log</li> <li>• DBMS_MACUTL.G_SIMULATION or 's' to enable SQL statements to execute but capture violations in the simulation log</li> </ul>
scope	<p>For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows:</p> <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the command rule is local in the current PDB</li> <li>• DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the command rule is in the application root</li> </ul> <p>If you update the common command rule in an application root and want it visible to the associated PDBs, then you must synchronize the application. For example:</p> <pre>ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;</pre>

**Example**

```
BEGIN
  DBMS_MACADM.UPDATE_CONNECT_COMMAND_RULE(
    rule_set_name => 'Allow Sessions',
    user_name     => 'PSMITH',
    enabled       => 'DBMS_MACUTL.G_YES',
    scope         => DBMS_MACUTL.G_SCOPE_LOCAL);
END;
/
```

**17.11 UPDATE\_SESSION\_EVENT\_CMD\_RULE Procedure**

The UPDATE\_SESSION\_EVENT\_CMD\_RULE procedure updates a session event command rule, based on the ALTER SESSION statement.

In a multitenant environment, you can update both common and local session event command rules.

**Syntax**

```
DBMS_MACADM.UPDATE_SESSION_EVENT_CMD_RULE(
  rule_set_name IN VARCHAR2,
```

```

enabled          IN VARCHAR2,
event_name       IN VARCHAR2 DEFAULT,
component_name   IN VARCHAR2 DEFAULT,
action_name      IN VARCHAR2 DEFAULT,
scope            IN NUMBER DEFAULT);

```

## Parameters

**Table 17-13 UPDATE\_SESSION\_EVENT\_CMD\_RULE Parameters**

Parameter	Description
rule_set_name	<p>Name of the rule set to associate with the command rule. In a multitenant environment, ensure that this rule set is common if the session event command rule is common, and local if the command rule is local.</p> <p>To find existing rule sets in the current database instance, query the <code>DBA_DV_RULE_SET</code> view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).</p>
enabled	<p>Specify one of the following options to set the status of the command rule:</p> <ul style="list-style-type: none"> <li>• <code>DBMS_MACUTL.G_YES</code> or <code>'y'</code> to enable the command rule (default)</li> <li>• <code>DBMS_MACUTL.G_NO</code> or <code>'n'</code> to disable the command rule, including the capture of violations in the simulation log</li> <li>• <code>DBMS_MACUTL.G_SIMULATION</code> or <code>'s'</code> to enable SQL statements to execute but capture violations in the simulation log</li> </ul>
event_name	<p>An event that the command rule defines. This setting enables the command rule to correspond with an <code>ALTER SESSION SET EVENTS event_name</code> statement. For example, to track trace events, you would set <code>event_name</code> to <code>TRACE</code>.</p>
component_name	<p>A component of the <code>event_name</code> setting. Example settings are <code>DV</code>, <code>OLS</code>, or <code>GCS</code>.</p> <p>You can find valid component names by issuing <code>ORADEBUG DOC COMPONENT RDBMS</code> as user <code>SYS</code>. The output displays parent and child components, which you can use for the <code>component_name</code> setting. For example, both <code>XS</code> (parent) and <code>XSESSION</code> (child of <code>XS</code>) are valid component names. If you select the parent component, then the command rule applies to it and the child components.</p>
action_name	<p>An action of the <code>component_name</code> setting</p>

**Table 17-13 (Cont.) UPDATE\_SESSION\_EVENT\_CMD\_RULE Parameters**

Parameter	Description
scope	<p>For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows:</p> <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the command rule is local in the current PDB</li> <li>• DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the command rule is in the application root</li> </ul> <p>If you update the common command rule in an application root and want it visible to the associated PDBs, then you must synchronize the application. For example:</p> <pre>ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;</pre>

**Example**

The following example shows how to update a common session event command rule in a multitenant environment. This command rule is in the application root, so the user running this procedure must be in the CDB root. Any user names or rule sets that are associated with this command rule must be common.

```
BEGIN
DBMS_MACADM.UPDATE_SESSION_EVENT_CMD_RULE(
  rule_set_name => 'Allow Sessions',
  event_name    => '47999',
  enabled       => DBMS_MACUTL.G_NO,
  scope         => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

**17.12 UPDATE\_SYSTEM\_EVENT\_CMD\_RULE Procedure**

The UPDATE\_SYSTEM\_EVENT\_CMD\_RULE procedure updates a system event command rule, based on the ALTER SYSTEM statement.

In a multitenant environment, you can update both common and local session event command rules.

**Syntax**

```
DBMS_MACADM.UPDATE_SYSTEM_EVENT_CMD_RULE(
  rule_set_name  IN VARCHAR2,
  enabled        IN VARCHAR2,
  event_name     IN VARCHAR2 DEFAULT,
  component_name IN VARCHAR2 DEFAULT,
  action_name    IN VARCHAR2 DEFAULT,
  scope          IN NUMBER DEFAULT);
```



## Parameters

**Table 17-14 UPDATE\_SYSTEM\_EVENT\_CMD\_RULE Parameters**

Parameter	Description
<code>rule_set_name</code>	<p>Name of the rule set to associate with the command rule. In a multitenant environment, ensure that this rule set is common if the system event command rule is common, and local if the command rule is local.</p> <p>To find existing rule sets in the current database instance, query the <code>DBA_DV_RULE_SET</code> view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).</p>
<code>enabled</code>	<p>Specify one of the following options to set the status of the command rule:</p> <ul style="list-style-type: none"> <li>• <code>DBMS_MACUTL.G_YES</code> or <code>'y'</code> to enable the command rule (default)</li> <li>• <code>DBMS_MACUTL.G_NO</code> or <code>'n'</code> to disable the command rule, including the capture of violations in the simulation log</li> <li>• <code>DBMS_MACUTL.G_SIMULATION</code> or <code>'s'</code> to enable SQL statements to execute but capture violations in the simulation log</li> </ul>
<code>event_name</code>	<p>An event that the command rule defines. This setting enables the command rule to correspond to an <code>ALTER SYSTEM SET EVENTS event_name</code> statement. For example, to track trace events, you would set <code>event_name</code> to <code>TRACE</code>.</p>
<code>component_name</code>	<p>A component of the <code>event_name</code> setting. Example settings are <code>DV</code>, <code>OLS</code>, or <code>GCS</code>.</p> <p>You can find valid component names by issuing <code>ORADEBUG DOC COMPONENT RDBMS</code> as user <code>SYS</code>. The output displays parent and child components, which you can use for the <code>component_name</code> setting. For example, both <code>XS</code> (parent) and <code>XSESSION</code> (child of <code>XS</code>) are valid component names. If you select the parent component, then the command rule applies to it and the child components.</p>
<code>action_name</code>	<p>An action of the <code>component_name</code> setting</p>
<code>scope</code>	<p>For a multitenant environment, determines how to execute this procedure. The default is <code>local</code>. Options are as follows:</p> <ul style="list-style-type: none"> <li>• <code>DBMS_MACUTL.G_SCOPE_LOCAL</code> (or <code>1</code>) if the command rule is local in the current PDB</li> <li>• <code>DBMS_MACUTL.G_SCOPE_COMMON</code> (or <code>2</code>) if the command rule is in the application root</li> </ul> <p>If you update the common command rule in an application root and want it visible to the associated PDBs, then you must synchronize the application. For example:</p> <pre>ALTER PLUGGABLE DATABASE APPLICATION saas_sales_app SYNC;</pre>

## Example

The following example shows how to update a common system event command rule in a multitenant environment. This command rule is in the application root, so the

user running this procedure must be in the CDB root. Any user names or rule sets that are associated with this command rule must be common.

```
BEGIN
  DBMS_MACADM.UPDATE_SYSTEM_EVENT_CMD_RULE(
    rule_set_name => 'Disabled',
    event_name    => 'TRACE',
    component_name => 'DV',
    enabled       => 'n',
    scope         => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

---

## Oracle Database Vault Factor APIs

The DBMS\_MACADM PL/SQL package has factor-related Oracle Database Vault rule procedures and functions, and DVF has functions to manage factors.

### [DBMS\\_MACADM Factor Procedures and Functions](#) (page 18-1)

The DBMS\_MACADM PL/SQL package provides procedures and functions to configure factors.

### [Oracle Database Vault Run-Time PL/SQL Procedures and Functions](#) (page 18-22)

Oracle Database Vault provides procedural interfaces to administer Database Vault security options and manage Database Vault security enforcements.

### [Oracle Database Vault DVF PL/SQL Factor Functions](#) (page 18-27)

Oracle Database Vault maintains the DVF schema functions when you use the DBMS\_MACADM PL/SQL package to manage the various factors.

## 18.1 DBMS\_MACADM Factor Procedures and Functions

The DBMS\_MACADM PL/SQL package provides procedures and functions to configure factors.

Only users who have been granted the DV\_OWNER or DV\_ADMIN role can use these procedures and functions.

### [ADD\\_FACTOR\\_LINK Procedure](#) (page 18-3)

The ADD\_FACTOR\_LINK procedure specifies a parent-child relationship for two factors.

### [ADD\\_POLICY\\_FACTOR Procedure](#) (page 18-4)

The ADD\_POLICY\_FACTOR procedure specifies that the label for a factor contributes to the Oracle Label Security label for a policy.

### [CHANGE\\_IDENTITY\\_FACTOR Procedure](#) (page 18-4)

The CHANGE\_IDENTITY\_FACTOR procedure associates an identity with a different factor.

### [CHANGE\\_IDENTITY\\_VALUE Procedure](#) (page 18-5)

The CHANGE\_IDENTITY\_FACTOR procedure updates the value of an identity.

### [CREATE\\_DOMAIN\\_IDENTITY Procedure](#) (page 18-6)

The CREATE\_DOMAIN\_IDENTITY procedure is used for Oracle Real Application Clusters (Oracle RAC) and Oracle Label Security.

### [CREATE\\_FACTOR Procedure](#) (page 18-7)

The CREATE\_FACTOR procedure creates a factor.

**[CREATE\\_FACTOR\\_TYPE Procedure](#)** (page 18-9)

The `CREATE_FACTOR_TYPE` procedure creates a user-defined factor type.

**[CREATE\\_IDENTITY\\_MAP Procedure](#)** (page 18-10)

The `CREATE_IDENTITY_MAP` procedure defines tests that can derive the identity of a factor from the value of linked child factors (subfactors).

**[CREATE\\_IDENTITY Procedure](#)** (page 18-11)

The `CREATE_IDENTITY` procedure assigns an identity and an associated trust level for a given factor.

**[DELETE\\_FACTOR Procedure](#)** (page 18-12)

The `DELETE_FACTOR` procedure deletes a factor.

**[DELETE\\_FACTOR\\_LINK Procedure](#)** (page 18-13)

The `DELETE_FACTOR_LINK` procedure removes a parent-child relationship for two factors.

**[DELETE\\_IDENTITY Procedure](#)** (page 18-13)

The `DELETE_IDENTITY` procedure removes an identity from an existing factor.

**[DELETE\\_FACTOR\\_TYPE Procedure](#)** (page 18-14)

The `DELETE_FACTOR_TYPE` procedure deletes a factor type.

**[DELETE\\_IDENTITY\\_MAP Procedure](#)** (page 18-14)

The `DELETE_IDENTITY_MAP` procedure removes an identity map for a factor.

**[DROP\\_DOMAIN\\_IDENTITY Procedure](#)** (page 18-15)

The `DROP_DOMAIN_IDENTITY` procedure removes an Oracle Real Application Clusters database node from a domain.

**[GET\\_SESSION\\_INFO Function](#)** (page 18-16)

The `GET_SESSION_INFO` function returns information from the `SYS.V_$SESSION` system table for the current session.

**[GET\\_INSTANCE\\_INFO Function](#)** (page 18-17)

The `GET_INSTANCE_INFO` function returns information from the `SYS.V_$INSTANCE` system table about the current database instance.

**[RENAME\\_FACTOR Procedure](#)** (page 18-17)

The `RENAME_FACTOR` procedure renames a factor; the name change takes effect everywhere the factor is used.

**[RENAME\\_FACTOR\\_TYPE Procedure](#)** (page 18-18)

The `RENAME_FACTOR` procedure renames a factor type; the name change takes effect everywhere the factor type is used.

**[UPDATE\\_FACTOR Procedure](#)** (page 18-18)

The `UPDATE_FACTOR` procedure updates the description of a factor type.

**[UPDATE\\_FACTOR\\_TYPE Procedure](#)** (page 18-21)

The `UPDATE_FACTOR_TYPE` procedure updates a factor type.

**[UPDATE\\_IDENTITY Procedure](#)** (page 18-21)

The `UPDATE_IDENTITY` procedure updates the trust level of a factor identity.

**Related Topics:**[Configuring Factors](#) (page 8-1)

Factors enable you to base Database Vault restrictions on attributes such as a client IP address or a domain.

[Oracle Database Vault Utility APIs](#) (page 21-1)

Oracle Database Vault provides a set of utility APIs in the DBMS\_MACUTL PL/SQL package.

**18.1.1 ADD\_FACTOR\_LINK Procedure**

The ADD\_FACTOR\_LINK procedure specifies a parent-child relationship for two factors.

**Syntax**

```
DBMS_MACADM.ADD_FACTOR_LINK(
  parent_factor_name IN VARCHAR2,
  child_factor_name  IN VARCHAR2,
  label_indicator    IN VARCHAR2);
```

**Parameters****Table 18-1 ADD\_FACTOR\_LINK Parameters**

Parameter	Description
parent_factor_name	Parent factor name. To find existing parent and child factors in the current database instance, query the DBA_DV_FACTOR_LINK view, described in <a href="#">DBA_DV_FACTOR_LINK View</a> (page 25-14).
child_factor_name	Child factor name.
label_indicator	Indicates that the child factor being linked to the parent factor contributes to the label of the parent factor in an Oracle Label Security integration. Specify either DBMS_MACUTL.G_YES (for Yes) or DBMS_MACUTL.G_NO (for No). To find the Oracle Label Security policies and labels associated with factors, query the following views, described in <a href="#">Oracle Database Vault Data Dictionary Views</a> (page 25-1): <ul style="list-style-type: none"> <li>DBA_DV_MAC_POLICY: Lists Oracle Label Security policies defined in the current database instance.</li> <li>DBA_DV_MAC_POLICY_FACTOR: Lists the factors that are associated with Oracle Label Security policies for the current database instance.</li> <li>DBA_DV_POLICY_LABEL: Lists the Oracle Label Security label for each factor identifier in the DBA_DV_IDENTITY view for each policy.</li> </ul>

**Example**

```
BEGIN
  DBMS_MACADM.ADD_FACTOR_LINK(
    parent_factor_name => 'HQ_ClientID',
    child_factor_name  => 'Div1_ClientID',
    label_indicator    => DBMS_MACUTL.G_YES);
```

```
END;  
/
```

## 18.1.2 ADD\_POLICY\_FACTOR Procedure

The `ADD_POLICY_FACTOR` procedure specifies that the label for a factor contributes to the Oracle Label Security label for a policy.

### Syntax

```
DBMS_MACADM.ADD_POLICY_FACTOR(  
  policy_name IN VARCHAR2,  
  factor_name IN VARCHAR2);
```

### Parameters

**Table 18-2 ADD\_POLICY\_FACTOR Parameters**

Parameter	Description
<code>policy_name</code>	Oracle Label Security policy name. To find the policies defined in the current database instance, query the <code>DBA_DV_MAC_POLICY</code> view, described in <a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17). To find factors that are associated with Oracle Label Security policies, query <code>DBA_DV_MAC_POLICY_FACTOR</code> , described in <a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17).
<code>factor_name</code>	Factor name. To find existing factors, query the <code>DBA_DV_FACTOR</code> view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).

### Example

```
BEGIN  
  DBMS_MACADM.ADD_POLICY_FACTOR(  
    policy_name => 'AccessData',  
    factor_name => 'Sector2_ClientID');  
END;  
/
```

## 18.1.3 CHANGE\_IDENTITY\_FACTOR Procedure

The `CHANGE_IDENTITY_FACTOR` procedure associates an identity with a different factor.

### Syntax

```
DBMS_MACADM.CHANGE_IDENTITY_FACTOR(  
  factor_name IN VARCHAR2,  
  value IN VARCHAR2,  
  new_factor_name IN VARCHAR2);
```

## Parameters

**Table 18-3** *CHANGE\_IDENTITY\_FACTOR Parameters*

Parameter	Description
factor_name	Current factor name. To find existing factors, query the <a href="#">DBA_DV_FACTOR</a> view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).
value	Value of the identity to update. To find existing identities for each factor in the current database instance, query the <a href="#">DBA_DV_IDENTITY</a> view, described in <a href="#">DBA_DV_IDENTITY View</a> (page 25-15). To find current identity mappings, query the <a href="#">DBA_DV_IDENTITY_MAP</a> view, described in <a href="#">DBA_DV_IDENTITY_MAP View</a> (page 25-15).
new_factor_name	Name of the factor to associate with the identity, which you can find by querying the <a href="#">DBA_DV_FACTOR</a> view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).

## Example

```
BEGIN
  DBMS_MACADM.CHANGE_IDENTITY_FACTOR(
    factor_name => 'Sector2_ClientID',
    value       => 'intranet',
    new_factor_name => 'Sector4_ClientID');
END;
/
```

## 18.1.4 CHANGE\_IDENTITY\_VALUE Procedure

The `CHANGE_IDENTITY_FACTOR` procedure updates the value of an identity.

### Syntax

```
DBMS_MACADM.CHANGE_IDENTITY_VALUE(
  factor_name IN VARCHAR2,
  value       IN VARCHAR2,
  new_value   IN VARCHAR2);
```

## Parameters

**Table 18-4** *CHANGE\_IDENTITY\_VALUE Parameters*

Parameter	Description
factor_name	Factor name. To find existing factors, query the <a href="#">DBA_DV_FACTOR</a> view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).

**Table 18-4 (Cont.) CHANGE\_IDENTITY\_VALUE Parameters**

Parameter	Description
value	Current value associated with the identity. To find existing identities for each factor in the current database instance, query the DBA_DV_IDENTITY view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11). To find current identity mappings, query the DBA_DV_IDENTITY_MAP view, described in <a href="#">DBA_DV_IDENTITY_MAP View</a> (page 25-15).
new_value	New identity value, up to 1024 characters in mixed-case.

**Example**

```
BEGIN
  DBMS_MACADM.CHANGE_IDENTITY_VALUE(
    factor_name => 'Sector2_ClientID',
    value       => 'remote',
    new_value   => 'intranet');
END;
/
```

**18.1.5 CREATE\_DOMAIN\_IDENTITY Procedure**

The CREATE\_DOMAIN\_IDENTITY procedure is used for Oracle Real Application Clusters (Oracle RAC) and Oracle Label Security.

It adds an Oracle RAC database node to the domain factor identities and labels it according to an Oracle Label Security policy

**Syntax**

```
DBMS_MACADM.CREATE_DOMAIN_IDENTITY(
  domain_name  IN VARCHAR2,
  domain_host  IN VARCHAR2,
  policy_name  IN VARCHAR2 DEFAULT NULL,
  domain_label IN VARCHAR2 DEFAULT NULL);
```

**Parameters****Table 18-5 CREATE\_DOMAIN\_IDENTITY Parameters**

Parameter	Description
domain_name	Name of the domain to which to add the host. To find the logical location of the database within the network structure within a distributed database system, run the DVF.F\$DATABASE_DOMAIN function, described in <a href="#">Oracle Database Vault DVF PL/SQL Factor Functions</a> (page 18-27).
domain_host	Oracle Real Application Clusters host name being added to the domain. To find host name of a database, run the DVF.F\$DATABASE_HOSTNAME function, described in <a href="#">Oracle Database Vault DVF PL/SQL Factor Functions</a> (page 18-27).



**Table 18-5 (Cont.) CREATE\_DOMAIN\_IDENTITY Parameters**

Parameter	Description
policy_name	Oracle Label Security policy name. If you omit the policy name, then the domain is not associated with any policy.  To find the available policies, query the DBA_DV_MAC_POLICY view, described in <a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17).
domain_label	Name of the domain to which to add the Oracle Label Security policy.

**Examples**

```

BEGIN
  DBMS_MACADM.CREATE_DOMAIN_IDENTITY(
    domain_name => 'example',
    domain_host => 'mydom_host',
    policy_name => 'AccessData',
    domain_label => 'sensitive');
END;
/

```

**18.1.6 CREATE\_FACTOR Procedure**

The CREATE\_FACTOR procedure creates a factor.

After you create a factor, you can give it an identity by using the CREATE\_IDENTITY procedure, described in [CREATE\\_IDENTITY Procedure](#) (page 18-11).

**Syntax**

```

DBMS_MACADM.CREATE_FACTOR(
  factor_name      IN VARCHAR2,
  factor_type_name IN VARCHAR2,
  description      IN VARCHAR2,
  rule_set_name   IN VARCHAR2,
  get_expr        IN VARCHAR2,
  validate_expr   IN VARCHAR2,
  identify_by     IN NUMBER,
  labeled_by      IN NUMBER,
  eval_options    IN NUMBER,
  audit_options   IN NUMBER,
  fail_options    IN NUMBER);

```

**Parameters****Table 18-6 CREATE\_FACTOR Parameters**

Parameter	Description
factor_name	Factor name, up to 128 characters in mixed-case, without spaces.  To find existing factors in the current database instance, query the DBA_DV_FACTOR view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).

**Table 18-6 (Cont.) CREATE\_FACTOR Parameters**

Parameter	Description
factor_type_name	Type of the factor, up to 128 characters in mixed-case, without spaces.  To find existing factor types, query the DBA_DV_FACTOR_TYPE view, described in <a href="#">DBA_DV_FACTOR_TYPE View</a> (page 25-13).
description	Description of the purpose of the factor, up to 1024 characters in mixed-case.
rule_set_name	Rule set name if you want to use a rule set to control when and how a factor identity is set.  To find existing rule sets, query the DBA_DV_RULE_SET view, described in <a href="#">Oracle Database Vault Data Dictionary Views</a> (page 25-1). See also <a href="#">Assigning a Rule Set to a Factor</a> (page 8-12) for more information about assigning rule sets to factors.
get_expr	Valid PL/SQL expression that retrieves the identity of a factor. It can use up to 255 characters in mixed-case. See <a href="#">Setting the Retrieval Method for a Factor</a> (page 8-10) for more information. See also the audit_options parameter.
validate_expr	Name of the procedure to validate the factor. This is a valid PL/SQL expression that returns a Boolean value (TRUE or FALSE) to validate the identity of the factor. See <a href="#">Setting the Validation Method for a Factor</a> (page 8-11) for more information.
identify_by	Options for determining the identity of a factor, based on the expression set for the get_expr parameter: <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_IDENTIFY_BY_CONSTANT: By constant</li> <li>• DBMS_MACUTL.G_IDENTIFY_BY_METHOD: By method</li> <li>• DBMS_MACUTL.G_IDENTIFY_BY_FACTOR: By factor</li> <li>• DBMS_MACUTL.G_IDENTIFY_BY_CONTEXT: By context</li> </ul> See <a href="#">Setting the Factor Identification Information</a> (page 8-7) for more information.
labeled_by	Options for labeling the factor: <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_LABELED_BY_SELF: Labels the identities for the factor directly from the labels associated with an Oracle Label Security policy (default)</li> <li>• DBMS_MACUTL.G_LABELED_BY_FACTORS: Derives the factor identity label from the labels of its child factor identities.</li> </ul> See <a href="#">Setting the Oracle Label Security Labeling Information for a Factor</a> (page 8-9) for more information.
eval_options	Options for evaluating the factor when the user logs on: <ul style="list-style-type: none"> <li>• DBMS_MACUTL.G_EVAL_ON_SESSION: When the database session is created (default)</li> <li>• DBMS_MACUTL.G_EVAL_ON_ACCESS: Each time the factor is accessed</li> <li>• DBMS_MACUTL.G_EVAL_ON_STARTUP: On start-up</li> </ul> See <a href="#">Setting the Evaluation Information for a Factor</a> (page 8-9) for more information.

**Table 18-6 (Cont.) CREATE\_FACTOR Parameters**

Parameter	Description
audit_options	<p>Options for auditing the factor if you want to generate a custom Oracle Database Vault audit record.</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_AUDIT_OFF: Disables auditing.</li> <li>DBMS_MACUTL.G_AUDIT_ALWAYS: Always audits.</li> <li>DBMS_MACUTL.G_AUDIT_ON_GET_ERROR: Audits if <code>get_expr</code> returns an error.</li> <li>DBMS_MACUTL.G_AUDIT_ON_GET_NULL: Audits if <code>get_expr</code> is null.</li> <li>DBMS_MACUTL.G_AUDIT_ON_VALIDATE_ERROR: Audits if the validation procedure returns an error.</li> <li>DBMS_MACUTL.G_AUDIT_ON_VALIDATE_FALSE: Audits if the validation procedure is false.</li> <li>DBMS_MACUTL.G_AUDIT_ON_TRUST_LEVEL_NULL: Audits if there is no trust level set.</li> <li>DBMS_MACUTL.G_AUDIT_ON_TRUST_LEVEL_NEG: Audits if the trust level is negative.</li> </ul> <p>See <a href="#">Setting Audit Options for a Factor</a> (page 8-13) for more information.</p>
fail_options	<p>Options for reporting factor errors:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_FAIL_WITH_MESSAGE: Shows an error message (default)</li> <li>DBMS_MACUTL.G_FAIL_SILENTLY: Does not show an error message</li> </ul> <p>See <a href="#">Setting Error Options for a Factor</a> (page 8-13) for more information.</p>

**Example**

```

BEGIN
  DBMS_MACADM.CREATE_FACTOR(
    factor_name      => 'Sector2_DB',
    factor_type_name => 'Instance',
    description     => '',
    rule_set_name   => 'Limit_DBA_Access',
    get_expr        => 'UPPER(SYS_CONTEXT(''USERENV'', ''DB_NAME''))',
    validate_expr   => 'dbavowner.check_db_access',
    identify_by     => DBMS_MACUTL.G_IDENTIFY_BY_METHOD,
    labeled_by      => DBMS_MACUTL.G_LABELED_BY_SELF,
    eval_options    => DBMS_MACUTL.G_EVAL_ON_SESSION,
    audit_options   => DBMS_MACUTL.G_AUDIT_OFF,
    fail_options    => DBMS_MACUTL.G_FAIL_SILENTLY);
END;
/

```

**18.1.7 CREATE\_FACTOR\_TYPE Procedure**

The `CREATE_FACTOR_TYPE` procedure creates a user-defined factor type.

**Syntax**

```
DBMS_MACADM.CREATE_FACTOR_TYPE(
  name          IN VARCHAR2,
  description   IN VARCHAR2);
```

**Parameters****Table 18-7 CREATE\_FACTOR\_TYPE Parameters**

Parameter	Description
name	Factor type name, up to 128 characters in mixed-case, without spaces. To find existing factor types, query the DBA_DV_FACTOR_TYPE view, described in <a href="#">DBA_DV_FACTOR_TYPE View</a> (page 25-13).
description	Description of the purpose of the factor type, up to 1024 characters in mixed-case.

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_FACTOR_TYPE(
    name          => 'Sector2Instance',
    description   => 'Checks DB instances used in Sector 2');
END;
/
```

**18.1.8 CREATE\_IDENTITY\_MAP Procedure**

The CREATE\_IDENTITY\_MAP procedure defines tests that can derive the identity of a factor from the value of linked child factors (subfactors).

**Syntax**

```
DBMS_MACADM.CREATE_IDENTITY_MAP(
  identity_factor_name IN VARCHAR2,
  identity_factor_value IN VARCHAR2,
  parent_factor_name   IN VARCHAR2,
  child_factor_name    IN VARCHAR2,
  operation             IN VARCHAR2,
  operand1             IN VARCHAR2,
  operand2             IN VARCHAR2);
```

**Parameters****Table 18-8 CREATE\_IDENTITY\_MAP Parameters**

Parameter	Description
identity_factor_name	Factor the identity map is for. To find existing factors in the current database instance, query the DBA_DV_FACTOR view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).

**Table 18-8 (Cont.) CREATE\_IDENTITY\_MAP Parameters**

Parameter	Description
identity_factor_value	Value the factor assumes if the identity map evaluates to TRUE.  To find existing factor identities, query the DBA_DV_IDENTITY view, described in <a href="#">DBA_DV_IDENTITY View</a> (page 25-15).  To find current factor identity mappings, use DBA_DV_IDENTITY_MAP, described in <a href="#">DBA_DV_IDENTITY_MAP View</a> (page 25-15).
parent_factor_name	The parent factor link to which the map is related.  To find existing parent-child factor mappings, query the DBA_DV_IDENTITY_MAP view, described in <a href="#">DBA_DV_IDENTITY_MAP View</a> (page 25-15).
child_factor_name	The child factor link to which the map is related.
operation	Relational operator for the identity map (for example, <, >, =, and so on).
operand1	Left operand for the relational operator; refers to the low value you enter.
operand2	Right operand for the relational operator; refers to the high value you enter.

### Example

```
BEGIN
DBMS_MACADM.CREATE_IDENTITY_MAP(
  identity_factor_name => 'Sector2_ClientID',
  identity_factor_value => 'intranet',
  parent_factor_name   => 'HQ_ClientID',
  child_factor_name    => 'Div1_ClientID',
  operation            => '<',
  operand1             => '192.0.2.50',
  operand2             => '192.0.2.100');
END;
/
```

## 18.1.9 CREATE\_IDENTITY Procedure

The CREATE\_IDENTITY procedure assigns an identity and an associated trust level for a given factor.

After you create a factor, you must assign it an identity.

### Syntax

```
DBMS_MACADM.CREATE_IDENTITY(
  factor_name IN VARCHAR2,
  value       IN VARCHAR2,
  trust_level IN NUMBER);
```

## Parameters

**Table 18-9 CREATE\_IDENTITY Parameters**

Parameter	Description
<code>factor_name</code>	Factor name. To find existing factors, query the <code>DBA_DV_FACTOR</code> view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).
<code>value</code>	The actual value of the factor, up to 1024 characters in mixed-case. For example, the identity of an <code>IP_Address</code> factor could be the IP address of 192.0.2.12.
<code>trust_level</code>	Number that indicates the magnitude of trust relative to other identities for the same factor. In general, the higher the trust level number is set, the greater the trust. A trust level of 10 indicates "very trusted." Negative trust levels are not trusted.  See <a href="#">Creating and Configuring a Factor Identity</a> (page 8-16) for more information about trust levels and label security.

## Example

```
BEGIN
  DBMS_MACADM.CREATE_IDENTITY(
    factor_name => 'Sector2_ClientID',
    value       => 'intranet',
    trust_level => 5);
END;
/
```

## 18.1.10 DELETE\_FACTOR Procedure

The `DELETE_FACTOR` procedure deletes a factor.

### Syntax

```
DBMS_MACADM.DELETE_FACTOR(
  factor_name IN VARCHAR2);
```

## Parameters

**Table 18-10 DELETE\_FACTOR Parameter**

Parameter	Description
<code>factor_name</code>	Factor name. To find existing factors in the current database instance, query the <code>DBA_DV_FACTOR</code> view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).

## Example

```
EXEC DBMS_MACADM.DELETE_FACTOR('Sector2_ClientID');
```

### 18.1.11 DELETE\_FACTOR\_LINK Procedure

The `DELETE_FACTOR_LINK` procedure removes a parent-child relationship for two factors.

#### Syntax

```
DBMS_MACADM.DELETE_FACTOR_LINK(
  parent_factor_name IN VARCHAR2,
  child_factor_name  IN VARCHAR2);
```

#### Parameters

**Table 18-11** *DELETE\_FACTOR\_LINK Parameters*

Parameter	Description
parent_factor_name	Factor name.
child_factor_name	To find factors that are used in parent-child mappings in the current database instance, query the <code>DBA_DV_FACTOR_LINK</code> view, described in <a href="#">DBA_DV_FACTOR_LINK View</a> (page 25-14).
child_factor_name	Factor name

#### Example

```
BEGIN
  DBMS_MACADM.DELETE_FACTOR_LINK(
    parent_factor_name => 'HQ_ClientID',
    child_factor_name  => 'Div1_ClientID');
END;
/
```

### 18.1.12 DELETE\_IDENTITY Procedure

The `DELETE_IDENTITY` procedure removes an identity from an existing factor.

#### Syntax

```
DBMS_MACADM.DELETE_IDENTITY(
  factor_name IN VARCHAR2,
  value       IN VARCHAR2);
```

#### Parameters

**Table 18-12** *DELETE\_IDENTITY Parameters*

Parameter	Description
factor_name	Factor name.
value	To find existing factors in the current database instance, query the <code>DBA_DV_FACTOR</code> view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).

**Table 18-12 (Cont.) DELETE\_IDENTITY Parameters**

Parameter	Description
value	Identity value associated with the factor. To find the identities for each factor in the current database instance, query the DBA_DV_IDENTITY view, described in <a href="#">DBA_DV_IDENTITY View</a> (page 25-15).

**Example**

```
BEGIN
  DBMS_MACADM.DELETE_IDENTITY(
    factor_name => 'Sector2_ClientID',
    value       => 'intranet');
END;
/
```

**18.1.13 DELETE\_FACTOR\_TYPE Procedure**

The DELETE\_FACTOR\_TYPE procedure deletes a factor type.

**Syntax**

```
DBMS_MACADM.DELETE_FACTOR_TYPE(
  name IN VARCHAR2);
```

**Parameters****Table 18-13 DELETE\_FACTOR\_TYPE Parameters**

Parameter	Description
name	Factor type name. To find existing factor types, query the DBA_DV_FACTOR_TYPE view, described in <a href="#">DBA_DV_FACTOR_TYPE View</a> (page 25-13).

**Example**

```
EXEC DBMS_MACADM.DELETE_FACTOR_TYPE('Sector2Instance');
```

**18.1.14 DELETE\_IDENTITY\_MAP Procedure**

The DELETE\_IDENTITY\_MAP procedure removes an identity map for a factor.

**Syntax**

```
DBMS_MACADM.DELETE_IDENTITY_MAP(
  identity_factor_name IN VARCHAR2,
  identity_factor_value IN VARCHAR2,
  parent_factor_name   IN VARCHAR2,
  child_factor_name    IN VARCHAR2,
  operation             IN VARCHAR2,
  operand1             IN VARCHAR2,
  operand2             IN VARCHAR2);
```



## Parameters

**Table 18-14** *DELETE\_IDENTITY\_MAP Parameters*

Parameter	Description
<code>identity_factor_name</code>	Factor the identity map is for. To find existing factors in the current database instance, query the <code>DBA_DV_FACTOR</code> view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).
<code>identity_factor_value</code>	Value the factor assumes if the identity map evaluates to TRUE. To find existing factor identities, query the <code>DBA_DV_IDENTITY</code> view, described in <a href="#">DBA_DV_IDENTITY View</a> (page 25-15). To find current factor identity mappings, query <code>DBA_DV_IDENTITY_MAP</code> , described in <a href="#">DBA_DV_IDENTITY_MAP View</a> (page 25-15).
<code>parent_factor_name</code>	The parent factor link to which the map is related. To find existing parent-child factors, query the <code>DBA_DV_FACTOR</code> view, described in <a href="#">DBA_DV_FACTOR_LINK View</a> (page 25-14).
<code>child_factor_name</code>	The child factor to which the map is related.
<code>operation</code>	Relational operator for the identity map (for example, <code>&lt;</code> , <code>&gt;</code> , <code>=</code> , and so on).
<code>operand1</code>	Left (low value) operand for the relational operator.
<code>operand2</code>	Right (high value) operand for the relational operator.

## Example

```
BEGIN
DBMS_MACADM.DELETE_IDENTITY_MAP(
  identity_factor_name => 'Sector2_ClientID',
  identity_factor_value => 'intranet',
  parent_factor_name   => 'HQ_ClientID',
  child_factor_name    => 'Div1_ClientID',
  operation             => '<',
  operand1             => '192.0.2.10',
  operand2             => '192.0.2.15');
END;
/
```

### 18.1.15 DROP\_DOMAIN\_IDENTITY Procedure

The `DROP_DOMAIN_IDENTITY` procedure removes an Oracle Real Application Clusters database node from a domain.

#### Syntax

```
DBMS_MACADM.DROP_DOMAIN_IDENTITY(
  domain_name  IN VARCHAR2,
  domain_host  IN VARCHAR2);
```

## Parameters

**Table 18-15** *DROP\_DOMAIN\_IDENTITY Parameters*

Parameter	Description
domain_name	Name of the domain to which the host was added. To find the domain of a database as specified by the DB_DOMAIN initialization parameter, run the DVF.F\$DATABASE_DOMAIN function, described in <a href="#">F\$DATABASE_DOMAIN Function</a> (page 18-31).
domain_host	Oracle Real Application Clusters host name being that was added to the domain. To find the host name for a specified database, run the DVF.F\$DATABASE_HOSTNAME function, described in <a href="#">F\$DATABASE_NAME Function</a> (page 18-32).

### Example

```
BEGIN
  DBMS_MACADM.DROP_DOMAIN_IDENTITY(
    domain_name => 'example',
    domain_host => 'mydom_host');
END;
/
```

## 18.1.16 GET\_SESSION\_INFO Function

The GET\_SESSION\_INFO function returns information from the SYS.V\_\$SESSION system table for the current session.

The V\$SESSION data dictionary view also contains session information from this table. See *Oracle Database Reference* for more information.

### Syntax

```
DBMS_MACADM.GET_SESSION_INFO(
  p_parameter IN VARCHAR2)
RETURN VARCHAR2;
```

## Parameters

**Table 18-16** *GET\_SESSION\_INFO Parameter*

Parameter	Description
p_parameter	Column name in the SYS.V_\$SESSION system table.

### Example

```
DECLARE
  session_var varchar2 := null;
BEGIN
  session_var = DBMS_MACADM.GET_SESSION_INFO('PROCESS');
END;
/
```

## 18.1.17 GET\_INSTANCE\_INFO Function

The GET\_INSTANCE\_INFO function returns information from the SYS.V\_\$INSTANCE system table about the current database instance.

The V\_\$INSTANCE data dictionary view also contains database instance information from this table. See *Oracle Database Reference* for more information.

### Syntax

```
DBMS_MACADM.GET_INSTANCE_INFO(
  p_parameter IN VARCHAR2)
RETURN VARCHAR2;
```

### Parameters

**Table 18-17 GET\_INSTANCE\_INFO Parameter**

Parameter	Description
p_parameter	Column name in the SYS.V_\$INSTANCE system table

### Example

```
DECLARE
  instance_var varchar2 := null;
BEGIN
  instance_var = DBMS_MACADM.GET_INSTANCE_INFO('INSTANCE_NAME');
END;
/
```

## 18.1.18 RENAME\_FACTOR Procedure

The RENAME\_FACTOR procedure renames a factor; the name change takes effect everywhere the factor is used.

### Syntax

```
DBMS_MACADM.RENAME_FACTOR(
  factor_name      IN VARCHAR2,
  new_factor_name IN VARCHAR2);
```

### Parameters

**Table 18-18 RENAME\_FACTOR Parameters**

Parameter	Description
factor_name	Current factor name. To find existing factors in the current database instance, query the DBA_DV_FACTOR view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).
new_factor_name	New factor name, up to 128 characters in mixed-case, without spaces.

**Example**

```

BEGIN
  DBMS_MACADM.RENAME_FACTOR(
    factor_name      => 'Sector2_ClientID',
    new_factor_name => 'Sector2_Clients');
END;
/

```

**18.1.19 RENAME\_FACTOR\_TYPE Procedure**

The `RENAME_FACTOR` procedure renames a factor type; the name change takes effect everywhere the factor type is used.

**Syntax**

```

DBMS_MACADM.RENAME_FACTOR_TYPE(
  old_name  IN VARCHAR2,
  new_name  IN VARCHAR2);

```

**Parameters****Table 18-19 RENAME\_FACTOR\_TYPE Parameters**

Parameter	Description
<code>old_name</code>	Current factor type name. To find existing factor types in the current database instance, query the <code>DBA_DV_FACTOR_TYPE</code> view, described in <a href="#">DBA_DV_FACTOR_TYPE View</a> (page 25-13).
<code>new_name</code>	New factor type name, up to 128 characters in mixed-case, without spaces.

**Example**

```

BEGIN
  DBMS_MACADM.RENAME_FACTOR_TYPE(
    old_name  => 'Sector2Instance',
    new_name  => 'Sector2DBInstance');
END;
/

```

**18.1.20 UPDATE\_FACTOR Procedure**

The `UPDATE_FACTOR` procedure updates the description of a factor type.

**Syntax**

```

DBMS_MACADM.UPDATE_FACTOR(
  factor_name          IN VARCHAR2,
  factor_type_name    IN VARCHAR2,
  description          IN VARCHAR2,
  rule_set_name       IN VARCHAR2,
  get_expr            IN VARCHAR2,
  validate_expr       IN VARCHAR2,
  identify_by         IN NUMBER,
  labeled_by          IN NUMBER,
  eval_options        IN NUMBER,

```

```

audit_options    IN NUMBER,
fail_options     IN NUMBER);

```

## Parameters

**Table 18-20 UPDATE\_FACTOR**

Parameter	Description
factor_name	Factor name. To find existing factors in the current database instance, query the DBA_DV_FACTOR view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).
factor_type_name	Factor type name. To find existing factor types, query the DBA_DV_FACTOR_TYPE view, described in <a href="#">DBA_DV_FACTOR_TYPE View</a> (page 25-13).
description	Description of the purpose of the factor, up to 1024 characters in mixed-case.
rule_set_name	Name of the rule set used to control when and how a factor identity is set. To find existing rule sets, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30). See also <a href="#">Assigning a Rule Set to a Factor</a> (page 8-12) for more information about assigning rule sets to factors.
get_expr	Valid PL/SQL expression that retrieves the identity of a factor. It can use up to 255 characters in mixed-case. See <a href="#">Setting the Retrieval Method for a Factor</a> (page 8-10) for more information. See also the audit_options parameter.
validate_expr	Name of the procedure to validate factor. This is a valid PL/SQL expression that returns a Boolean value (TRUE or FALSE) to validate the identity of the factor. See <a href="#">Setting the Validation Method for a Factor</a> (page 8-11) for more information.
identify_by	Options for determining the identity of a factor, based on the expression set for the get_expr parameter: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_IDENTIFY_BY_CONSTANT: By constant</li> <li>DBMS_MACUTL.G_IDENTIFY_BY_METHOD: By method</li> <li>DBMS_MACUTL.G_IDENTIFY_BY_FACTOR: By factor</li> <li>DBMS_MACUTL.G_IDENTIFY_BY_CONTEXT: By context</li> </ul> See <a href="#">Setting the Factor Identification Information</a> (page 8-7) for more information.
labeled_by	Options for labeling the factor: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_LABELED_BY_SELF: Labels the identities for the factor directly from the labels associated with an Oracle Label Security policy</li> <li>DBMS_MACUTL.G_LABELED_BY_FACTORS: Derives the factor identity label from the labels of its child factor identities.</li> </ul> The default for labeled_by is the previously set value, which you can find by querying the DBA_DV_FACTOR data dictionary view. See <a href="#">Setting the Oracle Label Security Labeling Information for a Factor</a> (page 8-9) for more information.

**Table 18-20 (Cont.) UPDATE\_FACTOR**

Parameter	Description
eval_options	<p>Options for evaluating the factor when the user logs on:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_EVAL_ON_SESSION: When the database session is created</li> <li>DBMS_MACUTL.G_EVAL_ON_ACCESS: Each time the factor is accessed</li> <li>DBMS_MACUTL.G_EVAL_ON_STARTUP: On start-up</li> </ul> <p>The default for eval_options is the previously set value, which you can find by querying the DBA_DV_FACTOR data dictionary view.</p> <p>See <a href="#">Setting the Evaluation Information for a Factor</a> (page 8-9) for more information.</p>
audit_options	<p>Options for auditing the factor if you want to generate a custom Oracle Database Vault audit record.</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_AUDIT_OFF: Disables auditing.</li> <li>DBMS_MACUTL.G_AUDIT_ALWAYS: Always audits.</li> <li>DBMS_MACUTL.G_AUDIT_ON_GET_ERROR: Audits if get_expr returns an error.</li> <li>DBMS_MACUTL.G_AUDIT_ON_GET_NULL: Audits if get_expr is null.</li> <li>DBMS_MACUTL.G_AUDIT_ON_VALIDATE_ERROR: Audits if the validation procedure returns an error.</li> <li>DBMS_MACUTL.G_AUDIT_ON_VALIDATE_FALSE: Audits if the validation procedure is false.</li> <li>DBMS_MACUTL.G_AUDIT_ON_TRUST_LEVEL_NULL: Audits if there is no trust level set.</li> <li>DBMS_MACUTL.G_AUDIT_ON_TRUST_LEVEL_NEG: Audits if the trust level is negative.</li> </ul> <p>The default for audit_options is the previously set value, which you can find by querying the DBA_DV_FACTOR data dictionary view.</p> <p>See <a href="#">Setting Audit Options for a Factor</a> (page 8-13) for more information.</p>
fail_options	<p>Options for reporting factor errors:</p> <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_FAIL_WITH_MESSAGE: Shows an error message.</li> <li>DBMS_MACUTL.G_FAIL_SILENTLY: Does not show an error message.</li> </ul> <p>The default for fail_options is the previously set value, which you can find by querying the DBA_DV_FACTOR data dictionary view.</p> <p>See <a href="#">Setting Error Options for a Factor</a> (page 8-13) for more information.</p>

**Example**

```

BEGIN
  DBMS_MACADM.UPDATE_FACTOR(
    factor_name      => 'Sector2_DB',
    factor_type_name => 'Instance',
    description     => ' ',
  )

```

```

rule_set_name      => 'Limit_DBA_Access',
get_expr           => 'UPPER(SYS_CONTEXT(''USERENV'', ''DB_NAME''))',
validate_expr      => 'dbavowner.check_db_access',
identify_by        => DBMS_MACUTL.G_IDENTIFY_BY_METHOD,
labeled_by         => DBMS_MACUTL.G_LABELED_BY_SELF,
eval_options       => DBMS_MACUTL.G_EVAL_ON_ACCESS,
audit_options      => DBMS_MACUTL.G_AUDIT_ALWAYS,
fail_options       => DBMS_MACUTL.G_FAIL_WITH_MESSAGE);
END;
/

```

## 18.1.21 UPDATE\_FACTOR\_TYPE Procedure

The UPDATE\_FACTOR\_TYPE procedure updates a factor type.

### Syntax

```

DBMS_MACADM.UPDATE_FACTOR_TYPE(
  name          IN VARCHAR2,
  description   IN VARCHAR2);

```

### Parameters

**Table 18-21 UPDATE\_FACTOR\_TYPE Parameters**

Parameter	Description
name	Factor type name. To find existing factor types in the current database instance, query the DBA_DV_FACTOR_TYPE view, described in <a href="#">DBA_DV_FACTOR_TYPE View</a> (page 25-13).
description	Description of the purpose of the factor type, up to 1024 characters in mixed case.

### Example

```

BEGIN
  DBMS_MACADM.UPDATE_FACTOR_TYPE(
    name          => 'Sector2DBInstance',
    description   => 'Checks DB instances used in Sector 2');
END;
/

```

## 18.1.22 UPDATE\_IDENTITY Procedure

The UPDATE\_IDENTITY procedure updates the trust level of a factor identity.

### Syntax

```

DBMS_MACADM.UPDATE_IDENTITY(
  factor_name  IN VARCHAR2,
  value        IN VARCHAR2,
  trust_level  IN NUMBER);

```

## Parameters

**Table 18-22 UPDATE\_IDENTITY Parameters**

Parameter	Description
factor_name	Factor name. To find existing factors in the current database instance, query the DBA_DV_FACTOR view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11). To find factors that have identities, query DBA_DV_IDENTITY, described in <a href="#">DBA_DV_IDENTITY View</a> (page 25-15).
value	New factor identity, up to 1024 characters in mixed-case. For example, the identity of an IP_Address factor could be the IP address of 192.0.2.12.
trust_level	Number that indicates the magnitude of trust relative to other identities for the same factor. In general, the higher the trust level number is set, the greater the trust. A trust level of 10 indicates "very trusted." Negative trust levels are not trusted. See <a href="#">Creating and Configuring a Factor Identity</a> (page 8-16) for more information about trust levels and label security.

## Example

```
BEGIN
  DBMS_MACADM.UPDATE_IDENTITY(
    factor_name => 'Sector2_ClientID',
    value       => 'intranet',
    trust_level => 10);
END;
/
```

## 18.2 Oracle Database Vault Run-Time PL/SQL Procedures and Functions

Oracle Database Vault provides procedural interfaces to administer Database Vault security options and manage Database Vault security enforcements.

### [About Oracle Database Vault Run-Time PL/SQL Procedures and Functions](#) (page 18-23)

Oracle Database Vault provides a set of PL/SQL procedures and functions that are specific to factors.

### [SET\\_FACTOR Procedure](#) (page 18-23)

The SET\_FACTOR procedure can be exposed to an application that requires the ability to set factor identities dynamically.

### [GET\\_FACTOR Function](#) (page 18-24)

The GET\_FACTOR function is exposed to the DVF schema to allow the public factor functions to resolve the identity of a factor. The return type is VARCHAR2.

### [GET\\_FACTOR\\_LABEL Function](#) (page 18-24)

The GET\_FACTOR\_LABEL function returns the label for the specified factor when the factor has a label assigned to it for the specified Oracle Label Security policy. The return type is VARCHAR2.



**GET\_TRUST\_LEVEL Function** (page 18-25)

The `GET_TRUST_LEVEL` function returns the trust level of the current session identity for the factor requested. The return type is `VARCHAR2`.

**GET\_TRUST\_LEVEL\_FOR\_IDENTITY Function** (page 18-26)

The `GET_TRUST_LEVEL_FOR_IDENTITY` function returns the trust level for the factor and identity requested. The return type is `VARCHAR2`.

**ROLE\_IS\_ENABLED Function** (page 18-27)

The `ROLE_IS_ENABLED` function returns a boolean value that specifies whether a database role has been enabled. The return type is `BOOLEAN`.

## 18.2.1 About Oracle Database Vault Run-Time PL/SQL Procedures and Functions

Oracle Database Vault provides a set of PL/SQL procedures and functions that are specific to factors.

These procedures and functions that expose the logic to validate a DDL command for realm violations and command authorizations. Additional procedures and functions are provided to set the value of a factor (assuming their associated rule sets evaluate to true) (for example, from a Web application), to retrieve the trust level for a session or specific factor identity, and to get the label for a factor identity. These procedures and functions are provided so that a database administrator does not grant the `EXECUTE` privilege on all `DVSYS` package procedures to the general database account population. The procedures and functions expose only the minimum methods that are required. All of these functions and procedures are publicly available for applications that need them.

## 18.2.2 SET\_FACTOR Procedure

The `SET_FACTOR` procedure can be exposed to an application that requires the ability to set factor identities dynamically.

It wraps the package procedure `DBMS_MACADM.SET_FACTOR`. When a factor has a rule set associated with it for assignment and if the rule set returns true, then the value is set. Normal rule set handling occurs, and the factor value (identity) validation method is called. This procedure is available (to execute) to the general database account population.

### Syntax

```
SET_FACTOR(
  p_factor IN VARCHAR2,
  p_value  IN VARCHAR2);
```

### Parameters

**Table 18-23** *SET\_FACTOR Parameters*

Parameter	Description
<code>p_factor</code>	Factor name. To find existing factors in the current database instance, query the <code>DBA_DV_FACTOR</code> data dictionary view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).

**Table 18-23 (Cont.) SET\_FACTOR Parameters**

Parameter	Description
p_value	Identity value, up to 1024 characters in mixed case. To find the identities for each factor in the current database instance, query the DBA_DV_IDENTITY data dictionary view, described in <a href="#">DBA_DV_IDENTITY View</a> (page 25-15).

**Example**

```
EXECUTE SET_FACTOR('Sector2_ClientID', 'identity');
```

**18.2.3 GET\_FACTOR Function**

The GET\_FACTOR function is exposed to the DVF schema to allow the public factor functions to resolve the identity of a factor. The return type is VARCHAR2.

This function enables the F\$ functions in the DVF schema. This function is available (to execute) to the general database account population.

**Syntax**

```
GET_FACTOR(
  p_factor IN VARCHAR2)
RETURN VARCHAR2;
```

**Parameter****Table 18-24 GET\_FACTOR Parameter**

Parameter	Description
p_factor	Factor name. To find existing factors in the current database instance, query the DBA_DV_FACTOR data dictionary view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Get Client ID Factor Identity',
    rule_expr => 'GET_FACTOR('Sector2_ClientID')');
END;
/
```

**18.2.4 GET\_FACTOR\_LABEL Function**

The GET\_FACTOR\_LABEL function returns the label for the specified factor when the factor has a label assigned to it for the specified Oracle Label Security policy. The return type is VARCHAR2.

The function returns a label that is merged with the maximum session label for the policy if the policy is configured with Oracle Label Security. The function is available (to execute) to the general database population.

**Syntax**

```
GET_FACTOR_LABEL(
  p_factor      IN VARCHAR2,
  p_policy_name IN VARCHAR2)
RETURN VARCHAR2;
```

**Parameters****Table 18-25 GET\_FACTOR\_LABEL Parameters**

Parameter	Description
p_factor	Factor name.  To find the available factors in the current database instance, query the DBA_DV_FACTOR data dictionary view. To find factors that are associated with Oracle Label Security policies, use DBA_DV_MAC_POLICY_FACTOR.  See <a href="#">DBA_DV_FACTOR View</a> (page 25-11) and <a href="#">DBA_DV_MAC_POLICY_FACTOR View</a> (page 25-17).
p_policy_name	Oracle Label Security policy name.  Use the following data dictionary views to find information about policies and factors in the current database instance: <ul style="list-style-type: none"> <li>DBA_DV_MAC_POLICY: Lists Oracle Label Security policies defined in the current database instance. See <a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17).</li> <li>DBA_DV_MAC_POLICY_FACTOR: Lists the factors that are associated with Oracle Label Security policies for the current database instance. See <a href="#">DBA_DV_MAC_POLICY_FACTOR View</a> (page 25-17).</li> <li>DBA_DV_POLICY_LABEL: Lists the Oracle Label Security label for each factor identifier in the DBA_DV_IDENTITY view for each policy. See <a href="#">DBA_DV_POLICY_LABEL View</a> (page 25-20).</li> </ul>

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Get the ClientID Factor Label',
    rule_expr => 'GET_FACTOR_LABEL(''Sector2_ClientID'', ''Access Locations'');
END;
/
```

**18.2.5 GET\_TRUST\_LEVEL Function**

The GET\_TRUST\_LEVEL function returns the trust level of the current session identity for the factor requested. The return type is VARCHAR2.

This function is available (to execute) to the general database account population. See [Creating and Configuring a Factor Identity](#) (page 8-16) for a listing of the available trust levels.

**Syntax**

```
GET_TRUST_LEVEL(
  p_factor IN VARCHAR2)
RETURN VARCHAR2;
```

## Parameter

**Table 18-26** *GET\_TRUST\_LEVEL* Parameter

Parameter	Description
p_factor	Factor name. To find existing factors in the current database instance, query the DBA_DV_FACTOR data dictionary view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).

## Example

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Get Client ID Trust Level',
    rule_expr => 'GET_TRUST_LEVEL(''Sector2_ClientID'')');
END;
/
```

## 18.2.6 GET\_TRUST\_LEVEL\_FOR\_IDENTITY Function

The GET\_TRUST\_LEVEL\_FOR\_IDENTITY function returns the trust level for the factor and identity requested. The return type is VARCHAR2.

This function is available (to execute) to the general database account population. See [Creating and Configuring a Factor Identity](#) (page 8-16) for a listing of the available trust levels.

## Syntax

```
GET_TRUST_LEVEL_FOR_IDENTITY(
  p_factor   IN VARCHAR2,
  p_identity IN VARCHAR2)
RETURN VARCHAR2;
```

## Parameters

**Table 18-27** *GET\_TRUST\_LEVEL\_FOR\_IDENTITY* Parameters

Parameter	Description
p_factor	Factor name. To find existing factors in the current database instance, query the DBA_DV_FACTOR view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11).
p_identity	Identity value. To find the identities for each factor in the current database instance, use the DBA_DV_IDENTITY data dictionary view, described in <a href="#">DBA_DV_IDENTITY View</a> (page 25-15).

## Example

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Get Client ID Identity Trust Level',
    rule_expr => 'GET_TRUST_LEVEL_FOR_IDENTITY(''Sector2_ClientID'', ''identity'')');
```

```
END;
/
```

## 18.2.7 ROLE\_IS\_ENABLED Function

The `ROLE_IS_ENABLED` function returns a boolean value that specifies whether a database role has been enabled. The return type is `BOOLEAN`.

This function is available (to execute) to the general database account population.

### Syntax

```
ROLE_IS_ENABLED(
  p_role IN VARCHAR2)
RETURN BOOLEAN;
```

### Parameter

**Table 18-28** *ROLE\_IS\_ENABLED* Parameter

Parameter	Description
<code>p_role</code>	<p>Database role name to check.</p> <p>To find existing roles, use the following data dictionary views:</p> <ul style="list-style-type: none"> <li><code>DBA_ROLES</code>: Finds available roles in the current database instance. See <i>Oracle Database Reference</i>.</li> <li><code>DBA_DV_REALM_AUTH</code>: Finds the authorization of a particular role. See <a href="#">DBA_DV_REALM View</a> (page 25-24).</li> <li><code>DBA_DV_ROLE</code>: Finds existing secure application roles used in privilege management. See <a href="#">DBA_DV_ROLE View</a> (page 25-28).</li> </ul>

### Example

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check if SYSADM Role Is Enabled',
    rule_expr => 'ROLE_IS_ENABLED(''SYSADM'')');
END;
/
```

## 18.3 Oracle Database Vault DVF PL/SQL Factor Functions

Oracle Database Vault maintains the DVF schema functions when you use the `DBMS_MACADM` PL/SQL package to manage the various factors.

### [About Oracle Database Vault DVF PL/SQL Factor Functions](#) (page 18-29)

Oracle Database Vault provides DVF factor-specific functions for frequently used activities.

### [F\\$AUTHENTICATION\\_METHOD](#) Function (page 18-29)

The `F$AUTHENTICATION_METHOD` function returns the method of authentication in `VARCHAR2` data type.

### [F\\$CLIENT\\_IP](#) Function (page 18-30)

The `F$CLIENT_IP` function returns the IP address of the computer from which the client is connected, in `VARCHAR2` data type.

**F\$DATABASE\_DOMAIN Function** (page 18-31)

The F\$DATABASE\_DOMAIN function returns the domain of the database as specified in the DB\_DOMAIN initialization parameter, in VARCHAR2 data type.

**F\$DATABASE\_HOSTNAME Function** (page 18-31)

The F\$DATABASE\_HOSTNAME function returns the host name of the computer on which the instance is running, in VARCHAR2 data type.

**F\$DATABASE\_INSTANCE Function** (page 18-31)

The F\$DATABASE\_INSTANCE function returns the instance identification number of the current database instance, in VARCHAR2 data type.

**F\$DATABASE\_IP Function** (page 18-32)

The F\$DATABASE\_IP function returns the IP address of the computer on which the database instance is running, in VARCHAR2 data type.

**F\$DATABASE\_NAME Function** (page 18-32)

The F\$DATABASE\_NAME function returns the name of the database as specified in the DB\_NAME initialization parameter, in VARCHAR2 data type.

**F\$DOMAIN Function** (page 18-33)

The F\$DOMAIN function returns a named collection of physical, configuration, or implementation-specific factors in the run-time environment (for example, a networked IT environment or subset of it) that operates at a specific sensitivity level. The return type is VARCHAR2.

**F\$ENTERPRISE\_IDENTITY Function** (page 18-33)

The F\$ENTERPRISE\_IDENTITY function returns the enterprise-wide identity for a user, in VARCHAR2 data type.

**F\$IDENTIFICATION\_TYPE Function** (page 18-34)

The F\$IDENTIFICATION\_TYPE function returns the way the schema of a user was created in the database. Specifically, it reflects the IDENTIFIED clause in the CREATE/ALTER USER syntax. The return type is VARCHAR2.

**F\$LANG Function** (page 18-34)

The F\$LANG function returns the ISO abbreviation for the language name, a shorter form than the existing LANGUAGE parameter, for the session of the user. The return type is VARCHAR2.

**F\$LANGUAGE Function** (page 18-35)

The F\$LANGUAGE function returns the language and territory currently used by a user session, along with the database character set. The return type is VARCHAR2.

**F\$MACHINE Function** (page 18-35)

The F\$MACHINE function returns the computer (host) name for the database client that established the database session. The return type is VARCHAR2.

**F\$NETWORK\_PROTOCOL Function** (page 18-36)

The F\$NETWORK\_PROTOCOL function returns the network protocol being used for communication, as specified in the PROTOCOL=*protocol* portion of the connect string. The return type is VARCHAR2.

**F\$PROXY\_ENTERPRISE\_IDENTITY Function** (page 18-36)

The F\$PROXY\_ENTERPRISE\_IDENTITY function returns the Oracle Internet Directory distinguished name (DN) when the proxy user is an enterprise user. The return type is VARCHAR2.

**F\$SESSION\_USER Function** (page 18-37)

The F\$SESSION\_USER function returns the database user name by which the current user is authenticated. This value remains the same throughout the session. The return type is VARCHAR2.

### 18.3.1 About Oracle Database Vault DVF PL/SQL Factor Functions

Oracle Database Vault provides DVF factor-specific functions for frequently used activities.

In addition to the functions and procedures made available from the DVSYS schema, the DVF schema contains a single function for each factor defined in the system.

The functions are then available to the general database account population through PL/SQL functions and standard SQL. This enables factors to be used in Oracle Label Security, Oracle Virtual Private Database (VPD), and so on.

Typically, you can incorporate these functions into rule expressions. For example:

The functions are then available to the general database account population through PL/SQL functions and standard SQL. This enables factors to be used in Oracle Label Security, Oracle Virtual Private Database (VPD), and so on.

Typically, you can incorporate these functions into rule expressions. For example:

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Not Internal DBA',
    rule_expr => 'DVF.F$SESSION_USER NOT IN (''JSMTIH'', ''TBROWN'')');
END;
/
```

To find the value of a factor function, select from the DUAL system table. For example:

```
SELECT DVF.F$SESSION_USER FROM DUAL;
```

```
F$SESSION_USER
```

```
-----
LEO_DVOWNER
```

The name of the factor itself is case-insensitive. For example, the following statements return the same result

```
select dvf.f$session_user from dual;
```

```
SELECT DVF.F$SESSION_USER FROM DUAL;
```

### 18.3.2 F\$AUTHENTICATION\_METHOD Function

The F\$AUTHENTICATION\_METHOD function returns the method of authentication in VARCHAR2 data type.

In the list that follows, the type of user is followed by the method returned:

- Password-authenticated enterprise user, local database user, or SYSDBA/SYSOPER using Password File; proxy with user name using password: PASSWORD

- Kerberos-authenticated enterprise or external user: KERBEROS
- SSL-authenticated enterprise or external user: SSL
- Radius-authenticated external user: RADIUS
- Operating system-authenticated external user or SYSDBA/SYSOPER: OS
- DCE-authenticated external user: DCE
- Proxy with certificate, distinguished name (DN), or user name without using password: NONE

You can use `IDENTIFICATION_TYPE` to distinguish between external and enterprise users when the authentication method is Password, Kerberos, or SSL.

### Syntax

```
DVF.F$AUTHENTICATION_METHOD ()  
RETURN VARCHAR2;
```

### Parameters

None

### Example

```
BEGIN  
  DBMS_MACADM.CREATE_RULE(  
    rule_name => 'Check SSL Authentication Method',  
    rule_expr => 'DVF.F$AUTHENTICATION_METHOD = ''SSL''');  
END;  
/
```

## 18.3.3 F\$CLIENT\_IP Function

The `F$CLIENT_IP` function returns the IP address of the computer from which the client is connected, in `VARCHAR2` data type.

### Syntax

```
DVF.F$CLIENT_IP ()  
RETURN VARCHAR2;
```

### Parameters

None

### Example

The following example shows how to use `DVF.F$CLIENT_IP` in a rule creation statement. Note that you can only enter one IP address, not a range of IP addresses.

```
BEGIN  
  DBMS_MACADM.CREATE_RULE(  
    rule_name => 'Check Client IP Address',  
    rule_expr => 'DVF.F$CLIENT_IP = ''192.0.2.10''');  
END;  
/
```



### 18.3.4 F\$DATABASE\_DOMAIN Function

The F\$DATABASE\_DOMAIN function returns the domain of the database as specified in the DB\_DOMAIN initialization parameter, in VARCHAR2 data type.

#### Syntax

```
DVF.F$DATABASE_DOMAIN ()
RETURN VARCHAR2;
```

#### Parameters

None

#### Example

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Client Database Domain',
    rule_expr => 'DVF.F$DATABASE_DOMAIN NOT IN (''EXAMPLE'', ''YOURDOMAIN'')');
END;
/
```

### 18.3.5 F\$DATABASE\_HOSTNAME Function

The F\$DATABASE\_HOSTNAME function returns the host name of the computer on which the instance is running, in VARCHAR2 data type.

#### Syntax

```
DVF.F$DATABASE_HOSTNAME ()
RETURN VARCHAR2;
```

#### Parameters

None

#### Example

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Host Name',
    rule_expr => 'DVF.F$DATABASE_HOSTNAME IN (''SHOBEEN'', ''MAU'')');
END;
/
```

### 18.3.6 F\$DATABASE\_INSTANCE Function

The F\$DATABASE\_INSTANCE function returns the instance identification number of the current database instance, in VARCHAR2 data type.

#### Syntax

```
DVF.F$DATABASE_INSTANCE ()
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Database Instance ID',
    rule_expr => 'DVF.F$DATABASE_INSTANCE = ''SALES_DB''');
END;
/
```

**18.3.7 F\$DATABASE\_IP Function**

The F\$DATABASE\_IP function returns the IP address of the computer on which the database instance is running, in VARCHAR2 data type.

**Syntax**

```
DVF.F$DATABASE_IP ()
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Database IP address',
    rule_expr => 'DVF.F$DATABASE_IP = ''192.0.2.5''');
END;
/
```

**18.3.8 F\$DATABASE\_NAME Function**

The F\$DATABASE\_NAME function returns the name of the database as specified in the DB\_NAME initialization parameter, in VARCHAR2 data type.

**Syntax**

```
DVF.F$DATABASE_NAME ()
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Database DB_NAME Name',
    rule_expr => 'DVF.F$DATABASE_NAME = ''ORCL''');
END;
/
```

### 18.3.9 F\$DOMAIN Function

The F\$DOMAIN function returns a named collection of physical, configuration, or implementation-specific factors in the run-time environment (for example, a networked IT environment or subset of it) that operates at a specific sensitivity level. The return type is VARCHAR2.

You can identify a domain using factors such as host name, IP address, and database instance names of the Oracle Database Vault nodes in a secure access path to the database. Each domain can be uniquely determined using a combination of the factor identifiers that identify the domain. You can use these identifying factors and possibly additional factors to define the Maximum Security Label within the domain. This restricts data access and commands, depending on the physical factors about the Oracle Database Vault session. Example domains of interest may be Corporate Sensitive, Internal Public, Partners, and Customers.

#### Syntax

```
DVF.F$DOMAIN ( )
RETURN VARCHAR2;
```

#### Parameters

None

#### Example

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Domain',
    rule_expr => 'DVF.F$DOMAIN = ''EXAMPLE.COM''');
END;
/
```

### 18.3.10 F\$ENTERPRISE\_IDENTITY Function

The F\$ENTERPRISE\_IDENTITY function returns the enterprise-wide identity for a user, in VARCHAR2 data type.

- For enterprise users: the Oracle Internet Directory DN.
- For external users: the external identity (Kerberos principal name, Radius and DCE schema names, operating system user name, certificate DN).
- For local users and SYSDBA/SYSOPER logins: NULL.

The value of the attribute differs by proxy method:

- For a proxy with DN: the Oracle Internet Directory DN of the client.
- For a proxy with certificate: the certificate DN of the client for external users; the Oracle Internet Directory DN for global users.
- For a proxy with user name: the Oracle Internet Directory DN if the client is an enterprise user; NULL if the client is a local database user.

**Syntax**

```
DVF.F$ENTERPRISE_IDENTITY ()  
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```
BEGIN  
  DBMS_MACADM.CREATE_RULE(  
    rule_name => 'Check User Enterprise Identity',  
    rule_expr => 'DVF.F$ENTERPRISE_IDENTITY NOT IN (''JSMITH'', ''TSMITH'')');  
END;  
/
```

### 18.3.11 F\$IDENTIFICATION\_TYPE Function

The F\$IDENTIFICATION\_TYPE function returns the way the schema of a user was created in the database. Specifically, it reflects the IDENTIFIED clause in the CREATE/ALTER USER syntax. The return type is VARCHAR2.

In the list that follows, the syntax used during schema creation is followed by the identification type returned:

- IDENTIFIED BY *password*: LOCAL
- IDENTIFIED EXTERNALLY: EXTERNAL
- IDENTIFIED GLOBALLY: GLOBAL SHARED
- IDENTIFIED GLOBALLY AS DN: GLOBAL PRIVATE

**Syntax**

```
DVF.F$IDENTIFICATION_TYPE ()  
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```
BEGIN  
  DBMS_MACADM.CREATE_RULE(  
    rule_name => 'Check User Schema Creation Type',  
    rule_expr => 'DVF.F$IDENTIFICATION_TYPE = ''GLOBAL SHARED''');  
END;  
/
```

### 18.3.12 F\$LANG Function

The F\$LANG function returns the ISO abbreviation for the language name, a shorter form than the existing LANGUAGE parameter, for the session of the user. The return type is VARCHAR2.

See *Oracle Database Globalization Support Guide* for a listing of supported languages for Oracle Database.

### Syntax

```
DVF.F$LANG ()
RETURN VARCHAR2;
```

### Parameters

None

### Example

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check ISO Abbreviated Language Name',
    rule_expr => 'DVF.F$LANG IN (''EN'', ''DE'', ''FR'')');
END;
/
```

## 18.3.13 F\$LANGUAGE Function

The F\$LANGUAGE function returns the language and territory currently used by a user session, along with the database character set. The return type is VARCHAR2.

The return type is in the following format:

*language\_territory.characterset*

See *Oracle Database Globalization Support Guide* for a listing of supported languages and territories for Oracle Database.

### Syntax

```
DVF.F$LANGUAGE ()
RETURN VARCHAR2;
```

### Parameters

None

### Example

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Session Language and Territory',
    rule_expr => 'DVF.F$LANGUAGE = ''AMERICAN_AMERICA.WE8ISO8859P1''');
END;
/
```

## 18.3.14 F\$MACHINE Function

The F\$MACHINE function returns the computer (host) name for the database client that established the database session. The return type is VARCHAR2.

### Syntax

```
DVF.F$MACHINE ()
RETURN VARCHAR2;
```

**Parameter**

None

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Client Computer Host Name',
    rule_expr => 'DVF.F$MACHINE NOT IN (''SHOBEEN'', ''SEBASTIAN'')');
END;
/
```

### 18.3.15 F\$NETWORK\_PROTOCOL Function

The F\$NETWORK\_PROTOCOL function returns the network protocol being used for communication, as specified in the `PROTOCOL=protocol` portion of the connect string. The return type is VARCHAR2.

**Syntax**

```
DVF.F$NETWORK_PROTOCOL ()
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Check Network Protocol',
    rule_expr => 'DVF.F$NETWORK_PROTOCOL = ''TCP''');
END;
/
```

### 18.3.16 F\$PROXY\_ENTERPRISE\_IDENTITY Function

The F\$PROXY\_ENTERPRISE\_IDENTITY function returns the Oracle Internet Directory distinguished name (DN) when the proxy user is an enterprise user. The return type is VARCHAR2.

**Syntax**

```
DVF.F$PROXY_ENTERPRISE_IDENTITY ()
RETURN VARCHAR2;
```

**Parameters**

None

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Get OID DN of Enterprise User',
    rule_expr => 'DVF.F$PROXY_ENTERPRISE_IDENTITY = ''cn=Provisioning Admins''');
END;
```

```
END;  
/
```

### 18.3.17 F\$SESSION\_USER Function

The F\$SESSION\_USER function returns the database user name by which the current user is authenticated. This value remains the same throughout the session. The return type is VARCHAR2.

#### Syntax

```
DVF.F$SESSION_USER (  
RETURN VARCHAR2;
```

#### Parameters

None

#### Example

```
BEGIN  
  DBMS_MACADM.CREATE_RULE(  
    rule_name => 'Check Database User Name',  
    rule_expr => 'DVF.F$SESSION_USER IN (''JSMITH'', ''TSMITH'')');  
END;  
/
```





---

# Oracle Database Vault Secure Application Role APIs

The DBMS\_MACADM and DBMS\_MACSEC\_ROLES PL/SQL packages manage Database Vault secure application roles.

[DBMS\\_MACADM Secure Application Role Procedures](#) (page 19-1)

The DBMS\_MACADM package creates, renames, assigns, unassigns, updates, and deletes Oracle Database Vault secure application roles.

[DBMS\\_MACSEC\\_ROLES Secure Application Role Procedure and Function](#) (page 19-6)

The DBMS\_MACSEC\_ROLES package checks the authorization for users and sets Oracle Database Vault secure application roles.

**Related Topics:**

[Configuring Secure Application Roles for Oracle Database Vault](#) (page 9-1)

Secure application roles enable you to control how much access users have to an application.

[Oracle Database Vault Utility APIs](#) (page 21-1)

Oracle Database Vault provides a set of utility APIs in the DBMS\_MACUTL PL/SQL package.

## 19.1 DBMS\_MACADM Secure Application Role Procedures

The DBMS\_MACADM package creates, renames, assigns, unassigns, updates, and deletes Oracle Database Vault secure application roles.

[ASSIGN\\_ROLE Procedure](#) (page 19-2)

The ASSIGN\_ROLE procedure assigns an Oracle Database Vault secure application role to a user.

[CREATE\\_ROLE Procedure](#) (page 19-2)

The CREATE\_ROLE procedure creates an Oracle Database Vault secure application role.

[DELETE\\_ROLE Procedure](#) (page 19-3)

The DELETE\_ROLE procedure deletes an Oracle Database Vault secure application role.

[RENAME\\_ROLE Procedure](#) (page 19-4)

The RENAME\_ROLE procedure renames an Oracle Database Vault secure application role. The name change takes effect everywhere the role is used.

**UPDATE\_ROLE Procedure** (page 19-4)

The UPDATE\_ROLE procedure updates a Oracle Database Vault secure application role.

**UNASSIGN\_ROLE Procedure** (page 19-5)

The ASSIGN\_ROLE procedure unassigns an Oracle Database Vault secure application role from a user.

**19.1.1 ASSIGN\_ROLE Procedure**

The ASSIGN\_ROLE procedure assigns an Oracle Database Vault secure application role to a user.

**Syntax**

```
DBMS_MACADM.ASSIGN_ROLE(
  role_name      IN VARCHAR2,
  assignee       IN VARCHAR2);
```

**Parameters****Table 19-1 ASSIGN\_ROLE Parameters**

Parameter	Description
role_name	Role name, up to 128 characters, with no spaces. To find existing secure application roles in the current database instance, query the DBA_DV_ROLE view, described in <a href="#">DBA_DV_ROLE View</a> (page 25-28).
assignee	User to be assigned the secure application role To find existing database users in the current instance, query the DBA_USERS view, described in <i>Oracle Database Reference</i> .

**Example**

```
BEGIN
  DBMS_MACADM.ASSIGN_ROLE(
    role_name      => 'Sector2_APP_MGR',
    assignee       => 'PSMITH');
END;
/
```

**19.1.2 CREATE\_ROLE Procedure**

The CREATE\_ROLE procedure creates an Oracle Database Vault secure application role.

**Syntax**

```
DBMS_MACADM.CREATE_ROLE(
  role_name      IN VARCHAR2,
  enabled        IN VARCHAR2,
  rule_set_name  IN VARCHAR2);
```

## Parameters

**Table 19-2 CREATE\_ROLE Parameters**

Parameter	Description
role_name	Role name, up to 128 characters, with no spaces. In a multitenant environment, prepend the role name with c## or C##. To find existing secure application roles in the current database instance, query the DBA_DV_ROLE view, described in <a href="#">DBA_DV_ROLE View</a> (page 25-28).
enabled	DBMS_MACUTL.G_YES (Yes) makes the role available for enabling; DBMS_MACUTL.G_NO (No) prevents the role from being enabled. The default is DBMS_MACUTL.G_YES.
rule_set_name	Name of rule set to determine whether this secure application can be enabled. To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).

## Example

```
BEGIN
  DBMS_MACADM.CREATE_ROLE(
    role_name      => 'Sector2_APP_MGR',
    enabled        => DBMS_MACUTL.G_YES,
    rule_set_name  => 'Check App2 Access');
END;
/
```

### 19.1.3 DELETE\_ROLE Procedure

The DELETE\_ROLE procedure deletes an Oracle Database Vault secure application role.

## Syntax

```
DBMS_MACADM.DELETE_ROLE(
  role_name IN VARCHAR2);
```

## Parameters

**Table 19-3 DELETE\_ROLE Parameter**

Parameter	Description
role_name	Role name. To find existing secure application roles in the current database instance, query the DBA_DV_ROLE view, described in <a href="#">DBA_DV_ROLE View</a> (page 25-28).

## Example

```
EXEC DBMS_MACADM.DELETE_ROLE('SECT2_APP_MGR');
```

## 19.1.4 RENAME\_ROLE Procedure

The `RENAME_ROLE` procedure renames an Oracle Database Vault secure application role. The name change takes effect everywhere the role is used.

### Syntax

```
DBMS_MACADM.RENAME_ROLE(
  role_name      IN VARCHAR2,
  new_role_name  IN VARCHAR2);
```

### Parameters

**Table 19-4** *RENAME\_ROLE* Parameters

Parameter	Description
<code>role_name</code>	Current role name. To find existing secure application roles in the current database instance, query the <code>DBA_DV_ROLE</code> view, described in <a href="#">DBA_DV_ROLE View</a> (page 25-28).
<code>new_role_name</code>	Role name, up to 128 characters, with no spaces. Ensure that this name follows the standard Oracle naming conventions for role creation described in <i>Oracle Database SQL Language Reference</i> . In a multitenant environment, prepend the role name with <code>c##</code> or <code>C##</code> .

### Example

```
BEGIN
  DBMS_MACADM.RENAME_ROLE(
    role_name      => 'SECT2_APP_MGR',
    new_role_name  => 'SECT2_SYSADMIN');
END;
/
```

## 19.1.5 UPDATE\_ROLE Procedure

The `UPDATE_ROLE` procedure updates a Oracle Database Vault secure application role.

### Syntax

```
DBMS_MACADM.UPDATE_ROLE(
  role_name      IN VARCHAR2,
  enabled        IN VARCHAR2,
  rule_set_name  IN VARCHAR2);
```

## Parameters

**Table 19-5 UPDATE\_ROLE Parameters**

Parameter	Description
role_name	Role name. To find existing secure application roles in the current database instance, query the DBA_DV_ROLE view, described in <a href="#">DBA_DV_ROLE View</a> (page 25-28).
enabled	DBMS_MACUTL.G_YES (Yes) makes the role available for enabling; DBMS_MACUTL.G_NO (No) prevents the role from being enabled. The default for enabled is the previously set value, which you can find by querying the DBA_DV_ROLE data dictionary view.
rule_set_name	Name of rule set to determine whether this secure application can be enabled. To find existing rule sets in the current database instance, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30).

## Example

```
BEGIN
  DBMS_MACADM.UPDATE_ROLE(
    role_name      => 'SECT2_SYSADMIN',
    enabled        => DBMS_MACUTL.G_YES,
    rule_set_name  => 'System Access Controls');
END;
/
```

## 19.1.6 UNASSIGN\_ROLE Procedure

The ASSIGN\_ROLE procedure unassigns an Oracle Database Vault secure application role from a user.

### Syntax

```
DBMS_MACADM.UNASSIGN_ROLE(
  role_name      IN VARCHAR2,
  assignee      IN VARCHAR2);
```

## Parameters

**Table 19-6 UNASSIGN\_ROLE Parameters**

Parameter	Description
role_name	Role name. To find existing secure application roles in the current database instance, query the DBA_DV_ROLE view, described in <a href="#">DBA_DV_ROLE View</a> (page 25-28).
assignee	User who was assigned the Secure Application role To find existing database users in the current instance, query the DBA_USERS view, described in <i>Oracle Database Reference</i> .

**Example**

```

BEGIN
  DBMS_MACADM.UNASSIGN_ROLE(
    role_name      => 'Sector2_APP_MGR',
    assignee       => 'PSMITH');
END;
/

```

**19.2 DBMS\_MACSEC\_ROLES Secure Application Role Procedure and Function**

The DBMS\_MACSEC\_ROLES package checks the authorization for users and sets Oracle Database Vault secure application roles.

The DBMS\_MACSEC\_ROLES package is available to all users.

**CAN\_SET\_ROLE Function** (page 19-6)

The CAN\_SET\_ROLE function checks if the user invoking the method is authorized to use an Oracle Database Vault secure application role.

**SET\_ROLE Procedure** (page 19-7)

The SET\_ROLE procedure issues the SET ROLE PL/SQL statement for specified roles.

**19.2.1 CAN\_SET\_ROLE Function**

The CAN\_SET\_ROLE function checks if the user invoking the method is authorized to use an Oracle Database Vault secure application role.

The authorization is determined by checking the rule set associated with the role. The return type is BOOLEAN.

**Syntax**

```

DBMS_MACSEC_ROLES.CAN_SET_ROLE(
  p_role IN VARCHAR2)
RETURN BOOLEAN;

```

**Parameters****Table 19-7 CAN\_SET\_ROLE Parameter**

Parameter	Description
p_role	Role name. To find existing secure application roles in the current database instance, query the DBA_DV_ROLE view, described in <a href="#">DBA_DV_ROLE View</a> (page 25-28).

**Example**

```

SET SERVEROUTPUT ON
BEGIN
  IF DBMS_MACSEC_ROLES.CAN_SET_ROLE('SECTOR2_APP_MGR')
    THEN DBMS_OUTPUT.PUT_LINE('SECTOR2_APP_MGR' can be enabled.);
  END IF;
END;
/

```

## 19.2.2 SET\_ROLE Procedure

The `SET_ROLE` procedure issues the `SET ROLE` PL/SQL statement for specified roles.

This procedure includes both Oracle Database Vault secure application roles and regular Oracle Database roles in its checking process.

This procedure sets an Oracle Database Vault secure application role only if the rule set that is associated with the role evaluates to true. Before `SET_ROLE` is issued, the `CAN_SET_ROLE` method is called to check the rule set associated with the role. Run-time rule set behavior such as auditing, failure processing, and event handling occur during this process.

The `SET_ROLE` procedure is available to the general database account population.

### Syntax

```
DBMS_MACSEC_ROLES.SET_ROLE(
  p_role IN VARCHAR2);
```

### Parameters

**Table 19-8 SET\_ROLE Parameter**

Parameter	Description
<code>p_role</code>	<p>Role names. You can enter multiple roles, separated by commas (,), including secure application roles and regular roles.</p> <p>To find existing secure application roles in the current database instance, query the <code>DBA_DV_ROLE</code> view, described in <a href="#">DBA_DV_ROLE View</a> (page 25-28).</p> <p>To find all of the existing roles in the database, query the <code>DBA_ROLES</code> data dictionary view, described in <i>Oracle Database Reference</i>.</p>

### Example

```
EXEC DBMS_MACSEC_ROLES.SET_ROLE('SECTOR2_APP_MGR, APPS_MGR');
```

You can enter the name of the role in any case (for example, `Sector2_APP_MGR`).





---

## Oracle Database Vault Oracle Label Security APIs

You can use the `DBMS_MACADM` PL/SQL package to manage Oracle Label Security labels and policies in Oracle Database Vault.

### [CREATE\\_MAC\\_POLICY Procedure](#) (page 20-1)

The `CREATE_MAC_POLICY` procedure specifies the algorithm to merge labels when computing the label for a factor, or the Oracle Label Security Session label.

### [CREATE\\_POLICY\\_LABEL Procedure](#) (page 20-3)

The `CREATE_POLICY_LABEL` procedure labels an identity within an Oracle Label Security policy.

### [DELETE\\_MAC\\_POLICY\\_CASCADE Procedure](#) (page 20-4)

The `DELETE_MAC_POLICY_CASCADE` procedure deletes all Oracle Database Vault objects related to an Oracle Label Security policy.

### [DELETE\\_POLICY\\_FACTOR Procedure](#) (page 20-5)

The `DELETE_POLICY_FACTOR` procedure removes the factor from contributing to the Oracle Label Security label.

### [DELETE\\_POLICY\\_LABEL Procedure](#) (page 20-5)

The `DELETE_POLICY_LABEL` procedure removes the label from an identity within an Oracle Label Security policy.

### [UPDATE\\_MAC\\_POLICY Procedure](#) (page 20-6)

The `UPDATE_MAC_POLICY` procedure specifies the algorithm to merge labels when computing the label for a factor, or the Oracle Label Security Session label.

#### Related Topics:

### [Integrating Oracle Database Vault with Other Oracle Products](#) (page 12-1)

You can integrate Oracle Database Vault with other Oracle products, such as Oracle Enterprise User Security.

### [Oracle Database Vault Utility APIs](#) (page 21-1)

Oracle Database Vault provides a set of utility APIs in the `DBMS_MACUTL` PL/SQL package.

## 20.1 CREATE\_MAC\_POLICY Procedure

The `CREATE_MAC_POLICY` procedure specifies the algorithm to merge labels when computing the label for a factor, or the Oracle Label Security Session label.

**Syntax**

```
DBMS_MACADM.CREATE_MAC_POLICY(
  policy_name IN VARCHAR2,
  algorithm   IN VARCHAR2);
```

**Parameters****Table 20-1 CREATE\_MAC\_POLICY Parameters**

Parameter	Description
policy_name	Name of an existing policy. To find existing policies in the current database instance, query the DBA_DV_MAC_POLICY view, described in <a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17).
algorithm	Merge algorithm for cases when Oracle Label Security has merged two labels. Enter the code listed in <a href="#">Table 20-2</a> (page 20-2) that corresponds to the merge algorithm you want. For example, enter HUU to if you want to select the Maximum Level/Union/Union merge algorithm.

**Table 20-2 Oracle Label Security Merge Algorithm Codes**

Code	Value
HUU	Maximum Level/Union/Union
HIU	Maximum Level/Intersection/Union
HMU	Maximum Level/Minus/Union
HNU	Maximum Level/Null/Union
HUI	Maximum Level/Union/Intersection
HI I	Maximum Level/Intersection/Intersection
HMI	Maximum Level/Minus/Intersection
HNI	Maximum Level/Null/Intersection
HUM	Maximum Level/Union/Minus
HIM	Maximum Level/Intersection/Minus
HMM	Maximum Level/Minus/Minus
HNM	Maximum Level/Null/Minus
HUN	Maximum Level/Union/Null
HIN	Maximum Level/Intersection/Null
HMN	Maximum Level/Minus/Null
HNN	Maximum Level/Null/Null
LUU	Minimum Level/Union/Union
LIU	Minimum Level/Intersection/Union

**Table 20-2 (Cont.) Oracle Label Security Merge Algorithm Codes**

Code	Value
LMU	Minimum Level/Minus/Union
LNU	Minimum Level/Null/Union
LUI	Minimum Level/Union/Intersection
LI I	Minimum Level/Intersection/Intersection
LMI	Minimum Level/Minus/Intersection
LNI	Minimum Level/Null/Intersection
LUM	Minimum Level/Union/Minus
LIM	Minimum Level/Intersection/Minus
LMM	Minimum Level/Minus/Minus
LN M	Minimum Level/Null/Minus
LUN	Minimum Level/Union/Null
LIN	Minimum Level/Intersection/Null
LMN	Minimum Level/Minus/Null
LNN	Minimum Level/Null/Null

**Example**

```

BEGIN
  DBMS_MACADM.CREATE_MAC_POLICY(
    policy_name => 'Access Locations',
    algorithm   => 'HUU');
END;
/

```

**20.2 CREATE\_POLICY\_LABEL Procedure**

The CREATE\_POLICY\_LABEL procedure labels an identity within an Oracle Label Security policy.

**Syntax**

```

DBMS_MACADM.CREATE_POLICY_LABEL(
  identity_factor_name  IN VARCHAR2,
  identity_factor_value IN VARCHAR2,
  policy_name          IN VARCHAR2,
  label                IN VARCHAR2);

```

## Parameters

**Table 20-3 CREATE\_POLICY\_LABEL Parameters**

Parameter	Description
identity_factor_name	Name of the factor being labeled. To find existing factors in the current database instance, query the DBA_DV_FACTOR view, described in <a href="#">DBA_DV_FACTOR View</a> (page 25-11). To find factors that are associated with Oracle Label Security policies, use DBA_DV_MAC_POLICY_FACTOR, described in <a href="#">DBA_DV_MAC_POLICY_FACTOR View</a> (page 25-17).
identity_factor_value	Value of identity for the factor being labeled. To find the identities of existing factors in the current database instance, query the DBA_DV_IDENTITY view, described in <a href="#">DBA_DV_IDENTITY View</a> (page 25-15).
policy_name	Name of an existing policy. To find existing policies in the current database instance, query the DBA_DV_MAC_POLICY view, described in <a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17).
label	Oracle Label Security label name. To find existing policy labels for factor identifiers, query the DBA_DV_POLICY_LABEL view, described in <a href="#">DBA_DV_POLICY_LABEL View</a> (page 25-20).

## Example

```
BEGIN
  DBMS_MACADM.CREATE_POLICY_LABEL(
    identity_factor_name => 'App_Host_Name',
    identity_factor_value => 'Sect2_Fin_Apps',
    policy_name          => 'Access Locations',
    label                => 'Sensitive');
END;
/
```

## 20.3 DELETE\_MAC\_POLICY\_CASCADE Procedure

The DELETE\_MAC\_POLICY\_CASCADE procedure deletes all Oracle Database Vault objects related to an Oracle Label Security policy.

### Syntax

```
DBMS_MACADM.DELETE_MAC_POLICY_CASCADE(
  policy_name IN VARCHAR2);
```

## Parameters

**Table 20-4** *DELETE\_MAC\_POLICY\_CASCADE Parameter*

Parameter	Description
policy_name	Name of an existing policy. To find existing policies in the current database instance, query the DBA_DV_MAC_POLICY view, described in <a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17).

## Example

```
EXEC DBMS_MACADM.DELETE_MAC_POLICY_CASCADE('Access Locations');
```

## 20.4 DELETE\_POLICY\_FACTOR Procedure

The DELETE\_POLICY\_FACTOR procedure removes the factor from contributing to the Oracle Label Security label.

## Syntax

```
DBMS_MACADM.DELETE_POLICY_FACTOR(
  policy_name IN VARCHAR2,
  factor_name IN VARCHAR2);
```

## Parameters

**Table 20-5** *DELETE\_POLICY\_FACTOR Parameters*

Parameter	Description
policy_name	Name of an existing policy. To find existing policies in the current database instance, query the DBA_DV_MAC_POLICY view, described in <a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17).
factor_name	Name of factor associated with the Oracle Label Security label. To find factors that are associated with Oracle Label Security policies, query DBA_DV_MAC_POLICY_FACTOR, described in <a href="#">DBA_DV_MAC_POLICY_FACTOR View</a> (page 25-17).

## Example

```
BEGIN
  DBMS_MACADM.DELETE_POLICY_FACTOR(
    policy_name => 'Access Locations',
    factor_name => 'App_Host_Name');
END;
/
```

## 20.5 DELETE\_POLICY\_LABEL Procedure

The DELETE\_POLICY\_LABEL procedure removes the label from an identity within an Oracle Label Security policy.

**Syntax**

```
DBMS_MACADM.DELETE_POLICY_LABEL(
  identity_factor_name  IN VARCHAR2,
  identity_factor_value IN VARCHAR2,
  policy_name          IN VARCHAR2,
  label                IN VARCHAR2);
```

**Parameters****Table 20-6 DELETE\_POLICY\_LABEL Parameters**

Parameter	Description
identity_factor_name	Name of the factor that was labeled. To find existing factors in the current database instance that are associated with Oracle Label Security policies, query <a href="#">DBA_DV_MAC_POLICY_FACTOR</a> , described in <a href="#">DBA_DV_MAC_POLICY_FACTOR View</a> (page 25-17).
identity_factor_value	Value of identity for the factor that was labeled. To find the identities of existing factors in the current database instance, query the <a href="#">DBA_DV_IDENTITY</a> view, described in <a href="#">DBA_DV_IDENTITY View</a> (page 25-15).
policy_name	Name of an existing policy. To find existing policies in the current database instance, query the <a href="#">DBA_DV_MAC_POLICY</a> view, described in <a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17).
label	Oracle Label Security label name. To find existing policy labels for factor identifiers, query the <a href="#">DBA_DV_POLICY_LABEL</a> view, described in <a href="#">DBA_DV_POLICY_LABEL View</a> (page 25-20).

**Example**

```
BEGIN
  DBMS_MACADM.DELETE_POLICY_LABEL(
    identity_factor_name => 'App_Host_Name',
    identity_factor_value => 'Sect2_Fin_Apps',
    policy_name          => 'Access Locations',
    label                => 'Sensitive');
END;
/
```

**20.6 UPDATE\_MAC\_POLICY Procedure**

The `UPDATE_MAC_POLICY` procedure specifies the algorithm to merge labels when computing the label for a factor, or the Oracle Label Security Session label.

**Syntax**

```
DBMS_MACADM.UPDATE_MAC_POLICY(
  policy_name  IN VARCHAR2,
  algorithm    IN VARCHAR2);
```

## Parameters

**Table 20-7 UPDATE\_MAC\_POLICY**

Parameter	Description
policy_name	Name of an existing policy. To find existing policies in the current database instance, query the DBA_DV_MAC_POLICY view, described in <a href="#">DBA_DV_MAC_POLICY View</a> (page 25-17).
algorithm	Merge algorithm for cases when Oracle Label Security has merged two labels. See <a href="#">Table 20-2</a> (page 20-2) for listing of the available algorithms.

## Example

```
BEGIN
  DBMS_MACADM.UPDATE_MAC_POLICY(
    policy_name => 'Access Locations',
    algorithm   => 'LUI');
END;
/
```





---

## Oracle Database Vault Utility APIs

Oracle Database Vault provides a set of utility APIs in the DBMS\_MACUTL PL/SQL package.

### [DBMS\\_MACUTL Constants](#) (page 21-1)

You can use a set of constants, available in the DBMS\_MACUTL PL/SQL package.

### [DBMS\\_MACUTL Package Procedures and Functions](#) (page 21-7)

The DBMS\_MACUTL PL/SQL package can perform tasks such as finding a time value or whether a user has the the appropriate privileges.

## 21.1 DBMS\_MACUTL Constants

You can use a set of constants, available in the DBMS\_MACUTL PL/SQL package.

### [DBMS\\_MACUTL Listing of Constants](#) (page 21-1)

The DBMS\_MACUTL PL/SQL package provides constants (fields) to use with Oracle Database Vault PL/SQL packages.

### [Example: Creating a Realm Using DBMS\\_MACUTL Constants](#) (page 21-6)

Constants can be used to answer simple Yes or No settings when you create objects in Oracle Database Vault.

### [Example: Creating a Rule Set Using DBMS\\_MACUTL Constants](#) (page 21-6)

Constants can be used to set options such as the type of auditing used or fail options.

### [Example: Creating a Factor Using DBMS\\_MACUTL Constants](#) (page 21-7)

Constants can be used to set information specific to factors, such as identity or labeling.

### 21.1.1 DBMS\_MACUTL Listing of Constants

The DBMS\_MACUTL PL/SQL package provides constants (fields) to use with Oracle Database Vault PL/SQL packages.

[Table 21-1](#) (page 21-2) summarizes constant (that is, fields) descriptions for the DBMS\_MACUTL package.

Many of these constants have equivalents in the Oracle Database Vault package. For example, the `enabled` parameter, which is available in several procedures, can accept either `Y` (for Yes) or the constant `G_YES`. Choosing one over the other is a matter of personal preference. They both have the same result.

**Table 21-1 DBMS\_MACUTL Listing of Constants**

Constant Name	Data Type	Description
G_ALL_OBJECT	VARCHAR2(1)	Used with the realm API <code>object_name</code> and <code>object_type</code> parameters as a wildcard to indicate all object names or all object types.
G_AUDIT_ALWAYS	NUMBER	Used with the factor API <code>audit_options</code> parameter to enable an audit.
G_AUDIT_OFF	NUMBER	Used with the factor API <code>audit_options</code> parameter to disable auditing.
G_AUDIT_ON_GET_ERROR	NUMBER	Used with the factor API <code>audit_options</code> parameter to audit if the expression specified in the <code>get_expr</code> parameter returns an error.
G_AUDIT_ON_GET_NULL	NUMBER	Used with the factor API <code>audit_options</code> parameter to audit if the expression in the <code>get_expr</code> field is null.
G_AUDIT_ON_TRUST_LEVEL_NEG	NUMBER	Used with the factor API <code>audit_options</code> parameter to audit if the trust level is negative.
G_AUDIT_ON_TRUST_LEVEL_NULL	NUMBER	Used with the factor API <code>audit_options</code> parameter to audit if no trust level exists.
G_AUDIT_ON_VALIDATE_ERROR	NUMBER	Used with the factor API <code>audit_options</code> parameter to audit if the validation function returns an error.
G_AUDIT_ON_VALIDATE_FALSE	NUMBER	Used with the factor API <code>audit_options</code> parameter to audit if validation function is false.
G_DISABLE	NUMBER	Used to disable Oracle Database Vault policies and command rules
G_ENABLE	NUMBER	Used to enable Oracle Database Vault policies and command rules
G_EVAL_ON_ACCESS	NUMBER	Used with the factor API <code>eval_options</code> parameter to reevaluate the factor each time it is accessed.

**Table 21-1 (Cont.) DBMS\_MACUTL Listing of Constants**

Constant Name	Data Type	Description
G_EVAL_ON_SESSION	NUMBER	Used with the factor API <code>eval_options</code> parameter to evaluate the factor only once, when the user logs in to the session.
G_FAIL_SILENTLY	NUMBER	Used with the <code>fail_options</code> parameter to fail and show no error message.
G_FAIL_WITH_MESSAGE	NUMBER	Used with the <code>fail_options</code> parameter to fail and show an error message.
G_IDENTIFY_BY_CONSTANT	NUMBER	Used with the factor API <code>identify_by</code> parameter: Fixed value in PL/SQL expression defined in the <code>get_expr</code> parameter.
G_IDENTIFY_BY_CONTEXT	NUMBER	Used with the factor API <code>identify_by</code> parameter to indicate context.
G_IDENTIFY_BY_FACTOR	NUMBER	Used with the factor API <code>identify_by</code> parameter for subfactors through the <code>factor_link\$</code> table.
G_IDENTIFY_BY_METHOD	NUMBER	Used with the factor API <code>identify_by</code> parameter: Expression in <code>get_expr</code> field
G_IDENTIFY_BY_RULESET	NUMBER	Used with the factor API <code>identify_by</code> parameter: Expression and Rule Set with the <code>factor_expr\$</code> table
G_LABELED_BY_FACTORS	NUMBER	Used with the factor API <code>labeled_by</code> parameter to derive the label from subfactor and merge algorithm.
G_LABELED_BY_SELF	NUMBER	Used with the factor API <code>labeled_by</code> parameter to label the factor identities.
G_MAX_SESSION_LABEL	VARCHAR2(30)	This is the highest label a user could set based on the factors. It does not consider the label for a user.
G_MIN_POLICY_LABEL	VARCHAR2(30)	The label to which a factor with a null label defaults.

**Table 21-1 (Cont.) DBMS\_MACUTL Listing of Constants**

Constant Name	Data Type	Description
G_NO	VARCHAR2(1)	Used with the following APIs: <ul style="list-style-type: none"> <li>The factor API <code>label_indicator</code> parameter to indicate that a child factor linked to a parent factor does not contribute to the label of the parent factor in an Oracle Label Security integration.</li> <li>Any API that uses the <code>enabled</code> parameter.</li> </ul>
G_OLS_SESSION_LABEL	VARCHAR2(30)	The Oracle Label Security session label for a user at the time <code>init_session</code> is run.
G_PARTIAL	NUMBER	Sets the enforcement state of the realms and command rules under an Oracle Database Vault policy to be changed individually
G_REALM_AUDIT_FAIL	NUMBER	Used with the realm API <code>audit_options</code> parameter to audit when the realm is violated.
G_REALM_AUDIT_OFF	NUMBER	Used with the realm API <code>audit_options</code> parameter to disable auditing.
G_REALM_AUDIT_SUCCESS	NUMBER	Used with the realm API <code>audit_options</code> parameter: Audit on successful realm access
G_REALM_AUTH_OWNER	NUMBER	Used with the realm API <code>auth_options</code> parameter to set the realm authorization to Owner.
G_REALM_AUTH_PARTICIPANT	NUMBER	Used with the realm API <code>auth_options</code> parameter to set the realm authorization to Participant.
G_RULESET_AUDIT_FAIL	NUMBER	Used with the rule set API <code>audit_options</code> parameter to audit on rule set failure.
G_RULESET_AUDIT_OFF	NUMBER	Used with the rule set API <code>audit_options</code> parameter to disable auditing.
G_RULESET_AUDIT_SUCCESS	NUMBER	Used with the rule set API <code>audit_options</code> parameter to audit on rule set success.

**Table 21-1 (Cont.) DBMS\_MACUTL Listing of Constants**

Constant Name	Data Type	Description
G_RULESET_EVAL_ALL	NUMBER	Used with the rule set API <code>eval_options</code> parameter to enable the rule set to succeed if all rules evaluate to true.
G_RULESET_EVAL_ANY	NUMBER	Used with the rule set API <code>eval_options</code> parameter to succeed if any of the rules evaluate to true.
G_RULESET_FAIL_SHOW	NUMBER	Used with the rule set API <code>fail_options</code> parameter to show an error message if the rule set fails.
G_RULESET_FAIL_SILENT	NUMBER	Used with the rule set API <code>fail_options</code> parameter to not show an error message if the rule set fails.
G_RULESET_HANDLER_FAIL	NUMBER	Used with the rule set API <code>handler_options</code> parameter to call a handler (specified by the <code>handler</code> parameter) if the rule set fails.
G_RULESET_HANDLER_OFF	NUMBER	Used with the rule set API <code>handler_options</code> parameter to disable calls to a handler or if no handler is used.
G_RULESET_HANDLER_SUCCESS	NUMBER	Used with the rule set API <code>handler_options</code> parameter to call a handler if the rule set succeeds.
G_SIMULATION	NUMBER	Used to set the enforcement state of a policy to simulation mode. This mode does not raise errors for realm or command rule violations. Instead, an error is logged in a designated log table with sufficient information relevant to the error (for example, users or SQL command.)
G_USER_POLICY_LABEL	VARCHAR2(30)	This is what Oracle Label Security has decided the user's label should be set to after factoring in the preceding values.

**Table 21-1 (Cont.) DBMS\_MACUTL Listing of Constants**

Constant Name	Data Type	Description
G_YES	VARCHAR2(1)	Used with the following APIs: <ul style="list-style-type: none"> <li>The factor API label_indicator parameter to indicate that a child factor linked to a parent factor contributes to the label of the parent factor in an Oracle Label Security integration.</li> <li>Any API that uses the enabled parameter.</li> </ul>

### 21.1.2 Example: Creating a Realm Using DBMS\_MACUTL Constants

Constants can be used to answer simple Yes or No settings when you create objects in Oracle Database Vault.

[Example 21-1](#) (page 21-6) shows how to use the G\_YES and G\_REALM\_AUDIT\_FAIL DBMS\_MACUTL constants when creating a realm.

#### **Example 21-1 Creating a Realm Using DBMS\_MACUTL Constants**

```
BEGIN
DBMS_MACADM.CREATE_REALM(
  realm_name    => 'Performance Statistics Realm',
  description   => 'Realm to measure performance',
  enabled       => DBMS_MACUTL.G_YES,
  audit_options => DBMS_MACUTL.G_REALM_AUDIT_FAIL);
END;
/
```

### 21.1.3 Example: Creating a Rule Set Using DBMS\_MACUTL Constants

Constants can be used to set options such as the type of auditing used or fail options.

[Example 21-2](#) (page 21-6) shows how to use several DBMS\_MACUTL constants when creating a rule set.

#### **Example 21-2 Creating a Rule Set Using DBMS\_MACUTL Constants**

```
BEGIN
DBMS_MACADM.CREATE_RULE_SET(
  rule_set_name => 'Limit_DBA_Access',
  description   => 'DBA access through predefined processes',
  enabled       => DBMS_MACUTL.G_YES,
  eval_options  => DBMS_MACUTL.G_RULESET_EVAL_ALL,
  audit_options => DBMS_MACUTL.G_RULESET_AUDIT_FAIL,
  fail_options  => DBMS_MACUTL.G_RULESET_FAIL_SHOW,
  fail_message  => 'Rule Set Limit_DBA_Access has failed.',
  fail_code     => 20000,
  handler_options => DBMS_MACUTL.G_RULESET_HANDLER_FAIL,
  handler       => 'dbavowner.email_alert');
END;
/
```

### 21.1.4 Example: Creating a Factor Using DBMS\_MACUTL Constants

Constants can be used to set information specific to factors, such as identity or labeling.

[Example 21-3](#) (page 21-7) shows how to use constants when creating a factor.

#### **Example 21-3 Creating a Factor Using DBMS\_MACUTL Constants**

```
BEGIN
DBMS_MACADM.CREATE_FACTOR(
  factor_name      => 'Sector2_DB',
  factor_type_name => 'Instance',
  description      => ' ',
  rule_set_name    => 'DB_access',
  get_expr         => 'UPPER(SYS_CONTEXT(''USERENV'', ''DB_NAME''))',
  validate_expr    => 'dbavowner.check_db_access',
  identify_by      => DBMS_MACUTL.G_IDENTIFY_BY_FACTOR,
  labeled_by       => DBMS_MACUTL.G_LABELED_BY_SELF,
  eval_options     => DBMS_MACUTL.G_EVAL_ON_SESSION,
  audit_options    => DBMS_MACUTL.G_AUDIT_ALWAYS,
  fail_options     => DBMS_MACUTL.G_FAIL_SILENTLY);
END;
/
```

## 21.2 DBMS\_MACUTL Package Procedures and Functions

The DBMS\_MACUTL PL/SQL package can perform tasks such as finding a time value or whether a user has the the appropriate privileges.

#### [CHECK\\_DVSYSDML\\_ALLOWED Procedure](#) (page 21-8)

The CHECK\_DVSYSDML\_ALLOWED procedure checks if a user can issue Data Modification Language (DML) commands to access the DVSYSDML objects.

#### [GET\\_CODE\\_VALUE Function](#) (page 21-9)

The GET\_CODE\_VALUE function finds the value for a code within a code group, and then returns a VARCHAR2 value.

#### [GET\\_SECONDS Function](#) (page 21-10)

The GET\_SECONDS function returns the seconds in Oracle SS (seconds) format (00–59), and then returns a NUMBER value.

#### [GET\\_MINUTE Function](#) (page 21-11)

The GET\_MINUTE function returns the minute in Oracle MI (minute) format (00–59), in a NUMBER value.

#### [GET\\_HOUR Function](#) (page 21-11)

The GET\_HOUR function returns the hour in Oracle HH24 (hour) format (00–23), in a NUMBER value.

#### [GET\\_DAY Function](#) (page 21-12)

The GET\_DAY function returns the day in Oracle DD (day) format (01–31), in a NUMBER value.

#### [GET\\_MONTH Function](#) (page 21-13)

The GET\_MONTH function returns the month in Oracle MM (month) format (01–12), in a NUMBER value.

**GET\_YEAR Function** (page 21-13)

The GET\_YEAR function returns the year in Oracle YYYY (year) format (0001–9999), in a NUMBER value.

**IS\_ALPHA Function** (page 21-14)

The IS\_ALPHA function returns a BOOLEAN value indicating if a character is alphabetic.

**IS\_DIGIT Function** (page 21-15)

The IS\_DIGIT function checks returns a BOOLEAN value indicating if a character is numeric.

**IS\_DVSYSD\_OWNER Function** (page 21-15)

The IS\_DVSYSD\_OWNER function returns a BOOLEAN value indicating if a user is authorized to manage the Oracle Database Vault configuration.

**IS\_OLS\_INSTALLED Function** (page 21-16)

The IS\_OLS\_INSTALLED function returns a BOOLEAN value indicating if Oracle Label Security is installed.

**IS\_OLS\_INSTALLED\_VARCHAR Function** (page 21-16)

The IS\_OLS\_INSTALLED\_VARCHAR function returns a BOOLEAN value indicating if Oracle Label Security is installed.

**USER\_HAS\_OBJECT\_PRIVILEGE Function** (page 21-17)

The USER\_HAS\_OBJECT\_PRIVILEGE function returns a BOOLEAN value indicating if user or role can access an object through a single specified object privilege grant.

**USER\_HAS\_ROLE Function** (page 21-18)

The USER\_HAS\_ROLE function returns a BOOLEAN value indicating if a user has a role privilege, directly or indirectly (through another role).

**USER\_HAS\_ROLE\_VARCHAR Function** (page 21-19)

The USER\_HAS\_ROLE\_VARCHAR function returns a VARCHAR2 value indicating if a user has a role privilege, directly or indirectly (through another role).

**USER\_HAS\_SYSTEM\_PRIVILEGE Function** (page 21-20)

The USER\_HAS\_SYSTEM\_PRIVILEGE function returns a BOOLEAN value indicating if a user has a system privilege, directly or indirectly (through a role).

## 21.2.1 CHECK\_DVSYSD\_DML\_ALLOWED Procedure

The CHECK\_DVSYSD\_DML\_ALLOWED procedure checks if a user can issue Data Modification Language (DML) commands to access the DVSYSD objects.

**Syntax**

```
DBMS_MACUTL.CHECK_DVSYSD_DML_ALLOWED(  
    p_user IN VARCHAR2 DEFAULT USER);
```



## Parameter

**Table 21-2** *CHECK\_DVSYSDML\_ALLOWED* Parameter

Parameter	Description
p_user	<p>User to check.</p> <p>To find existing users in the current database instance, query the following views:</p> <ul style="list-style-type: none"> <li>DBA_USERS: Finds available users for the current database instance. See <i>Oracle Database Reference</i>.</li> <li>DBA_DV_REALM_AUTH: Finds the authorization of a particular user or role. See <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</li> <li>DBA_DV_ROLE: Finds existing secure application roles used in privilege management. See <a href="#">DBA_DV_ROLE View</a> (page 25-28).</li> </ul>

## Example

User SYSTEM fails the check:

```
EXEC DBMS_MACUTL.CHECK_DVSYSDML_ALLOWED('system');
```

```
ERROR at line 1:
ORA-47920: Authorization failed for user system to perform this operation
ORA-06512: at "DBMS_MACUTL", line 23
ORA-06512: at "DBMS_MACUTL", line 372
ORA-06512: at "DBMS_MACUTL", line 508
ORA-06512: at "DBMS_MACUTL", line 572
ORA-06512: at line 1
```

User leo\_dvowner, who has the DV\_OWNER role, passes the check:

```
EXEC DBMS_MACUTL.CHECK_DVSYSDML_ALLOWED('leo_dvowner');
```

```
PL/SQL procedure successfully completed.
```

## 21.2.2 GET\_CODE\_VALUE Function

The GET\_CODE\_VALUE function finds the value for a code within a code group, and then returns a VARCHAR2 value.

### Syntax

```
DBMS_MACUTL.GET_CODE_VALUE(
  p_code_group IN VARCHAR2,
  p_code       IN VARCHAR2)
RETURN VARCHAR2;
```

### Parameters

**Table 21-3** *GET\_CODE\_VALUE* Parameters

Parameter	Description
p_code_group	<p>Code group (for example, AUDIT_EVENTS or BOOLEAN).</p> <p>To find available code groups in the current database instance, query the DBA_DV_CODE view, described in <a href="#">DBA_DV_CODE View</a> (page 25-6).</p>

**Table 21-3 (Cont.) GET\_CODE\_VALUE Parameters**

Parameter	Description
p_code	ID of the code. This ID is listed when you run the DBA_DV_CODE view.

**Example**

```
BEGIN
  DBMS_MACADM.CREATE_RULE(
    rule_name => 'Get Label Algorithm for Maximum Level/Union/Null',
    rule_expr => 'DBMS_MACUTL.GET_CODE_VALUE(''LABEL_ALG'', ''HUN'') = ''Union''');
END;
/
```

**21.2.3 GET\_SECOND Function**

The GET\_SECOND function returns the seconds in Oracle SS (seconds) format (00–59), and then returns a NUMBER value.

It is useful for rule expressions based on time data.

**Syntax**

```
DBMS_MACUTL.GET_SECOND(
  p_date IN DATE DEFAULT SYSDATE)
RETURN NUMBER;
```

**Parameter****Table 21-4 GET\_SECOND Parameter**

Parameter	Description
p_date	Date in SS format (for example, 59). If you do not specify a date, then Oracle Database Vault uses the Oracle Database SYSDATE function to retrieve the current date and time set for the operating system on which the database resides.

**Example**

```
SET SERVEROUTPUT ON
DECLARE
  seconds number;
BEGIN
  seconds := DBMS_MACUTL.GET_SECOND(TO_DATE('03-APR-2009 6:56 PM',
    'dd-mon-yyyy hh:mi PM'));
  DBMS_OUTPUT.PUT_LINE('Seconds: ' || seconds);
END;
/
```

This example, which uses a fixed date and time, returns the following:

```
Seconds: 56
```

## 21.2.4 GET\_MINUTE Function

The `GET_MINUTE` function returns the minute in Oracle MI (minute) format (00–59), in a `NUMBER` value.

It is useful for rule expressions based on time data.

### Syntax

```
DBMS_MACUTL.GET_MINUTE(
  p_date IN DATE DEFAULT SYSDATE)
RETURN NUMBER;
```

### Parameter

**Table 21-5** *GET\_MINUTE Parameter*

Parameter	Description
<code>p_date</code>	Date in MI format (for example, 30, as in 2:30). If you do not specify a date, then Oracle Database Vault uses the Oracle Database <code>SYSDATE</code> function to retrieve the current date and time set for the operating system on which the database resides.

### Example

```
SET SERVEROUTPUT ON
DECLARE
  minute number;
BEGIN
  minute := DBMS_MACUTL.GET_MINUTE(SYSDATE);
  DBMS_OUTPUT.PUT_LINE('Minute: '||minute);
END;
/
```

Output similar to the following appears:

```
Minute: 17
```

## 21.2.5 GET\_HOUR Function

The `GET_HOUR` function returns the hour in Oracle HH24 (hour) format (00–23), in a `NUMBER` value.

It is useful for rule expressions based on time data.

### Syntax

```
DBMS_MACUTL.GET_HOUR(
  p_date IN DATE DEFAULT SYSDATE)
RETURN NUMBER;
```

**Parameter****Table 21-6** *GET\_HOUR Parameter*

Parameter	Description
p_date	Date in HH24 format (for example, 14 for 2:00 p.m.) If you do not specify a date, then Oracle Database Vault uses the Oracle Database SYSDATE function to retrieve the current date and time set for the operating system on which the database resides.

**Example**

```
SET SERVEROUTPUT ON
DECLARE
  hours number;
BEGIN
  hours := DBMS_MACUTL.GET_HOUR(SYSDATE);
  DBMS_OUTPUT.PUT_LINE('Hour: ' || hours);
END;
/
```

Output similar to the following appears:

```
Hour: 12
```

**21.2.6 GET\_DAY Function**

The GET\_DAY function returns the day in Oracle DD (day) format (01–31), in a NUMBER value.

It is useful for rule expressions based on time data.

**Syntax**

```
DBMS_MACUTL.GET_DAY(
  p_date IN DATE DEFAULT SYSDATE)
RETURN NUMBER;
```

**Parameter****Table 21-7** *GET\_DAY Parameter*

Parameter	Description
p_date	Date in DD format (for example, 01 for the first day of the month). If you do not specify a date, then Oracle Database Vault uses the Oracle Database SYSDATE function to retrieve the current date and time set for the operating system on which the database resides.

**Example**

```
SET SERVEROUTPUT ON
DECLARE
  day number;
BEGIN
  day := DBMS_MACUTL.GET_DAY(SYSDATE);
  DBMS_OUTPUT.PUT_LINE('Day: ' || day);
```

```
END;
/
```

Output similar to the following appears:

```
Day: 3
```

## 21.2.7 GET\_MONTH Function

The GET\_MONTH function returns the month in Oracle MM (month) format (01–12), in a NUMBER value.

It is useful for rule expressions based on time data.

### Syntax

```
DBMS_MACUTL.GET_MONTH(
  p_date IN DATE DEFAULT SYSDATE)
RETURN NUMBER;
```

### Parameter

**Table 21-8 GET\_MONTH Parameter**

Parameter	Description
p_date	Date in MM format (for example, 08 for the month of August). If you do not specify a date, then Oracle Database Vault uses the Oracle Database SYSDATE function to retrieve the current date and time set for the operating system on which the database resides.

### Example

```
SET SERVEROUTPUT ON
DECLARE
  month number;
BEGIN
  month := DBMS_MACUTL.GET_MONTH(SYSDATE);
  DBMS_OUTPUT.PUT_LINE('Month: ' || month);
END;
/
```

Output similar to the following appears:

```
Month: 4
```

## 21.2.8 GET\_YEAR Function

The GET\_YEAR function returns the year in Oracle YYYY (year) format (0001–9999), in a NUMBER value.

It is useful for rule expressions based on time data.

### Syntax

```
DBMS_MACUTL.GET_YEAR(
  p_date IN DATE DEFAULT SYSDATE)
RETURN NUMBER;
```

**Parameter****Table 21-9** *GET\_YEAR Parameter*

Parameter	Description
p_date	Date in YYYY format (for example, 1984). If you do not specify a date, then Oracle Database Vault uses the SYSDATE function to retrieve the current date and time set for the operating system on which the database resides.

**Example**

```

SET SERVEROUTPUT ON
DECLARE
  year number;
BEGIN
  year := DBMS_MACUTL.GET_YEAR(SYSDATE);
  DBMS_OUTPUT.PUT_LINE('Year: '||year);
END;
/

```

**21.2.9 IS\_ALPHA Function**

The IS\_ALPHA function returns a BOOLEAN value indicating if a character is alphabetic.

IS\_ALPHA returns TRUE if the character is alphabetic.

**Syntax**

```

DBMS_MACUTL.IS_ALPHA(
  c IN VARCHAR2)
RETURN BOOLEAN;

```

**Parameter****Table 21-10** *IS\_ALPHA Parameter*

Parameter	Description
c	String with one character

**Example**

```

SET SERVEROUTPUT ON
BEGIN
  IF DBMS_MACUTL.IS_ALPHA('z')
  THEN DBMS_OUTPUT.PUT_LINE('The alphabetic character was found');
  ELSE
  DBMS_OUTPUT.PUT_LINE('No alphabetic characters today.');
```

```

END IF;
END;
/

```

## 21.2.10 IS\_DIGIT Function

The IS\_DIGIT function checks returns a BOOLEAN value indicating if a character is numeric.

IS\_DIGIT returns TRUE if the character is a digit.

### Syntax

```
DBMS_MACUTL.IS_DIGIT(
  c IN VARCHAR2)
RETURN BOOLEAN;
```

### Parameter

**Table 21-11 IS\_DIGIT Parameter**

Parameter	Description
c	String with one character

### Example

```
SET SERVEROUTPUT ON
BEGIN
  IF DBMS_MACUTL.IS_DIGIT('7')
    THEN DBMS_OUTPUT.PUT_LINE('The numeric character was found');
  ELSE
    DBMS_OUTPUT.PUT_LINE('No numeric characters today.');
```

```
END IF;
END;
```

## 21.2.11 IS\_DVSYST\_OWNER Function

The IS\_DVSYST\_OWNER function returns a BOOLEAN value indicating if a user is authorized to manage the Oracle Database Vault configuration.

IS\_DVSYST\_OWNER returns TRUE if the user is authorized.

### Syntax

```
DBMS_MACUTL.IS_DVSYST_OWNER(
  p_user IN VARCHAR2 DEFAULT USER)
RETURN BOOLEAN;
```

**Parameter****Table 21-12 IS\_DVSYN\_OWNER Parameter**

Parameter	Description
p_user	User to check. To find existing users, query the following views: <ul style="list-style-type: none"> <li>DBA_USERS: Finds available users for the current database instance. See <i>Oracle Database Reference</i>.</li> <li>DBA_DV_REALM_AUTH: Finds the authorization of a particular user or role. See <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</li> <li>DBA_DV_ROLE: Finds existing secure application roles used in privilege management. See <a href="#">DBA_DV_ROLE View</a> (page 25-28).</li> </ul>

**Example**

```

SET SERVEROUTPUT ON
BEGIN
  IF DBMS_MACUTL.IS_DVSYN_OWNER('PSMITH')
    THEN DBMS_OUTPUT.PUT_LINE('PSMITH is authorized to manage Database Vault.');
```

**21.2.12 IS\_OLS\_INSTALLED Function**

The `IS_OLS_INSTALLED` function returns a `BOOLEAN` value indicating if Oracle Label Security is installed.

If Oracle Label Security is installed, `IS_OLS_INSTALLED` returns `TRUE`.

**Syntax**

```

DBMS_MACUTL.IS_OLS_INSTALLED()
RETURN BOOLEAN;
```

**Parameters**

None

**Example**

```

SET SERVEROUTPUT ON
BEGIN
  IF DBMS_MACUTL.IS_OLS_INSTALLED()
    THEN DBMS_OUTPUT.PUT_LINE('OLS is installed');
```

**21.2.13 IS\_OLS\_INSTALLED\_VARCHAR Function**

The `IS_OLS_INSTALLED_VARCHAR` function returns a `BOOLEAN` value indicating if Oracle Label Security is installed.



If Oracle Label Security is installed, then `IS_OLS_INSTALLED_VARCHAR` returns Y.

### Syntax

```
DBMS_MACUTL.IS_OLS_INSTALLED_VARCHAR( )
RETURN VARCHAR2;
```

### Parameters

None

### Example

See [IS\\_OLS\\_INSTALLED Function](#) (page 21-16) for an example.

## 21.2.14 USER\_HAS\_OBJECT\_PRIVILEGE Function

The `USER_HAS_OBJECT_PRIVILEGE` function returns a `BOOLEAN` value indicating if user or role can access an object through a single specified object privilege grant.

If the user or role has the object privilege, then `USER_HAS_OBJECT_PRIVILEGE` returns `TRUE`.

### Syntax

```
DBMS_MACUTL.USER_HAS_OBJECT_PRIVILEGE(
  p_user          VARCHAR2,
  p_object_owner  VARCHAR2,
  p_object_name   VARCHAR2,
  p_privilege     VARCHAR2)
RETURNS BOOLEAN;
```

### Parameters

**Table 21-13** *USER\_HAS\_OBJECT\_PRIVILEGE Parameters*

Parameter	Description
<code>p_user</code>	User or role to check. To find existing users, query the following views: <ul style="list-style-type: none"> <li><code>DBA_USERS</code>: Finds available users for the current database instance. See <i>Oracle Database Reference</i>.</li> <li><code>DBA_ROLES</code>: Finds available roles in the current database instance. See <i>Oracle Database Reference</i>.</li> <li><code>DVA_DV_REALM_AUTH</code>: Finds the authorization of a particular user or role. See <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</li> <li><code>DBA_DV_ROLE</code>: Finds existing secure application roles used in privilege management. See <a href="#">DBA_DV_ROLE View</a> (page 25-28).</li> </ul>
<code>p_object_owner</code>	Object owner, such as a schema. To find the available users, query the <code>DBA_USERS</code> view, described in <i>Oracle Database Reference</i> . To find the authorization of a particular user, query the <code>DVA_DV_REALM_AUTH</code> view.

**Table 21-13 (Cont.) USER\_HAS\_OBJECT\_PRIVILEGE Parameters**

Parameter	Description
p_object_name	Object name, such as a table within the schema specified in the p_object_owner parameter. To find the available objects, query the ALL_OBJECTS view, described in <i>Oracle Database Reference</i> . To find objects that are secured by existing realms, query the DBA_DV_REALM_OBJECT view.
p_privilege	Object privilege, such as, UPDATE. To find privileges for a database account excluding PUBLIC privileges, query the DBA_DV_USER_PRIVS view. To find all privileges for a database account, query the DBA_DV_USER_PRIVS_ALL view.

**Example**

```

SET SERVEROUTPUT ON
BEGIN
  IF DBMS_MACUTL.USER_HAS_OBJECT_PRIVILEGE(
    'SECTOR2_APP_MGR', 'OE', 'ORDERS', 'UPDATE')
  THEN DBMS_OUTPUT.PUT_LINE('SECTOR2_APP_MGR has the UPDATE privilege for the
OE.ORDERS table');
  ELSE
    DBMS_OUTPUT.PUT_LINE('SECTOR2_APP_MGR does not have the UPDATE privilege for the
OE.ORDERS table.');
```

**21.2.15 USER\_HAS\_ROLE Function**

The USER\_HAS\_ROLE function returns a BOOLEAN value indicating if a user has a role privilege, directly or indirectly (through another role).

If the user has a role privilege, then USER\_HAS\_ROLE returns TRUE.

**Syntax**

```

DBMS_MACUTL.USER_HAS_ROLE(
  p_role IN VARCHAR2,
  p_user IN VARCHAR2 DEFAULT USER)
RETURN BOOLEAN;
```

## Parameters

**Table 21-14** *USER\_HAS\_ROLE Parameters*

Parameter	Description
p_role	<p>Role privilege to check.</p> <p>To find existing roles, query the following views:</p> <ul style="list-style-type: none"> <li>DBA_ROLES: Finds available roles in the current database instance. See <i>Oracle Database Reference</i>.</li> <li>DBA_DV_REALM_AUTH: Finds the authorization of a particular user or role. See <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</li> <li>DBA_DV_ROLE: Finds existing secure application roles used in privilege management. See <a href="#">DBA_DV_ROLE View</a> (page 25-28).</li> </ul>
p_user	<p>User to check.</p> <p>To find existing users, query the following views:</p> <ul style="list-style-type: none"> <li>DBA_USERS: Finds available users for the current database instance. See <i>Oracle Database Reference</i>.</li> <li>DBA_DV_REALM_AUTH: Finds the authorization of a particular user or role. See <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</li> </ul>

## Example

```

SET SERVEROUTPUT ON
BEGIN
  IF DBMS_MACUTL.USER_HAS_ROLE('SECTOR2_APP_MGR', 'PSMITH')
    THEN DBMS_OUTPUT.PUT_LINE('User PSMITH has the SECTOR2_APP_MGR role');
    ELSE
    DBMS_OUTPUT.PUT_LINE('User PSMITH does not have the SECTOR2_APP_MGR role.');
```

## 21.2.16 USER\_HAS\_ROLE\_VARCHAR Function

The `USER_HAS_ROLE_VARCHAR` function returns a `VARCHAR2` value indicating if a user has a role privilege, directly or indirectly (through another role).

If the user has the role privilege specified, then `USER_HAS_ROLE_VARCHAR` returns Y.

### Syntax

```

DBMS_MACUTL.USER_HAS_ROLE_VARCHAR(
  p_role IN VARCHAR2,
  p_user IN VARCHAR2 DEFAULT USER)
RETURN VARCHAR2;
```

## Parameters

**Table 21-15 USER\_HAS\_ROLE\_VARCHAR Parameters**

Parameter	Description
p_role	<p>Role to check.</p> <p>To find existing roles, query the following views:</p> <ul style="list-style-type: none"> <li>DBA_ROLES: Finds available roles in the current database instance. See <i>Oracle Database Reference</i>.</li> <li>DBA_DV_REALM_AUTH: Finds the authorization of a particular user or role. See <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</li> <li>DBA_DV_ROLE: Finds existing secure application roles used in privilege management. See <a href="#">DBA_DV_ROLE View</a> (page 25-28).</li> </ul>
p_user	<p>User to check.</p> <p>To find existing users, query the following views:</p> <ul style="list-style-type: none"> <li>DBA_USERS: Finds available users for the current database instance. See <i>Oracle Database Reference</i>.</li> <li>DBA_DV_REALM_AUTH: Finds the authorization of a particular user or role. See <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</li> </ul>

## 21.2.17 USER\_HAS\_SYSTEM\_PRIVILEGE Function

The `USER_HAS_SYSTEM_PRIVILEGE` function returns a `BOOLEAN` value indicating if a user has a system privilege, directly or indirectly (through a role).

If the user has the system privilege specified, then `USER_HAS_SYSTEM_PRIVILEGE` returns `TRUE`.

### Syntax

```
DBMS_MACUTL.USER_HAS_SYSTEM_PRIVILEGE(
  p_privilege IN VARCHAR2,
  p_user      IN VARCHAR2 DEFAULT USER)
RETURN BOOLEAN;
```

### Parameters

**Table 21-16 USER\_HAS\_SYSTEM\_PRIVILEGE Parameters**

Parameter	Description
p_privilege	<p>System privilege to check for.</p> <p>To find privileges for a database account excluding <code>PUBLIC</code> privileges, query the <code>DBA_DV_USER_PRIVS</code> view, described in <a href="#">DBA_DV_USER_PRIVS View</a> (page 25-36).</p> <p>To find all privileges for a database account, use <code>DBA_DV_USER_PRIVS_ALL</code>, described in <a href="#">DBA_DV_USER_PRIVS_ALL View</a> (page 25-37).</p>
p_user	<p>User to check.</p> <p>To find existing users, query the following views:</p> <ul style="list-style-type: none"> <li>DBA_USERS: Finds available users for the current database instance. See <i>Oracle Database Reference</i>.</li> <li>DBA_DV_REALM_AUTH: Finds the authorization of a particular user or role. See <a href="#">DBA_DV_REALM_AUTH View</a> (page 25-25).</li> </ul>

**Example**

```
SET SERVEROUTPUT ON
BEGIN
  IF DBMS_MACUTL.USER_HAS_SYSTEM_PRIVILEGE('EXECUTE', 'PSMITH')
    THEN DBMS_OUTPUT.PUT_LINE('User PSMITH has the EXECUTE ANY PRIVILEGE privilege.');
```

ELSE

```
  DBMS_OUTPUT.PUT_LINE('User PSMITH does not have the EXECUTE ANY PRIVILEGE
privilege.');
```

END IF;

```
END;
/
```



---

## Oracle Database Vault General Administrative APIs

The `DBMS_MACADM` PL/SQL package and the `CONFIGURE_DV` standalone procedure enable you to you perform general maintenance tasks.

### [DBMS\\_MACADM General System Maintenance Procedures](#) (page 22-1)

The `DBMS_MACADM` PL/SQL package general system maintenance procedures perform tasks such as authorizing users or adding new language to Oracle Database Vault.

### [CONFIGURE\\_DV General System Maintenance Procedure](#) (page 22-18)

The `CONFIGURE_DV` procedure configures the initial two Oracle Database user accounts, which are granted the `DV_OWNER` and `DV_ACCTMGR` roles, respectively.

## 22.1 DBMS\_MACADM General System Maintenance Procedures

The `DBMS_MACADM` PL/SQL package general system maintenance procedures perform tasks such as authorizing users or adding new language to Oracle Database Vault.

### [ADD-NLS\\_DATA Procedure](#) (page 22-3)

The `ADD-NLS_DATA` procedure adds a new language to Oracle Database Vault.

### [AUTHORIZE\\_DATAPUMP\\_USER Procedure](#) (page 22-3)

The `AUTHORIZE_DATAPUMP_USER` procedure authorizes a user to perform Oracle Data Pump operations when Oracle Database Vault is enabled.

### [AUTHORIZE\\_DDL Procedure](#) (page 22-4)

The `AUTHORIZE_DDL` procedure grants a user authorization to execute Data Definition Language (DDL) statements on the specified schema.

### [AUTHORIZE\\_MAINTENANCE\\_USER Procedure](#) (page 22-5)

The `AUTHORIZE_MAINTENANCE_USER` procedure grants a user authorization to perform Information Lifecycle Management (ILM) operations in an Oracle Database Vault environment.

### [AUTHORIZE\\_PROXY\\_USER Procedure](#) (page 22-6)

The `AUTHORIZE_PROXY_USER` procedure grants a proxy user authorization to proxy other user accounts, as long as the proxy user has database authorization.

### [AUTHORIZE\\_SCHEDULER\\_USER Procedure](#) (page 22-7)

The `AUTHORIZE_SCHEDULER_USER` procedure grants a user authorization to schedule database jobs when Oracle Database Vault is enabled.

**[AUTHORIZE\\_TTS\\_USER Procedure](#)** (page 22-7)

The `AUTHORIZE_TTS_USER` procedure authorizes a user to perform Oracle Data Pump transportable tablespace operations for a tablespace when Oracle Database Vault is enabled.

**[UNAUTHORIZE\\_DATAPUMP\\_USER Procedure](#)** (page 22-8)

The `UNAUTHORIZE_DATAPUMP_USER` procedure revokes the authorization that was granted by the `AUTHORIZE_DATAPUMP_USER` procedure.

**[UNAUTHORIZE\\_DDL Procedure](#)** (page 22-9)

The `UNAUTHORIZE_DDL` procedure revokes authorization from a user who was granted authorization to execute DDL statements through the `DBMS_MACADM.AUTHORIZE_DDL` procedure.

**[UNAUTHORIZE\\_MAINTENANCE\\_USER Procedure](#)** (page 22-10)

The `UNAUTHORIZE_MAINTENANCE_USER` procedure revokes privileges from users who have been granted authorization to perform Information Lifecycle Management (ILM) operations in an Oracle Database Vault environment.

**[UNAUTHORIZE\\_PROXY\\_USER Procedure](#)** (page 22-11)

The `UNAUTHORIZE_PROXY_USER` procedure revokes authorization from a user who was granted proxy authorization from the `DBMS_MACADM.AUTHORIZE_PROXY_USER` procedure.

**[UNAUTHORIZE\\_SCHEDULER\\_USER Procedure](#)** (page 22-12)

The `UNAUTHORIZE_SCHEDULER_USER` procedure revokes the authorization that was granted by the `AUTHORIZE_SCHEDULER_USER` procedure.

**[UNAUTHORIZE\\_TTS\\_USER Procedure](#)** (page 22-13)

The `UNAUTHORIZE_TTS_USER` procedure removes from authorization users who had previously been granted the authorization to perform Oracle Data Pump transportable tablespace operations.

**[DISABLE\\_DV Procedure](#)** (page 22-13)

The `DISABLE_DV` procedure disables Oracle Database Vault.

**[DISABLE\\_DV\\_DICTIONARY\\_ACCTS Procedure](#)** (page 22-14)

The `DISABLE_DV_DICTIONARY_ACCTS` procedure prevents any user from logging into the database as the `DVSYS` or `DVF` schema user.

**[DISABLE\\_DV\\_PATCH\\_ADMIN\\_AUDIT Procedure](#)** (page 22-14)

The `DISABLE_DV_PATCH_ADMIN_AUDIT` procedure disables realm, command rule, and rule set auditing of the actions by users who have the `DV_PATCH_ADMIN` role.

**[DISABLE\\_ORADEBUG Procedure](#)** (page 22-15)

The `DISABLE_ORADEBUG` procedure disables the use of the `ORADEBUG` utility in an Oracle Database Vault environment.

**[ENABLE\\_DV Procedure](#)** (page 22-15)

The `ENABLE_DV` procedure enables Oracle Database Vault and Oracle Label Security.



**[ENABLE\\_DV\\_PATCH\\_ADMIN\\_AUDIT Procedure](#)** (page 22-16)

The `ENABLE_DV_PATCH_ADMIN_AUDIT` procedure enables realm, command rule, and rule set auditing of the actions by users who have the `DV_PATCH_ADMIN` role.

**[ENABLE\\_DV\\_DICTIONARY\\_ACCTS Procedure](#)** (page 22-17)

The `ENABLE_DV_DICTIONARY_ACCTS` procedure enables users to log into the database as the `DVSYS` or `DVF` user.

**[ENABLE\\_ORADEBUG Procedure](#)** (page 22-17)

The `ENABLE_ORADEBUG` procedure enables the use of the `ORADEBUG` utility in an Oracle Database Vault environment.

**22.1.1 ADD-NLS\_DATA Procedure**

The `ADD-NLS_DATA` procedure adds a new language to Oracle Database Vault.

**Syntax**

```
DBMS_MACADM.ADD-NLS_DATA(
    language      IN VARCHAR );
```

**Parameters****Table 22-1 ADD-NLS\_DATA**

Parameter	Description
language	Enter one of the following settings. (This parameter is case insensitive.) <ul style="list-style-type: none"> <li>• ENGLISH</li> <li>• GERMAN</li> <li>• SPANISH</li> <li>• FRENCH</li> <li>• ITALIAN</li> <li>• JAPANESE</li> <li>• KOREAN</li> <li>• BRAZILIAN PORTUGUESE</li> <li>• SIMPLIFIED CHINESE</li> <li>• TRADITIONAL CHINESE</li> </ul>

**Examples**

```
EXEC DBMS_MACADM.ADD-NLS_DATA('french');
```

**22.1.2 AUTHORIZE\_DATAPUMP\_USER Procedure**

The `AUTHORIZE_DATAPUMP_USER` procedure authorizes a user to perform Oracle Data Pump operations when Oracle Database Vault is enabled.

It applies to both the `expdp` and `impdp` utilities.

See [Authorizing Users for Oracle Data Pump Regular Operations in Database Vault](#) (page 13-7) for full usage information, including the levels of additional authorization the user must have to use Oracle Data Pump in an Oracle Database Vault environment.

**Syntax**

```
DBMS_MACADM.AUTHORIZE_DATAPUMP_USER(
  user_name      IN VARCHAR2,
  schema_name    IN VARCHAR2 DEFAULT NULL,
  table_name     IN VARCHAR2 DEFAULT NULL);
```

**Parameters****Table 22-2 AUTHORIZE\_DATAPUMP\_USER**

Parameter	Description
user_name	Name of the Oracle Data Pump user to whom you want to grant authorization.  To find a list of users who have privileges to use Oracle Data Pump (that is, the EXP_FULL_DATABASE and IMP_FULL_DATABASE roles), query the DBA_ROLE_PRIVS data dictionary view as follows:  SELECT GRANTEE, GRANTED_ROLE FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE LIKE '%FULL%'
schema_name	Name of the database schema that the Oracle Data Pump user must export or import. If you omit this parameter, then the user is granted global authorization to export and import any schema in the database. In this case, ensure the user has been granted the DV_OWNER role.
table_name	Name of the table within the schema specified by the schema_name parameter. If you omit this parameter, then the user you specified can export and import all tables within the schema specified by the schema_name parameter.

**Examples**

```
EXEC DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DP_MGR');

EXEC DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DP_MGR', 'HR');

EXEC DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DP_MGR', 'HR', 'EMPLOYEES');
```

**22.1.3 AUTHORIZE\_DDL Procedure**

The AUTHORIZE\_DDL procedure grants a user authorization to execute Data Definition Language (DDL) statements on the specified schema.

To find information about users who have been granted this authorization, query the DBA\_DV\_DDL\_AUTH data dictionary view.

**Syntax**

```
DBMS_MACADM.AUTHORIZE_DDL(
  user_name      IN VARCHAR2,
  schema_name    IN VARCHAR2);
```

## Parameters

**Table 22-3 AUTHORIZE\_DDL**

Parameter	Description
user_name	Name of the user to whom you want to grant DDL authorization.
schema_name	Name of the database schema in which the user wants to perform the DDL statements. Enter % to specify all schemas.

## Examples

The following example enables user `psmith` to execute DDL statements in any schema:

```
EXEC DBMS_MACADM.AUTHORIZE_DDL('psmith', '%');
```

This example enables user `psmith` to execute DDL statements in the HR schema only.

```
EXEC DBMS_MACADM.AUTHORIZE_DDL('psmith', 'HR');
```

## 22.1.4 AUTHORIZE\_MAINTENANCE\_USER Procedure

The `AUTHORIZE_MAINTENANCE_USER` procedure grants a user authorization to perform Information Lifecycle Management (ILM) operations in an Oracle Database Vault environment.

To find information about users who have been granted this authorization, query the `DBA_DV_MAINTENANCE_AUTH` view.

## Syntax

```
DBMS_MACADM.AUTHORIZE_MAINTENANCE_USER(
  uname      IN VARCHAR2,
  sname      IN VARCHAR2 DEFAULT NULL,
  objname    IN VARCHAR2 DEFAULT NULL,
  objtype    IN VARCHAR2 DEFAULT NULL,
  action     IN VARCHAR2 DEFAULT NULL);
```

## Parameters

**Table 22-4 AUTHORIZE\_MAINTENANCE\_USER**

Parameter	Description
uname	Name of the user to whom you want to grant authorization
sname	Name of the database schema for which the maintenance operations are to be performed. Enter % to specify all schemas.
objname	Name of the object (such as the name of a table) in the schema that is specified in the <code>sname</code> parameter for which maintenance operations are to be performed
objtype	Type of the <code>objname</code> object, such as <code>table</code> , <code>index</code> , <code>tablespace</code> , and so on
action	Maintenance action. Enter <code>ilm</code> for Information Lifecycle Management

**Example**

The following example enables user `psmith` to have Database Vault authorization to manage ILM features for the `HR.EMPLOYEES` table:

```
BEGIN
  DBMS_MACADM.AUTHORIZE_MAINTENANCE_USER (
    uname      => 'psmith',
    sname      => 'HR',
    objname    => 'EMPLOYEES',
    objtype    => 'TABLE',
    action     => 'ILM');
END;
/
```

**Related Topics:**

[Using Information Lifecycle Management with Oracle Database Vault](#)  
(page 13-16)

Users who perform Information Lifecycle Management operations on an Oracle Database Vault-enabled database must be granted authorization to perform these operations.

**22.1.5 AUTHORIZE\_PROXY\_USER Procedure**

The `AUTHORIZE_PROXY_USER` procedure grants a proxy user authorization to proxy other user accounts, as long as the proxy user has database authorization.

For example, the `CREATE SESSION` privilege is a valid database authorization.

To find information about users who have been granted this authorization, query the `DBA_DV_PROXY_AUTH` view.

**Syntax**

```
DBMS_MACADM.AUTHORIZE_PROXY_USER(
  proxy_user  IN VARCHAR2,
  user_name   IN VARCHAR2);
```

**Parameters****Table 22-5 AUTHORIZE\_PROXY\_USER**

Parameter	Description
<code>proxy_user</code>	Name of the proxy user.
<code>user_name</code>	Name of the database user who will be proxied by the <code>proxy_user</code> user. Enter % to specify all users.

**Examples**

The following example enables proxy user `preston` to proxy all users:

```
EXEC DBMS_MACADM.AUTHORIZE_PROXY_USER('preston', '%');
```

This example enables proxy user `preston` to proxy database user `dkent` only.

```
EXEC DBMS_MACADM.AUTHORIZE_PROXY_USER('preston', 'dkent');
```

## 22.1.6 AUTHORIZE\_SCHEDULER\_USER Procedure

The `AUTHORIZE_SCHEDULER_USER` procedure grants a user authorization to schedule database jobs when Oracle Database Vault is enabled.

This authorization applies to anyone who has privileges to schedule database jobs. These privileges include any of the following: `CREATE JOB`, `CREATE ANY JOB`, `CREATE EXTERNAL JOB`, `EXECUTE ANY PROGRAM`, `EXECUTE ANY CLASS`, `MANAGE SCHEDULER`. See [Using Oracle Scheduler with Oracle Database Vault](#) (page 13-14) full usage information, including the levels of authorization the user must have to schedule database jobs in an Oracle Database Vault environment.

### Syntax

```
DBMS_MACADM.AUTHORIZE_SCHEDULER_USER(
  user_name      IN VARCHAR2,
  schema_name    IN VARCHAR2 DEFAULT NULL);
```

### Parameters

**Table 22-6** *AUTHORIZE\_SCHEDULER\_USER*

Parameter	Description
<code>user_name</code>	Name of the user to whom you want to grant authorization. To find a list of users who have privileges to schedule jobs, query the <code>DBA_SYS_PRIVS</code> data dictionary view. See Step 2 (page 13-15) in <a href="#">Granting a Job Scheduling Administrator Authorization for Database Vault</a> (page 13-15).
<code>schema_name</code>	Name of the database schema for which a job will be scheduled. If you omit this parameter, then the user is granted global authorization to schedule a job for any schema in the database.

### Examples

The following example authorizes the user `JOB_MGR` to run a job under any schema.

```
EXEC DBMS_MACADM.AUTHORIZE_SCHEDULER_USER('JOB_MGR');
```

This example authorizes user `JOB_MGR` to run a job under the `HR` schema only.

```
EXEC DBMS_MACADM.AUTHORIZE_SCHEDULER_USER('JOB_MGR', 'HR');
```

## 22.1.7 AUTHORIZE\_TTS\_USER Procedure

The `AUTHORIZE_TTS_USER` procedure authorizes a user to perform Oracle Data Pump transportable tablespace operations for a tablespace when Oracle Database Vault is enabled.

It applies to both the `EXPDP` and `IMPDP` utilities.

[Authorizing Users for Oracle Data Pump Regular Operations in Database Vault](#) (page 13-7) describes full usage information, including the levels of additional authorization the user must have to use Oracle Data Pump to conduct transportable operations in an Oracle Database Vault environment.

**Syntax**

```
DBMS_MACADM.AUTHORIZE_TTS_USER(
  uname      IN VARCHAR2,
  tname      IN VARCHAR2);
```

**Parameters****Table 22-7 AUTHORIZE\_TTS\_USER**

Parameter	Description
uname	Name of the user who you want to authorize to perform Oracle Data Pump transportable tablespace operations. To find a list of users and their current privileges, query the DBA_SYS_PRIVS data dictionary view.
tname	Name of the tablespace in which the uname user is to perform the transportable tablespace operation. To find a list of tablespaces, query the DBA_TABLESPACES data dictionary view.

**Example**

```
EXEC DBMS_MACADM.AUTHORIZE_TTS_USER('PSMITH', 'HR_TS');
```

**22.1.8 UNAUTHORIZE\_DATAPUMP\_USER Procedure**

The UNAUTHORIZE\_DATAPUMP\_USER procedure revokes the authorization that was granted by the AUTHORIZE\_DATAPUMP\_USER procedure.

When you run this procedure, ensure that its settings correspond exactly to the equivalent AUTHORIZE\_DATAPUMP\_USER procedure.

For example, the following two procedures will work because the parameters are consistent:

```
EXEC DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('DP_MGR');
```

```
EXEC DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('DP_MGR');
```

However, because the parameters in the following procedures are not consistent, the UNAUTHORIZE\_DATAPUMP\_USER procedure will not work:

```
EXEC DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('JSMITH');
```

```
EXEC DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('JSMITH', 'HR');
```

**Syntax**

```
DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER(
  user_name  IN VARCHAR2,
  schema_name IN VARCHAR2 DEFAULT NULL,
  table_name IN VARCHAR2 DEFAULT NULL);
```

## Parameters

**Table 22-8 UNAUTHORIZE\_DATAPUMP\_USER**

Parameter	Description
user_name	Name of the Oracle Data Pump user from whom you want to revoke authorization.  To find a list of users and authorizations from the AUTHORIZATE_DATAPUMP_USER procedure, query the DBA_DV_DATAPUMP_AUTH data dictionary view as follows:  SELECT * FROM DBA_DV_DATAPUMP_AUTH;
schema_name	Name of the database schema that the Oracle Data Pump user is authorized to export or import.
table_name	Name of the table within the schema specified by the schema name parameter.

## Examples

```
EXEC DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('JSMITH');
```

```
EXEC DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('JSMITH', 'HR');
```

```
EXEC DBMS_MACADM.UNAUTHORIZE_DATAPUMP_USER('JSMITH', 'HR', 'SALARY');
```

## 22.1.9 UNAUTHORIZE\_DDL Procedure

The UNAUTHORIZE\_DDL procedure revokes authorization from a user who was granted authorization to execute DDL statements through the DBMS\_MACADM.AUTHORIZE\_DDL procedure.

To find information about users who have been granted this authorization, query the DBA\_DV\_DDL\_AUTH data dictionary view.

## Syntax

```
DBMS_MACADM.UNAUTHORIZE_DDL(
  user_name      IN VARCHAR2,
  schema_name    IN VARCHAR2);
```

## Parameters

**Table 22-9 UNAUTHORIZE\_DDL**

Parameter	Description
user_name	Name of the user from whom you want to revoke DDL authorization.
schema_name	Name of the database schema in which the user wants to perform the DDL statements. Enter % specify all schemas.

## Examples

The following example revokes DDL statement execution authorization from user psmith for all schemas:

```
EXEC DBMS_MACADM.UNAUTHORIZE_DDL('psmith', '%');
```

This example revokes DDL statement execution authorization from user `psmith` for the HR schema only.

```
EXEC DBMS_MACADM.UNAUTHORIZE_DDL('psmith', 'HR');
```

## 22.1.10 UNAUTHORIZE\_MAINTENANCE\_USER Procedure

The `UNAUTHORIZE_MAINTENANCE_USER` procedure revokes privileges from users who have been granted authorization to perform Information Lifecycle Management (ILM) operations in an Oracle Database Vault environment.

To find information about the settings for the ILM authorization, query the `DBA_DV_MAINTENANCE_AUTH` view.

When you run this procedure, ensure that its settings correspond exactly to the equivalent `AUTHORIZE_MAINTENANCE_USER` procedure.

For example, the following two procedures will work because the parameter settings correspond:

```
EXEC DBMS_MACADM.AUTHORIZE_MAINTENANCE_USER('psmith', 'OE', 'ORDERS', 'TABLE',
'ILM');
EXEC DBMS_MACADM.UNAUTHORIZE_MAINTENANCE_USER('psmith', 'OE', 'ORDERS', 'TABLE',
'ILM');
```

However, these two statements will fail because the settings do not correspond:

```
EXEC DBMS_MACADM.AUTHORIZE_MAINTENANCE_USER('psmith', 'OE', 'ORDERS', 'TABLE',
'ILM');

EXEC DBMS_MACADM.UNAUTHORIZE_MAINTENANCE_USER('psmith', '%', '%', '%', 'ILM');
```

### Syntax

```
DBMS_MACADM.UNAUTHORIZE_MAINTENANCE_USER(
  uname          IN VARCHAR2,
  sname          IN VARCHAR2 DEFAULT NULL,
  objname       IN VARCHAR2 DEFAULT NULL,
  objtype       IN VARCHAR2 DEFAULT NULL,
  action        IN VARCHAR2 DEFAULT NULL);
```

### Parameters

**Table 22-10 UNAUTHORIZE\_MAINTENANCE\_USER**

Parameter	Description
<code>uname</code>	Name of the user to whom you want to revoke authorization
<code>sname</code>	Name of the database schema for which the maintenance operations are performed. Enter <code>%</code> to specify all schemas.
<code>objname</code>	Name of the object (such as the name of a table) in the schema that is specified in the <code>sname</code> parameter for which maintenance operations are performed
<code>objtype</code>	Type of the <code>objname</code> object, such as table, index, tablespace, and so on



**Table 22-10 (Cont.) UNAUTHORIZE\_MAINTENANCE\_USER**

Parameter	Description
action	Maintenance action. Enter ilm for Information Lifecycle Management

**Example**

The following example revokes privileges from Database Vault user psmith so that she can no longer perform ILM operations in any HR schema objects:

```
BEGIN
DBMS_MACADM.UNAUTHORIZE_MAINTENANCE_USER (
  uname      => 'psmith',
  sname      => 'HR',
  objname    => 'EMPLOYEES',
  objtype    => 'TABLE',
  action     => 'ILM');
END;
/
```

**Related Topics:**

[Using Information Lifecycle Management with Oracle Database Vault](#)  
(page 13-16)

Users who perform Information Lifecycle Management operations on an Oracle Database Vault-enabled database must be granted authorization to perform these operations.

**22.1.11 UNAUTHORIZE\_PROXY\_USER Procedure**

The UNAUTHORIZE\_PROXY\_USER procedure revokes authorization from a user who was granted proxy authorization from the DBMS\_MACADM.AUTHORIZE\_PROXY\_USER procedure.

**Syntax**

```
DBMS_MACADM.UNAUTHORIZE_PROXY_USER(
  proxy_user  IN VARCHAR2,
  user_name   IN VARCHAR2);
```

**Parameters****Table 22-11 UNAUTHORIZE\_PROXY\_USER**

Parameter	Description
proxy_user	Name of the proxy user.
user_name	Name of the database user who was proxied by the proxy_user user. Enter % to specify all users.

**Examples**

The following example revokes proxy authorization from user preston for proxying all users:

```
DBMS_MACADM.UNAUTHORIZE_PROXY_USER('preston', '%');
```

This example revokes proxy authorization from user `preston` for proxying database user `psmith` only.

```
EXEC DBMS_MACADM.UNAUTHORIZE_PROXY_USER('preston', 'psmith');
```

## 22.1.12 UNAUTHORIZE\_SCHEDULER\_USER Procedure

The `UNAUTHORIZE_SCHEDULER_USER` procedure revokes the authorization that was granted by the `AUTHORIZE_SCHEDULER_USER` procedure.

When you run this procedure, ensure that its settings correspond exactly to the equivalent `AUTHORIZE_SCHEDULER_USER` procedure. For example, the following two procedures will work because the parameters are consistent:

```
EXEC DBMS_MACADM.AUTHORIZE_SCHEDULER_USER('JOB_MGR');
```

```
EXEC DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER('JOB_MGR');
```

However, because the parameters in the following procedures are not consistent, the `UNAUTHORIZE_SCHEDULER_USER` procedure will not work:

```
EXEC DBMS_MACADM.AUTHORIZE_SCHEDULER_USER('JOB_MGR');
```

```
EXEC DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER('JOB_MGR', 'HR');
```

### Syntax

```
DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER
  user_name      IN VARCHAR2,
  schema_name    IN VARCHAR2 DEFAULT NULL);
```

### Parameters

**Table 22-12 UNAUTHORIZE\_SCHEDULER\_USER**

Parameter	Description
<code>user_name</code>	Name of the job scheduling user from whom you want to revoke authorization.  To find a list of users and authorizations from the <code>AUTHORIZE_SCHEDULER_USER</code> procedure, query the <code>DBA_DV_JOB_AUTH</code> data dictionary view as follows:  <pre>SELECT * FROM DBA_DV_JOB_AUTH;</pre>
<code>schema_name</code>	Name of the database schema for which the user is authorized to schedule jobs.

### Examples

```
EXEC DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER('JOB_MGR');
```

```
EXEC DBMS_MACADM.UNAUTHORIZE_SCHEDULER_USER('JOB_MGR', 'HR');
```

## 22.1.13 UNAUTHORIZE\_TTS\_USER Procedure

The UNAUTHORIZE\_TTS\_USER procedure removes from authorization users who had previously been granted the authorization to perform Oracle Data Pump transportable tablespace operations.

### Syntax

```
DBMS_MACADM.UNAUTHORIZE_TTS_USER
  uname      IN VARCHAR2,
  tname      IN VARCHAR2);
```

### Parameters

**Table 22-13 UNAUTHORIZE\_TTS\_USER**

Parameter	Description
uname	Name of the user who you want to remove from being authorized to perform Oracle Data Pump transportable tablespace operations. To find a list of users and their current privileges, query the DBA_SYS_PRIVS data dictionary view.
tname	Name of the tablespace that is used in the transportable tablespace operation. To find a list of tablespaces, query the DBA_TABLESPACES data dictionary view.

### Example

```
EXEC DBMS_MACADM.UNAUTHORIZE_TTS_USER('PSMITH', 'HR_TS');
```

## 22.1.14 DISABLE\_DV Procedure

The DISABLE\_DV procedure disables Oracle Database Vault.

After you run this procedure, you must restart the database.

### Syntax

```
DBMS_MACADM.DISABLE_DV;
```

### Parameters

None

### Example

```
EXEC DBMS_MACADM.DISABLE_DV;
```

### Related Topics:

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

## 22.1.15 DISABLE\_DV\_DICTIONARY\_ACCTS Procedure

The `DISABLE_DV_DICTIONARY_ACCTS` procedure prevents any user from logging into the database as the `DVSYS` or `DVF` schema user.

By default these two accounts are locked. Only a user who has been granted the `DV_OWNER` role can execute this procedure. To find the status of whether users can log into `DVSYS` and `DVF`, query the `DBA_DV_DICTIONARY_ACCTS` data dictionary view. For stronger security, run this procedure to better protect the `DVSYS` and `DVF` schemas. The disablement takes place immediately, so you do not need to restart the database after running this procedure.

### Syntax

```
DBMS_MACADM.DISABLE_DV_DICTIONARY_ACCTS;
```

### Parameters

None

### Example

```
EXEC DBMS_MACADM.DISABLE_DV_DICTIONARY_ACCTS;
```

### Related Topics:

[Archiving and Purging the Oracle Database Vault Audit Trail](#) (page A-6)

If you have not migrated to unified auditing, you should periodically archive and purge the Oracle Database Vault audit trail.

## 22.1.16 DISABLE\_DV\_PATCH\_ADMIN\_AUDIT Procedure

The `DISABLE_DV_PATCH_ADMIN_AUDIT` procedure disables realm, command rule, and rule set auditing of the actions by users who have the `DV_PATCH_ADMIN` role.

This procedure disables the successful actions of this user, not the failed actions. You should run this procedure after the `DV_PATCH_ADMIN` user has completed database patch operation. To find if auditing is enabled or not, query the `DBA_DV_PATCH_AUDIT` data dictionary view.

### Syntax

```
DBMS_MACADM.DISABLE_DV_PATCH_ADMIN_AUDIT;
```

### Parameters

None

### Example

```
EXEC DBMS_MACADM.DISABLE_DV_PATCH_ADMIN_AUDIT;
```

### Related Topics:

[DV\\_PATCH\\_ADMIN Database Vault Database Patch Role](#) (page 14-18)

The `DV_PATCH_ADMIN` role is used for patching operations.

[ENABLE\\_DV\\_PATCH\\_ADMIN\\_AUDIT Procedure](#) (page 22-16)

The `ENABLE_DV_PATCH_ADMIN_AUDIT` procedure enables realm, command rule, and rule set auditing of the actions by users who have the `DV_PATCH_ADMIN` role.

### 22.1.17 DISABLE\_ORADEBUG Procedure

The `DISABLE_ORADEBUG` procedure disables the use of the `ORADEBUG` utility in an Oracle Database Vault environment.

The disablement takes place immediately, so you do not need to restart the database after running this procedure. To find the status of whether the `ORADEBUG` utility is available in Database Vault, query the `DVYS.DBA_DV_ORADEBUG` data dictionary view.

#### Syntax

```
DBMS_MACADM.DISABLE_ORADEBUG;
```

#### Parameters

None

#### Example

```
EXEC DBMS_MACADM.DISABLE_ORADEBUG;
```

#### Related Topics:

[Using the ORADEBUG Utility with Oracle Database Vault](#) (page 13-26)

The `ORADEBUG` utility is used primarily by Oracle Support to diagnose problems that may arise with an Oracle database.

### 22.1.18 ENABLE\_DV Procedure

The `ENABLE_DV` procedure enables Oracle Database Vault and Oracle Label Security. After you run this procedure, you must restart the database.

#### Syntax

```
DBMS_MACADM.ENABLE_DV(  
  strict_mode IN VARCHAR2 DEFAULT);
```

## Parameters

**Table 22-14** *ENABLE\_DV*

Parameter	Description
<code>strict_mode</code>	<p>In a multitenant environment, specifies one of the following modes:</p> <ul style="list-style-type: none"> <li><code>n</code> specifies regular mode, which allows the PDBs to be Database Vault enabled or disabled. (Default)</li> <li><code>y</code> specifies strict mode, which puts the PDBs that have not been Database Vault-enabled in restricted mode, until you enable Database Vault in them and then restart the PDB.</li> </ul> <p>To apply this setting to all PDBs in the multitenant environment, run the <code>DBMS_MACADM.ENABLE_DV</code> procedure in the CDB root. To apply it to all PDBs in an application container, run the procedure in the application root.</p> <p>In a non-multitenant environment, omit this parameter.</p>

## Examples

The following example enables Oracle Database Vault in regular mode.

```
EXEC DBMS_MACADM.ENABLE_DV;
```

This example enables Oracle Database Vault in strict mode in a multitenant environment.

```
EXEC DBMS_MACADM.ENABLE_DV (strict_mode => 'y');
```

## Related Topics:

[Disabling and Enabling Oracle Database Vault](#) (page B-1)

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

## 22.1.19 ENABLE\_DV\_PATCH\_ADMIN\_AUDIT Procedure

The `ENABLE_DV_PATCH_ADMIN_AUDIT` procedure enables realm, command rule, and rule set auditing of the actions by users who have the `DV_PATCH_ADMIN` role.

This procedure is designed to audit these users' actions during a patch upgrade. To find if this auditing is enabled or not, query the `DBA_DV_PATCH_AUDIT` data dictionary view.

### Syntax

```
DBMS_MACADM.ENABLE_DV_PATCH_ADMIN_AUDIT;
```

### Parameters

None

### Example

```
EXEC DBMS_MACADM.ENABLE_DV_PATCH_ADMIN_AUDIT;
```

**Related Topics:**

[DV\\_PATCH\\_ADMIN Database Vault Database Patch Role](#) (page 14-18)

The DV\_PATCH\_ADMIN role is used for patching operations.

[DISABLE\\_DV\\_PATCH\\_ADMIN\\_AUDIT Procedure](#) (page 22-14)

The DISABLE\_DV\_PATCH\_ADMIN\_AUDIT procedure disables realm, command rule, and rule set auditing of the actions by users who have the DV\_PATCH\_ADMIN role.

**22.1.20 ENABLE\_DV\_DICTIONARY\_ACCTS Procedure**

The ENABLE\_DV\_DICTIONARY\_ACCTS procedure enables users to log into the database as the DVSYS or DVF user.

By default, the DVSYS and DVF accounts are locked.

Only a user who has been granted the DV\_OWNER role can execute this procedure. To find the status of whether users can log into DVSYS and DVF, query the DBA\_DV\_DICTIONARY\_ACCTS data dictionary view. For stronger security, only run this procedure when you need to better protect the DVSYS and DVF schemas. The enablement takes place immediately, so you do not need to restart the database after running this procedure.

**Syntax**

```
DBMS_MACADM.ENABLE_DV_DICTIONARY_ACCTS;
```

**Parameters**

None

**Example**

```
EXEC DBMS_MACADM.ENABLE_DV_DICTIONARY_ACCTS;
```

**Related Topics:**

[Archiving and Purging the Oracle Database Vault Audit Trail](#) (page A-6)

If you have not migrated to unified auditing, you should periodically archive and purge the Oracle Database Vault audit trail.

**22.1.21 ENABLE\_ORADEBUG Procedure**

The ENABLE\_ORADEBUG procedure enables the use of the ORADEBUG utility in an Oracle Database Vault environment.

The enablement takes place immediately, so you do not need to restart the database after running this procedure. To find the status of whether the ORADEBUG utility is available in Database Vault, query the DVYS.DBA\_DV\_ORADEBUG data dictionary view.

**Syntax**

```
DBMS_MACADM.ENABLE_ORADEBUG;
```

**Parameters**

None

**Example**

```
EXEC DBMS_MACADM.ENABLE_ORADEBUG;
```

**Related Topics:**

[Using the ORADEBUG Utility with Oracle Database Vault](#) (page 13-26)

The ORADEBUG utility is used primarily by Oracle Support to diagnose problems that may arise with an Oracle database.

## 22.2 CONFIGURE\_DV General System Maintenance Procedure

The CONFIGURE\_DV procedure configures the initial two Oracle Database user accounts, which are granted the DV\_OWNER and DV\_ACCTMGR roles, respectively.

You can check the status of this configuration by querying the DBA\_DV\_STATUS data dictionary view. Before you run the CONFIGURE\_DV procedure, you must create the two user accounts and grant them the CREATE SESSION privilege. The accounts can be either local or common. If you create common user accounts, then the Database Vault roles that are granted to these users apply to the current pluggable database (PDB) only. You then refer to these user accounts for the CONFIGURE\_DV procedure.

The CONFIGURE\_DV procedure resides in the SYS schema. Oracle provides a synonym, DVSYS.CONFIGURE\_DV, so that any existing Oracle Database Vault configuration scripts that you may have created in previous releases will continue to work in this release.

You only can run the CONFIGURE\_DV procedure once, when you are ready to register Oracle Database Vault with an Oracle database. After you run this procedure, you must run utlrvp.sql script and then DBMS\_MACADM.ENABLE\_DV to complete the registration process. Oracle strongly recommends that for better security, you use the two accounts you create here as back-up accounts and then create additional accounts for every day use. See [Backup Oracle Database Vault Accounts](#) (page 14-25) for guidance.

When you run the CONFIGURE\_DV procedure, it checks the DVSYS schema for problems such as missing tables or packages. If it finds problems, then it raises an ORA-47500 Database Vault cannot be configured error. If this happens, then you must deinstall and then reinstall Oracle Database Vault.

Together, the CONFIGURE\_DV and DBMS\_MACADM.ENABLE\_DV procedures, and the utlrvp.sql script, are designed to be a command-line alternative to using Oracle Database Configuration Assistant (DBCA) to register Oracle Database Vault with an Oracle database.

You must run the CONFIGURE\_DV procedure as user SYS. [Registering Oracle Database Vault with an Oracle Database](#) (page 3-2) describes the process that you would use.

**Syntax**

```
CONFIGURE_DV  
  dvowner_username          IN VARCHAR2,  
  dvacctmgr_username       IN VARCHAR2;
```



## Parameters

**Table 22-15 CONFIGURE\_DV**

Parameter	Description
<code>dvowner_username</code>	Name of the user who will be the Database Vault Owner. This user will be granted the <code>DV_OWNER</code> role.
<code>dvacctmgr_username</code>	Name of the user who will be the Database Vault Account Manager. This user will be granted the <code>DV_ACCTMGR</code> role. If you omit this setting, the user specified by the <code>dvowner_username</code> parameter is made the Database Vault Account Manager and granted the <code>DV_ACCTMGR</code> role.

## Example

```
CREATE USER dbv_owner IDENTIFIED BY password CONTAINER = CURRENT;
CREATE USER dbv_acctmgr IDENTIFIED BY password CONTAINER = CURRENT;
GRANT CREATE SESSION TO dbv_owner, dbv_acctmgr;
```

```
BEGIN
CONFIGURE_DV (
  dvowner_username      => 'dbv_owner',
  dvacctmgr_username    => 'dbv_acctmgr';
END;
/
```

## Related Topics:

### [Deinstalling Oracle Database Vault \(page C-2\)](#)

You can remove Oracle Database Vault from an Oracle Database installation, for both to both single-instance and Oracle RAC installations.

### [Reinstalling Oracle Database Vault \(page C-4\)](#)

You can reinstall Oracle Database Vault by using Database Configuration Assistant and afterward, register Database Vault.



---

## Oracle Database Vault Policy APIs

You can use the `DBMS_MACADM` PL/SQL package to manage Oracle Database Vault policies.

Only users who have been granted the `DV_OWNER` or `DV_ADMIN` role can use these procedures.

### [ADD\\_CMD\\_RULE\\_TO\\_POLICY Procedure](#) (page 23-2)

The `ADD_COMMAND_RULE_TO_POLICY` procedure enables you to add an existing command rule to an Oracle Database Vault policy.

### [ADD\\_OWNER\\_TO\\_POLICY Procedure](#) (page 23-4)

The `ADD_OWNER_TO_POLICY` procedure enables you to add an existing database user to an Oracle Database Vault policy as an owner.

### [ADD\\_REALM\\_TO\\_POLICY Procedure](#) (page 23-4)

The `ADD_REALM_TO_POLICY` procedure enables you to add an existing realm to an Oracle Database Vault policy.

### [CREATE\\_POLICY Procedure](#) (page 23-5)

The `CREATE_POLICY` procedure enables you to create an Oracle Database Vault policy.

### [DELETE\\_CMD\\_RULE\\_FROM\\_POLICY Procedure](#) (page 23-6)

The `DELETE_CMD_RULE_FROM_POLICY` procedure enables you to remove an existing command rule from an Oracle Database Vault policy.

### [DELETE\\_OWNER\\_FROM\\_POLICY Procedure](#) (page 23-8)

The `DELETE_OWNER_FROM_POLICY` procedure enables you to remove an owner from an Oracle Database Vault policy.

### [DELETE\\_REALM\\_FROM\\_POLICY Procedure](#) (page 23-9)

The `DELETE_REALM_FROM_POLICY` procedure enables you to remove an existing realm from an Oracle Database Vault policy.

### [DROP\\_POLICY Procedure](#) (page 23-10)

The `DROP_POLICY` procedure enables you to drop an existing Oracle Database Vault policy.

### [RENAME\\_POLICY Procedure](#) (page 23-10)

The `UPDATE_POLICY_DESCRIPTION` procedure enables you to rename an existing Oracle Database Vault policy.

### [UPDATE\\_POLICY\\_DESCRIPTION Procedure](#) (page 23-11)

The `UPDATE_POLICY_DESCRIPTION` procedure enables you to update the `description` field in an Oracle Database Vault policy.

[UPDATE\\_POLICY\\_STATE Procedure](#) (page 23-11)

The `UPDATE_POLICY_STATE` procedure enables you to update the `policy_state` field in an Oracle Database Vault policy.

**Related Topics:**[Configuring Oracle Database Vault Policies](#) (page 10-1)

You can use Oracle Database Vault policies to implement frequently used realm and command rule settings.

[Oracle Database Vault Utility APIs](#) (page 21-1)

Oracle Database Vault provides a set of utility APIs in the `DBMS_MACUTL` PL/SQL package.

## 23.1 ADD\_CMD\_RULE\_TO\_POLICY Procedure

The `ADD_COMMAND_RULE_TO_POLICY` procedure enables you to add an existing command rule to an Oracle Database Vault policy.

You can add a command rule to a policy when the command rule is in any state. For example, you can add a disabled command rule to an enabled policy. In this case, the disabled command rule will automatically become enabled when it is added to the policy. A command rule can be added to only one policy. In other words, you cannot assign the same command rule to multiple policies.

**Syntax**

```
DBMS_MACADM.ADD_CMD_RULE_TO_POLICY(
  policy_name    IN VARCHAR2,
  command        IN VARCHAR2,
  object_owner   IN VARCHAR2,
  object_name    IN VARCHAR2,
  clause_name    IN VARCHAR2 DEFAULT,
  parameter_name IN VARCHAR2 DEFAULT,
  event_name     IN VARCHAR2 DEFAULT,
  component_name IN VARCHAR2 DEFAULT,
  action_name    IN VARCHAR2 DEFAULT,
  scope          IN NUMBER DEFAULT);
```

**Parameters****Table 23-1 ADD\_CMD\_RULE\_TO\_POLICY Parameters**

Parameter	Description
<code>policy_name</code>	Policy name. To find existing Database Vault policies in the current database instance, query the <code>DBA_DV_POLICY</code> view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).
<code>command</code>	Command rule name To find existing Database Vault command rules in the current database instance, query the <code>DBA_DV_COMMAND_RULE</code> view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8).
<code>object_owner</code>	Database schema to which the command rule applies To find existing object owners for this command rule, query the <code>DBA_DV_COMMAND_RULE</code> view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)

**Table 23-1 (Cont.) ADD\_CMD\_RULE\_TO\_POLICY Parameters**

Parameter	Description
object_name	Object to be protected by the command rule To find existing objects for this command rule, query the DBA_DV_COMMAND_RULE view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
clause_name	For ALTER SYSTEM and ALTER SESSION command rules, a clause from the SQL statement that was used to create the command rule To find existing clauses for this command rule, query the DBA_DV_COMMAND_RULE view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
parameter_name	For ALTER SYSTEM and ALTER SESSION command rules, a parameter from the clause_name parameter. To find existing parameters for this command rule, query the DBA_DV_COMMAND_RULE view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
event_name	For ALTER SYSTEM and ALTER SESSION command rules, an event that the command rule defines To find existing event names for this command rule, query the DBA_DV_COMMAND_RULE view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
component_name	A component of the event_name setting To find existing component names for this command rule, query the DBA_DV_COMMAND_RULE view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
action_name	An action of the component_name setting. To find existing action names for this command rule, query the DBA_DV_COMMAND_RULE view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
scope	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the command rule is local in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the command rule applies to all the PDBs</li> </ul>

**Example**

The following example shows how to add a common command rule to a Database Vault policy. This command rule is in the application root of a multitenant environment, so the user running this procedure must be in the application root or the CDB root. Any rules or rule sets that are associated with this command rule must be common.

```
BEGIN
DBMS_MACADM.ADD_CMD_RULE_TO_POLICY(
  policy_name => 'HR_DV_Policy',
  command     => 'ALTER SESSION',
  object_owner => '%',
  object_name  => '%',
```

```

clause_name    => 'PARALLEL DDL',
parameter_name => '',
event_name     => '',
action_name    => '',
scope         => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/

```

## 23.2 ADD\_OWNER\_TO\_POLICY Procedure

The ADD\_OWNER\_TO\_POLICY procedure enables you to add an existing database user to an Oracle Database Vault policy as an owner.

When you add an owner to an enabled policy, the change takes place immediately. There is no limit to the number of users that you add to the policy.

### Syntax

```

DBMS_MACADM.ADD_OWNER_TO_POLICY(
  policy_name  IN VARCHAR2,
  owner_name   IN VARCHAR2);

```

### Parameters

**Table 23-2 ADD\_OWNER\_TO\_POLICY Parameters**

Parameter	Description
policy_name	Policy name. To find existing Database Vault policies in the current database instance, query the DBA_DV_POLICY view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).
owner_name	User name. To find existing database users (not roles) in the current instance, query the DBA_USERS view, described in <i>Oracle Database Reference</i> . To find existing policy owners, query the DBA_DV_POLICY_OWNER view, described in <a href="#">DBA_DV_POLICY_OWNER View</a> (page 25-22).

### Example

```

BEGIN
  DBMS_MACADM.ADD_OWNER_TO_POLICY(
    policy_name => 'HR_DV_Policy',
    owner_name  => 'PSMITH');
END;
/

```

## 23.3 ADD\_REALM\_TO\_POLICY Procedure

The ADD\_REALM\_TO\_POLICY procedure enables you to add an existing realm to an Oracle Database Vault policy.

You can add a disabled realm to an enabled policy. In this case, the realm automatically becomes enabled when it is added. A realm can be added to only one policy. In other words, you cannot assign the same realm to multiple policies.

**Syntax**

```
DBMS_MACADM.ADD_REALM_TO_POLICY(
  policy_name  IN VARCHAR2,
  realm_name   IN VARCHAR2);
```

**Parameters****Table 23-3 ADD\_REALM\_TO\_POLICY Parameters**

Parameter	Description
policy_name	Policy name. To find existing Database Vault policies in the current database instance, query the DBA_DV_POLICY view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).
realm_name	Realm name. To find existing Database Vault realms in the current database instance, query the DV_REALM view, described in <a href="#">DVSYS.DV_REALM View</a> (page 25-46).

**Example**

```
BEGIN
  DBMS_MACADM.ADD_REALM_TO_POLICY(
    policy_name => 'HR_DV_Policy',
    realm_name  => 'HR realm');
END;
/
```

## 23.4 CREATE\_POLICY Procedure

The CREATE\_POLICY procedure enables you to create an Oracle Database Vault policy.

After you create the policy, you must add at least one realm and one command rule to the policy. Optionally, you can set these realms and command rules to be enforced individually or use the enforcement that the policy uses.

An owner for the policy is not required, but if you do not assign an owner to the policy, a user who has been granted the DV\_OWNER or DV\_ADMIN role must administer the policy.

After you create the policy, use the following procedures to complete the policy definition:

- ADD\_REALM\_TO\_POLICY adds realms to the policy.
- ADD\_CMD\_RULE\_TO\_POLICY adds command rules to the policy.
- ADD\_OWNER\_TO\_POLICY enables the specified database users to manage the policy.

**Syntax**

```
DBMS_MACADM.CREATE_POLICY(
  policy_name  IN VARCHAR2,
  description  IN VARCHAR2 DEFAULT,
  policy_state IN NUMBER);
```

## Parameters

**Table 23-4 CREATE\_POLICY Parameters**

Parameter	Description
policy_name	Policy name, up to 128 characters in mixed case To find existing policies in the current database instance, query the DBA_DV_POLICY view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).
description	Description of the purpose of the policy, up to 4000 characters in mixed-case.
policy_state	Specifies how the policy is enabled. Possible values are: <ul style="list-style-type: none"> <li>DBMS_MACADM.G_ENABLED (1), which enables the policy after you create it</li> <li>DBMS_MACADM.G_DISABLED (0), which disables the policy after you create it</li> <li>DBMS_MACADM.G_SIMULATION (2), which sets the policy to simulation mode. In simulation mode, any violations to realms or command rules used in the policy are logged in a designated log table with sufficient information to describe the error, such as the user name or SQL statement used.</li> <li>DBMS_MACADM.G_PARTIAL (3), which sets the policy to partial mode. In partial mode, the enforcement state of realms or command rules associated with the policy can be changed individually.</li> </ul> See <a href="#">About Simulation Mode</a> (page 11-1) for more information about simulation mode

## Example

The following example creates a policy that uses the partial state. Later on, when a realm or a command rule is added to this policy, their enforcement state will be able to be changed individually.

```
BEGIN
  DBMS_MACADM.CREATE_POLICY(
    policy_name => 'HR Database Vault Policy',
    description => 'Policy to protect the HR schema',
    policy_state => DBMS_MACADM.G_ENABLED);
END;
/
```

## 23.5 DELETE\_CMD\_RULE\_FROM\_POLICY Procedure

The DELETE\_CMD\_RULE\_FROM\_POLICY procedure enables you to remove an existing command rule from an Oracle Database Vault policy.

You can remove command rules from a policy anytime regardless of the state of the policy. When a command rule is removed from a policy, the state of command rule remains the same. That is, if the policy is enabled, and a command rule is removed from the policy, then the command rule will be still enabled after you have removed it from the policy.



## Syntax

```
DBMS_MACADM.DELETE_CMD_RULE_FROM_POLICY(
  policy_name    IN VARCHAR2,
  command        IN VARCHAR2,
  object_owner   IN VARCHAR2,
  object_name    IN VARCHAR2,
  clause_name    IN VARCHAR2 DEFAULT,
  parameter_name IN VARCHAR2 DEFAULT,
  event_name     IN VARCHAR2 DEFAULT,
  component_name IN VARCHAR2 DEFAULT,
  action_name    IN VARCHAR2 DEFAULT,
  scope          IN NUMBER DEFAULT);
```

## Parameters

**Table 23-5** *DELETE\_CMD\_RULE\_FROM\_POLICY* Parameters

Parameter	Description
policy_name	Policy name. To find existing Database Vault policies in the current database instance, query the <a href="#">DBA_DV_POLICY</a> view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).
command	Command rule name To find existing Database Vault command rules in the current database instance, query the <a href="#">DBA_DV_COMMAND_RULE</a> view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8).
object_owner	Database schema to which the command rule applies To find existing object owners for this command rule, query the <a href="#">DBA_DV_COMMAND_RULE</a> view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
object_name	Object to be protected by the command rule To find existing objects for this command rule, query the <a href="#">DBA_DV_COMMAND_RULE</a> view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
clause_name	For ALTER SYSTEM and ALTER SESSION command rules, a clause from the SQL statement that was used to create the command rule To find existing clauses for this command rule, query the <a href="#">DBA_DV_COMMAND_RULE</a> view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
parameter_name	For ALTER SYSTEM and ALTER SESSION command rules, a parameter from the clause_name parameter. To find existing parameters for this command rule, query the <a href="#">DBA_DV_COMMAND_RULE</a> view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
event_name	For ALTER SYSTEM and ALTER SESSION command rules, an event that the command rule defines To find existing event names for this command rule, query the <a href="#">DBA_DV_COMMAND_RULE</a> view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)

**Table 23-5 (Cont.) DELETE\_CMD\_RULE\_FROM\_POLICY Parameters**

Parameter	Description
component_name	A component of the event_name setting To find existing component names for this command rule, query the DBA_DV_COMMAND_RULE view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
action_name	An action of the component_name setting. To find existing action names for this command rule, query the DBA_DV_COMMAND_RULE view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8)
scope	For a multitenant environment, determines how to execute this procedure. The default is local. Options are as follows: <ul style="list-style-type: none"> <li>DBMS_MACUTL.G_SCOPE_LOCAL (or 1) if the command rule is local in the current PDB</li> <li>DBMS_MACUTL.G_SCOPE_COMMON (or 2) if the command rule is in the application root</li> </ul>

**Example**

The following example shows how to delete a common command rule from a Database Vault policy. This command rule is in the application root of a multitenant environment, so the user running this procedure must be in the CDB root.

```
BEGIN
DBMS_MACADM.DELETE_CMD_RULE_FROM_POLICY(
  policy_name => 'HR_DV_Policy',
  command     => 'ALTER SESSION',
  object_owner => '%',
  object_name  => '%',
  clause_name  => 'END SESSION',
  parameter_name => 'KILL SESSION',
  event_name   => '',
  action_name  => '',
  scope       => DBMS_MACUTL.G_SCOPE_COMMON);
END;
/
```

**23.6 DELETE\_OWNER\_FROM\_POLICY Procedure**

The DELETE\_OWNER\_FROM\_POLICY procedure enables you to remove an owner from an Oracle Database Vault policy.

You can remove owners from policies any time, regardless of the state (enabled or disabled) of the policy. The change takes effect immediately.

**Syntax**

```
DBMS_MACADM.DELETE_OWNER_FROM_POLICY(
  policy_name IN VARCHAR2,
  owner_name  IN VARCHAR2);
```

## Parameters

**Table 23-6** *DELETE\_OWNER\_FROM\_POLICY Parameters*

Parameter	Description
policy_name	Policy name. To find existing Database Vault policies in the current database instance, query the DBA_DV_POLICY view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).
owner_name	User name. To find existing policy owners in the current instance, query the DBA_DV_POLICY_OWNER view, described in <a href="#">DBA_DV_POLICY_OWNER View</a> (page 25-22).

## Example

```
BEGIN
  DBMS_MACADM.DELETE_OWNER_FROM_POLICY(
    policy_name => 'HR_DV_Policy',
    owner_name  => 'PSMITH');
END;
/
```

## 23.7 DELETE\_REALM\_FROM\_POLICY Procedure

The DELETE\_REALM\_FROM\_POLICY procedure enables you to remove an existing realm from an Oracle Database Vault policy.

You can remove realms from policies any time, regardless of the state (enabled or disabled) of the policy. The change takes effect immediately.

## Syntax

```
DBMS_MACADM.DELETE_REALM_FROM_POLICY(
  policy_name  IN VARCHAR2,
  realm_name   IN VARCHAR2);
```

## Parameters

**Table 23-7** *DELETE\_REALM\_FROM\_POLICY Parameters*

Parameter	Description
policy_name	Policy name. To find existing Database Vault policies in the current database instance, query the DBA_DV_POLICY view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).
realm_name	Realm name. To find existing Database Vault realms in the current database instance, query the DV_REALM view, described in <a href="#">DVSYS.DV \$REALM View</a> (page 25-46).

## Example

```
BEGIN
  DBMS_MACADM.ADD_DELETE_REALM_FROM_POLICY(
    policy_name => 'HR_DV_Policy',
    realm_name  => 'HR realm');
```

```
END;
/
```

## 23.8 DROP\_POLICY Procedure

The `DROP_POLICY` procedure enables you to drop an existing Oracle Database Vault policy.

You can remove a policy at any time, regardless of the state (enabled or disabled) of the policy.

### Syntax

```
DBMS_MACADM.DROP_POLICY(
  policy_name      IN VARCHAR2);
```

### Parameters

**Table 23-8** *DROP\_POLICY Parameters*

Parameter	Description
<code>policy_name</code>	Policy name. To find existing Database Vault policies in the current database instance, query the <code>DBA_DV_POLICY</code> view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).

### Example

```
BEGIN
  DBMS_MACADM.DROP_POLICY(
    policy_name      => 'HR_DV_Policy');
END;
/
```

## 23.9 RENAME\_POLICY Procedure

The `UPDATE_POLICY_DESCRIPTION` procedure enables you to rename an existing Oracle Database Vault policy.

You can rename a policy at any time, regardless of the state (enabled or disabled) of the policy. The change takes effect immediately.

### Syntax

```
DBMS_MACADM.RENAME_POLICY(
  policy_name      IN VARCHAR2,
  new_policy_name  IN VARCHAR2);
```

### Parameters

**Table 23-9** *RENAME\_POLICY Parameters*

Parameter	Description
<code>policy_name</code>	Policy name. To find existing Database Vault policies in the current database instance, query the <code>DBA_DV_POLICY</code> view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).

**Table 23-9 (Cont.) RENAME\_POLICY Parameters**

Parameter	Description
new_policy_name	New policy name, up to 128 characters in mixed case

**Example**

```
BEGIN
  DBMS_MACADM.RENAME_POLICY(
    policy_name      => 'HR Database Vault Policy',
    new_policy_name => 'HR_DV_Policy');
END;
/
```

## 23.10 UPDATE\_POLICY\_DESCRIPTION Procedure

The UPDATE\_POLICY\_DESCRIPTION procedure enables you to update the description field in an Oracle Database Vault policy.

**Syntax**

```
DBMS_MACADM.UPDATE_POLICY_DESCRIPTION(
  policy_name  IN VARCHAR2,
  description  IN VARCHAR2 DEFAULT);
```

**Parameters****Table 23-10 UPDATE\_POLICY\_DESCRIPTION Parameters**

Parameter	Description
policy_name	Policy name. To find existing Database Vault policies in the current database instance, query the DBA_DV_POLICY view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).
description	New description of the purpose of the policy, up to 4000 characters in mixed-case

**Example**

```
BEGIN
  DBMS_MACADM.UPDATE_POLICY_DESCRIPTION(
    policy_name => 'HR_DV_Policy',
    description => 'HR schema protection policy');
END;
/
```

## 23.11 UPDATE\_POLICY\_STATE Procedure

The UPDATE\_POLICY\_STATE procedure enables you to update the policy\_state field in an Oracle Database Vault policy.

**Syntax**

```
DBMS_MACADM.UPDATE_POLICY_STATE(
  policy_name  IN VARCHAR2,
  policy_state IN NUMBER);
```

**Parameters****Table 23-11 UPDATE\_POLICY\_STATE Parameters**

Parameter	Description
policy_name	Policy name. To find existing Database Vault policies in the current database instance, query the DBA_DV_POLICY view, described in <a href="#">DBA_DV_POLICY View</a> (page 25-19).
policy_state	Specifies how the policy is enabled. Possible values are: <ul style="list-style-type: none"> <li>• DBMS_MACADM.G_ENABLED (1), which enables the policy after you create it</li> <li>• DBMS_MACADM.G_DISABLED (0), which disables the policy after you create it</li> <li>• DBMS_MACADM. (2), which sets the policy to simulation mode. In simulation mode, any violations to realms or command rules used in the policy are logged in a designated log table with sufficient information to describe the error, such as the user name or SQL statement used.</li> <li>• DBMS_MACADM.G_PARTIAL (3), which sets the policy to partial mode. In partial mode, the enforcement state of realms or command rules associated with the policy can be changed individually.</li> </ul> See <a href="#">About Simulation Mode</a> (page 11-1) for more information about simulation mode

**Example**

```
BEGIN
  DBMS_MACADM.UPDATE_POLICY_STATE(
    policy_name => 'HR_DV_Policy',
    policy_state => DBMS_MACADM.G_DISABLED);
END;
/
```

## Oracle Database Vault API Reference

Oracle Database Vault provides a rich set of APIs, both in PL/SQL packages and in standalone procedures.

### [DBMS\\_MACADM PL/SQL Package Contents](#) (page 24-1)

The DBMS\_MACADM package enables you to configure the realms, factors, rule sets, command rules, secure application roles, and Oracle Label Security policies.

### [DBMS\\_MACSEC\\_ROLES PL/SQL Package Contents](#) (page 24-8)

The DBMS\_MACSEC\_ROLES package enables you to check and set Oracle Database Vault secure application roles.

### [DBMS\\_MACUTL PL/SQL Package Contents](#) (page 24-8)

The DBMS\_MACUTL PL/SQL package defines constants and utility methods that are commonly used by other Oracle Database Vault packages, such as error handling.

### [CONFIGURE\\_DV PL/SQL Procedure](#) (page 24-9)

The CONFIGURE\_DV configures the initial two Oracle Database user accounts, which are granted the DV\_OWNER and DV\_ACCTMGR roles, respectively.

### [DVF PL/SQL Interface Contents](#) (page 24-9)

The DVF schema provides a set of factor-related PL/SQL functions.

## 24.1 DBMS\_MACADM PL/SQL Package Contents

The DBMS\_MACADM package enables you to configure the realms, factors, rule sets, command rules, secure application roles, and Oracle Label Security policies.

The DBMS\_MACADM package is available only for users who have been granted the DV\_ADMIN or DV\_OWNER role.

### DBMS\_MACADM Realm Procedures

[Table 24-1](#) (page 24-1) lists the realm procedures in the DBMS\_MACADM package.

**Table 24-1 DBMS\_MACADM Realm Procedures**

Procedure	Description
ADD_AUTH_TO_REALM procedure	Authorizes a user or role to access a realm as an owner or a participant
ADD_OBJECT_TO_REALM procedure	Registers a set of objects for realm protection
CREATE_REALM procedure	Creates a realm

**Table 24-1 (Cont.) DBMS\_MACADM Realm Procedures**

Procedure	Description
DELETE_AUTH_FROM_REALM procedure	Removes the authorization of a user or role to access a realm
DELETE_OBJECT_FROM_REALM procedure	Removes a set of objects from realm protection
DELETE_REALM procedure	Deletes a realm, including its related Database Vault configuration information that specifies who is authorized and what objects are protected
DELETE_REALM_CASCADE procedure	Deletes a realm, including its related Database Vault configuration information that specifies who is authorized and what objects are protected
RENAME_REALM procedure	Renames a realm. The name change takes effect everywhere the realm is used.
UPDATE_REALM procedure	Updates a realm
UPDATE_REALM_AUTH procedure	Updates the authorization of a user or role to access a realm

### DBMS\_MACADM Rule Set and Rule Procedures

Table 24-2 (page 24-2) lists the rule set and rule procedures in the DBMS\_MACADM package.

**Table 24-2 DBMS\_MACADM Rule Set and Rule Procedures**

Procedure	Description
CREATE_RULE_SET procedure	Creates a rule set
RENAME_RULE_SET procedure	Renames a rule set. The name change takes effect everywhere the rule set is used.
DELETE_RULE_FROM_RULE_SET procedure	Deletes a rule from a rule set
DELETE_RULE_SET procedure	Deletes a rule set
UPDATE_RULE_SET procedure	Updates a rule set
CREATE_RULE procedure	Creates a rule
ADD_RULE_TO_RULE_SET procedure	Adds a rule to a rule set
DELETE_RULE procedure	Deletes a rule
RENAME_RULE procedure	Renames a rule. The name change takes effect everywhere the rule is used.



**Table 24-2 (Cont.) DBMS\_MACADM Rule Set and Rule Procedures**

Procedure	Description
UPDATE_RULE procedure	Updates a rule

**DBMS\_MACADM Command Rule Procedures**

Table 24-3 (page 24-3) lists the command rule procedures in the DBMS\_MACADM package.

**Table 24-3 DBMS\_MACADM Command Rule Procedures**

Procedure	Description
CREATE_COMMAND_RULE procedure	Creates a command rule, associates it with a rule set, and lets you enable the command rule for rule checking with a rule set
CREATE_CONNECT_COMMAND_RULE procedure	Creates a CONNECT command rule
CREATE_SESSION_EVENT_CMD_RULE procedure	Creates a session event command rule, using the ALTER SESSION SQL statement
CREATE_SYSTEM_EVENT_CMD_RULE procedure	Creates a system event command rule, using the ALTER SYSTEM SQL statement
DELETE_COMMAND_RULE procedure	Drops a command rule declaration
DELETE_CONNECT_COMMAND_RULE procedure	Drops a CONNECT command rule declaration
DELETE_SESSION_EVENT_CMD_RULE procedure	Drops a SESSION_EVENT_CMD command rule declaration
DELETE_SYSTEM_EVENT_CMD_RULE procedure	Drops a SYSTEM_EVENT_CMD command rule declaration
UPDATE_COMMAND_RULE procedure	Updates a command rule declaration
UPDATE_CONNECT_COMMAND_RULE procedure	Updates a CONNECT command rule declaration
UPDATE_SESSION_EVENT_CMD_RULE procedure	Updates a SESSION_EVENT_CMD command rule declaration
UPDATE_SYSTEM_EVENT_CMD_RULE procedure	Updates a SYSTEM_EVENT_CMD command rule declaration

**DBMS\_MACADM Factor Procedures and Functions**

lists the factor procedures and functions in the DBMS\_MACADM package.

**Table 24-4 DBMS\_MACADM Factor Procedures and Functions**

<b>Procedure or Function</b>	<b>Description</b>
ADD_FACTOR_LINK procedure	Specifies a parent-child relationship for two factors
ADD_POLICY_FACTOR procedure	Specifies that the label for a factor contributes to the Oracle Label Security label for a policy.
CHANGE_IDENTITY_FACTOR procedure	Associates an identity with a different factor
CHANGE_IDENTITY_VALUE procedure	Updates the value of an identity
CREATE_DOMAIN_IDENTITY procedure	Adds an Oracle Real Application Clusters (Oracle RAC) database node to the domain factor identities and labels it according to the Oracle Label Security policy.
CREATE_FACTOR procedure	Creates a factor
CREATE_FACTOR_TYPE procedure	Creates a factor type
CREATE_IDENTITY procedure	Creates an identity
CREATE_IDENTITY_MAP procedure	Defines a set of tests that are used to derive the identity of a factor from the value of linked child factors (subfactors)
DELETE_FACTOR procedure	Deletes a factor
DELETE_FACTOR_LINK procedure	Removes a parent-child relationship for two factors
DELETE_FACTOR_TYPE procedure	Deletes a factor type
DELETE_IDENTITY procedure	Removes an identity
DELETE_IDENTITY_MAP procedure	Removes an identity map from a factor
DROP_DOMAIN_IDENTITY procedure	Removes an Oracle RAC database node from a domain
GET_INSTANCE_INFO function	Returns information from the SYS.V_\$INSTANCE system table about the current database instance; returns a VARCHAR2 value
GET_SESSION_INFO function	Returns information from the SYS.V_\$SESSION system table for the current session; returns a VARCHAR2 value
RENAME_FACTOR procedure	Renames a factor. The name change takes effect everywhere the factor is used.
RENAME_FACTOR_TYPE procedure	Renames a factor type. The name change takes effect everywhere the factor type is used.

**Table 24-4 (Cont.) DBMS\_MACADM Factor Procedures and Functions**

Procedure or Function	Description
UPDATE_FACTOR procedure	Updates a factor
UPDATE_FACTOR_TYPE procedure	Updates the description of a factor type
UPDATE_IDENTITY procedure	Updates the trust level of a factor identity

### DBMS\_MACADM Secure Application Role Procedures

[Table 24-5](#) (page 24-5) lists the secure application role procedures in the DBMS\_MACADM package.

**Table 24-5 DBMS\_MACADM Secure Application Role Procedures**

Procedure	Description
CREATE_ROLE procedure	Creates an Oracle Database Vault secure application role
DELETE_ROLE procedure	Deletes an Oracle Database Vault secure application role
RENAME_ROLE procedure	Renames an Oracle Database Vault secure application role. The name change takes effect everywhere the role is used.
UNASSIGN_ROLE procedure	Unassigns an Oracle Database Vault secure application role from a user
UPDATE_ROLE procedure	Updates a Oracle Database Vault secure application role

### DBMS\_MACADM Oracle Label Security Procedures

[Table 24-6](#) (page 24-5) lists the Oracle Label Security procedures in the DBMS\_MACADM package.

**Table 24-6 DBMS\_MACADM Oracle Label Security Procedures**

Procedure	Description
CREATE_MAC_POLICY procedure	Specifies the algorithm that is used to merge labels when computing the label for a factor, or the Oracle Label Security Session label
CREATE_POLICY_LABEL procedure	Labels an identity within an Oracle Label Security policy
DELETE_MAC_POLICY_CASCADE procedure	Deletes all Oracle Database Vault objects related to an Oracle Label Security policy.

**Table 24-6 (Cont.) DBMS\_MACADM Oracle Label Security Procedures**

Procedure	Description
DELETE_POLICY_FACTOR procedure	Removes the factor from contributing to the Oracle Label Security label
DELETE_POLICY_LABEL procedure	Removes the label from an identity within an Oracle Label Security policy
UPDATE_MAC_POLICY procedure	Specifies the algorithm that is used to merge labels when computing the label for a factor, or the Oracle Label Security Session label

**DBMS\_MACADM Database Vault Policy Procedures**

Table 24-7 (page 24-6) lists the Database Vault policy procedures in the DBMS\_MACADM package.

**Table 24-7 DBMS\_MACADM Database Vault Policy Procedures**

Procedure	Description
ADD_CMD_RULE_TO_POLICY procedure	Adds a command rule to a Database Vault policy
ADD_OWNER_TO_POLICY procedure	Adds an owner to a Database Vault policy
ADD_REALM_TO_POLICY procedure	Adds a realm to a Database Vault policy
CREATE_POLICY procedure	Creates a Database Vault policy
DELETE_CMD_RULE_FROM_POLICY procedure	Deletes a command rule from a Database Vault policy
DELETE_OWNER_FROM_POLICY procedure	Deletes an owner from a Database Vault policy
DELETE_REALM_FROM_POLICY procedure	Deletes a realm from a Database Vault policy
DROP_POLICY procedure	Drops a Database Vault policy
RENAME_POLICY procedure	Renames a Database Vault policy
UPDATE_POLICY_DESCRIPTION procedure	Updates a Database Vault policy description
UPDATE_POLICY_STATE procedure	Updates the enablement status of the a Database Vault policy

**DBMS\_MACADM General Administrative Procedures**

Table 24-8 (page 24-7) lists the general administrative procedures in the DBMS\_MACADM package.

**Table 24-8 DBMS\_MACADM General Administrative Procedures**

<b>Procedure</b>	<b>Description</b>
ADD-NLS_DATA procedure	Adds a new language to Oracle Database Vault
AUTHORIZE_DATAPUMP_USER procedure	Authorizes a user to perform Oracle Data Pump operations when Oracle Database Vault is enabled
AUTHORIZE_DDL procedure	Grants a user authorization to execute data definition language (DDL) statements
AUTHORIZE_MAINTENANCE_USER procedure	Grants a user authorization to perform Information Lifecycle Management (ILM) operations
AUTHORIZE_PROXY_USER procedure	Grants a proxy user authorization to proxy other user accounts
AUTHORIZE_SCHEDULER_USER procedure	Authorizes a user to schedule database jobs when Oracle Database Vault is enabled
AUTHORIZE_TTS_USER procedure	Authorizes a user to perform Oracle Data Pump transportable tablespace operations for a tablespace when Oracle Database Vault is enabled
UNAUTHORIZE_DATAPUMP_USER procedure	Revokes the authorization that was granted by the DBMS_MACADM.AUTHORIZE_DATAPUMP_USER procedure
UNAUTHORIZE_DDL procedure	Revokes authorization from a user who was granted authorization to execute DDL statements through the DBMS_MACADM.AUTHORIZE_DDL procedure
UNAUTHORIZE_MAINTENANCE_USER procedure	Revokes authorization to perform ILM operations
UNAUTHORIZE_PROXY_USER procedure	Revokes authorization from a user who was granted proxy authorization from the DBMS_MACADM.AUTHORIZE_PROXY_USER procedure
UNAUTHORIZE_SCHEDULER_USER procedure	Revokes authorization that was granted by the DBMS_MACADM.AUTHORIZE_SCHEDULER_USER procedure
UNAUTHORIZE_TTS_USER procedure	Revokes from authorization a user who had been granted authorization to perform Oracle Data Pump transportable tablespace operations for a tablespace when Oracle Database Vault is enabled
DISABLE_DV procedure	Disables Oracle Database Vault
DISABLE_DV_DICTIONARY_ACCTS procedure	Prevents users from logging into the DVSYS and DFV schema accounts
DISABLE_DV_PATCH_ADMIN	Disables auditing of the DV_PATCH_ADMIN user

**Table 24-8 (Cont.) DBMS\_MACADM General Administrative Procedures**

Procedure	Description
DISABLE_ORADEBUG procedure	Disables the use of the ORADEBUG utility in an Oracle Database Vault environment
ENABLE_DV procedure	Enables Oracle Database Vault
ENABLE_DV_DICTIONARY_ACCTS procedure	Enables users to log into the DVSYS and DFV schema accounts
ENABLE_DV_PATCH_ADMIN	Enables auditing of the DV_PATCH_ADMIN user
ENABLE_ORADEBUG procedure	Enables the use of the ORADEBUG utility in an Oracle Database Vault environment

## 24.2 DBMS\_MACSEC\_ROLES PL/SQL Package Contents

The DBMS\_MACSEC\_ROLES package enables you to check and set Oracle Database Vault secure application roles.

This package is available to the general database account population.

[Table 24-9](#) (page 24-8) lists the contents of the DBMS\_MACSEC\_ROLES package.

**Table 24-9 DBMS\_MACSEC\_ROLES PL/SQL Package Contents**

Procedure or Function	Description
CAN_SET_ROLE function	Checks whether the user invoking the method is authorized to use the specified Oracle Database Vault secure application role. Returns a BOOLEAN value.
SET_ROLE procedure	Issues the SET ROLE statement for an Oracle Database Vault secure application role.

## 24.3 DBMS\_MACUTL PL/SQL Package Contents

The DBMS\_MACUTL PL/SQL package defines constants and utility methods that are commonly used by other Oracle Database Vault packages, such as error handling.

This package can be run by the general database account population. This allows for security developers to leverage the constants in scripted configuration files. Utility methods such as USER\_HAS\_ROLE can also be used in Oracle Database Vault rules.

[Table 24-10](#) (page 24-8) lists the DBMS\_MACUTL package contents.

**Table 24-10 DBMS\_MACUTL PL/SQL Package Contents**

Procedure or Function	Description
CHECK_DVSYS_DML_ALLOWED procedure	Verifies that public-packages are not being bypassed by users updating the Oracle Database Vault configuration
GET_CODE_VALUE function	Looks up the value for a code within a code group.
GET_SECONDS function	Returns the seconds in Oracle SS format (00-59). Useful for rule expressions based on time data

**Table 24-10 (Cont.) DBMS\_MACUTL PL/SQL Package Contents**

Procedure or Function	Description
GET_MINUTE function	Returns the minute in Oracle MI format (00–59). Useful for rule expressions based on time data
GET_HOUR function	Returns the month in Oracle HH24 format (00–23). Useful for rule expressions based on time data
GET_DAY function	Returns the day in Oracle DD format (01–31). Useful for rule expressions based on time data
GET_MONTH function	Returns the month in Oracle MM format (01–12). Useful for rule expressions based on time data
GET_YEAR function	Returns the year in Oracle YYYY format (0001–9999). Useful for rule expressions based on time data
IS_ALPHA function	Checks whether the character is alphabetic
IS_DIGIT function	Checks whether the character is numeric
IS_DVSYS_OWNER function	Determines whether a user is authorized to manage the Oracle Database Vault configuration
IS_OLS_INSTALLED function	Returns an indicator regarding whether Oracle Label Security is installed
IS_OLS_INSTALLED_VARCHAR function	Returns an indicator regarding whether Oracle Label Security is installed
USER_HAS_ROLE function	Checks whether a user has a role privilege, directly or indirectly (through another role)
USER_HAS_ROLE_VARCHAR function	Checks whether a user has a role privilege, directly or indirectly (through another role)
USER_HAS_SYSTEM_PRIVILEGE function	Checks whether a user has a system privilege, directly or indirectly (through a role)

## 24.4 CONFIGURE\_DV PL/SQL Procedure

The CONFIGURE\_DV configures the initial two Oracle Database user accounts, which are granted the DV\_OWNER and DV\_ACCTMGR roles, respectively.

This procedure is used as part of the registration process for Oracle Database Vault with an Oracle database. You only need to use it once for the database instance.

## 24.5 DVF PL/SQL Interface Contents

The DVF schema provides a set of factor-related PL/SQL functions.

The functions are then available to the general database account population through PL/SQL functions and standard SQL.

[Table 24-11](#) (page 24-10) lists the DVF factor functions.

**Table 24-11 DVF PL/SQL Interface Contents**

Function	Description
F\$CLIENT_IP	Returns the IP address of the computer from which the client is connected
F\$DATABASE_DOMAIN	Returns the domain of the database as specified in the DB_DOMAIN initialization parameter
F\$DATABASE_HOSTNAME	Returns the host name of the computer on which the database instance is running
F\$DATABASE_INSTANCE	Returns the database instance identification number of the current database instance
F\$DATABASE_IP	Returns the IP address of the computer on which the database instance is running
F\$DATABASE_NAME	Returns the name of the database as specified in the DB_NAME initialization parameter
F\$DOMAIN	Returns a named collection of physical, configuration, or implementation-specific factors in the run-time environment (for example, a networked IT environment or subset of it) that operates at a specific sensitivity level
F\$ENTERPRISE_IDENTITY	Returns the enterprise-wide identity for a user
F\$IDENTIFICATION_TYPE	Returns the way the schema of a user was created in the database. Specifically, it reflects the IDENTIFIED clause in the CREATE USER or ALTER USER syntax.
F\$LANG	Returns the ISO abbreviation for the language name, a shorter form than the existing LANGUAGE parameter
F\$LANGUAGE	Returns the language and territory currently used by your session, in VARCHAR2 data type, along with the database character set
F\$MACHINE	Returns the computer (host) name for the database client that established the database session.
F\$NETWORK_PROTOCOL	Returns the network protocol being used for communication, as specified in the PROTOCOL= <i>protocol</i> portion of the connect string
F\$PROXY_ENTERPRISE_IDENTITY	Returns the Oracle Internet Directory distinguished name (DN) when the proxy user is an enterprise user
F\$SESSION_USER	Returns the database user name by which the current user is authenticated



---

# Oracle Database Vault Data Dictionary Views

You can find information about the Oracle Database Vault configuration settings by querying the Database Vault-specific data dictionary views.

## [About the Oracle Database Vault Data Dictionary Views](#) (page 25-5)

Oracle Database Vault provides a set of DBA-style data dictionary views that can be accessed through the `DV_SECANALYST` role or the `DV_ADMIN` role.

## [CDB\\_DV\\_STATUS View](#) (page 25-5)

The `CDB_DV_STATUS` data dictionary view shows the status of Oracle Database Vault being enabled and configured in a multitenant environment.

## [DBA\\_DV\\_CODE View](#) (page 25-6)

The `DBA_DV_CODE` data dictionary view lists generic lookup codes for the user interface, error messages, and constraint checking.

## [DBA\\_DV\\_COMMAND\\_RULE View](#) (page 25-8)

The `DBA_DV_COMMAND_RULE` data dictionary view lists the SQL statements that are protected by command rules.

## [DBA\\_DV\\_DATAPUMP\\_AUTH View](#) (page 25-10)

The `DBA_DV_DATAPUMP_AUTH` data dictionary view lists the authorizations for using Oracle Data Pump in an Oracle Database Vault environment.

## [DBA\\_DV\\_DDL\\_AUTH View](#) (page 25-10)

The `DBA_DV_DDL` data dictionary view lists the users and schemas that were specified by the `DBMS_MACADM.AUTHORIZE_DDL` procedure.

## [DBA\\_DV\\_DICTIONARY\\_ACCTS View](#) (page 25-11)

The `DBA_DV_DICTIONARY_ACCTS` data dictionary view indicates whether users can directly log into the `DVSYSD` and `DVFS` schema accounts.

## [DBA\\_DV\\_FACTOR View](#) (page 25-11)

The `DBA_DV_FACTOR` data dictionary view lists the existing factors in the current database instance.

## [DBA\\_DV\\_FACTOR\\_TYPE View](#) (page 25-13)

The `DBA_DV_FACTOR_TYPE` data dictionary view lists the names and descriptions of factor types used in the system.

## [DBA\\_DV\\_FACTOR\\_LINK View](#) (page 25-14)

The `DBA_DV_FACTOR_LINK` data dictionary view shows the relationships of each factor whose identity is determined by the association of child factors.

---

[DBA\\_DV\\_IDENTITY View](#) (page 25-15)

The DBA\_DV\_IDENTITY data dictionary view lists the identities for each factor.

[DBA\\_DV\\_IDENTITY\\_MAP View](#) (page 25-15)

The DBA\_DV\_IDENTITY\_MAP data dictionary view lists the mappings for each factor identity.

[DBA\\_DV\\_JOB\\_AUTH View](#) (page 25-16)

The DBA\_DV\_JOB\_AUTH data dictionary view lists the authorizations for using Oracle Scheduler in an Oracle Database Vault environment.

[DBA\\_DV\\_MAC\\_POLICY View](#) (page 25-17)

The DBA\_DV\_MAC\_POLICY data dictionary view lists the Oracle Label Security policies defined for use with Oracle Database Vault.

[DBA\\_DV\\_MAC\\_POLICY\\_FACTOR View](#) (page 25-17)

The DBA\_DV\_MAC\_POLICY data dictionary view lists the factors that are associated with Oracle Label Security policies.

[DBA\\_DV\\_MAINTENANCE\\_AUTH View](#) (page 25-18)

The DBA\_DV\_MAINTENANCE\_AUTH data dictionary view provides information about the configuration of Oracle Database Vault authorizations to use Information Life Management (ILM) features.

[DBA\\_DV\\_ORADEBUG View](#) (page 25-18)

The DBA\_DV\_ORADEBUG data dictionary view indicates whether users can use the ORADEBUG utility in an Oracle Database Vault environment.

[DBA\\_DV\\_PATCH\\_ADMIN\\_AUDIT View](#) (page 25-19)

The DBA\_DV\_PATCH\_ADMIN\_AUDIT data dictionary view indicates if auditing has been enabled or disabled for the user who has been granted the DV\_ADMIN\_PATCH role.

[DBA\\_DV\\_POLICY View](#) (page 25-19)

The DBA\_DV\_POLICY data dictionary view lists the Oracle Database Vault policies that were created in the current database instance.

[DBA\\_DV\\_POLICY\\_LABEL View](#) (page 25-20)

The DBA\_DV\_POLICY\_LABEL data dictionary view lists the Oracle Label Security label for each factor identifier in the DBA\_DV\_IDENTITY view for each policy.

[DBA\\_DV\\_POLICY\\_OBJECT View](#) (page 25-21)

The DBA\_DV\_POLICY\_OBJECT data dictionary view lists information about the objects that are protected by Oracle Database Vault policies in the current database instance.

[DBA\\_DV\\_POLICY\\_OWNER View](#) (page 25-22)

The DBA\_DV\_POLICY\_OWNER data dictionary view lists the owners of Oracle Database Vault policies that were created in the current database instance.

[DBA\\_DV\\_PROXY\\_AUTH View](#) (page 25-23)

The DBA\_DV\_PROXY\_AUTH data dictionary view lists the proxy users and schemas that were specified by the DBMS\_MACADM.AUTHORIZE\_PROXY\_USER procedure.

---

[DBA\\_DV\\_PUB\\_PRIVS View](#) (page 25-23)

The DBA\_DV\_PUB\_PRIVS data dictionary view lists data reflected in the Oracle Database Vault privilege management reports used in Oracle Database Vault Administrator.

[DBA\\_DV\\_REALM View](#) (page 25-24)

The DBA\_DV\_REALM data dictionary view lists the realms created in the current database instance.

[DBA\\_DV\\_REALM\\_AUTH View](#) (page 25-25)

The DBA\_DV\_REALM\_AUTH data dictionary view lists database user account or role authorization (GRANTEE) who can access realm objects.

[DBA\\_DV\\_REALM\\_OBJECT View](#) (page 25-27)

The DBA\_DV\_REALM\_OBJECT data dictionary view lists the database schemas, or subsets of schemas, that are secured by the realms.

[DBA\\_DV\\_ROLE View](#) (page 25-28)

The DBA\_DV\_ROLE data dictionary view lists the Oracle Database Vault secure application roles used in privilege management.

[DBA\\_DV\\_RULE View](#) (page 25-29)

The DBA\_DV\_RULE data dictionary view lists the rules that have been defined.

[DBA\\_DV\\_RULE\\_SET View](#) (page 25-30)

The DBA\_DV\_RULE\_SET data dictionary view lists the rules sets that have been created.

[DBA\\_DV\\_RULE\\_SET\\_RULE View](#) (page 25-32)

The DBA\_DV\_RULE\_SET\_RULE data dictionary view lists rules that are associated with existing rule sets.

[DBA\\_DV\\_STATUS View](#) (page 25-33)

The DBA\_DV\_STATUS data dictionary view shows the status of Oracle Database Vault being enabled and configured.

[DBA\\_DV\\_SIMULATION\\_LOG View](#) (page 25-34)

The DBA\_DV\_SIMULATION\_LOG data dictionary view captures simulation log information for realms and command rules that have had simulation mode enabled.

[DBA\\_DV\\_TTS\\_AUTH View](#) (page 25-36)

The DBA\_DV\_TTS\_AUTH data dictionary view lists users who have been granted authorization through the DBMS\_MACADM.AUTHORIZE\_TTS\_USER procedure to perform Oracle Data Pump transportable operations.

[DBA\\_DV\\_USER\\_PRIVS View](#) (page 25-36)

The DBA\_DV\_USER\_PRIVS data dictionary view lists the privileges for a database user account excluding privileges granted through the PUBLIC role.

[DBA\\_DV\\_USER\\_PRIVS\\_ALL View](#) (page 25-37)

The DBA\_DV\_USER\_PRIVS\_ALL data dictionary view lists the privileges for a database account including privileges granted through PUBLIC.

---

[DVSYS.DV\\$CONFIGURATION\\_AUDIT View](#) (page 25-38)

The `DVSYS.DV$CONFIGURATION_AUDIT` data dictionary view captures `DVSYS.AUDIT_TRAIL$` table audit trail records.

[DVSYS.DV\\$ENFORCEMENT\\_AUDIT View](#) (page 25-43)

The `DVSYS.DV$ENFORCEMENT_AUDIT` data dictionary view provides information about enforcement-related audits from the `DVSYS.AUDIT_TRAIL$` table.

[DVSYS.DV\\$REALM View](#) (page 25-46)

The `DVSYS.DV$REALM` data dictionary view describes settings that were used to create Oracle Database Vault realms, such as which audit options have been assigned or whether the realm is a mandatory realm.

[DVSYS.POLICY\\_OWNER\\_COMMAND\\_RULE View](#) (page 25-48)

The `DVSYS.POLICY_OWNER_COMMAND_RULE` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the command rules that have been associated with Database Vault policies.

[DVSYS.POLICY\\_OWNER\\_POLICY View](#) (page 25-49)

The `DVSYS.POLICY_OWNER_POLICY` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information such as the names, descriptions, and states of existing policies in the current database instance, including policies created by other policy owners.

[DVSYS.POLICY\\_OWNER\\_REALM View](#) (page 25-49)

The `POLICY_OWNER_REALM` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the realms that have been associated with Database Vault policies.

[DVSYS.POLICY\\_OWNER\\_REALM\\_AUTH View](#) (page 25-51)

The `DVSYS.POLICY_OWNER_REALM_AUTH` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the authorization that was granted to realms that have been associated with Database Vault policies.

[DVSYS.POLICY\\_OWNER\\_REALM\\_OBJECT View](#) (page 25-52)

The `DVSYS.POLICY_OWNER_REALM_OBJECT` data dictionary view enables users to find information about the objects that have been added to realms that are associated with Database Vault policies, such as. Only users who have been granted the `DV_POLICY_OWNER` role can query this view.

[DVSYS.POLICY\\_OWNER\\_RULE View](#) (page 25-53)

The `DVSYS.POLICY_OWNER_RULE` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the rules that have been associated with rule sets in Database Vault policies, such as the rule name and its expression. Only users who have been granted the `DV_POLICY_OWNER` role can query this view.

[DVSYS.POLICY\\_OWNER\\_RULE\\_SET View](#) (page 25-54)

The `DVSYS.POLICY_OWNER_RULE_SET` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the rule sets that have been associated with Database Vault policies.

[DVSYS.POLICY\\_OWNER\\_RULE\\_SET\\_RULE View](#) (page 25-56)

The `DVSYS.POLICY_OWNER_RULE_SET_RULE` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the rule sets that contain rules used in Database Vault policies.

[SYS.DV\\$CONFIGURATION\\_AUDIT View](#) (page 25-56)

The `SYS.DV$CONFIGURATION_AUDIT` view is almost the same as the `DVSYS.DV$CONFIGURATION_AUDIT` view except that it captures unified audit trail Database Vault audit records.

[SYS.DV\\$ENFORCEMENT\\_AUDIT View](#) (page 25-57)

The `SYS.DV$ENFORCEMENT_AUDIT` view is almost the same as the `DVSYS.DV$ENFORCEMENT_AUDIT` view except that it captures unified audit trail Database Vault audit records.

## 25.1 About the Oracle Database Vault Data Dictionary Views

Oracle Database Vault provides a set of DBA-style data dictionary views that can be accessed through the `DV_SECANALYST` role or the `DV_ADMIN` role.

These views provide access to the various underlying Oracle Database Vault tables in the `DVSYS` and `LBACSYS` schemas without exposing the primary and foreign key columns that may be present. These views are intended for the database administrative user to report on the state of the Oracle Database Vault configuration without having to perform the joins required to get the labels for codes that are stored in the core tables or from the related tables.

---



---

**See Also:**

[Oracle Database Vault Reports](#) (page 27-1) if you are interested in running reports on Oracle Database Vault

---



---

## 25.2 CDB\_DV\_STATUS View

The `CDB_DV_STATUS` data dictionary view shows the status of Oracle Database Vault being enabled and configured in a multitenant environment.

Only Oracle Database administrative users, such users who have been granted the `DBA` role, can query this view. Database Vault administrators do not have access to this view.

For example:

```
SELECT * FROM CDB_DV_STATUS;
```

Output similar to the following appears:

NAME	STATUS	CON_ID
DV_CONFIGURE_STATUS	TRUE	0
DV_ENABLE_STATUS	TRUE	0

### Related Views

- [DBA\\_DV\\_STATUS View](#) (page 25-33)

Column	Datatype	Null	Description
NAME	VARCHAR2 ( 19 )	NOT NULL	Shows either of the following settings: <ul style="list-style-type: none"> <li>DV_CONFIGURE_STATUS shows whether Oracle Database Vault has been configured, that is, with the CONFIGURE_DV procedure.</li> <li>DV_ENABLE_STATUS shows whether Oracle Database Vault has been enabled, that is, with the DBMS_MACADM.ENABLE_DV procedure.</li> </ul>
STATUS	VARCHAR2 ( 64 )	NOT NULL	TRUE means that Oracle Database Vault is configured or enabled; FALSE means that it is not.
CON_ID	NUMBER	NOT NULL	The identification number of the container in which Oracle Database Vault is used

## 25.3 DBA\_DV\_CODE View

The DBA\_DV\_CODE data dictionary view lists generic lookup codes for the user interface, error messages, and constraint checking.

These codes are used for the user interface, views, and for validating input in a translatable fashion.

For example:

```
SELECT CODE, VALUE FROM DBA_DV_CODE WHERE CODE_GROUP = 'BOOLEAN';
```

Output similar to the following appears:

```
CODE    VALUE
-----
Y       True
N       False
```

Column	Datatype	Null	Description
CODE_GROUP	VARCHAR ( 128 )	NOT NULL	Displays one of the code groups that are listed in <a href="#">Table 25-1</a> (page 25-7)
CODE	VARCHAR ( 128 )	NOT NULL	Boolean code used; either Y (Yes) or N (No).
VALUE	VARCHAR ( 4000 )	NULL	Boolean value used; either True if the Boolean code is Y or False if the Boolean code is N.

Column	Datatype	Null	Description
LANGUAGE	VARCHAR ( 3 )	NOT NULL	Language for this installation of Oracle Database Vault. Supported languages are as follows: <ul style="list-style-type: none"> <li>• en: English</li> <li>• de: German</li> <li>• es: Spanish</li> <li>• fr: French</li> <li>• it: Italian</li> <li>• ja: Japanese</li> <li>• ko: Korean</li> <li>• pt_BR: Brazilian Portuguese</li> <li>• zh_CN: Simplified Chinese</li> <li>• zh_TW: Traditional Chinese</li> </ul>
DESCRIPTION	VARCHAR (1024)	NULL	Brief description of the code group.

[Table 25-1](#) (page 25-7) describes the possible values from the CODE\_GROUP column in the DBA\_DV\_CODE data dictionary view.

**Table 25-1 DBA\_DV\_CODE View CODE\_GROUP Values**

CODE_GROUP Name	Description
AUDIT_EVENTS	Contains the action numbers and action names that are used for the custom event audit trail records
BOOLEAN	A simple Yes or No or True or False lookup
DB_OBJECT_TYPE	The database object types that can be used for realm objects and command authorizations
SQL_CMDS	The DDL commands that can be protected through command rules
FACTOR_AUDIT	The auditing options for factor retrieval processing
FACTOR_EVALUATE	The evaluation options (by session or by access) for factor retrieval
FACTOR_FAIL	The options for propagating errors when a factor retrieval method fails
FACTOR_IDENTIFY	The options for determining how a factor identifier is resolved (for example, by method or by factors)
FACTOR_LABEL	The options for determining how a factor identifier is labeled in the session establishment phase
LABEL_ALG	The algorithms that can be used to determine the maximum session label for a database session for each policy. See <a href="#">Table 20-2</a> (page 20-2) for a listing of the Oracle Label Security merge algorithm codes.
OPERATORS	The Boolean operators that can be used for identity maps
REALM_AUDIT	The options for auditing realm access or realm violations

**Table 25-1 (Cont.) DBA\_DV\_CODE View CODE\_GROUP Values**

CODE_GROUP Name	Description
REALM_OPTION	The options for ownership of a realm
RULESET_AUDIT	The options for auditing rule set execution or rule set errors
RULESET_EVALUATE	The options for determining the success or failure of a rule set based on all associated rules being true or any associated rule being true
RULESET_EVENT	The options to invoke a custom event handler when a rule set evaluates to Succeeds or Fails
RULESET_FAIL	The options to determine the run-time visibility of a rule set failing

## 25.4 DBA\_DV\_COMMAND\_RULE View

The DBA\_DV\_COMMAND\_RULE data dictionary view lists the SQL statements that are protected by command rules.

See [Configuring Command Rules](#) (page 7-1), for more information about command rules.

For example:

```
SELECT COMMAND, RULE_SET_NAME FROM DBA_DV_COMMAND_RULE;
```

Output similar to the following appears:

```
COMMAND          RULE_SET_NAME
-----
GRANT             Can Grant VPD Administration
REVOKE           Can Grant VPD Administration
ALTER SYSTEM     Allow System Parameters
ALTER USER       Can Maintain Own Account
CREATE USER       Can Maintain Account/Profiles
DROP USER        Can Maintain Account/Profiles
CREATE PROFILE    Can Maintain Account/Profiles
DROP PROFILE     Can Maintain Account/Profiles
ALTER PROFILE    Can Maintain Account/Profiles
```

Column	Datatype	Null	Description
COMMAND	VARCHAR(128)	NOT NULL	Name of the command rule. For a list of default command rules, see <a href="#">Default Command Rules</a> (page 7-7).
CLAUSE_NAME	VARCHAR(100)	NOT NULL	A clause from either the ALTER SYSTEM or ALTER SESSION SQL statement, which was used to create the command rule. For example, you it could list the SET clause for the ALTER SESSION statement.  For a full list of possible clause values, see the following topics: <ul style="list-style-type: none"> <li><a href="#">Table 17-2</a> (page 17-4)</li> <li><a href="#">Table 17-3</a> (page 17-6)</li> </ul>



Column	Datatype	Null	Description
PARAMETER_NAME	VARCHAR(128)	NOT NULL	A parameter from the ALTER SYSTEM or ALTER SESSION command rule CLAUSE_NAME setting
EVENT_NAME	VARCHAR(128)	NOT NULL	An event that the ALTER SYSTEM or ALTER SESSION command rule defines
COMPONENT_NAME	VARCHAR(128)	NOT NULL	A component of the EVENT_NAME setting for the ALTER SYSTEM or ALTER SESSION command rule.
ACTION_NAME	VARCHAR(128)	NOT NULL	An action of the EVENT_NAME setting for the ALTER SYSTEM or ALTER SESSION command rule
RULE_SET_NAME	VARCHAR(128)	NOT NULL	Name of the rule set associated with this command rule.
OBJECT_OWNER	VARCHAR(128)	NOT NULL	The owner of the object that the command rule affects.
OBJECT_NAME	VARCHAR(128)	NOT NULL	The name of the database object the command rule affects (for example, a database table).
ENABLED	VARCHAR(1)	NOT NULL	Possible values are as follows: <ul style="list-style-type: none"> <li>Y indicates the command rule is enabled</li> <li>N indicates it is disabled</li> <li>S indicates it is in simulation mode</li> </ul>
PRIVILEGE_SCOPE	NUMBER	NOT NULL	Obsolete column
COMMON	VARCHAR(3)	NOT NULL	For a multitenant environment, indicates whether the command rule is local or common. Possible values are: <ul style="list-style-type: none"> <li>YES if the command rule is common</li> <li>NO if the command rule is local</li> </ul>
INHERITED	VARCHAR(3)	NOT NULL	Shows the inheritance status of the command rule, when the COMMON column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>YES means that the command rule was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>NO means that the command rule is a local object, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED value NO but a CDB root common command rule will have an INHERITED value of YES.</li> </ul>
ID#	NUMBER	NOT NULL	The ID number of the command rule, which is automatically generated when the command rule is created

Column	Datatype	Null	Description
ORACLE_SUPPLIED	VARCHAR(3)	NULL	Indicates whether the command rule is a default (that is, Oracle-supplied) command rule or a user-created command rule. Possible values are: <ul style="list-style-type: none"> <li>• YES if the command rule is a default command rule</li> <li>• NO if the command rule is a user-created command rule</li> </ul>

## 25.5 DBA\_DV\_DATAPUMP\_AUTH View

The DBA\_DV\_DATAPUMP\_AUTH data dictionary view lists the authorizations for using Oracle Data Pump in an Oracle Database Vault environment.

See [Using Oracle Data Pump with Oracle Database Vault](#) (page 13-5) for more information.

For example:

```
SELECT * FROM DBA_DV_DATAPUMP_AUTH WHERE GRANTEE = 'PRESTON';
```

Output similar to the following appears:

```
GRANTEE SCHEMA OBJECT
-----
PRESTON OE      ORDERS
```

Column	Datatype	Null	Description
GRANTEE	VARCHAR2(128)	NOT NULL	Name of the user who has been granted Data Pump authorization
SCHEMA	VARCHAR2(128)	NOT NULL	Name of the schema on which the user GRANTEE is authorized to perform Data Pump operations
OBJECT	VARCHAR2(128)	NOT NULL	Name of the object within the schema specified by the SCHEMA parameter on which the GRANTEE user has Data Pump authorization (such as a table)

## 25.6 DBA\_DV\_DDL\_AUTH View

The DBA\_DV\_DDL data dictionary view lists the users and schemas that were specified by the DBMS\_MACADM.AUTHORIZE\_DDL procedure.

This procedure grants a user authorization to execute Data Definition Language (DDL) statements.

For example:

```
SELECT * FROM DBA_DV_DDL_AUTH WHERE GRANTEE = 'psmith';
```

Output similar to the following appears:

```
GRANTEE SCHEMA
-----
PSMITH  HR
```

Column	Datatype	Null	Description
GRANTEE	VARCHAR2(128)	NOT NULL	Name of the user who has been granted DDL authorization
SCHEMA	VARCHAR2(128)	NOT NULL	Name of the schema on which the user GRANTEE is authorized to perform DDL operations

---

**See Also:**

- [AUTHORIZE\\_DDL Procedure](#) (page 22-4)
  - [UNAUTHORIZE\\_DDL Procedure](#) (page 22-9)
- 

## 25.7 DBA\_DV\_DICTIONARY\_ACCTS View

The DBA\_DV\_DICTIONARY\_ACCTS data dictionary view indicates whether users can directly log into the DVSYS and DVF schema accounts.

For example:

```
SELECT * FROM DBA_DV_DICTIONARY_ACCTS;
```

Output similar to the following appears:

```
STATE
-----
ENABLED
```

Column	Datatype	Null	Description
STATE	VARCHAR2(8)	NOT NULL	Describes whether users can log directly into the DVSYS and DVF schemas. Possible values are: <ul style="list-style-type: none"> <li>• ENABLED means that users can log directly into the DVSYS and DVF schemas</li> <li>• DISABLED means that users cannot log directly into the DVSYS and DVF schemas</li> </ul>

## 25.8 DBA\_DV\_FACTOR View

The DBA\_DV\_FACTOR data dictionary view lists the existing factors in the current database instance.

For example:

```
SELECT NAME, GET_EXPR FROM DBA_DV_FACTOR WHERE NAME = 'Session_User';
```

Output similar to the following appears:

```
NAME          GET_EXPR
-----
Session_User  UPPER(SYS_CONTEXT('USERENV', 'SESSION_USER'))
```

**Related Views**

- [DBA\\_DV\\_FACTOR\\_LINK View](#) (page 25-14)
- [View](#) (page 25-13)

Column	Datatype	Null	Description
NAME	VARCHAR2 ( 128 )	NOT NULL	Name of the factor. See <a href="#">Default Factors</a> (page 8-2) for a list of default factors.
DESCRIPTION	VARCHAR2 ( 4000 )	NULL	Description of the factor.
FACTOR_TYPE_NAME	VARCHAR2 ( 128 )	NOT NULL	Category of the factor, which is used to classify the purpose of the factor.
ASSIGN_RULE_SET_NAME	VARCHAR2 ( 128 )	NULL	Rule set used to control the identify of the factor.
GET_EXPR	VARCHAR2 ( 1024 )	NULL	PL/SQL expression that retrieves the identity of a factor.
VALIDATE_EXPR	VARCHAR2 ( 1024 )	NULL	PL/SQL expression used to validate the identify of the factor. It returns a Boolean value.
IDENTIFIED_BY	NUMBER	NOT NULL	Determines the identity of a factor, based on the expression listed in the GET_EXPR column. Possible values are: <ul style="list-style-type: none"> <li>• 0: By constant</li> <li>• 1: By method</li> <li>• 2: By factors</li> </ul>
IDENTIFIED_BY_MEANING	VARCHAR2 ( 4000 )	NULL	Provides a text description for the corresponding value in the IDENTIFIED_BY column. Possible values are: <ul style="list-style-type: none"> <li>• By Constant: If IDENTIFIED_COLUMN is 0</li> <li>• By Method: If IDENTIFIED_COLUMN is 1</li> <li>• By Factors: If IDENTIFIED_COLUMN is 2</li> </ul>
LABELED_BY	NUMBER	NOT NULL	Determines the labeling the factor: <ul style="list-style-type: none"> <li>• 0: Labels the identities for the factor directly from the labels associated with an Oracle Label Security policy</li> <li>• 1: Derives the factor identity label from the labels of its child factor identities.</li> </ul>
LABELED_BY_MEANING	VARCHAR2 ( 4000 )	NULL	Provides a text description for the corresponding value in the LABELED_BY column. Possible values are: <ul style="list-style-type: none"> <li>• By Self: If LABELED_BY column is 0</li> <li>• By Factors: If LABELED_BY column is 1</li> </ul>

Column	Datatype	Null	Description
EVAL_OPTIONS	NUMBER	NOT NULL	Determines how the factor is evaluated when the user logs on: <ul style="list-style-type: none"> <li>0: When the database session is created</li> <li>1: Each time the factor is accessed</li> <li>2: On start-up</li> </ul>
EVAL_OPTIONS_MEANING	VARCHAR2(4000)	NULL	Provides a text description for the corresponding value in the EVAL_OPTIONS column. Possible values are: <ul style="list-style-type: none"> <li>For Session: If EVAL_OPTIONS is 0</li> <li>By Access: If EVAL_OPTIONS is 1</li> <li>On Startup: If EVAL_OPTIONS is 2</li> </ul>
AUDIT_OPTIONS	NUMBER	NOT NULL	Option for auditing the factor if you want to generate a custom Oracle Database Vault audit record. Possible values are: <ul style="list-style-type: none"> <li>0: No auditing set</li> <li>1: Always audits</li> <li>2: Audits if get_expr returns an error</li> <li>4: Audits if get_expr is null</li> <li>8: Audits if the validation procedure returns an error</li> <li>16: Audits if the validation procedure is false</li> <li>32: Audits if there is no trust level set</li> <li>64: Audits if the trust level is negative.</li> </ul>
FAIL_OPTIONS	NUMBER	NOT NULL	Options for reporting factor errors: <ul style="list-style-type: none"> <li>1: Shows an error message.</li> <li>2: Does not show an error message.</li> </ul>
FAIL_OPTIONS_MEANING	VARCHAR2(4000)	NULL	Provides a text description for the corresponding value in the FAIL_OPTIONS column. Possible values are: <ul style="list-style-type: none"> <li>Show Error Message</li> <li>Do Not Show Error Message:</li> </ul>
ID#	NUMBER	NOT NULL	The ID number of the factor, which is automatically generated when the factor is created
ORACLE_SUPPLIED	VARCHAR(3)	NOT NULL	Indicates whether the factor is a default (that is, Oracle-supplied) factor or a user-created factor. Possible values are: <ul style="list-style-type: none"> <li>YES if the factor is a default factor</li> <li>NO if the factor is a user-created factor</li> </ul>

## 25.9 DBA\_DV\_FACTOR\_TYPE View

The DBA\_DV\_FACTOR\_TYPE data dictionary view lists the names and descriptions of factor types used in the system.

For example:

```
SELECT * FROM DBA_DV_FACTOR_TYPE WHERE NAME = 'Hostname';
```

Output similar to the following appears:

```
NAME          DESCRIPTION
-----
```

```
Time          Time-based factor
```

### Related Views

- [DBA\\_DV\\_FACTOR View](#) (page 25-11)
- [DBA\\_DV\\_FACTOR\\_LINK View](#) (page 25-14)

Column	Datatype	Null	Description
NAME	VARCHAR(128)	NOT NULL	Name of the factor type.
DESCRIPTION	VARCHAR(1024 )	NULL	Description of the factor type.

## 25.10 DBA\_DV\_FACTOR\_LINK View

The DBA\_DV\_FACTOR\_LINK data dictionary view shows the relationships of each factor whose identity is determined by the association of child factors.

This view contains one entry for each parent factor and child factor. You can use this view to resolve the relationships from the factor links to identity maps.

For example:

```
SELECT PARENT_FACTOR_NAME, CHILD_FACTOR_NAME FROM DBA_DV_FACTOR_LINK;
```

Output similar to the following appears:

```
PARENT_FACTOR_NAME          CHILD_FACTOR_NAME
-----
```

Domain	Database_Instance
Domain	Database_IP
Domain	Database_Hostname

### Related Views

- [DBA\\_DV\\_FACTOR View](#) (page 25-11)
- [DBA\\_DV\\_FACTOR\\_TYPE View](#) (page 25-13)

Column	Datatype	Null	Description
PARENT_FACTOR_NAME	VARCHAR(128 )	NOT NULL	Name of the parent factor
CHILD_FACTOR_NAME	VARCHAR(128 )	NOT NULL	Name of the child factor of the parent factor

Column	Datatype	Null	Description
LABEL_IND	VARCHAR(1)	NOT NULL	Indicates whether the child factor that is linked to the parent factor contributes to the label of the parent factor in an Oracle Label Security integration. Possible values are: <ul style="list-style-type: none"> <li>Y (for Yes)</li> <li>N (for No)</li> </ul>

## 25.11 DBA\_DV\_IDENTITY View

The DBA\_DV\_IDENTITY data dictionary view lists the identities for each factor.

For example:

```
SELECT * FROM DBA_DV_IDENTITY WHERE VALUE = 'GLOBAL SHARED';
```

Output similar to the following appears, assuming you have created only one factor identity:

```

FACTOR_NAME          VALUE          TRUST_LEVEL
-----
Identification_Type  GLOBAL SHARED  1

```

### Related Views

- [DBA\\_DV\\_FACTOR View](#) (page 25-11)
- [DBA\\_DV\\_IDENTITY\\_MAP View](#) (page 25-15)

Column	Datatype	Null	Description
FACTOR_NAME	VARCHAR(128)	NOT NULL	Name of the factor.
VALUE	VARCHAR(1024)	NOT NULL	Value of the factor.
TRUST_LEVEL	NUMBER	NOT NULL	Number that indicates the magnitude of trust relative to other identities for the same factor.

## 25.12 DBA\_DV\_IDENTITY\_MAP View

The DBA\_DV\_IDENTITY\_MAP data dictionary view lists the mappings for each factor identity.

The view includes mapping factors that are identified by other factors to combinations of parent-child factor links. For each factor, the maps are joined by the OR operation, and for different factors, the maps are joined by the AND operation.

You can use this view to resolve the identity for factors that are identified by other factors (for example, a domain) or for factors that have continuous domains (for example, Age or Temperature).

For example:

```
SELECT FACTOR_NAME, IDENTITY_VALUE FROM DBA_DV_IDENTITY_MAP;
```

Output similar to the following appears:

```

FACTOR_NAME      IDENTITY_VALUE
-----
Sector2_Program  Accounting-Sensitive

```

### Related Views

- [DBA\\_DV\\_FACTOR View](#) (page 25-11)
- [DBA\\_DV\\_IDENTITY View](#) (page 25-15)

Column	Datatype	Null	Description
FACTOR_NAME	VARCHAR(128)	NOT NULL	Factor the identity map is for.
IDENTITY_VALUE	VARCHAR(1024)	NOT NULL	Value the factor assumes if the identity map evaluates to TRUE.
OPERATION_CODE	VARCHAR(128)	NOT NULL	Descriptive name of the operation in the OPERATION_VALUE column.
OPERATION_VALUE	VARCHAR(4000)	NULL	Relational operator for the identity map (for example, <, >, =, and so on).
OPERAND1	VARCHAR(1024)	NULL	Left operand for the relational operator; refers to the low value you enter.
OPERAND2	VARCHAR(1024)	NULL	Right operand for the relational operator; refers to the high value you enter.
PARENT_FACTOR_NAME	VARCHAR(128)	NULL	The parent factor link to which the map is related.
CHILD_FACTOR_NAME	VARCHAR(128)	NULL	The child factor link to which the map is related.
LABEL_IND	VARCHAR(1)	NULL	Indicates whether the child factor being linked to the parent factor contributes to the label of the parent factor in an Oracle Label Security integration. Possible values are: <ul style="list-style-type: none"> <li>• Y (for Yes)</li> <li>• N (for No)</li> </ul>

## 25.13 DBA\_DV\_JOB\_AUTH View

The DBA\_DV\_JOB\_AUTH data dictionary view lists the authorizations for using Oracle Scheduler in an Oracle Database Vault environment.

For example:

```
SELECT * FROM DBA_DV_JOB_AUTH WHERE GRANTEE = 'PRESTON';
```

Output similar to the following appears:

```

GRANTEE SCHEMA
-----
PRESTON OE

```

Column	Datatype	Null	Description
GRANTEE	VARCHAR2(128)	NOT NULL	Name of the user who has been granted Oracle Scheduler authorization



Column	Datatype	Null	Description
SCHEMA	VARCHAR2(128)	NOT NULL	Name of the schema on which the user GRANTEE is authorized to perform Oracle Scheduler operations

## 25.14 DBA\_DV\_MAC\_POLICY View

The DBA\_DV\_MAC\_POLICY data dictionary view lists the Oracle Label Security policies defined for use with Oracle Database Vault.

For example:

```
SELECT POLICY_NAME, ALGORITHM_CODE, ALGORITHM_MEANING
FROM DBA_DV_MAC_POLICY;
```

Output similar to the following appears:

```
POLICY_NAME      ALGORITHM_CODE      ALGORITHM_MEANING
-----
ACCESS_DATA      LUI                  Minimum Level/Union/Intersection
```

### Related Views

- [DBA\\_DV\\_MAC\\_POLICY\\_FACTOR View](#) (page 25-17)
- [DBA\\_DV\\_POLICY\\_LABEL View](#) (page 25-20)

Column	Datatype	Null	Description
POLICY_NAME	VARCHAR(128)	NOT NULL	Name of the policy.
ALGORITHM_CODE	VARCHAR(128)	NOT NULL	Merge algorithm code used for the policy. See <a href="#">Table 20-2</a> (page 20-2) for a listing of algorithm codes.
ALGORITHM_MEANING	VARCHAR(4000)	NULL	Provides a text description for the corresponding value in the ALGORITHM_CODE column. See <a href="#">Table 20-2</a> (page 20-2) for a listing of algorithm code descriptions.
ERROR_LABEL	VARCHAR(4000)	NULL	Label specified for initialization errors, to be set when a configuration error or run-time error occurs during session initialization.

## 25.15 DBA\_DV\_MAC\_POLICY\_FACTOR View

The DBA\_DV\_MAC\_POLICY\_FACTOR data dictionary view lists the factors that are associated with Oracle Label Security policies.

You can use this view to determine what factors contribute to the maximum session label for each policy using the DBA\_DV\_MAC\_POLICY view.

For example:

```
SELECT * FROM DBA_DV_MAC_POLICY_FACTOR;
```

Output similar to the following appears:

```

FACTOR_NAME      MAC_POLICY_NAME
-----
App_Host_Name    Access Locations

```

### Related Views

- [DBA\\_DV\\_MAC\\_POLICY View](#) (page 25-17)
- [DBA\\_DV\\_POLICY\\_LABEL View](#) (page 25-20)

Column	Datatype	Null	Description
FACTOR_NAME	VARCHAR(128)	NOT NULL	Name of the factor
MAC_POLICY_NAME	VARCHAR(128)	NOT NULL	Name of the Oracle Label Security policy associated with this facto

## 25.16 DBA\_DV\_MAINTENANCE\_AUTH View

The DBA\_DV\_MAINTENANCE\_AUTH data dictionary view provides information about the configuration of Oracle Database Vault authorizations to use Information Life Management (ILM) features.

For example:

```
SELECT GRANTEE, ACTION STATE FROM DBA_DV_MAINTENANCE_AUTH;
```

Output similar to the following appears:

```

GRANTEE          ACTION
-----
PSMITH           ILM

```

Column	Datatype	Null	Description
GRANTEE	VARCHAR(128)	NOT NULL	Name of the grantee
SCHEMA	VARCHAR(128)	NOT NULL	Schema name or % (for all schemas)
OBJECT	VARCHAR(128)	NOT NULL	Object name or % (for all objects in a schema)
OBJECT_TYPE	VARCHAR(30)	NOT NULL	Object type
ACTION	VARCHAR(30)	NOT NULL	Maintenance action ILM for ILM operations

## 25.17 DBA\_DV\_ORADEBUG View

The DBA\_DV\_ORADEBUG data dictionary view indicates whether users can use the ORADEBUG utility in an Oracle Database Vault environment.

For example:

```
SELECT * FROM DBA_DV_ORADEBUG;
```

Output similar to the following appears:

```

STATE
-----
DISABLED

```

Column	Datatype	Null	Description
STATE	VARCHAR2(8)	NOT NULL	Describes whether the ORADEBUG utility can be used in a Database Vault-enabled environment. Possible values are: <ul style="list-style-type: none"> <li>ENABLED means that users can run the ORADEBUG utility</li> <li>DISABLED means that users cannot run the ORADEBUG utility</li> </ul>

## 25.18 DBA\_DV\_PATCH\_ADMIN\_AUDIT View

The DBA\_DV\_PATCH\_ADMIN\_AUDIT data dictionary view indicates if auditing has been enabled or disabled for the user who has been granted the DV\_ADMIN\_PATCH role.

The DBMS\_MACADM.ENABLE\_DV\_PATCH\_ADMIN\_AUDIT procedure enables this type of auditing.

For example:

```
SELECT * FROM DBA_DV_PATCH_ADMIN_AUDIT;
```

Output similar to the following appears:

```
STATE
-----
DISABLED
```

Column	Datatype	Null	Description
STATE	VARCHAR2(8)	NOT NULL	Describes whether auditing has been enabled or disabled for the DV_ADMIN_PATCH role user. Possible values are: <ul style="list-style-type: none"> <li>ENABLED means that the auditing has been enabled</li> <li>DISABLED means that the auditing has been disabled</li> </ul>

---

### See Also:

- [ENABLE\\_DV\\_PATCH\\_ADMIN\\_AUDIT Procedure](#) (page 22-16)
  - [DISABLE\\_DV\\_PATCH\\_ADMIN\\_AUDIT Procedure](#) (page 22-14)
- 

## 25.19 DBA\_DV\_POLICY View

The DBA\_DV\_POLICY data dictionary view lists the Oracle Database Vault policies that were created in the current database instance.

For example:

```
SELECT POLICY_NAME, STATE FROM DBA_DV_POLICY
WHERE STATE = 'ENABLED';
```

Output similar to the following appears:

```
POLICY_NAME          STATE
-----
```

Oracle Account Management Controls ENABLED  
 Oracle System Protection Controls ENABLED

### Related Views

- [DBA\\_DV\\_POLICY\\_OWNER View](#) (page 25-22)
- [DBA\\_DV\\_POLICY\\_OBJECT View](#) (page 25-21)
- [DBA\\_DV\\_SIMULATION\\_LOG View](#) (page 25-34)
- [DVSYS.POLICY\\_OWNER\\_POLICY View](#) (page 25-49)

Column	Datatype	Null	Description
POLICY_NAME	VARCHAR(128)	NOT NULL	Names of the Oracle Database Vault policies that have been created. See <a href="#">Default Oracle Database Vault Policies</a> (page 10-3) for a listing of default policies.
DESCRIPTION	VARCHAR(1024)	NULL	Description of the policy that was created
STATE	VARCHAR(8)	NULL	Specifies whether the policy is enabled. Possible values are: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> <li>• SIMULATION</li> </ul>
ID#	VARCHAR(1)	NOT NULL	Is a system-generated ID that was assigned to the policy when the policy was created
ORACLE_SUPPLIE D	VARCHAR(3)	NULL	Indicates whether the policy is a default Oracle Database Vault policy

## 25.20 DBA\_DV\_POLICY\_LABEL View

The DBA\_DV\_POLICY\_LABEL data dictionary view lists the Oracle Label Security label for each factor identifier in the DBA\_DV\_IDENTITY view for each policy.

For example:

```
SELECT * FROM DBA_DV_POLICY_LABEL;
```

Output similar to the following appears:

```
IDENTITY_VALUE  FACTOR_NAME      POLICY_NAME      LABEL
-----
App_Host_Name   Sect2_Fin_Apps   Access Locations Sensitive
```

### Related Views

- [DBA\\_DV\\_MAC\\_POLICY View](#) (page 25-17)
- [DBA\\_DV\\_MAC\\_POLICY\\_FACTOR View](#) (page 25-17)

Column	Datatype	Null	Description
IDENTITY_VALUE	VARCHAR(1024)	NOT NULL	Name of the factor identifier.
FACTOR_NAME	VARCHAR(128)	NOT NULL	Name of the factor associated with the factor identifier.

Column	Datatype	Null	Description
POLICY_NAME	VARCHAR(128)	NOT NULL	Name of the Oracle Label Security policy associated with this factor.
LABEL	VARCHAR(4000)	NOT NULL	Name of the Oracle Label Security label associated with the policy.

## 25.21 DBA\_DV\_POLICY\_OBJECT View

The `DBA_DV_POLICY_OBJECT` data dictionary view lists information about the objects that are protected by Oracle Database Vault policies in the current database instance.

For example:

```
SELECT POLICY_NAME, OBJECT_TYPE FROM DBA_DV_POLICY_OBJECT WHERE POLICY_NAME LIKE
'%Protection Controls';
```

Output similar to the following appears:

```
POLICY_NAME                                OBJECT_TYPE
-----
Oracle System Protection Controls    REALM
```

### Related Views

- [DBA\\_DV\\_POLICY View](#) (page 25-19)
- [DBA\\_DV\\_POLICY\\_OWNER View](#) (page 25-22)

Column	Datatype	Null	Description
POLICY_NAME	VARCHAR(128)	NOT NULL	Names of the Oracle Database Vault policies that have been created. See <a href="#">Default Oracle Database Vault Policies</a> (page 10-3) for a listing of default policies.
OBJECT_TYPE	VARCHAR(12)	NULL	Type of object that is being protected, such as REALM
COMMAND	VARCHAR(128)	NULL	Name of the command rules that are protected by Database Vault policies
COMMAND_OBJ_OWNER	VARCHAR(128)	NULL	Names of object owners that are associated with Database Vault policies
COMMAND_OBJ_NAME	VARCHAR(128)	NULL	Names of objects that are associated with Database Vault policies
COMMAND_CLAUSE	VARCHAR(100)	NULL	A clause from either the <code>ALTER SYSTEM</code> or <code>ALTER SESSION SQL</code> statement, which was used to create the command rule. For example, you it could list the <code>SET</code> clause for the <code>ALTER SESSION</code> statement. For a full list of possible clause values, see the following topics: <ul style="list-style-type: none"> <li>• <a href="#">Table 17-2</a> (page 17-4)</li> <li>• <a href="#">Table 17-3</a> (page 17-6)</li> </ul>

Column	Datatype	Null	Description
COMMAND_PARAMETER	VARCHAR(128)	NULL	A parameter from the ALTER SYSTEM or ALTER SESSION command rule CLAUSE_NAME setting
COMMAND_EVENT	VARCHAR(128)	NULL	An event that the ALTER SYSTEM or ALTER SESSION command rule defines
COMMAND_COMPONENT	VARCHAR(128)	NULL	A component of the EVENT_NAME setting for the ALTER SYSTEM or ALTER SESSION command rule
COMMAND_ACTION	VARCHAR(128)	NULL	An action of the EVENT_NAME setting for the ALTER SYSTEM or ALTER SESSION command rule
COMMON	VARCHAR(3)	NULL	For a multitenant environment, indicates if the policy objects are local or common. Possible values are: <ul style="list-style-type: none"> <li>YES if the policy objects are common</li> <li>NO if the policy objects are local</li> </ul>
INHERITED	VARCHAR(3)	NULL	Shows the inheritance status of the policy object, when the COMMON column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>YES means that the policy object was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>NO means that the policy object is a local object, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED value NO but a CDB root common command rule will have an INHERITED value of YES.</li> </ul>

## 25.22 DBA\_DV\_POLICY\_OWNER View

The DBA\_DV\_POLICY\_OWNER data dictionary view lists the owners of Oracle Database Vault policies that were created in the current database instance.

For example:

```
SELECT * FROM DBA_DV_POLICY_OWNER;
```

Output similar to the following appears:

```
POLICY_OWNER          POLICY_OWNER
-----
Oracle System Protection Controls  PSMITH
```

### Related Views

- [DBA\\_DV\\_POLICY View](#) (page 25-19)
- [DBA\\_DV\\_POLICY\\_OBJECT View](#) (page 25-21)

Column	Datatype	Null	Description
POLICY_NAME	VARCHAR(128)	NOT NULL	Names of the Oracle Database Vault policies that have been created. See <a href="#">Default Oracle Database Vault Policies</a> (page 10-3) for a listing of default policies.
POLICY_OWNER	VARCHAR(128)	NOT NULL	Names of users who have own Database Vault policies

## 25.23 DBA\_DV\_PROXY\_AUTH View

The DBA\_DV\_PROXY\_AUTH data dictionary view lists the proxy users and schemas that were specified by the DBMS\_MACADM.AUTHORIZE\_PROXY\_USER procedure.

This procedure grants a proxy user authorization to proxy other user accounts.

For example:

```
SELECT * FROM DBA_DV_DDL_AUTH WHERE GRANTEE = 'PRESTON';
```

Output similar to the following appears:

```
GRANTEE SCHEMA
-----
PRESTON DKENT
```

Column	Datatype	Null	Description
GRANTEE	VARCHAR2(128)	NOT NULL	Name of the proxy user
SCHEMA	VARCHAR2(128)	NOT NULL	Name of the schema that is proxied by the GRANTEE user.

### See Also:

- [AUTHORIZE\\_PROXY\\_USER Procedure](#) (page 22-6)
- [UNAUTHORIZE\\_PROXY\\_USER Procedure](#) (page 22-11)

## 25.24 DBA\_DV\_PUB\_PRIVS View

The DBA\_DV\_PUB\_PRIVS data dictionary view lists data reflected in the Oracle Database Vault privilege management reports used in Oracle Database Vault Administrator.

See also [Privilege Management - Summary Reports](#) (page 27-12).

For example:

```
SELECT USERNAME, ACCESS_TYPE FROM DBA_DV_PUB_PRIVS WHERE USERNAME = 'OE';
```

Output similar to the following appears:

```
USERNAME    ACCESS_TYPE
-----
OE          PUBLIC
```

**Related Views**

- [DBA\\_DV\\_USER\\_PRIVS View](#) (page 25-36)
- [DBA\\_DV\\_USER\\_PRIVS\\_ALL View](#) (page 25-37)
- [DBA\\_DV\\_ROLE View](#) (page 25-28)

Column	Datatype	Null	Description
USERNAME	VARCHAR(128)	NOT NULL	Database schema in the current database instance.access
ACCESS_TYPE	VARCHAR(128)	NULL	Access type granted to the user listed in the USERNAME column (for example, PUBLIC).
PRIVILEGE	VARCHAR(40)	NOT NULL	Privilege granted to the user listed in the USERNAME column.
OWNER	VARCHAR(128)	NOT NULL	Owner of the database schema to which the USERNAME user has been granted privileges.
OBJECT_NAME	VARCHAR(128)	NOT NULL	Name of the object within the schema listed in the OWNER column.

**25.25 DBA\_DV\_REALM View**

The DBA\_DV\_REALM data dictionary view lists the realms created in the current database instance.

For example:

```
SELECT NAME, AUDIT_OPTIONS, ENABLED, COMMON FROM DBA_DV_REALM
WHERE AUDIT_OPTIONS = '1';
```

Output similar to the following appears:

```
NAME                                AUDIT_OPTIONS  ENABLED  COMMON
-----
Performance Statistics Realm 1      Y        NO
```

**Related Views**

- [DBA\\_DV\\_REALM\\_AUTH View](#) (page 25-25)
- [DBA\\_DV\\_REALM\\_OBJECT View](#) (page 25-27)

Column	Datatype	Null	Description
NAME	VARCHAR(128)	NOT NULL	Names of the realms created. See <a href="#">Default Realms</a> (page 5-5) for a listing of default realms.
DESCRIPTION	VARCHAR(1024)	NOT NULL	Description of the realm created.



Column	Datatype	Null	Description
AUDIT_OPTIONS	NUMBER	NOT NULL	Specifies whether auditing is enabled. Possible values are: <ul style="list-style-type: none"> <li>• 0: No auditing for the realm.</li> <li>• 1: Creates an audit record when a realm violation occurs (for example, when an unauthorized user tries to modify an object that is protected by the realm).</li> <li>• 2: Creates an audit record for authorized activities on objects protected by the realm.</li> <li>• 3: Creates an audit record for both authorized and unauthorized activities on objects protected by the realm.</li> </ul>
REALM_TYPE	VARCHAR(9)	NULL	Type of realm: whether it is a regular realm or a mandatory realm. See <code>realm_type</code> in <a href="#">Table 15-9</a> (page 15-12) for a description of the possible values.
COMMON	VARCHAR(3)	NOT NULL	For a multitenant environment, indicates whether the realm is local or common. Possible values are: <ul style="list-style-type: none"> <li>• YES if the realm is common</li> <li>• NO if the realm is local</li> </ul>
INHERITED	VARCHAR(3)	NULL	Shows the inheritance status of the realm, when the <code>COMMON</code> column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>• YES means that the realm was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>• NO means that the realm is a local object, or it is common from that container. For example, in an application root, an application common realm will have an <code>INHERITED</code> value NO but a CDB root common command rule will have an <code>INHERITED</code> value of YES.</li> </ul>
ENABLED	VARCHAR(1)	NOT NULL	Possible values are as follows: <ul style="list-style-type: none"> <li>• Y indicates that realm checking is enabled</li> <li>• N indicates it is disabled</li> <li>• S indicates the realm is in simulation mode</li> </ul>
ID#	NUMBER	NOT NULL	The ID number of the realm, which is automatically generated when the realm is created
ORACLE_SUPPLIED	VARCHAR(3)	NOT NULL	Indicates whether the realm is a default (that is, Oracle-supplied) realm or a user-created command rule. Possible values are: <ul style="list-style-type: none"> <li>• YES if the realm is a default realm</li> <li>• NO if the realm is a user-created realm</li> </ul>

## 25.26 DBA\_DV\_REALM\_AUTH View

The `DBA_DV_REALM_AUTH` data dictionary view lists database user account or role authorization (`GRANTEE`) who can access realm objects.

See [About Realm Authorization](#) (page 5-13) for more information.

For example:

```
SELECT REALM_NAME, GRANTEE, AUTH_RULE_SET_NAME FROM DBA_DV_REALM_AUTH;
```

Output similar to the following appears:

```
REALM_NAME                GRANTEE  AUTH_RULE_SET_NAME
-----
Performance Statistics Realm  SYSADM  Check Conf Access
```

### Related Views

- [DBA\\_DV\\_REALM View](#) (page 25-24)
- [DBA\\_DV\\_REALM\\_OBJECT View](#) (page 25-27)

Column	Datatype	Null	Description
REALM_NAME	VARCHAR(128)	NULL	Name of the realm.
COMMON_REALM	VARCHAR(3)	NULL	For a multitenant environment, indicates whether the realm is local or common. Possible values are: <ul style="list-style-type: none"> <li>• YES if the realm is common</li> <li>• NO if the realm is local</li> </ul>
INHERITED_REALM	VARCHAR(3)	NULL	Shows the inheritance status of the realm, when the COMMON column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>• YES means that the realm was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>• NO means that the realm is a local object, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED value NO but a CDB root common command rule will have an INHERITED value of YES.</li> </ul>
GRANTEE	VARCHAR(128)	NOT NULL	User or role name to authorize as owner or participant.
AUTH_RULE_SET_NAME	VARCHAR(128)	NULL	Rule set to check before authorizing. If the rule set evaluates to TRUE, then the authorization is allowed.
AUTH_OPTIONS	VARCHAR(4000)	NULL	Type of realm authorization: either Participant or Owner.
COMMON_AUTH	VARCHAR(3)	NULL	For a multitenant environment, indicates whether the authorization to the common realm is local or common. Possible values are: <ul style="list-style-type: none"> <li>• YES if the authorization is common</li> <li>• NO if the authorization is local to this PDB</li> </ul>

Column	Datatype	Null	Description
INHERITED_AUTH	VARCHAR(3)	NULL	Shows the inheritance status of the realm authorization, when the COMMON_AUTH column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>YES means that the realm authorization was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was applied.</li> <li>NO means that the realm authorization is local, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED_AUTH value NO but a CDB root common command rule will have an INHERITED_AUTH value of YES.</li> </ul>

## 25.27 DBA\_DV\_REALM\_OBJECT View

The DBA\_DV\_REALM\_OBJECT data dictionary view lists the database schemas, or subsets of schemas, that are secured by the realms.

See [About Realm-Secured Objects](#) (page 5-12) for more information.

For example:

```
SELECT REALM_NAME, OWNER, OBJECT_NAME, COMMON_REALM FROM DBA_DV_REALM_OBJECT;
```

Output similar to the following appears:

```
REALM_NAME          OWNER  OBJECT_NAME  COMMON_REALM
-----
Performance Statistics Realm OE          ORDERS      NO
```

### Related Views

- [DBA\\_DV\\_REALM View](#) (page 25-24)
- [DBA\\_DV\\_REALM\\_AUTH View](#) (page 25-25)

Column	Datatype	Null	Description
REALM_NAME	VARCHAR(128)	NOT NULL	Name of the realm.
COMMON_REALM	VARCHAR(3)	NOT NULL	Indicates whether this realm is a common realm or a local realm. Possible values are: <ul style="list-style-type: none"> <li>YES if the realm is common</li> <li>NO if the realm is local</li> </ul>

Column	Datatype	Null	Description
INHERITED_REALM	VARCHAR(3)	NOT NULL	Shows the inheritance status of the realm when the COMMON column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>YES means that the realm was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>NO means that the realm is a local object, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED value NO but a CDB root common command rule will have an INHERITED value of YES.</li> </ul>
OWNER	VARCHAR(128)	NOT NULL	Database schema owner who owns the realm.
OBJECT_NAME	VARCHAR(128)	NOT NULL	Name of the object the realm protects.
OBJECT_TYPE	VARCHAR(32)	NOT NULL	Type of object the realm protects, such as a database table, view, index, or role.

## 25.28 DBA\_DV\_ROLE View

The DBA\_DV\_ROLE data dictionary view lists the Oracle Database Vault secure application roles used in privilege management.

For example:

```
SELECT ROLE, RULE_NAME FROM DBA_DV_ROLE;
```

Output similar to the following appears:

```
ROLE                RULE_NAME
-----
Sector2_APP_MGR     Check App2 Access
Sector2_APP_DBA     Check App2 Access
```

### Related Views

- [DBA\\_DV\\_PUB\\_PRIVS View](#) (page 25-23)
- [DBA\\_DV\\_USER\\_PRIVS View](#) (page 25-36)
- [DBA\\_DV\\_USER\\_PRIVS\\_ALL View](#) (page 25-37)

Column	Datatype	Null	Description
ROLE	VARCHAR(128)	NOT NULL	Name of the secure application role.
RULE_NAME	VARCHAR(128)	NOT NULL	Name of the rule set associated with the secure application role.

Column	Datatype	Null	Description
ENABLED	VARCHAR(1)	NOT NULL	Indicates whether the secure application role is enabled. Possible values are: <ul style="list-style-type: none"> <li>Y (Yes) if the role is enabled</li> <li>N (No) if the role is disabled</li> </ul>
ID#	NUMBER	NOT NULL	The ID number of the command rule, which is automatically generated when the command rule is created
ORACLE_SUPPLIED	VARCHAR(3)	NOT NULL	Indicates whether the command rule is a default (that is, Oracle-supplied) command rule or a user-created command rule. Possible values are: <ul style="list-style-type: none"> <li>YES if the command rule is a default command rule</li> <li>NO if the command rule is a user-created command rule</li> </ul>

## 25.29 DBA\_DV\_RULE View

The DBA\_DV\_RULE data dictionary view lists the rules that have been defined.

For example:

```
SELECT NAME, RULE_EXPR FROM DBA_DV_RULE WHERE NAME = 'Maintenance Window';
```

Output similar to the following appears:

```
NAME                RULE_EXP
-----
Maintenance Window TO_CHAR(SYSDATE,'HH24') BETWEEN '10' AND '12'
```

To find the rule sets that use specific rules, query the DBA\_DV\_RULE\_SET\_RULE view.

### Related Views

- [DBA\\_DV\\_RULE\\_SET View](#) (page 25-30)
- [DBA\\_DV\\_RULE\\_SET\\_RULE View](#) (page 25-32)

Column	Datatype	Null	Description
NAME	VARCHAR(128)	NOT NULL	Name of the rule.
RULE_EXPR	VARCHAR(1024)	NOT NULL	PL/SQL expression for the rule.
COMMON	VARCHAR(3)	NOT NULL	For a multitenant environment, indicates whether the rule is local or common. Possible values are: <ul style="list-style-type: none"> <li>YES if the rule is common</li> <li>NO if the rule is local</li> </ul>

Column	Datatype	Null	Description
INHERITED	VARCHAR(3)	NULL	Shows the inheritance status of the rule, when the COMMON column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>YES means that the rule was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>NO means that the rule is a local object, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED value NO but a CDB root common command rule will have an INHERITED value of YES.</li> </ul>
ID#	NUMBER	NOT NULL	The ID number of the rule, which is automatically generated when the rule is created
ORACLE_SUPPLIED	VARCHAR(3)	NULL	Indicates whether the rule is a default (that is, Oracle-supplied) rule or a user-created rule. Possible values are: <ul style="list-style-type: none"> <li>YES if the rule is a default rule</li> <li>NO if the rule is a user-created rule</li> </ul>

## 25.30 DBA\_DV\_RULE\_SET View

The DBA\_DV\_RULE\_SET data dictionary view lists the rules sets that have been created.

For example:

```
SELECT RULE_SET_NAME, HANDLER_OPTIONS, HANDLER FROM DBA_DV_RULE_SET
WHERE RULE_SET_NAME = 'Maintenance Period';
```

Output similar to the following appears:

```
RULE_SET_NAME      HANDLER_OPTIONS  HANDLER
-----
Maintenance Period          1 dbavowner.email_alert
```

### Related Views

- [DBA\\_DV\\_RULE View](#) (page 25-29)
- [DBA\\_DV\\_RULE\\_SET\\_RULE View](#) (page 25-32)

Column	Datatype	Null	Description
RULE_SET_NAME	VARCHAR(128)	NOT NULL	Name of the rule set.
DESCRIPTION	VARCHAR(1024)	NULL	Description of the rule set.
ENABLED	VARCHAR(1)	NOT NULL	Indicates whether the rule set has been enabled. Y (Yes) enables the rule set; N (No) disables it.

Column	Datatype	Null	Description
EVAL_OPTIONS_MEANING	VARCHAR(4000)	NULL	For rules sets that contain multiple rules, determines how many rules are evaluated. Possible values are: <ul style="list-style-type: none"> <li>All True: All rules in the rule set must evaluate to true for the rule set itself to evaluate to TRUE.</li> <li>Any True: At least one rule in the rule set must evaluate to true for the rule set itself to evaluate to TRUE.</li> </ul>
AUDIT_OPTIONS	NUMBER	NOT NULL	Indicates when auditing is used. Possible values are: <ul style="list-style-type: none"> <li>0: No auditing</li> <li>1: Audit on failure</li> <li>2: Audit on success</li> <li>3: Audit on both failure and success</li> </ul>
FAIL_OPTIONS_MEANING	VARCHAR(4000)	NULL	Determines when an audit record is created for the rule set. Possible values are: <ul style="list-style-type: none"> <li>Do Not Show Error Message.</li> <li>Show Error Message</li> </ul>
FAIL_MESSAGE	VARCHAR(80)	NULL	Error message for failure that is associated with the fail code listed in the FAIL_CODE column.
FAIL_CODE	VARCHAR(10)	NULL	The error message number associated with the message listed in the FAIL_MESSAGE column. Possible values are in the ranges of -20000 to -20999 or 20000 to 20999.
HANDLER_OPTIONS	NUMBER	NOT NULL	Determines how error handling is used. Possible values are: <ul style="list-style-type: none"> <li>0: Disables error handling.</li> <li>1: Call handler on rule set failure.</li> <li>2: Call handler on rule set success.</li> </ul>
HANDLER	VARCHAR(1024)	NULL	Name of the PL/SQL function or procedure that defines the custom event handler logic.
IS_STATIC	VARCHAR2(5)	NULL	Indicates how often the rule set is evaluated during a user session. Possible values are: <ul style="list-style-type: none"> <li>TRUE: The rule set is evaluated once, and result of the rule set is reused throughout the user session.</li> <li>FALSE (default): The rule set is evaluated each time it is accessed during the user session.</li> </ul>
COMMON	VARCHAR2(3)	NULL	For a multitenant environment, indicates whether the rule set is local or common. Possible values are: <ul style="list-style-type: none"> <li>YES if the rule set is common</li> <li>NO if the rule set is local</li> </ul>

Column	Datatype	Null	Description
INHERITED	VARCHAR2(3)	NULL	Shows the inheritance status of the rule set, when the COMMON column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>YES means that the rule set was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>NO means that the rule set is a local object, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED value NO but a CDB root common command rule will have an INHERITED value of YES.</li> </ul>
ID#	NUMBER	NOT NULL	The ID number of the rule set, which is automatically generated when the rule set is created
ORACLE_SUPPLIED	VARCHAR2(3)	NULL	Indicates whether the rule set is a default (that is, Oracle-supplied) rule set or a user-created rule set. Possible values are: <ul style="list-style-type: none"> <li>YES if the rule set is a default rule set</li> <li>NO if the rule set is a user-created rule set</li> </ul>

## 25.31 DBA\_DV\_RULE\_SET\_RULE View

The DBA\_DV\_RULE\_SET\_RULE data dictionary view lists rules that are associated with existing rule sets.

For example:

```
SELECT RULE_SET_NAME, RULE_NAME, RULE_EXPR FROM DBA_DV_RULE_SET_RULE
WHERE RULE_NAME = 'Is Security Officer';
```

Output similar to the following appears:

```
RULE_SET_NAME          RULE_NAME          RULE_EXPR
-----
Can Grant VPD Administration Is Security Owner  DBMS_MACUTL.USER_HAS_ROLE_VARCHAR
('DV_OWNER',
dvsys.dv_login_user) = 'Y'
```

### Related Views

- [DBA\\_DV\\_RULE View](#) (page 25-29)
- [DBA\\_DV\\_RULE\\_SET View](#) (page 25-30)

Column	Datatype	Null	Description
RULE_SET_NAME	VARCHAR(128)	NOT NULL	Name of the rule set that contains the rule.



Column	Datatype	Null	Description
RULE_NAME	VARCHAR(128)	NOT NULL	Name of the rule.
RULE_EXPR	VARCHAR(1024)	NOT NULL	PL/SQL expression that defines the rule listed in the RULE_NAME column.
ENABLED	VARCHAR(1)		Indicates whether the rule is enabled or disabled. Y (Yes) enables the rule set; N (No) disables it.
RULE_ORDER	NUMBER	NOT NULL	The order in which rules are used within the rule set. Does not apply to this release.
COMMON	VARCHAR(3)	NOT NULL	For a multitenant environment, indicates whether the rule is local or common. Possible values are: <ul style="list-style-type: none"> <li>• YES if the rule is common</li> <li>• NO if the rule is local</li> </ul>
INHERITED	VARCHAR(3)	NOT NULL	Shows the inheritance status of the rule, when the COMMON column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>• YES means that the rule was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>• NO means that the rule is a local object, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED value NO but a CDB root common command rule will have an INHERITED value of YES.</li> </ul>

## 25.32 DBA\_DV\_STATUS View

The DBA\_DV\_STATUS data dictionary view shows the status of Oracle Database Vault being enabled and configured.

For example:

```
SELECT * FROM DBA_DV_STATUS;
```

Output similar to the following appears:

```
NAME                STATUS
-----
DV_CONFIGURE_STATUS TRUE
DV_ENABLE_STATUS    TRUE
```

### Related Views

- [CDB\\_DV\\_STATUS View](#) (page 25-5)

Column	Datatype	Null	Description
NAME	VARCHAR2 ( 19 )	NOT NULL	Shows either of the following settings: <ul style="list-style-type: none"> <li>DV_CONFIGURE_STATUS shows whether Oracle Database Vault has been configured, that is, with the CONFIGURE_DV procedure.</li> <li>DV_ENABLE_STATUS shows whether Oracle Database Vault has been enabled, that is, with the DBMS_MACADM.ENABLE_DV procedure.</li> </ul>
STATUS	VARCHAR2 ( 64 )	NOT NULL	TRUE means that Oracle Database Vault is configured or enabled; FALSE means that it is not.

### 25.33 DBA\_DV\_SIMULATION\_LOG View

The DBA\_DV\_SIMULATION\_LOG data dictionary view captures simulation log information for realms and command rules that have had simulation mode enabled.

For example:

```
SELECT USERNAME, COMMAND FROM DBA_DV_SIMULATION_LOG WHERE REALM = 'HR Realm';
```

Output similar to the following appears:

```

USERNAME      COMMAND
-----
PSMITH        SELECT

```

#### Related Views

- [DBA\\_DV\\_REALM View](#) (page 25-24) for information about simulation mode settings for realms
- [DBA\\_DV\\_COMMAND\\_RULE View](#) (page 25-8) for information about simulation mode settings for command rules
- [DBA\\_DV\\_POLICY View](#) (page 25-19) for information about simulation mode settings in Oracle Database Vault policies

Column	Datatype	Null	Description
USERNAME	VARCHAR2 ( 128 )	NOT NULL	Name of the user whose information is being tracked
COMMAND	VARCHAR2 ( 128 )	NOT NULL	Command rule being tracked For a listing of existing command rules, query the DBA_DV_COMMAND_RULE view, described in <a href="#">DBA_DV_COMMAND_RULE View</a> (page 25-8).
VIOLATION_TYPE	VARCHAR2 ( 4000 )	NULL	Type of violation. See <a href="#">Table 25-2</a> (page 25-35) for more information.

Column	Datatype	Null	Description
REALM_NAME	VARCHAR2 ( 128 )	NULL	Realm being tracked. For a listing of existing realms, query the DBA_DV_REALM view, described in <a href="#">DBA_DV_REALM View</a> (page 25-24).
OBJECT_OWNER	VARCHAR2 ( 128 )	NULL	For command rules, the database schema to which the command rule applied
OBJECT_NAME	VARCHAR2 ( 128 )	NULL	For command rules, the database object that the command rule protects
OBJECT_TYPE	VARCHAR2 ( 129 )	NULL	For command rules, the type of object that is being protected
RULE_SET_NAME	VARCHAR2 ( 128 )	NULL	Rule set being tracked; it is associated with a command rule For a listing of existing rule sets, query the DBA_DV_RULE_SET view, described in <a href="#">DBA_DV_RULE_SET View</a> (page 25-30)
RETURN_CODE	NUMBER	NOT NULL	The Oracle Database ORA error that results if the Database Vault entity was in the enabled state rather than in simulation state
SQLTEXT	VARCHAR2 ( 4000 )	NULL	SQL text that the simulation mode captures
FACTOR_CONTEXT	VARCHAR2 ( 4000 )	NULL	An XML document that contains all of the factor identifiers for the current session at the point when the audit event was triggered
TIMESTAMP	TIMESTAMP ( 6 ) WITH TIME ZONE	NULL	Time stamp of user action, in UTC (Coordinated Universal Time) time zone

### VIOLATION\_TYPE Code Values

[Table 25-2](#) (page 25-35) lists the VIOLATION\_TYPE code values for the DBA\_DV\_SIMULATION\_LOG view.

**Table 25-2 DBA\_DV\_SIMULATION\_LOG VIOLATION\_TYPE Code Values**

Code	Meaning
1000	Realm violation
1001	Command rule violation
1002	Oracle Data Pump authorization violation
1003	Simulation violation
1004	Oracle Scheduler authorization violation
1005	DDL authorization violation

**Table 25-2 (Cont.) DBA\_DV\_SIMULATION\_LOG VIOLATION\_TYPE Code Values**

Code	Meaning
1006	PARSE_AS_USER violation

**Related Topics:**

[Using Simulation Mode for Logging Realm and Command Rule Activities](#)  
(page 11-1)

## 25.34 DBA\_DV\_TTS\_AUTH View

The DBA\_DV\_TTS\_AUTH data dictionary view lists users who have been granted authorization through the DBMS\_MACADM.AUTHORIZE\_TTS\_USER procedure to perform Oracle Data Pump transportable operations.

See [Using Oracle Data Pump with Oracle Database Vault](#) (page 13-5) for more information.

For example:

```
SELECT * FROM DBA_DV_TTS_AUTH;
```

Output similar to the following appears:

```
GRANTEE  TSNAME
-----  -
DB_MGR   HR_TS
```

**Related Views**

- [DBA\\_DV\\_DATAPUMP\\_AUTH View](#) (page 25-10)

Column	Datatype	Null	Description
GRANTEE	VARCHAR(128)	NOT NULL	Name of the user who has been granted transportable tablespace authorization
TSNAME	VARCHAR(128)	NOT NULL	Name of the transportable tablespace to which the GRANTEE user has been granted authorization

## 25.35 DBA\_DV\_USER\_PRIVS View

The DBA\_DV\_USER\_PRIVS data dictionary view lists the privileges for a database user account excluding privileges granted through the PUBLIC role.

For example:

```
SELECT USERNAME, ACCESS_TYPE, PRIVILEGE FROM DBA_DV_USER_PRIVS;
```

Output similar to the following appears:

```
USERNAME  ACCESS_TYPE  PRIVILEGE
-----  -
DVSYS     DV_PUBLIC    EXECUTE
DOWNER    DV_ADMIN     SELECT
SYS       SELECT_CATALOG_ROLE  SELECT
...
```

**Related Views**

- [DBA\\_DV\\_PUB\\_PRIVS View](#) (page 25-23)
- [DBA\\_DV\\_ROLE View](#) (page 25-28)
- [DBA\\_DV\\_USER\\_PRIVS\\_ALL View](#) (page 25-37)

Column	Datatype	Null	Description
USERNAME	VARCHAR(128)	NOT NULL	Name of the database schema account in which privileges have been defined.
ACCESS_TYPE	VARCHAR(128)	NULL	Role the database user account listed in the USERNAME column uses to access the database. Oracle Database Vault accounts have direct access.
PRIVILEGE	VARCHAR(40)	NOT NULL	Privilege granted to the user listed in the USERNAME column.
OWNER	VARCHAR(128)	NOT NULL	Name of the database user account.
OBJECT_NAME	VARCHAR(128)	NOT NULL	Name of the PL/SQL function or procedure used to define privileges.

**25.36 DBA\_DV\_USER\_PRIVS\_ALL View**

The DBA\_DV\_USER\_PRIVS\_ALL data dictionary view lists the privileges for a database account including privileges granted through PUBLIC.

For example:

```
SELECT USERNAME, ACCESS_TYPE, PRIVILEGE FROM DBA_DV_USER_PRIVS;
```

Output similar to the following appears:

```

USERNAME          ACCESS_TYPE  PRIVILEGE
-----
BEA_DVACCTMGR     CONNECT     CREATE_SESSION
LEO_DVOWNER       DIRECT      CREATE PROCEDURE
...

```

**Related Views**

- [DBA\\_DV\\_PUB\\_PRIVS View](#) (page 25-23)
- [DBA\\_DV\\_ROLE View](#) (page 25-28)
- [DBA\\_DV\\_USER\\_PRIVS View](#) (page 25-36)

Column	Datatype	Null	Description
USERNAME	VARCHAR(128)	NULL	Name of the database schema account in which privileges have been defined.
ACCESS_TYPE	VARCHAR(128)	NULL	Role the database user account listed in the USERNAME column uses to access the database. Oracle Database Vault accounts have direct access.

Column	Datatype	Null	Description
PRIVILEGE	VARCHAR(40)	NULL	Privilege granted to the user listed in the USERNAME column.
OWNER	VARCHAR(128)	NULL	Name of the database user account.
OBJECT_NAME	VARCHAR(128)	NULL	Name of the PL/SQL function or procedure used to define privileges.

## 25.37 DVSYS.DV\$CONFIGURATION\_AUDIT View

The DVSYS.DV\$CONFIGURATION\_AUDIT data dictionary view captures DVSYS.AUDIT\_TRAIL\$ table audit trail records.

It includes records that are related to successful and failed configuration changes made to realms, rules, rule sets, factors, and other Oracle Database Vault policy configuration activities.

For example:

```
SELECT USERNAME, ACTION_NAME FROM DVSYS.DV$CONFIGURATION_AUDIT
WHERE USERNAME = 'PSMITH';
```

Output similar to the following appears:

```
USERNAME  ACTION_NAME
-----
PSMITH    Realm Creation Audit
PSMITH    Rule Set Update Audit
```

### Related View

- [SYS.DV\\$CONFIGURATION\\_AUDIT View](#) (page 25-56)

Column	Datatype	Null	Description
ID#	NUMBER	NOT NULL	Numeric identifier for the audit record
OS_USERNAME	VARCHAR(255)	NULL	Operating system login user name of the user whose actions were audited
USERNAME	VARCHAR(128)	NULL	Name of the database user whose actions were audited
USERHOST	VARCHAR2(128)	NULL	Client computer name
TERMINAL	VARCHAR2(30)	NULL	Identifier for the user's terminal
TIMESTAMP	DATA	NULL	Date and time of creation of the audit trail entry (in the local database session time zone)
OWNER	VARCHAR2(128)	NULL	Creator of the object affected by the action, always DVSYS (because DVSYS is where objects are created)

Column	Datatype	Null	Description
OBJ_NAME	VARCHAR2(128)	NULL	Name of the object affected by the action. Expected values are: <ul style="list-style-type: none"> <li>• ROLE\$</li> <li>• REALM\$</li> <li>• CODE\$</li> <li>• FACTOR\$</li> </ul>
ACTION	NUMBER	NOT NULL	Numeric action type code. The corresponding name of the action type is in the ACTION_NAME column. See <a href="#">Table 25-3</a> (page 25-40) for a listing of the possible actions.
ACTION_NAME	VARCHAR2(128)	NULL	Name of the action type corresponding to the numeric code in the ACTION column. See <a href="#">Table 25-3</a> (page 25-40) for a listing of the possible actions.
ACTION_OBJECT_ID	NUMBER	NULL	The unique identifier of the record in the table specified under OBJ_NAME
ACTION_OBJECT_NAME	VARCHAR2(128)	NULL	The unique name or natural key of the record in the table specified under OBJ_NAME
ACTION_COMMAND	VARCHAR2(4000)	NULL	The SQL text of the command procedure that was executed that resulted in the audit event being triggered
AUDIT_OPTION	VARCHAR2(4000)	NULL	The labels for all audit options specified in the record that resulted in the audit event being triggered. For example, a factor set operation that is supposed to audit on get failure and get NULL would indicate these two options.
RULE_SET_ID	NUMBER	NULL	The unique identifier of the rule set that was executing and caused the audit event to trigger
RULE_SET_NAME	VARCHAR2(128)	NULL	The unique name of the rule set that was executing and caused the audit event to trigger
RULE_ID	NUMBER	NULL	Not used
RULE_NAME	VARCHAR2(128)	NULL	Not used
FACTOR_CONTEXT	VARCHAR2(4000)	NULL	An XML document that contains all of the factor identifiers for the current session at the point when the audit event was triggered
COMMENT_TEXT	VARCHAR2(4000)	NULL	Text comment on the audit trail entry, providing more information about the statement audited
SESSIONID	NUMBER	NOT NULL	Numeric identifier for each Oracle session
ENTRYID	NUMBER	NOT NULL	Same as the value in the ID# column
STATEMENTID	NUMBER	NOT NULL	Numeric identifier for the statement invoked that caused the audit event to be generated. This is empty for most Oracle Database Vault events.

Column	Datatype	Null	Description
RETURNCODE	NUMBER	NOT NULL	Oracle error code generated by the action. The error code for a statement or procedure invoked that caused the audit event to be generated. This is empty for most Oracle Database Vault events.
EXTENDED_TIMESTAMP	TIMESTAMP(6) WITH TIME ZONE	NULL	Time stamp of creation of the audit trail entry (time stamp of user login for entries) in UTC (Coordinated Universal Time) time zone
PROXY_SESSIONID	NUMBER	NULL	Proxy session serial number, if an enterprise user has logged in through the proxy mechanism
GLOBAL_UID	VARCHAR2(32)	NULL	Global user identifier for the user, if the user has logged in as an enterprise user
INSTANCE_NUMBER	NUMBER	NULL	Instance number as specified by the INSTANCE_NUMBER initialization parameter
OS_PROCESS	VARCHAR2(16)	NULL	Operating system process identifier of the Oracle process
CREATED_BY	VARCHAR2(128)	NULL	Database login user name of the user whose actions were audited
CREATE_DATE	DATE	NULL	Date on which the action occurred, based on the SYSDATE date
UPDATED_BY	VARCHAR2(128)	NULL	Same as CREATED_BY column value
UPDATE_DATE	DATE	NULL	Same as UPDATED_BY column value
GRANTEE	VARCHAR2(128)	NULL	User ID of users who have been granted Database Vault-protected roles, realm authorization, command-rule authorization, job scheduler authorization, or Oracle Data Pump authorizations
ENABLED_STATUS	VARCHAR2(1)	NULL	Indicates whether the configuration was enabled

[Table 25-3](#) (page 25-40) describes the possible values for the ACTION column of the DVSYS.DV\$CONFIGURATION\_AUDIT view.

**Table 25-3 DVSYS.DV\$CONFIGURATION\_AUDIT View ACTION Values**

Action Type Code	Action Name
20001	Enable DV enforcement Audit
20002	Disable DV enforcement Audit
20003	Realm Creation Audit
20004	Realm Update Audit
20005	Realm Rename Audit
20006	Realm Deletion Audit
20007	Add Realm Auth Audit



**Table 25-3 (Cont.) DVSYS.DV\$CONFIGURATION\_AUDIT View ACTION Values**

Action Type Code	Action Name
20008	Delete Realm Auth Audit
20009	Update Realm Auth Audit
20010	Add Realm Object Audit
20011	Update Realm Object Audit
20012	Delete Realm Object Audit
20013	Enable Event Audit
20014	Disable Event Audit
20015	Rule Set Creation Audit
20016	Rule Set Update Audit
20017	Rule Set Rename Audit
20018	Rule Set Deletion Audit
20019	Add Rule To Rule Set Audit
20020	Delete Rule From Rule Set Audit
20021	Rule Creation Audit
20022	Rule Update Audit
20023	Rule Rename Audit
20024	Rule Deletion Audit
20025	CommandRule Creation Audit
20026	CommandRule Update Audit
20027	CommandRule Deletion Audit
20028	Authorize Datapump User Audit
20029	Unauthorize Datapump User Audit
20030	Authorize Job User Audit
20031	Unauthorize Job User Audit
20032	Factor_Type Creation Audit
20033	Factor_Type Deletion Audit
20034	Factor_Type Update Audit
20035	Factor_Type Rename Audit
20036	Factor Creation Audit

**Table 25-3 (Cont.) DVSYS.DV\$CONFIGURATION\_AUDIT View ACTION Values**

Action Type Code	Action Name
20037	G_FACTOR_DELETION_AUDIT_CODE
20038	Factor Update Audit
20039	Factor Rename Audit
20040	Add Factor Link Audit
20041	Delete Factor Link Audit
20042	Add Policy Factor Audit
20043	Delete Policy Factor Audit
20044	Create Identity Audit
20045	Delete Identity Audit
20046	Update Identity Audit
20047	Change Identity Factor Audit
20048	Change Identity Value Audit
20049	Create Identity Map Audit
20050	Delete Identity Map Audit
20051	Create Policy Label Audit
20052	Delete Policy Label Audit
20053	Create Mac Policy Audit
20054	Update Mac Policy Audit
20055	Delete Mac Policy Audit
20056	Create Role Audit
20057	Delete Role Audit
20058	Update Role Audit
20059	Rename Role Audit
20060	Create Domain Identity Audit
20061	Drop Domain Identity Audit
20062	Enable Oradebug Audit
20063	Disable Oradebug Audit
20064	Authorize Proxy User Audit
20065	Unauthorize Proxy User Audit

**Table 25-3 (Cont.) DVSYS.DV\$CONFIGURATION\_AUDIT View ACTION Values**

Action Type Code	Action Name
20066	Enable DV Dictionary Accounts Audit
20067	Disable DV Dictionary Accounts Audit
20068	Authorize DDL Audit
20069	Unauthorize DDL Audit
20070	Authorize TTS Audit
20071	Unauthorize TTS Audit
20072	Authorize PREPROCESSOR Audit
20073	Unauthorize PREPROCESSOR Audit
20074	Create Policy Audit
20075	Update Policy Description Audit
20076	Update Policy State Audit
20077	Rename Policy Audit
20078	Drop Policy Audit
20079	Add Realm to Policy Audit
20080	Delete Realm From Policy Audit
20081	Add Command Rule to Policy Audit
20082	Delete Command Rule from Policy Audit
20083	Add Policy Owner Audit
20084	Delete Policy Owner Audit
20085	Authorize Maintenance Audit
20086	Unauthorize Maintenance Audit

## 25.38 DVSYS.DV\$ENFORCEMENT\_AUDIT View

The DVSYS.DV\$ENFORCEMENT\_AUDIT data dictionary view provides information about enforcement-related audits from the DVSYS.AUDIT\_TRAIL\$ table.

It captures user violations on command rules, realms, and factors.

For example:

```
SELECT USERNAME, ACTION_COMMAND FROM DVSYS.DV$ENFORCEMENT_AUDIT
WHERE OWNER = 'HR';
```

Output similar to the following appears:

USERNAME    ACTION\_COMMMAND

-----  
PSMITH      CREATE\_REALM

### Related View

- [SYS.DV\\$ENFORCEMENT\\_AUDIT View](#) (page 25-57)

Column	Datatype	Null	Description
ID#	NUMBER	NOT NULL	Numeric identifier for the audit record
OS_USERNAME	VARCHAR ( 255 )	NULL	Operating system login user name of the user whose actions were audited
USERNAME	VARCHAR ( 128 )	NULL	Name of the database user whose actions were audited
USERHOST	VARCHAR ( 255 )	NULL	Client computer name
TERMINAL	VARCHAR ( 255 )	NULL	Identifier for the user's terminal
TIMESTAMP	DATE	NULL	Date and time of creation of the audit trail entry (in the local database session time zone)
OWNER	VARCHAR ( 128 )	NULL	Creator of the object affected by the action, always DVSYS (because DVSYS is where objects are created)
OBJ_NAME	VARCHAR ( 128 )	NULL	Name of the object affected by the action. Expected values are: <ul style="list-style-type: none"> <li>• ROLE\$</li> <li>• REALM\$</li> <li>• CODE\$</li> <li>• FACTOR\$</li> </ul>
ACTION	NUMBER	NOT NULL	Numeric action type code. The corresponding name of the action type is in the ACTION_NAME column. See <a href="#">Table 25-4</a> (page 25-46) for a listing of the possible actions.
ACTION_NAME	VARCHAR ( 128 )	NULL	Name of the action type corresponding to the numeric code in the ACTION column
ACTION_OBJECT_ID	NUMBER	NULL	The unique identifier of the record in the table specified under OBJ_NAME
ACTION_OBJECT_NAME	VARCHAR ( 128 )	NULL	The unique name or natural key of the record in the table specified under OBJ_NAME
ACTION_COMMAND	VARCHAR2 ( 4000 )	NULL	The SQL text of the command procedure that was executed that resulted in the audit event being triggered

Column	Datatype	Null	Description
AUDIT_OPTION	VARCHAR2(4000)	NULL	The labels for all audit options specified in the record that resulted in the audit event being triggered. For example, a factor set operation that is supposed to audit on get failure and get NULL would indicate these two options.
RULE_SET_ID	NUMBER	NULL	The unique identifier of the rule set that was executing and caused the audit event to trigger
RULE_SET_NAME	VARCHAR(128)	NULL	The unique name of the rule set that was executing and caused the audit event to trigger
RULE_ID	NUMBER	NULL	Not used
RULE_NAME	VARCHAR2(128)	NULL	Not used
FACTOR_CONTEXT	VARCHAR2(4000)	NULL	An XML document that contains all of the factor identifiers for the current session at the point when the audit event was triggered
COMMENT_TEXT	VARCHAR2(4000)	NULL	Text comment on the audit trail entry, providing more information about the statement audited
SESSIONID	NUMBER	NOT NULL	Numeric identifier for each Oracle session
ENTRYID	NUMBER	NOT NULL	Same as the value in the ID# column
STATEMENTID	NUMBER	NOT NULL	Numeric identifier for the statement invoked that caused the audit event to be generated. This is empty for most Oracle Database Vault events.
RETURNCODE	NUMBER	NOT NULL	Oracle error code generated by the action. The error code for a statement or procedure invoked that caused the audit event to be generated. This is empty for most Oracle Database Vault events.
EXTENDED_TIMESTAMP	TIMESTAMP(6) WITH TIME ZONE	NULL	Time stamp of creation of the audit trail entry (time stamp of user login for entries) in UTC (Coordinated Universal Time) time zone
PROXY_SESSIONID	NUMBER	NULL	Proxy session serial number, if an enterprise user has logged in through the proxy mechanism
GLOBAL_UID	VARCHAR2(32)	NULL	Global user identifier for the user, if the user has logged in as an enterprise user
INSTANCE_NUMBER	NUMBER	NULL	Instance number as specified by the INSTANCE_NUMBER initialization parameter

Column	Datatype	Null	Description
OS_PROCESS	VARCHAR2(16)	NULL	Operating system process identifier of the Oracle process
CREATED_BY	VARCHAR2(128)	NULL	Database login user name of the user whose actions were audited
CREATE_DATE	DATE	NULL	Date on which the action occurred, based on the SYSDATE date
UPDATED_BY	VARCHAR2(128)	NULL	Same as CREATED_BY column value
UPDATE_DATE	DATE	NULL	Same as UPDATED_BY column value

The following table describes the possible values for the ACTION column of the DVSYS.DV\$ENFORCEMENT\_AUDIT view.

**Table 25-4 DVSYS.DV\$ENFORCEMENT\_AUDIT View ACTION Values**

Action Type Code	Action Name
10000	Factor Evaluation Audit
10001	Factor Assignment Audit
10002	Factor Expression Audit
10003	Realm Violation Audit
10004	Realm Authorization Audit
10005	Command Authorization Audit
10006	Secure Role Audit
10007	Session Initialization Audit
10008	Secure Command Authorization Audit
10009	OLS Session Initialization Audit
10010	OLS Attempt to Upgrade Label Audit
10011	Command Failure Audit

## 25.39 DVSYS.DV\$REALM View

The DVSYS.DV\$REALM data dictionary view describes settings that were used to create Oracle Database Vault realms, such as which audit options have been assigned or whether the realm is a mandatory realm.

This view also indicates information such as who created and updated the realm, and when the realm was created and updated.

For example:

```
SELECT NAME, CREATED_BY, TYPE FROM DVSYS.DV$REALM WHERE NAME LIKE 'Statistics';
```

Output similar to the following appears:

```

NAME                                CREATED_BY TYPE
-----
Performance Statistics Realm JGODFREY 2

```

### Related Views

- [DBA\\_DV\\_REALM View](#) (page 25-24)

Column	Datatype	Null	Description
ID#	NUMBER	NOT NULL	ID number of the realm
NAME	VARCHAR2(128)	NOT NULL	Name of the realm
DESCRIPTION	VARCHAR2(1024)	NULL	Description of the realm
AUDIT_OPTIONS	NUMBER	NOT NULL	Audit options set for the realm. See <code>audit_options</code> in <a href="#">Table 15-9</a> (page 15-12) for a description of the possible values.
REALM_TYPE	NUMBER	NULL	Type of realm: whether it is a regular realm or a mandatory realm. See <code>realm_type</code> in <a href="#">Table 15-9</a> (page 15-12) for a description of the possible values.
COMMON	VARCHAR2(3)	NULL	For a multitenant environment, indicates whether the realm is local or common. Possible values are: <ul style="list-style-type: none"> <li>• YES if the realm is common</li> <li>• NO if the realm is local</li> </ul>
INHERITED	VARCHAR2(3)	NULL	Shows the inheritance status of the realm, when the <code>COMMON</code> column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>• YES means that the realm was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>• NO means that the realm is a local object, or it is common from that container. For example, in an application root, an application common realm will have an <code>INHERITED</code> value NO but a CDB root common command rule will have an <code>INHERITED</code> value of YES.</li> </ul>
ENABLED	VARCHAR2(1)	NOT NULL	Whether the realm has been enabled. See <code>enabled</code> in <a href="#">Table 15-9</a> (page 15-12) for a description of the possible values.
VERSION	NUMBER	NULL	Version of Oracle Database Vault in which the realm was created
CREATED_BY	VARCHAR2(128)	NULL	User who created the realm
CREATE_DATE	DATE	NULL	Date on which the realm was created.
UPDATED_BY	VARCHAR2(128)	NULL	User who last updated the realm

Column	Datatype	Null	Description
UPDATE_DATE	DATE	NULL	Date on which the realm was last updated

## 25.40 DVSYS.POLICY\_OWNER\_COMMAND\_RULE View

The `DVSYS.POLICY_OWNER_COMMAND_RULE` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the command rules that have been associated with Database Vault policies.

Examples of information that users can find include the command rule name, its associated rule set, and whether it is enabled. Only users who have been granted the `DV_POLICY_OWNER` role can query this view.

For example:

```
SELECT COMMAND, OBJECT_OWNER, OBJECT_NAME FROM DVSYS.POLICY_OWNER_COMMAND_RULE;
```

Output similar to the following appears:

```
COMMAND      OBJECT_OWNER  OBJECT_NAME
-----
SELECT       HR            EMPLOYEES
```

### Related Views

- [DVSYS.POLICY\\_OWNER\\_POLICY View](#) (page 25-49)

Column	Datatype	Null	Description
COMMAND	VARCHAR(128)	NOT NULL	Name of the command rule. For a list of default command rules, see <a href="#">Default Command Rules</a> (page 7-7).
CLAUSE_NAME	VARCHAR(100)	NOT NULL	A clause from either the <code>ALTER SYSTEM</code> or <code>ALTER SESSION SQL</code> statement, which was used to create the command rule. For example, you it could list the <code>SET</code> clause for the <code>ALTER SESSION</code> statement.  For a full list of possible clause values, see the following topics: <ul style="list-style-type: none"> <li>• <a href="#">Table 17-2</a> (page 17-4)</li> <li>• <a href="#">Table 17-3</a> (page 17-6)</li> </ul>
PARAMETER_NAME	VARCHAR(128)	NOT NULL	A parameter from the <code>ALTER SYSTEM</code> or <code>ALTER SESSION</code> command rule <code>CLAUSE_NAME</code> setting
EVENT_NAME	VARCHAR(128)	NOT NULL	An event that the <code>ALTER SYSTEM</code> or <code>ALTER SESSION</code> command rule defines
COMPONENT_NAME	VARCHAR(128)	NOT NULL	A component of the <code>EVENT_NAME</code> setting for the <code>ALTER SYSTEM</code> or <code>ALTER SESSION</code> command rule.
ACTION_NAME	VARCHAR(128)	NOT NULL	An action of the <code>EVENT_NAME</code> setting for the <code>ALTER SYSTEM</code> or <code>ALTER SESSION</code> command rule
RULE_SET_NAME	VARCHAR(128)	NOT NULL	Name of the rule set associated with this command rule.
OBJECT_OWNER	VARCHAR(128)	NOT NULL	The owner of the object that the command rule affects.



Column	Datatype	Null	Description
OBJECT_NAME	VARCHAR(128)	NOT NULL	The name of the database object the command rule affects (for example, a database table).
ENABLED	VARCHAR(1)	NOT NULL	Y indicates the command rule is enabled; N indicates it is disabled.
PRIVILEGE_SCOP E	NUMBER	NOT NULL	Obsolete column
ID#	NUMBER	NOT NULL	The ID number of the command rule, which is automatically generated when the command rule is created
ORACLE_SUPPLIE D	VARCHAR(3)	NULL	Indicates whether the command rule is a default (that is, Oracle-supplied) command rule or a user-created command rule. Possible values are: <ul style="list-style-type: none"> <li>YES if the command rule is a default command rule</li> <li>NO if the command rule is a user-created command rule</li> </ul>

## 25.41 DVSYS.POLICY\_OWNER\_POLICY View

The `DVSYS.POLICY_OWNER_POLICY` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information such as the names, descriptions, and states of existing policies in the current database instance, including policies created by other policy owners.

The columns of the `DVSYS.POLICY_OWNER_POLICY` view are the same as those in `DBA_DV_POLICY`. Only users who have been granted the `DV_POLICY_OWNER` role can query this view.

For example:

```
SELECT POLICY_NAME, STATE FROM DVSYS.POLICY_OWNER_POLICY
WHERE STATE != 'ENABLED';
```

Output similar to the following appears:

```
POLICY_NAME                                STATE
-----
HR.EMPLOYEES_pol                           ENABLED
```

### Related View

- [DBA\\_DV\\_POLICY View](#) (page 25-19)

## 25.42 DVSYS.POLICY\_OWNER\_REALM View

The `POLICY_OWNER_REALM` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the realms that have been associated with Database Vault policies.

Examples of information that users can find include the realm name, audit options, type, whether it is inherited, and if it is enabled. Only users who have been granted the `DV_POLICY_OWNER` role can query this view.

For example:

```
SELECT NAME, ENABLED FROM DVSYS.POLICY_OWNER_REALM;
```

Output similar to the following appears:

```
NAME                                ENABLED
-----
HR.EMPLOYEES_realm                 S
```

### Related Views

- [DVSYS.POLICY\\_OWNER\\_REALM\\_AUTH View](#) (page 25-51)
- [DVSYS.POLICY\\_OWNER\\_REALM\\_OBJECT View](#) (page 25-52)

Column	Datatype	Null	Description
NAME	VARCHAR(128)	NOT NULL	Names of the realms that have been associated with Database Vault policies. See <a href="#">DBA_DV_REALM View</a> (page 25-24) for a full listing of realms.
DESCRIPTION	VARCHAR(1024)	NULL	Description of the realm
AUDIT_OPTIONS	NUMBER	NOT NULL	Audit options set for the realm. See <code>audit_options</code> in <a href="#">Table 15-9</a> (page 15-12) for a description of the possible values.
REALM_TYPE	NUMBER	NULL	Type of realm: whether it is a regular realm or a mandatory realm. See <code>realm_type</code> in <a href="#">Table 15-9</a> (page 15-12) for a description of the possible values.
COMMON_REALM	VARCHAR2(3)	NULL	For a multitenant environment, indicates whether the realm is local or common. Possible values are: <ul style="list-style-type: none"> <li>• YES if the realm is common</li> <li>• NO if the realm is local</li> </ul>
INHERITED_REALM	VARCHAR2(3)	NULL	Shows the inheritance status of the realm, when the <code>COMMON</code> column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>• YES means that the realm was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>• NO means that the realm is a local object, or it is common from that container. For example, in an application root, an application common realm will have an <code>INHERITED</code> value NO but a CDB root common command rule will have an <code>INHERITED</code> value of YES.</li> </ul>
ENABLED	VARCHAR2(1)	NOT NULL	Indicates the enablement status of the realm. Possible values are: <ul style="list-style-type: none"> <li>• Y for yes (enabled)</li> <li>• N for no (not enabled)</li> <li>• S for simulation mode</li> </ul>
ID#	NUMBER	NOT NULL	The ID number of the realm, which is automatically generated when the realm is created

Column	Datatype	Null	Description
ORACLE_SUPPLIED	VARCHAR(3)	NOT NULL	Indicates whether the realm is a default (that is, Oracle-supplied) realm or a user-created realm. Possible values are: <ul style="list-style-type: none"> <li>YES if the realm is a default realm</li> <li>NO if the realm is a user-created realm</li> </ul>

## 25.43 DVSYS.POLICY\_OWNER\_REALM\_AUTH View

The `DVSYS.POLICY_OWNER_REALM_AUTH` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the authorization that was granted to realms that have been associated with Database Vault policies.

Examples of the information that users can find are the realm name, grantee, and associated rule set. Only users who have been granted the `DV_POLICY_OWNER` role can query this view.

For example:

```
SELECT REALM_NAME, INHERITED_REALM FROM DVSYS.POLICY_OWNER_REALM_AUTH;
```

Output similar to the following appears:

```
REALM_NAME                INHERITED
-----
HR.EMPLOYEES_realm        NO
```

### Related Views

- [DVSYS.POLICY\\_OWNER\\_REALM View](#) (page 25-49)
- [DVSYS.POLICY\\_OWNER\\_REALM\\_OBJECT View](#) (page 25-52)

Column	Datatype	Null	Description
REALM_NAME	VARCHAR(128)	NOT NULL	Names of the realms that have been associated with Database Vault policies. See <a href="#">DBA_DV_REALM View</a> (page 25-24) for a full listing of realms.
COMMON_REALM	VARCHAR2(3)	NULL	For a multitenant environment, indicates whether the realm is local or common.

Column	Datatype	Null	Description
INHERITED_REALM	VARCHAR2(3)	NULL	Shows the inheritance status of the realm, when the COMMON column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>YES means that the realm was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>NO means that the realm is a local object, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED value NO but a CDB root common command rule will have an INHERITED value of YES.</li> </ul>
GRANTEE	VARCHAR(128)	NOT NULL	User or role name to authorize as owner or participant.
AUTH_RULE_SET_NAME	VARCHAR(128)	NULL	Rule set to check before authorizing. If the rule set evaluates to TRUE, then the authorization is allowed.
AUTH_OPTIONS	VARCHAR(4000)	NULL	Type of realm authorization: either Participant or Owner.
COMMON_AUTH	VARCHAR(3)	NULL	For a multitenant environment, indicates whether the user who is authorized for this realm is local or common. Possible values are: <ul style="list-style-type: none"> <li>YES if the user is a common user</li> <li>NO if the users is a local user</li> </ul>
INHERITED_AUTH	VARCHAR(3)	NULL	Possible values are: <ul style="list-style-type: none"> <li>YES</li> <li>NO</li> </ul>

## 25.44 DVSYS.POLICY\_OWNER\_REALM\_OBJECT View

The `DVSYS.POLICY_OWNER_REALM_OBJECT` data dictionary view enables users to find information about the objects that have been added to realms that are associated with Database Vault policies, such as. Only users who have been granted the `DV_POLICY_OWNER` role can query this view.

Examples of information that users can find include the realm name, grantee, and associated rule set.

For example:

```
SELECT REALM_NAME, OWNER, OBJECT_NAME, OBJECT_TYPE FROM
DVSYS.POLICY_OWNER_REALM_OBJECT;
```

Output similar to the following appears:

```
REALM_NAME          OWNER  OBJECT_NAME  OBJECT_TYPE
-----
HR.EMPLOYEES_realm HR      EMPLOYEES    TABLE
```

### Related Views

- [DVSYS.POLICY\\_OWNER\\_REALM View](#) (page 25-49)

- [DVSYS.POLICY\\_OWNER\\_REALM\\_AUTH View](#) (page 25-51)

Column	Datatype	Null	Description
REALM_NAME	VARCHAR(128)	NOT NULL	Names of the realms that have been associated with Database Vault policies. See <a href="#">DBA_DV_REALM View</a> (page 25-24) for a full listing of realms.
COMMON_REALM	VARCHAR2(3)	NULL	For a multitenant environment, indicates whether the realm is local or common.
INHERITED_REALM	VARCHAR2(3)	NULL	Shows the inheritance status of the realm, when the COMMON column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>• YES means that the realm was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>• NO means that the realm is a local object, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED value NO but a CDB root common command rule will have an INHERITED value of YES.</li> </ul>
OWNER	VARCHAR(128)	NOT NULL	Database schema owner who owns the realm.
OBJECT_NAME	VARCHAR(128)	NOT NULL	Name of the object the realm protects.
OBJECT_TYPE	VARCHAR(32)	NOT NULL	Type of object the realm protects, such as a database table, view, index, or role.

## 25.45 DVSYS.POLICY\_OWNER\_RULE View

The `DVSYS.POLICY_OWNER_RULE` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the rules that have been associated with rule sets in Database Vault policies, such as the rule name and its expression. Only users who have been granted the `DV_POLICY_OWNER` role can query this view.

For example:

```
SELECT NAME, RULE_EXPR FROM DVSYS.POLICY_OWNER_RULE WHERE NAME = 'True';
```

Output similar to the following appears:

```
NAME          RULE_EXPR
-----
True          1=1
```

### Related Views

- [DVSYS.POLICY\\_OWNER\\_COMMAND\\_RULE View](#) (page 25-48)
- [DVSYS.POLICY\\_OWNER\\_RULE\\_SET View](#) (page 25-54)

Column	Datatype	Null	Description
NAME	VARCHAR ( 128 )	NOT NULL	Name of the rule.
RULE_EXPR	VARCHAR ( 1024 )	NOT NULL	PL/SQL expression for the rule.
COMMON	VARCHAR ( 3 )	NOT NULL	For a multitenant environment, indicates whether the rule is local or common. Possible values are: <ul style="list-style-type: none"> <li>YES if the rule is common</li> <li>NO if the rule is local</li> </ul>
INHERITED	VARCHAR ( 3 )	NULL	Shows the inheritance status of the rule, when the COMMON column output is YES. Values are as follows: <ul style="list-style-type: none"> <li>YES means that the rule was defined in another container that is higher in the hierarchy of the container tree, and inherited in this container when the Database Vault policy was synced during the synchronization process of applications in an application PDB.</li> <li>NO means that the rule is a local object, or it is common from that container. For example, in an application root, an application common realm will have an INHERITED value NO but a CDB root common command rule will have an INHERITED value of YES.</li> </ul>
ID#	NUMBER	NOT NULL	The ID number of the rule, which is automatically generated when the rule is created
ORACLE_SUPPLIED	VARCHAR ( 3 )	NULL	Indicates whether the rule is a default (that is, Oracle-supplied) rule or a user-created rule. Possible values are: <ul style="list-style-type: none"> <li>YES if the rule is a default rule</li> <li>NO if the rule is a user-created rule</li> </ul>

## 25.46 DVSYS.POLICY\_OWNER\_RULE\_SET View

The `DVSYS.POLICY_OWNER_RULE_SET` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the rule sets that have been associated with Database Vault policies.

Examples of information that users can find include the rule set name, its handler information, and whether it is enabled. Only users who have been granted the `DV_POLICY_OWNER` role can query this view.

For example:

```
SELECT RULE_SET_NAME, ENABLED FROM DVSYS.POLICY_OWNER_RULE_SET;
```

Output similar to the following appears:

```
RULE_SET_NAME  ENABLED
-----
Allow Sessions Y
```

### Related Views

- [DVSYS.POLICY\\_OWNER\\_COMMAND\\_RULE View](#) (page 25-48)
- [DVSYS.POLICY\\_OWNER\\_RULE View](#) (page 25-53)

- [DVSYS.POLICY\\_OWNER\\_RULE\\_SET\\_RULE View](#) (page 25-56)

Column	Datatype	Null	Description
RULE_SET_NAME	VARCHAR(128)	NOT NULL	Name of the rule set.
DESCRIPTION	VARCHAR(1024)	NULL	Description of the rule set.
ENABLED	VARCHAR(1)	NOT NULL	Indicates whether the rule set has been enabled. Y (Yes) enables the rule set; N (No) disables it.
EVAL_OPTIONS_MEANING	VARCHAR(4000)	NULL	For rules sets that contain multiple rules, determines how many rules are evaluated. Possible values are: <ul style="list-style-type: none"> <li>• All True: All rules in the rule set must evaluate to true for the rule set itself to evaluate to TRUE.</li> <li>• Any True: At least one rule in the rule set must evaluate to true for the rule set itself to evaluate to TRUE.</li> </ul>
AUDIT_OPTIONS	NUMBER	NOT NULL	Indicates when auditing is used. Possible values are: <ul style="list-style-type: none"> <li>• 0: No auditing</li> <li>• 1: Audit on failure</li> <li>• 2: Audit on success</li> <li>• 3: Audit on both failure and success</li> </ul>
FAIL_OPTIONS_MEANING	VARCHAR(4000)	NULL	Determines when an audit record is created for the rule set. Possible values are: <ul style="list-style-type: none"> <li>• Do Not Show Error Message.</li> <li>• Show Error Message</li> </ul>
FAIL_MESSAGE	VARCHAR(80)	NULL	Error message for failure that is associated with the fail code listed in the FAIL_CODE column.
FAIL_CODE	VARCHAR(10)	NULL	The error message number associated with the message listed in the FAIL_MESSAGE column. Possible values are in the ranges of -20000 to -20999 or 20000 to 20999.
HANDLER_OPTIONS	NUMBER	NOT NULL	Determines how error handling is used. Possible values are: <ul style="list-style-type: none"> <li>• 0: Disables error handling.</li> <li>• 1: Call handler on rule set failure.</li> <li>• 2: Call handler on rule set success.</li> </ul>
HANDLER	VARCHAR(1024)	NULL	Name of the PL/SQL function or procedure that defines the custom event handler logic.
IS_STATIC	VARCHAR2(5)	NULL	Indicates how often the rule set is evaluated during a user session. Possible values are: <ul style="list-style-type: none"> <li>• TRUE: The rule set is evaluated once, and result of the rule set is reused throughout the user session.</li> <li>• FALSE (default): The rule set is evaluated each time it is accessed during the user session.</li> </ul>
ID#	NUMBER)	NOT NULL	The ID number of the rule set, which is automatically generated when the rule set is created

Column	Datatype	Null	Description
ORACLE_SUPPLIED	VARCHAR2(3)	NULL	Indicates whether the rule set is a default (that is, Oracle-supplied) rule set or a user-created rule set. Possible values are: <ul style="list-style-type: none"> <li>• YES if the rule set is a default rule set</li> <li>• NO if the rule set is a user-created rule set</li> </ul>

## 25.47 DVSYS.POLICY\_OWNER\_RULE\_SET\_RULE View

The `DVSYS.POLICY_OWNER_RULE_SET_RULE` data dictionary view enables users who have been granted the `DV_POLICY_OWNER` role to find information about the rule sets that contain rules used in Database Vault policies.

Examples of information that users can find include the rule set name and whether it is enabled. Only users who have been granted the `DV_POLICY_OWNER` role can query this view.

For example:

```
SELECT ENABLED FROM DVSYS.POLICY_OWNER_RULE_SET_RULE WHERE RULE_SET_NAME = 'Can
Maintain Own Account';
```

Output similar to the following appears:

```
ENABLED
-----
Y
```

### Related Views

- [DVSYS.POLICY\\_OWNER\\_COMMAND\\_RULE View](#) (page 25-48)
- [DVSYS.POLICY\\_OWNER\\_RULE\\_SET View](#) (page 25-54)
- [DVSYS.POLICY\\_OWNER\\_RULE View](#) (page 25-53)

Column	Datatype	Null	Description
RULE_SET_NAME	VARCHAR(128)	NOT NULL	Name of the rule set that contains the rule.
RULE_NAME	VARCHAR(128)	NOT NULL	Name of the rule.
RULE_EXPR	VARCHAR(1024)	NOT NULL	PL/SQL expression that defines the rule listed in the <code>RULE_NAME</code> column.
ENABLED	VARCHAR(1)		Indicates whether the rule is enabled or disabled. Y (Yes) enables the rule set; N (No) disables it.
RULE_ORDER	NUMBER	NOT NULL	The order in which rules are used within the rule set. Does not apply to this release.

## 25.48 SYS.DV\$CONFIGURATION\_AUDIT View

The `SYS.DV$CONFIGURATION_AUDIT` view is almost the same as the `DVSYS.DV$CONFIGURATION_AUDIT` view except that it captures unified audit trail Database Vault audit records.



**Related Topics:**

[DVSYS.DV\\$CONFIGURATION\\_AUDIT View](#) (page 25-38)

The DVSYS.DV\$CONFIGURATION\_AUDIT data dictionary view captures DVSYS.AUDIT\_TRAIL\$ table audit trail records.

## 25.49 SYS.DV\$ENFORCEMENT\_AUDIT View

The SYS.DV\$ENFORCEMENT\_AUDIT view is almost the same as the DVSYS.DV\$ENFORCEMENT\_AUDIT view except that it captures unified audit trail Database Vault audit records.

**Related Topics:**

[DVSYS.DV\\$ENFORCEMENT\\_AUDIT View](#) (page 25-43)

The DVSYS.DV\$ENFORCEMENT\_AUDIT data dictionary view provides information about enforcement-related audits from the DVSYS.AUDIT\_TRAIL\$ table.



---

## Monitoring Oracle Database Vault

You can monitor Oracle Database Vault by checking for violations to the Database Vault configurations and by tracking changes to policies.

### [About Monitoring Oracle Database Vault](#) (page 26-1)

You can use the Database Vault home page in Oracle Enterprise Manager Cloud Control to monitor a Database Vault-enabled database.

### [Monitoring Security Violations and Configuration Changes](#) (page 26-1)

A user who has been granted the appropriate role can use Oracle Database Vault Administrator to monitor security violations and configuration changes.

## 26.1 About Monitoring Oracle Database Vault

You can use the Database Vault home page in Oracle Enterprise Manager Cloud Control to monitor a Database Vault-enabled database.

This feature displays the top five attempted violations and who the top five attempted violators are. The attempted violations cover violations to realms and to command rules. The attempted violators is categorized into users and client hosts. By clicking the **Oracle Database Vault** link under Top 5 Attempted Violations, you can find details such as the type of violation, when it occurred, who the user was, and so on. Similarly, if you click the user link (for example, **SYS**) under Top 5 Attempted Violators, you can find detailed information about each violator, such as the action they performed, the client host name where the action originated, and when the violation occurred. You can manually refresh the data, and restrict the data view, such as within the last 24 hours. This page also shows a table listing all alerts that have been generated.

Before you can view these events, if you have not migrated your database to unified auditing, then you must ensure that the `AUDIT_TRAIL` initialization parameter is set to `DB` or `DB, EXTENDED`. If you have migrated your database to use unified auditing, then you do not need to configure any additional settings. You are ready to check for security violations.

### Related Topics:

### [Oracle Database Vault Reports](#) (page 27-1)

Oracle Database Vault provides reports that track activities, such as the Database Vault configuration settings.

## 26.2 Monitoring Security Violations and Configuration Changes

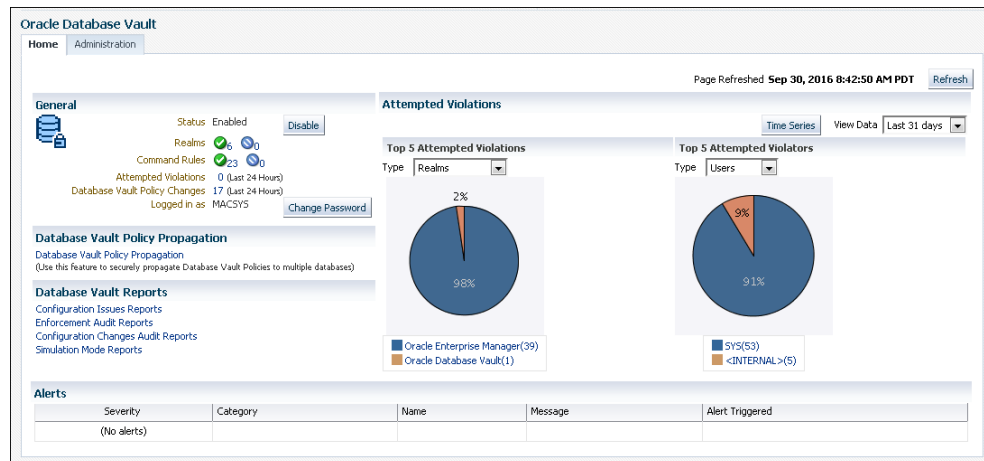
A user who has been granted the appropriate role can use Oracle Database Vault Administrator to monitor security violations and configuration changes.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the `DV_OWNER`, `DV_ADMIN`, or `DV_SECANALYST` role and the

SELECT ANY DICTIONARY privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.

2. Select the **Home** tab.

A page similar to the following appears:



3. To find attempted violations for a specific time, such as the last 7 days, select from the menu under the **Time Series** button in the upper right corner.

You also can change the pie chart to a graph by clicking the **Time Series** button.

4. To find the **Configuration Issues Reports**, **Enforcement Audit Reports**, **Configuration Changes Audit Reports**, and **Simulation Mode Reports**, select the appropriate link under Database Vault reports.

See [Oracle Database Vault Reports](#) (page 27-1) for detailed information about the Database Vault reports.

---

# Oracle Database Vault Reports

Oracle Database Vault provides reports that track activities, such as the Database Vault configuration settings.

[About the Oracle Database Vault Reports](#) (page 27-1)

Oracle Database Vault provides reports that display security-related information from the database.

[Who Can Run the Oracle Database Vault Reports?](#) (page 27-2)

Users must have the `DV_OWNER`, `DV_ADMIN`, or `DV_SECANALYST` role before they can run the Oracle Database Vault reports.

[Running the Oracle Database Vault Reports](#) (page 27-2)

A user who has been granted the appropriate roles can run the Oracle Database Vault reports from Database Vault Administrator.

[Oracle Database Vault Configuration Issues Reports](#) (page 27-3)

The configuration issues reports track the settings for command rules, rule sets, realms, and other Oracle Database Vault configurations.

[Oracle Database Vault Auditing Reports](#) (page 27-5)

If you have unified auditing enabled, then the Oracle Database Vault audit reports capture the results of unified audit policies.

[Oracle Database Vault General Security Reports](#) (page 27-7)

The general security reports track information such as object privileges related to `PUBLIC` or privileges granted to a database account or role.

## 27.1 About the Oracle Database Vault Reports

Oracle Database Vault provides reports that display security-related information from the database.

These reports also show custom Oracle Database Vault audit event information. If you have unified auditing enabled, then the reports capture the results of your unified audit policies.

The reports are in two categories:

- **Database Vault Reports.** These reports allow you to check configuration issues with realms, command rules, factors, factor identities, rule sets, and secure application roles. These reports also reveal realm violations, auditing results, and so on.
- **General Security Reports.** These reports allow you to check the status of object privileges, database account system privileges, sensitive objects, privilege management, powerful database accounts and roles, initialization parameters, profiles, account passwords, security audits, and other security vulnerability reports.

**Related Topics:**

[Oracle Database Vault-Specific Reports in Enterprise Manager Cloud Control](#) (page 13-4)

From the Database Vault home page, you can find information about violations.

[Oracle Database Vault Data Dictionary Views](#) (page 25-1)

You can find information about the Oracle Database Vault configuration settings by querying the Database Vault-specific data dictionary views.

## 27.2 Who Can Run the Oracle Database Vault Reports?

Users must have the `DV_OWNER`, `DV_ADMIN`, or `DV_SECANALYST` role before they can run the Oracle Database Vault reports.

**Related Topics:**

[DV\\_OWNER Database Vault Owner Role](#) (page 14-9)

The `DV_OWNER` role enables you to manage the Oracle Database Vault roles and its configuration.

[DV\\_ADMIN Database Vault Configuration Administrator Role](#) (page 14-11)

The `DV_ADMIN` role controls the Oracle Database Vault PL/SQL packages.

[DV\\_SECANALYST Database Vault Security Analyst Role](#) (page 14-13)

The `DV_SECANALYST` role enables users to analyze activities.

## 27.3 Running the Oracle Database Vault Reports

A user who has been granted the appropriate roles can run the Oracle Database Vault reports from Database Vault Administrator.

1. Log in to Oracle Database Vault Administrator from Cloud Control as a user who has been granted the `DV_OWNER`, `DV_ADMIN`, or `DV_SECANALYST` role and the `SELECT ANY DICTIONARY` privilege. [Logging into Oracle Database Vault](#) (page 3-10) explains how to log in.
2. In the Home page, under Reports, select **Database Vault Reports**.
3. On the left side, select the category of reports that you want.
  - Database Vault Configuration Issues
  - Database Vault Enforcement Audit Reports
  - Database Vault Configuration Changes
4. In the Reports page, expand the category that contains the report.

For example, to find the Rule Set Configurations Issues report, you must expand **Database Vault Configuration Issues**.

5. Select the report (for example, **Rule Set Configuration Issues**).

The report appears in the right pane.

6. Optionally, use the **Search** field to filter the report.

For example, you can search for reported incidents that involve a specific rule set. The Search field contents vary depending on the report.

7. When you finished viewing the report, click the **OK** button.

## 27.4 Oracle Database Vault Configuration Issues Reports

The configuration issues reports track the settings for command rules, rule sets, realms, and other Oracle Database Vault configurations.

### [Command Rule Configuration Issues Report](#) (page 27-3)

The Command Rule Configuration Issues Report displays command rules that have configuration issues.

### [Rule Set Configuration Issues Report](#) (page 27-3)

The Rule Set Configuration Issues Report displays Oracle Database Vault rule set configuration issues.

### [Realm Authorization Configuration Issues Report](#) (page 27-4)

The Realm Authorization Configuration Issues Report displays Oracle Database Vault realm configuration issues.

### [Factor Configuration Issues Report](#) (page 27-4)

The Factor Configuration Issues Report displays Oracle Database Vault factors configuration issues.

### [Factor Without Identities Report](#) (page 27-4)

The Factor Without Identities Report displays Oracle Database Vault factors that have no identities configured.

### [Identity Configuration Issues Report](#) (page 27-4)

The Identity Configuration Issues Report displays Oracle Database Vault factor identity configuration issues.

### [Secure Application Configuration Issues Report](#) (page 27-5)

The Secure Application Configuration Issues Report displays Database Vault secure application role configuration issues.

### 27.4.1 Command Rule Configuration Issues Report

The Command Rule Configuration Issues Report displays command rules that have configuration issues.

These issues are as follows:

- Rule set for the command rule is disabled.
- Rule set for the command rule is incomplete.
- Object owner for the command rule does not exist. This can happen when the user account for the object has been dropped.

### 27.4.2 Rule Set Configuration Issues Report

The Rule Set Configuration Issues Report displays Oracle Database Vault rule set configuration issues.

This report tracks when no rules are defined or enabled for a rule set.

### 27.4.3 Realm Authorization Configuration Issues Report

The Realm Authorization Configuration Issues Report displays Oracle Database Vault realm configuration issues.

These issues are as follows:

- Rule set for a realm authorization is disabled.
- Grantee does not exist for a realm authorization.
- Owner does not exist for a realm-secured object. This can happen when the user account has been dropped.

In most cases, however, these types of issues are caught when you configure the realm and during validation.

### 27.4.4 Factor Configuration Issues Report

The Factor Configuration Issues Report displays Oracle Database Vault factors configuration issues.

These issues are as follows:

- Rule set for factor assignment is disabled.
- Rule set for factor assignment is incomplete.
- Audit options for the factor are invalid.
- No factor retrieval method or constant exists.
- No subfactors (that is, child factors) are linked to a factor identity.
- No subfactors (child factors) are linked to a label factor.
- Oracle Label Security policy does not exist for the factor.

### 27.4.5 Factor Without Identities Report

The Factor Without Identities Report displays Oracle Database Vault factors that have no identities configured.

For some factors such as `Background_Job_Id`, this may not be a real problem, but the report can help you determine whether your access control configuration is complete and whether you have accounted for all factor configuration.

### 27.4.6 Identity Configuration Issues Report

The Identity Configuration Issues Report displays Oracle Database Vault factor identity configuration issues.

These issues are as follows:

- Label identity for the Oracle Label Security label for this identity has been removed and no longer exists.
- No map exists for the identity.



## 27.4.7 Secure Application Configuration Issues Report

The Secure Application Configuration Issues Report displays Database Vault secure application role configuration issues.

These issues are as follows:

- The database role does not exist. This can happen when the database role has been dropped.
- The rule set for role is disabled.
- The rule set for role is incomplete.

## 27.5 Oracle Database Vault Auditing Reports

If you have unified auditing enabled, then the Oracle Database Vault audit reports capture the results of unified audit policies.

### [Realm Audit Report](#) (page 27-5)

The Realm Audit Report shows audit records generated by the realm protection and realm authorization operations.

### [Command Rule Audit Report](#) (page 27-6)

The Command Rule Audit Report shows audit records generated by command rule processing operations.

### [Factor Audit Report](#) (page 27-6)

The Factor Audit Report shows factors that failed to evaluate or were set to create audit records under various conditions.

### [Label Security Integration Audit Report](#) (page 27-6)

The Label Security Integration Audit Report shows audit records the session initialization operation generates and the session label assignment operation of label security.

### [Core Database Vault Audit Trail Report](#) (page 27-6)

The Core Database Vault Audit Trail Report shows audit records that the core access security session initialization operation generates.

### [Secure Application Role Audit Report](#) (page 27-6)

The Secure Application Role Audit Report shows the audit records that the Oracle Database Vault secure application role-enabling operation generates.

### 27.5.1 Realm Audit Report

The Realm Audit Report shows audit records generated by the realm protection and realm authorization operations.

You can manage realm authorizations by using rule sets, and then audit the rule set processing results. A realm violation occurs when the database account, performing an action on a realm-protected object, is not authorized to perform that action. Oracle Database Vault audits the violation even if you do not specify any rule sets attached to the realm. When you configure a realm, you can set it to audit instances of realm violations. You can use this information to investigate attempts to break security.

## 27.5.2 Command Rule Audit Report

The Command Rule Audit Report shows audit records generated by command rule processing operations.

When you configure a command rule, you can set it to audit the rule set processing results.

## 27.5.3 Factor Audit Report

The Factor Audit Report shows factors that failed to evaluate or were set to create audit records under various conditions.

This report also shows failed attempts to set factors.

You can audit instances where a factor identity cannot be resolved and assigned (such as *No data found* or *Too many rows*). A factor can have an associated rule set that assigns an identity to the factor at run time. When you configure a factor, you can set it to audit the rule set processing results.

## 27.5.4 Label Security Integration Audit Report

The Label Security Integration Audit Report shows audit records the session initialization operation generates and the session label assignment operation of label security.

You can audit instances where the label security session fails to initialize, and where the label security component prevents a session from setting a label that exceeds the maximum session label.

## 27.5.5 Core Database Vault Audit Trail Report

The Core Database Vault Audit Trail Report shows audit records that the core access security session initialization operation generates.

You can audit instances where the access security session fails to initialize. It displays the following data:

<b>Data A-R</b>	<b>Data R-U</b>
Account	Rule Set
Command	Timestamp
Instance Number	Rule Set
Object Name	User Host
Return Code	-

## 27.5.6 Secure Application Role Audit Report

The Secure Application Role Audit Report shows the audit records that the Oracle Database Vault secure application role-enabling operation generates.

**Related Topics:**[Configuring Secure Application Roles for Oracle Database Vault](#) (page 9-1)

Secure application roles enable you to control how much access users have to an application.

## 27.6 Oracle Database Vault General Security Reports

The general security reports track information such as object privileges related to PUBLIC or privileges granted to a database account or role.

[Object Privilege Reports](#) (page 27-7)

The object privilege reports track privileges affected by PUBLIC, direct object privileges, and object dependencies.

[Database Account System Privileges Reports](#) (page 27-9)

The database account system privileges reports track activities such as direct, indirect, hierarchical, and ANY system privileges.

[Sensitive Objects Reports](#) (page 27-10)

The sensitive objects reports track activities such as grants on the EXECUTE privilege on SYS schema objects and access to sensitive objects.

[Privilege Management - Summary Reports](#) (page 27-12)

The privilege management summary reports track privilege distribution by grantees, owners, and privileges.

[Powerful Database Accounts and Roles Reports](#) (page 27-13)

The powerful database accounts and roles reports track information about users who have been granted power privileges, such as the WITH ADMIN privilege.

[Initialization Parameters and Profiles Reports](#) (page 27-16)

The initialization parameters and profiles reports track database parameters, resource profiles, and system limits.

[Database Account Password Reports](#) (page 27-17)

The database account password reports track default passwords and account statuses of database accounts.

[Security Audit Report: Core Database Audit Report](#) (page 27-17)

The Core Database Audit Report lists database audit trail records..

[Other Security Vulnerability Reports](#) (page 27-17)

Other security vulnerability reports track vulnerabilities that arise with activities such as Java policy grants in operating system directory objects.

### 27.6.1 Object Privilege Reports

The object privilege reports track privileges affected by PUBLIC, direct object privileges, and object dependencies.

[Object Access By PUBLIC Report](#) (page 27-8)

The Object Access By PUBLIC Report lists all objects whose access has been granted to PUBLIC.

[Object Access Not By PUBLIC Report](#) (page 27-8)

The Object Access Not By PUBLIC Report describes the object access used by the database accounts on the Report Parameters page.

**Direct Object Privileges Report** (page 27-8)

The Direct Object Privileges Report shows the direct object privileges granted to *nonsystem* database accounts.

**Object Dependencies Report** (page 27-9)

The Object Dependencies Report describes dependencies in the database between procedures, packages, functions, package bodies, and triggers.

**27.6.1.1 Object Access By PUBLIC Report**

The Object Access By PUBLIC Report lists all objects whose access has been granted to PUBLIC.

This report details all the object access the database accounts that you specify on the Report Parameters page, through object grants to PUBLIC. On the Reports Parameters page, you can filter the results based on the privilege, the object owner, or the object name.

---

---

**Note:**

This report can be quite large if you choose the defaults.

---

---

**27.6.1.2 Object Access Not By PUBLIC Report**

The Object Access Not By PUBLIC Report describes the object access used by the database accounts on the Report Parameters page.

It checks the grants to the account directly or through a role, but excluding the grants to PUBLIC.

On the Reports Parameters page, you can filter the results based on the privilege, the object owner or the object name.

---

---

**Note:**

This report can be quite large if you choose the defaults.

---

---

**27.6.1.3 Direct Object Privileges Report**

The Direct Object Privileges Report shows the direct object privileges granted to *nonsystem* database accounts.

The following database accounts are excluded from the report:

**Accounts C-O**

CTXSYS

DMSYS

DVSYS

LBACSYS

MDSYS

ORDSYS

**Accounts P-W**

PUBLIC

SYS

SYSMAN

SYSTEM

WKSYS

WMSYS

### 27.6.1.4 Object Dependencies Report

The Object Dependencies Report describes dependencies in the database between procedures, packages, functions, package bodies, and triggers.

The report includes dependencies on views created without any database links.

This report can help you develop a security policy using the principle of least privilege for existing applications. If a database object, such as a `UTL_FILE` package, has privileges granted to `PUBLIC` or some other global role, then you can use the Object Dependencies Report to determine an account that may depend on the object and to determine how the account uses the object. To run the report, enter the database account you are inspecting for dependency and the object it may be dependent on, in the Report Parameters page.

The Report Results page shows the dependent object and object type and the source object name and type. This report shows where the potentially sensitive object is being used. By looking at several accounts, you might be able to see patterns that can help you develop restricted roles. These restricted roles can replace `PUBLIC` grants on widely used sensitive objects.

## 27.6.2 Database Account System Privileges Reports

The database account system privileges reports track activities such as direct, indirect, hierarchical, and `ANY` system privileges.

### [Direct System Privileges By Database Account Report](#) (page 27-9)

The Direct System Privileges By Database Account Report lists system privileges directly granted to the database account selected on the Report Parameters page.

### [Direct and Indirect System Privileges By Database Account Report](#) (page 27-10)

The Direct and Indirect System Privileges By Database Account Report displays system privileges for the database account selected on the Report Parameters page.

### [Hierarchical System Privileges by Database Account Report](#) (page 27-10)

The Hierarchical System Privileges by Database Account Report shows a hierarchical breakdown of role-based system privileges and direct system privileges.

### [ANY System Privileges for Database Accounts Report](#) (page 27-10)

The ANY System Privileges for Database Accounts Report shows `ANY` system privileges granted to the specified database account or role.

### [System Privileges By Privilege Report](#) (page 27-10)

The System Privileges By Privilege Report lists database accounts and roles that have the system privilege selected on the Report Parameters page.

### 27.6.2.1 Direct System Privileges By Database Account Report

The Direct System Privileges By Database Account Report lists system privileges directly granted to the database account selected on the Report Parameters page.

This report also shows whether a privilege has been granted the `WITH ADMIN` option.

### 27.6.2.2 Direct and Indirect System Privileges By Database Account Report

The Direct and Indirect System Privileges By Database Account Report displays system privileges for the database account selected on the Report Parameters page.

The system privileges may have been granted directly or granted through a database role that has the `WITH ADMIN` status.

### 27.6.2.3 Hierarchical System Privileges by Database Account Report

The Hierarchical System Privileges by Database Account Report shows a hierarchical breakdown of role-based system privileges and direct system privileges.

These privileges are granted to the database account specified on the Report Parameters page.

### 27.6.2.4 ANY System Privileges for Database Accounts Report

The ANY System Privileges for Database Accounts Report shows ANY system privileges granted to the specified database account or role.

ANY system privileges are very powerful and should be judiciously assigned to accounts and roles.

### 27.6.2.5 System Privileges By Privilege Report

The System Privileges By Privilege Report lists database accounts and roles that have the system privilege selected on the Report Parameters page.

Another way to control privileges is to create privilege analysis policies to analyze privilege use.

## 27.6.3 Sensitive Objects Reports

The sensitive objects reports track activities such as grants on the `EXECUTE` privilege on `SYS` schema objects and access to sensitive objects.

#### [Execute Privileges to Strong SYS Packages Report](#) (page 27-10)

The Execute Privileges to Strong SYS Packages Report shows database accounts and roles with the `EXECUTE` privilege on powerful system packages.

#### [Access to Sensitive Objects Report](#) (page 27-11)

The Access to Sensitive Objects Report shows database accounts and roles that have object privileges on system tables or views that have sensitive information.

#### [Public Execute Privilege To SYS PL/SQL Procedures Report](#) (page 27-12)

The Public Execute Privilege to SYS PL/SQL Procedures Report shows database accounts and roles that have `EXECUTE` privileges on that `SYS` owns.

#### [Accounts with SYSDBA/SYSOPER Privilege Report](#) (page 27-12)

The Accounts with SYSDBA/SYSOPER Privilege Report displays database accounts that have `SYS`-privileged connection privileges.

### 27.6.3.1 Execute Privileges to Strong SYS Packages Report

The Execute Privileges to Strong SYS Packages Report shows database accounts and roles with the `EXECUTE` privilege on powerful system packages.

For example, these types of packages can be used to access operating system resources.

The following system PL/SQL packages are included:

#### Packages D-D

DBMS\_ALERT  
 DBMS\_BACKUP\_RESTORE  
 DBMS\_CAPTURE\_ADM  
 DBMS\_DDL  
 DBMS\_DISTRIBUTED\_TRUST\_ADMIN  
 DBMS\_FGA  
 DBMS\_JOB  
 DBMS\_LDAP  
 DBMS\_LOB  
 DBMS\_LOGMNR  
 DBMS\_LOGMNR\_D  
 DBMS\_OBFUSCATION\_TOOLKIT  
 DBMS\_ORACLE\_TRACE\_AGENT  
 DBMS\_PIPE

#### Packages D-U

DBMS\_RANDOM  
 DBMS\_REPAIR  
 DBMS\_REPCAT  
 DBMS\_REPCAT\_ADMIN  
 DBMS\_RESOURCE\_MANAGER  
 DBMS\_RESOURCE\_MANAGER\_PRIVS  
 DBMS\_RLS  
 DBMS\_SESSION  
 DEBUG\_EXTPROC  
 UTL\_FILE  
 UTL\_HTTP  
 UTL\_SMTP  
 UTL\_TCP  
 -

### 27.6.3.2 Access to Sensitive Objects Report

The Access to Sensitive Objects Report shows database accounts and roles that have object privileges on system tables or views that have sensitive information.

This report includes the following system tables and views:

#### Tables/Views A-O

ALL\_SOURCE  
 ALL\_USERS  
 APPROLE\$  
 AUD\$  
 AUDIT\_TRAIL\$  
 DBA\_ROLE\_PRIVS  
 DBA\_ROLES  
 DBA\_TAB\_PRIVS  
 DBMS\_BACKUP\_RESTORE

#### Tables/Views P-S

PROFILE\$  
 PROXY\_ROLE\_DATA\$  
 PROXY\_ROLE\_INFO\$  
 ROLE\_ROLE\_PRIVS  
 SOURCE\$  
 STATS\$SQLTEXT  
 STATS\$SQL\_SUMMARY  
 STREAMS\$\_PRIVILEGED\_USER  
 SYSTEM\_PRIVILEGE\_MAP

**Tables/Views A-O**

DEFROLE\$

FGA\_LOG\$

LINK\$

OBJ\$

OBJAUTH\$

OBJPRIV\$

**Tables/Views P-S**

TABLE\_PRIVILEGE\_MAP

TRIGGER\$

USER\$

USER\_HISTORY\$

USER\_TAB\_PRIVS

SYSTEM\_PRIVILEGE\_MAP

**27.6.3.3 Public Execute Privilege To SYS PL/SQL Procedures Report**

The Public Execute Privilege to SYS PL/SQL Procedures Report shows database accounts and roles that have EXECUTE privileges on that SYS owns.

This report can be used to determine which privileges can be revoked from PUBLIC, or from other accounts and roles. This reduces vulnerabilities as part of an overall security policy implementation using the principle of least privilege.

**27.6.3.4 Accounts with SYSDBA/SYSOPER Privilege Report**

The Accounts with SYSDBA/SYSOPER Privilege Report displays database accounts that have SYS-privileged connection privileges.

This report also shows whether the accounts use an external password. However, note that this report does not include operating system users who can become SYSDBA.

**27.6.4 Privilege Management - Summary Reports**

The privilege management summary reports track privilege distribution by grantees, owners, and privileges.

**[Privileges Distribution By Grantee Report](#)** (page 27-13)

The Privileges Distribution By Grantee Report displays the count of privileges granted to a database account or role.

**[Privileges Distribution By Grantee, Owner Report](#)** (page 27-13)

The Privileges Distribution By Grantee, Owner Report displays a count of privileges based on the grantee and the owner of the object.

**[Privileges Distribution By Grantee, Owner, Privilege Report](#)** (page 27-13)

The Privileges Distribution By Grantee, Owner, Privilege Report displays a count of privileges based on the privilege, the grantee, and the object owner.

---

---

**See Also:**

[DBA\\_DV\\_PUB\\_PRIVS View](#) (page 25-23) to find the values on which the counts listed in these reports are based

---

---



#### 27.6.4.1 Privileges Distribution By Grantee Report

The Privileges Distribution By Grantee Report displays the count of privileges granted to a database account or role.

This report provides insight into accounts and roles that may have powerful privileges.

#### 27.6.4.2 Privileges Distribution By Grantee, Owner Report

The Privileges Distribution By Grantee, Owner Report displays a count of privileges based on the grantee and the owner of the object.

This report provides insight into accounts or roles that may have powerful privileges. You can use this report if you suspect potential intruders or insider threats are looking for accounts that have powerful privileges as accounts to attack or compromise. If intruders can compromise the account (for example, by guessing the password), they can get more privileges than they already have.

#### 27.6.4.3 Privileges Distribution By Grantee, Owner, Privilege Report

The Privileges Distribution By Grantee, Owner, Privilege Report displays a count of privileges based on the privilege, the grantee, and the object owner.

This report provides insight into the accounts or roles that may have powerful privileges.

### 27.6.5 Powerful Database Accounts and Roles Reports

The powerful database accounts and roles reports track information about users who have been granted power privileges, such as the `WITH ADMIN` privilege.

#### [WITH ADMIN Privilege Grants Report](#) (page 27-14)

The WITH ADMIN Privileges Grants Report shows all database accounts and roles that have been granted privileges with the `WITH ADMIN` clause.

#### [Accounts With DBA Roles Report](#) (page 27-14)

The Accounts With DBA Roles Report shows all database accounts that have the `DBA` role granted to them.

#### [Security Policy Exemption Report](#) (page 27-14)

The Security Policy Exemption Report shows database (but not Oracle Database Vault) accounts and roles that have the `EXEMPT ACCESS POLICY` system privilege.

#### [BECOME USER Report](#) (page 27-14)

The BECOME USER Report shows database accounts roles that have the `BECOME USER` system privilege.

#### [ALTER SYSTEM or ALTER SESSION Report](#) (page 27-15)

The ALTER SYSTEM or ALTER SESSION Report shows database accounts and roles that have the `ALTER SYSTEM` or `ALTER SESSION` privilege.

#### [Password History Access Report](#) (page 27-15)

The Password History Access Report shows database accounts that have access to the `USER_HISTORY$` table.

**WITH GRANT Privileges Report** (page 27-15)

The WITH GRANT Privileges Report shows database accounts that are granted privileges with the WITH GRANT clause.

**Roles/Accounts That Have a Given Role Report** (page 27-15)

This report displays the database accounts and roles to which a role has been granted.

**Database Accounts With Catalog Roles Report** (page 27-15)

The Database Accounts With Catalog Roles Report displays all database accounts and roles that have the catalog-related roles granted to them.

**AUDIT Privileges Report** (page 27-16)

The AUDIT Privileges Report displays all database accounts and roles that have the AUDIT ANY or AUDIT SYSTEM privilege.

**OS Security Vulnerability Privileges Report** (page 27-16)

The OS Security Vulnerability Privileges Report lists database accounts and roles that have privileges to export sensitive information to the operating system.

**27.6.5.1 WITH ADMIN Privilege Grants Report**

The WITH ADMIN Privileges Grants Report shows all database accounts and roles that have been granted privileges with the WITH ADMIN clause.

This privilege can be misused to give another account more system privileges than required.

**27.6.5.2 Accounts With DBA Roles Report**

The Accounts With DBA Roles Report shows all database accounts that have the DBA role granted to them.

The DBA role is a privileged role that can be misused. It is often granted to a database account to save time and to avoid having to determine the least number of privileges an account really needs. This report can help you to start applying a policy using the principle of least privilege to an existing database.

---

---

**See Also:** [Oracle Database Vault Security Guidelines](#) (page D-1) for guidelines on deciding who should have privileged roles

---

---

**27.6.5.3 Security Policy Exemption Report**

The Security Policy Exemption Report shows database (but not Oracle Database Vault) accounts and roles that have the EXEMPT ACCESS POLICY system privilege.

Accounts that have this privilege can bypass all Virtual Private Database (VPD) policy filters and any Oracle Label Security policies that use Oracle Virtual Private Database indirectly. This is a powerful system privilege that should be granted only if absolutely necessary, as it presents a target to gain access to sensitive information in tables that are protected by Oracle Virtual Private Database or Oracle Label Security. You can use the auditing policies described in [Auditing Oracle Database Vault](#) (page A-1), to audit the use of this privilege.

**27.6.5.4 BECOME USER Report**

The BECOME USER Report shows database accounts roles that have the BECOME USER system privilege.

The `BECOME USER` privilege is a very powerful system privilege: it enables the `IMP_FULL_DATABASE` and `EXP_FULL_DATABASE` roles for use with Oracle Data Pump. Accounts that possess this privilege can be misused to get sensitive information or to compromise an application.

#### 27.6.5.5 ALTER SYSTEM or ALTER SESSION Report

The `ALTER SYSTEM` or `ALTER SESSION` Report shows database accounts and roles that have the `ALTER SYSTEM` or `ALTER SESSION` privilege.

Oracle recommends that you restrict these privileges only to those accounts and roles that truly need them (for example, the `SYS` account and the `DV_ADMIN` role). The `ALTER SYSTEM` statement can be used to change the security-related database initialization parameters that are set to recommended values as part of the Oracle Database Vault security strengthening service. Both the `ALTER SYSTEM` and `ALTER SESSION` statements can be used to dump database trace files, potentially containing sensitive configuration information, to the operating system.

---

**See Also:** [ALTER SYSTEM and ALTER SESSION Privilege Security Considerations](#) (page D-14) for guidelines on using the `ALTER SYSTEM` and `ALTER SESSION` privileges

---

#### 27.6.5.6 Password History Access Report

The Password History Access Report shows database accounts that have access to the `USER_HISTORY$` table.

This table stores hashed passwords that were previously used by each account.

Access to this table can make guessing the existing password for an account easier for someone hacking the database.

#### 27.6.5.7 WITH GRANT Privileges Report

The `WITH GRANT` Privileges Report shows database accounts that are granted privileges with the `WITH GRANT` clause.

Remember that `WITH GRANT` is used for object-level privileges: An account that has been granted privileges using the `WITH GRANT` option can be misused to grant object privileges to another account.

#### 27.6.5.8 Roles/Accounts That Have a Given Role Report

This report displays the database accounts and roles to which a role has been granted.

This report is provided for dependency analysis.

#### 27.6.5.9 Database Accounts With Catalog Roles Report

The Database Accounts With Catalog Roles Report displays all database accounts and roles that have the catalog-related roles granted to them.

These roles are as follows:

- `DELETE_CATALOG_ROLE`
- `EXECUTE_CATALOG_ROLE`
- `RECOVERY_CATALOG_OWNER`
- `SELECT_CATALOG_ROLE`

These catalog-based roles have a very large number of powerful privileges. They should be granted with caution, much like the DBA role, which uses them.

#### **27.6.5.10 AUDIT Privileges Report**

The AUDIT Privileges Report displays all database accounts and roles that have the `AUDIT ANY` or `AUDIT SYSTEM` privilege.

This privilege can be used to disable auditing, which could be used to eliminate the audit trail record of an intruder who has compromised the system. The accounts that have this privilege could be targets for intruders.

#### **27.6.5.11 OS Security Vulnerability Privileges Report**

The OS Security Vulnerability Privileges Report lists database accounts and roles that have privileges to export sensitive information to the operating system.

This report can reveal important vulnerabilities related to the operating system.

### **27.6.6 Initialization Parameters and Profiles Reports**

The initialization parameters and profiles reports track database parameters, resource profiles, and system limits.

#### [Security Related Database Parameters Report](#) (page 27-16)

The Security Related Database Parameters Report lists database parameters that can cause security vulnerabilities if they are not set correctly.

#### [Resource Profiles Report](#) (page 27-16)

The Resource Profiles Report lists resource profiles that may be allowing unlimited resource consumption.

#### [System Resource Limits Report](#) (page 27-16)

The System Resource Limits Report provides insight into the current system resource usage by the database.

#### **27.6.6.1 Security Related Database Parameters Report**

The Security Related Database Parameters Report lists database parameters that can cause security vulnerabilities if they are not set correctly.

This report can be used to compare the recommended settings with the current state of the database parameter values.

#### **27.6.6.2 Resource Profiles Report**

The Resource Profiles Report lists resource profiles that may be allowing unlimited resource consumption.

Examples of resource profiles are `CPU_PER_SESSION` and `IDLE_TIME`. You should review the profiles that might need a cap on the potential resource usage.

#### **27.6.6.3 System Resource Limits Report**

The System Resource Limits Report provides insight into the current system resource usage by the database.

This report helps determine whether any of these resources are approaching their limits under the existing application load. Resources that show large increases over a

short period may point to a denial-of-service (DoS) attack. You might want to reduce the upper limit for the resource to prevent the condition in the future.

## 27.6.7 Database Account Password Reports

The database account password reports track default passwords and account statuses of database accounts.

### [Database Account Default Password Report](#) (page 27-17)

The Database Account Default Password Report lists the database accounts that have default passwords.

### [Database Account Status Report](#) (page 27-17)

The Database Account Status Report lists existing database accounts.

### 27.6.7.1 Database Account Default Password Report

The Database Account Default Password Report lists the database accounts that have default passwords.

Default passwords are provided during the Oracle Database installation.

You should change the passwords for accounts included in this report to nondefault, complex passwords to help secure the database.

### 27.6.7.2 Database Account Status Report

The Database Account Status Report lists existing database accounts.

This report shows the account status for each account, which helps you identify accounts that must be locked. Lock and expiry dates provide information that helps determine whether the account was locked as a result of password aging. If a special password and resource secure profile is used, then you can identify accounts that are not using them. Accounts not using organizationally defined default tablespaces also can be identified, and the temporary tablespace for accounts can be determined. This report also identifies accounts that use external passwords.

## 27.6.8 Security Audit Report: Core Database Audit Report

The Core Database Audit Report lists database audit trail records..

This report applies to a non-unified auditing environment.

The Core Database Audit Report returns audit records for the audit policy defined in [Auditing Oracle Database Vault](#) (page A-1), and any auditing records that are generated for audit statements you have defined.

This report only displays audit records that are captured if the database initialization parameter `AUDIT_TRAIL` has been set to `DB` (with unified auditing disabled).

---

**See Also:** *Oracle Database Reference* for more information about the `AUDIT_TRAIL` parameter

---

## 27.6.9 Other Security Vulnerability Reports

Other security vulnerability reports track vulnerabilities that arise with activities such as Java policy grants in operating system directory objects.

**Java Policy Grants Report** (page 27-18)

The Java Policy Grants Report shows the Java policy permissions stored in the database.

**OS Directory Objects Report** (page 27-18)

The OS Directory Objects Report shows directory objects in the database, their privileges, and whether they are available to PUBLIC.

**Objects Dependent on Dynamic SQL Report** (page 27-18)

The Objects Dependent on Dynamic SQL Report lists objects that use dynamic SQL.

**Unwrapped PL/SQL Package Bodies Report** (page 27-19)

The Unwrapped PL/SQL Package Bodies Report lists PL/SQL package procedures that are not wrapped.

**Username/Password Tables Report** (page 27-19)

The Username/Password Tables Report identifies application tables in the database that store user names and password strings.

**Tablespace Quotas Report** (page 27-19)

The Tablespace Quotas Report lists database accounts that have quotas on one or more tablespaces.

**Non-Owner Object Trigger Report** (page 27-19)

The Non-Owner Object Trigger Report lists non-owner triggers.

**27.6.9.1 Java Policy Grants Report**

The Java Policy Grants Report shows the Java policy permissions stored in the database.

This report helps reveal violations to the principle of least privilege. Look for GRANT, READ, or WRITE privileges to PUBLIC or other accounts and roles that do not necessarily need the privilege. It is advisable to disable Java loading privileges from PUBLIC, if Java is not required in the database.

---

**Note:**

Oracle JVM, the Java virtual machine option provided with Oracle Database Vault, must be installed before you can run the Java Policy Grants Report.

---

**27.6.9.2 OS Directory Objects Report**

The OS Directory Objects Report shows directory objects in the database, their privileges, and whether they are available to PUBLIC.

Directory objects should exist only for secured operating system (OS) directories, and access to them within the database should be protected. You should never use the root operating system directory on any storage device (for example, /), because it allows remote database sessions to look at all files on the device.

**27.6.9.3 Objects Dependent on Dynamic SQL Report**

The Objects Dependent on Dynamic SQL Report lists objects that use dynamic SQL.

Potential intruders have a greater chance of using this channel if parameter checking or bind variables are not used. The report helps by narrowing the scope of where to look for problems by pointing out who is using dynamic SQL. Such objects can be a

target for a SQL injection attack and must be secured to avoid this type of attack. After determining the objects that use dynamic SQL, do the following:

- Check the privileges that client applications (for example, a Web application) have over the object.
- Check the access granted for the object to `PUBLIC` or a wider account base.
- Validate parameters.
- Use bind variables where possible.

#### **27.6.9.4 Unwrapped PL/SQL Package Bodies Report**

The Unwrapped PL/SQL Package Bodies Report lists PL/SQL package procedures that are not wrapped.

Oracle provides a wrap utility that obfuscates code to the point where it cannot be read in the data dictionary or from the data dictionary views. This helps reduce the ability of an intruder to circumvent data protection by eliminating the ability to read source code that manipulates data.

#### **27.6.9.5 Username/Password Tables Report**

The Username/Password Tables Report identifies application tables in the database that store user names and password strings.

You should examine these tables to determine if the information is encrypted. (Search for column names such as `%USER%NAME%` or `%PASSWORD%`.) If it is not, modify the code and applications using these tables to protect them from being visible to database sessions.

#### **27.6.9.6 Tablespace Quotas Report**

The Tablespace Quotas Report lists database accounts that have quotas on one or more tablespaces.

These tablespaces can become potential targets for denial-of-service (DoS) attacks.

#### **27.6.9.7 Non-Owner Object Trigger Report**

The Non-Owner Object Trigger Report lists non-owner triggers.

These are triggers that are owned by a database account that is different from the account that owns the database object on which the trigger acts.

If the trigger is not part of a trusted database application, then it can *steal* sensitive data, possibly from tables protected through Oracle Label Security or Virtual Private Database (VPD), and place it into an unprotected table for subsequent viewing or export.





---

# Auditing Oracle Database Vault

You can audit activities in Oracle Database Vault, such as changes to policy configurations.

[About Auditing in Oracle Database Vault](#) (page A-1)

All activities in Oracle Database Vault can be audited, including Database Vault administrator activities.

[Protection of the Unified Audit Trail in an Oracle Database Vault Environment](#) (page A-2)

By default, AUDSYS schema, which contains the unified audit trail, is not protected by a realm.

[Oracle Database Vault Specific Audit Events](#) (page A-3)

Oracle Database Vault audit events track activities such as whether an action attempted on a realm was successful.

[Archiving and Purging the Oracle Database Vault Audit Trail](#) (page A-6)

If you have not migrated to unified auditing, you should periodically archive and purge the Oracle Database Vault audit trail.

[Oracle Database Audit Settings Created for Oracle Database Vault](#) (page A-9)

When you install Oracle Database Vault, it creates several AUDIT settings in the database.

## A.1 About Auditing in Oracle Database Vault

All activities in Oracle Database Vault can be audited, including Database Vault administrator activities.

Optionally, you can audit individual policies that you create for realms, rule sets, and factors. The audit indicates if the user's action succeeded (that is, the policy enabled the user to accomplish a task) or if the user's action failed (the policy was violated). These actions are written to audit logs, whose contents you can find either by querying the appropriate data dictionary views, or running the reports described in [Oracle Database Vault Reports](#) (page 27-1).

All configuration changes made to Database Vault are mandatorily audited, including actions of unprivileged users who attempt to modify Database Vault policies.

When you install a new database and configure it to use Oracle Database Vault, then by default it uses a mixed-mode environment, that is, a mixture of unified auditing and pre-migrated auditing. If you have upgraded from previous release, then Database Vault uses the auditing that was available from that release.

Before you migrate to a full unified auditing environment, you can create audit policies as follows:

- **Using the Database Vault APIs:** That is, you use the `DBMS_MACADM` PL/SQL package or the Database Vault pages in Enterprise Manager. In this case, the audit records are written to the Database Vault audit trail, which is stored in the `DVSY$ . AUDIT_TRAIL$` table. You can query the `DVSY$ . DV$CONFIGURATION_AUDIT` and `DVSY$ . DV$ENFORCEMENT_AUDIT` views for these audit records.
- **Using the unified audit policy SQL statements:** These statements are the `CREATE AUDIT POLICY`, `ALTER AUDIT POLICY`, `DROP AUDIT POLICY`, `AUDIT`, and `NO AUDIT` statements. They are written to the unified audit trail, which is captured by the `UNIFIED_AUDIT_TRAIL`, `SYS . DV$CONFIGURATION_AUDIT`, and `SYS . DV$ENFORCEMENT_AUDIT` data dictionary views.

When you migrate to unified auditing, then the auditing features in the Database Vault APIs are no longer effective. You should archive and purge these audit records, as described in [Archiving and Purging the Oracle Database Vault Audit Trail](#) (page A-6). From then on, you can manage Database Vault audit policies through the unified audit policy PL/SQL statements.

Except where noted, the remaining sections of this chapter describe how Database Vault auditing works in a non-unified or mixed mode auditing environment.

---

---

**See Also:**

- *Oracle Database Security Guide* for information about how unified auditing works in Oracle Database Vault and how to create unified audit policies
  - [Oracle Database Vault Audit Trail Record Format](#) (page A-3)
  - The following data dictionary views, which are specific to Database Vault unified auditing:
    - [DVSY\\$ . DV\\$CONFIGURATION\\_AUDIT View](#) (page 25-38)
    - [DVSY\\$ . DV\\$ENFORCEMENT\\_AUDIT View](#) (page 25-43)
  - *Oracle Database Upgrade Guide* to migrate your database to unified auditing
- 
- 

## A.2 Protection of the Unified Audit Trail in an Oracle Database Vault Environment

By default, `AUDSYS` schema, which contains the unified audit trail, is not protected by a realm.

A realm is not necessary for the `AUDSYS` schema because the information it contains is internal and cannot be viewed in the same way that other database objects (such as tables or views) can be viewed in a schema. To protect the unified audit trail, create a realm around the `AUDIT_ADMIN` and `AUDIT_VIEWER` roles. This way, you can control who can grant these roles.

**Related Topics:**

[Creating a Realm](#) (page 5-8)

To enable realm protection, you create the realm and configure it to include realm-secured objects, roles, and authorizations.

## A.3 Oracle Database Vault Specific Audit Events

Oracle Database Vault audit events track activities such as whether an action attempted on a realm was successful.

### [Oracle Database Vault Policy Audit Events](#) (page A-3)

Oracle Database Vault uses audit events to track configuration activities.

### [Oracle Database Vault Audit Trail Record Format](#) (page A-3)

If you do not use unified auditing, then Oracle Database Vault writes audit records to the `DVSYSAUDIT_TRAIL$` table.

### A.3.1 Oracle Database Vault Policy Audit Events

Oracle Database Vault uses audit events to track configuration activities.

These activities are as follows:

- **Realm Audit.** You can audit both successful and failed actions, based on the auditing option that you set when you created the realm. The exception to this is actions performed by the schema owner.
- **Rule Set Audit.** Audits the rule set processing results. You can audit both successful and failed processing. Realm authorizations can be managed using rule sets. You can audit the rule set processing results. Factor assignments and secure application roles audits can be managed using a rule set.
- **Factor Audit.** You can audit both successful and failed factor processing. For failed factor processing, you can audit on all or any of the following events: Retrieval Error, Retrieval Null, Validation Error, Validation False, Trust Level Null, or Trust Level Less Than Zero.
- **Oracle Label Security Session Initialization Failed.** Audits instances where the Oracle Label Security session fails to initialize.
- **Oracle Label Security Attempt to Upgrade Session Label Failed.** Audits instances where the Oracle Label Security component prevents a session from setting a label that exceeds the maximum session label.

#### Related Topics:

### [Setting Audit Options for a Factor](#) (page 8-13)

Under Audit Options, you can generate an audit trail if you are not using a unified audit environment.

### [About Realm Authorization](#) (page 5-13)

Realm authorizations establish the set of database accounts and roles that manage or access objects protected in realms.

### [Oracle Database Vault Reports](#) (page 27-1)

Oracle Database Vault provides reports that track activities, such as the Database Vault configuration settings.

### A.3.2 Oracle Database Vault Audit Trail Record Format

If you do not use unified auditing, then Oracle Database Vault writes audit records to the `DVSYSAUDIT_TRAIL$` table.

These audit records are not part of the Oracle Database audit trail, and how auditing is enabled in the database has no effect how Oracle Database Vault collects its audit data in the `DVSYS.AUDIT_TRAIL$` table. In fact, even if auditing has been disabled in Oracle Database, then the Oracle Database Vault audit functionality continues to write to the `DVSYS.AUDIT_TRAIL$` table.

Users who have been granted the `DV_OWNER`, `DV_ADMIN`, `DV_SECANALYST` or `DV_MONITOR` role can directly query the `DVYS.AUDIT_TRAIL$` table.

[Table A-1](#) (page A-4) describes the format of the audit trail, which you must understand if you plan to create custom reports that use the `DVSYS.AUDIT_TRAIL$` table.

**Table A-1 Oracle Database Vault Audit Trail Format**

Column	Datatype	Null	Description
ID#	NUMBER	NOT NULL	Numeric identifier for the audit record
OS_USERNAME	VARCHAR2(255)	NULL	Operating system login user name of the user whose actions were audited
USERNAME	VARCHAR2(30)	NULL	Name of the database user whose actions were audited
USERHOST	VARCHAR2(128)	NULL	Client computer name
TERMINAL	VARCHAR2(255)	NULL	Identifier for the user's terminal
TIMESTAMP	DATE	NULL	Date and time of creation of the audit trail entry (in the local database session time zone)
OWNER	VARCHAR2(30)	NULL	Creator of the object affected by the action, always <code>DVSYS</code> (because <code>DVSYS</code> is where objects are created)
OBJ_NAME	VARCHAR2(128)	NULL	Name of the object affected by the action. Expected values are: <ul style="list-style-type: none"> <li>• <code>ROLE\$</code></li> <li>• <code>REALM\$</code></li> <li>• <code>CODE\$</code></li> <li>• <code>FACTOR\$</code></li> </ul>
ACTION	NUMBER	NOT NULL	Numeric action type code. The corresponding name of the action type is in the <code>ACTION_NAME</code> column. See <a href="#">Table 25-3</a> (page 25-40) for a list of the expected <code>ACTION</code> and <code>ACTION_NAME</code> values.
ACTION_NAME	VARCHAR2(128)	NULL	Name of the action type corresponding to the numeric code in the <code>ACTION</code> column
ACTION_OBJECT_ID	NUMBER	NULL	The unique identifier of the record in the table specified under <code>OBJ_NAME</code> . For realms, this field contains a list of comma-separated values of all realm IDs that have the Audit on Failure audit option.

**Table A-1 (Cont.) Oracle Database Vault Audit Trail Format**

Column	Datatype	Null	Description
ACTION_OBJECT_NAME	VARCHAR2 ( 128 )	NULL	The unique name or natural key of the record in the table specified under OBJ_NAME. For realms, this field contains a list of comma-separated values of all realm names that have the Audit on Failure audit option.
ACTION_COMMAND	VARCHAR2 ( 4000 )	NULL	The SQL text of the command procedure that was executed that resulted in the audit event being triggered
AUDIT_OPTION	VARCHAR2 ( 4000 )	NULL	The labels for all audit options specified in the record that resulted in the audit event being triggered. For example, a factor set operation that is supposed to audit on get failure and get NULL would indicate these two options.
RULE_SET_ID	NUMBER	NULL	The unique identifier of the rule set that was executing and caused the audit event to trigger
RULE_SET_NAME	VARCHAR2 ( 30 )	NULL	The unique name of the rule set that was executing and caused the audit event to trigger
RULE_ID	NUMBER	NULL	Not used
RULE_NAME	VARCHAR2 ( 30 )	NULL	Not used
FACTOR_CONTEXT	VARCHAR2 ( 4000 )	NULL	An XML document that contains all of the factor identifiers for the current session at the point when the audit event was triggered
COMMENT_TEXT	VARCHAR2 ( 4000 )	NULL	Text comment on the audit trail entry, providing more information about the statement audited
SESSIONID	NUMBER	NOT NULL	Numeric identifier for each Oracle session
ENTRYID	NUMBER	NOT NULL	Same as the value in the ID# column
STATEMENTID	NUMBER	NOT NULL	Numeric identifier for the statement invoked that caused the audit event to be generated. This is empty for most Oracle Database Vault events.
RETURNCODE	NUMBER	NOT NULL	Oracle error code generated by the action. The error code for a statement or procedure invoked that caused the audit event to be generated. This is empty for most Oracle Database Vault events.
EXTENDED_TIMESTAMP	TIMESTAMP ( 6 ) WITH TIME ZONE	NULL	Time stamp of creation of the audit trail entry (time stamp of user login for entries) in UTC (Coordinated Universal Time) time zone
PROXY_SESSIONID	NUMBER	NULL	Proxy session serial number, if an enterprise user has logged in through the proxy mechanism
GLOBAL_UID	VARCHAR2 ( 32 )	NULL	Global user identifier for the user, if the user has logged in as an enterprise user

**Table A-1 (Cont.) Oracle Database Vault Audit Trail Format**

Column	Datatype	Null	Description
INSTANCE_NUMBER	NUMBER	NULL	Instance number as specified by the INSTANCE_NUMBER initialization parameter
OS_PROCESS	VARCHAR2(16)	NULL	Operating system process identifier of the Oracle process
CREATED_BY	VARCHAR2(30)	NULL	Database login user name of the user whose actions were audited
CREATE_DATE	DATE	NULL	Date on which the action occurred, based on the SYSDATE date
UPDATED_BY	VARCHAR2(30)	NULL	Same as CREATED_BY column value
UPDATE_DATE	DATE	NULL	Same as UPDATED_BY column value

## A.4 Archiving and Purging the Oracle Database Vault Audit Trail

If you have not migrated to unified auditing, you should periodically archive and purge the Oracle Database Vault audit trail.

### [About Archiving and Purging the Oracle Database Vault Audit Trail](#) (page A-6)

In a non-unified auditing environment, you can archive the Oracle Database Vault audit trail by exporting the `DVSYS.AUDIT_TRAIL$` table to a dump file.

### [Archiving the Oracle Database Vault Audit Trail](#) (page A-6)

You can use SQL\*Plus and Oracle Data Pump to archive the Oracle Database Vault audit trail.

### [Purging the Oracle Database Vault Audit Trail](#) (page A-8)

You can purge the Oracle Database Vault audit trail in SQL\*Plus.

### A.4.1 About Archiving and Purging the Oracle Database Vault Audit Trail

In a non-unified auditing environment, you can archive the Oracle Database Vault audit trail by exporting the `DVSYS.AUDIT_TRAIL$` table to a dump file.

You should periodically archive and then purge the audit trail to prevent it from growing too large.

If you choose to migrate to unified auditing, then use this procedure to archive and purge the Database Vault audit trail records after you complete the migration. When unified auditing begins to collect records, then the new records will be available for viewing from the `UNIFIED_AUDIT_TRAIL`, `SYS.DV$CONFIGURATION_AUDIT`, and `SYS.DV$ENFORCEMENT_AUDIT` data dictionary views.

### A.4.2 Archiving the Oracle Database Vault Audit Trail

You can use SQL\*Plus and Oracle Data Pump to archive the Oracle Database Vault audit trail.

1. Log into the database instance as user `SYS` with the `SYSDBA` administrative privilege.

```
sqlplus sys as sysdba
Enter password: password
```

2. Ensure that the user who will perform archiving has the appropriate privileges.

For example:

```
GRANT CREATE ANY DIRECTORY, EXP_FULL_DATABASE, UNLIMITED TABLESPACE TO psmith;
```

3. Connect as a user who has been granted the `DV_OWNER` or `DV_AUDIT_CLEANUP` role.

For example:

```
connect ebrown
Enter password: password
```

4. Archive the Oracle Database Vault audit trail into a new table in an appropriate schema.

For example:

```
CREATE TABLE psmith.dv_audit_trail nologging \
AS SELECT * FROM DVSYS.AUDIT_TRAILS;
```

5. If the schema is already protected by a realm, then ensure that you or the user performing the export operation has been granted the appropriate authorization to use Oracle Data Pump in a Database Vault environment.

For example, to authorize user `psmith` to perform Data Pump operations on his own schema:

```
EXEC DBMS_MACADM.AUTHORIZE_DATAPUMP_USER('PSMITH', 'PSMITH');
```

6. Connect as the Data Pump user.

For example:

```
CONNECT psmith
Enter password: password
```

7. Create a directory for the Database Vault audit trail.

```
CREATE DIRECTORY dv_audit_dir AS 'dv_audit_trail_directory';
```

8. Exit `SQL*Plus`.

```
EXIT
```

9. Using Data Pump, export the Database Vault audit trail into the directory object that you just created.

```
expdp psmith directory=dv_audit_dir tables=psmith.dv_audit_trail \
dumpfile=dv_audit.dmp log=dv_audit_exp.log
```

10. Connect to `SQL*Plus` as a user who has been granted the `DV_OWNER` role.

```
sqlplus ebrown
Enter password: password
```

11. If you have not done so, then create a realm around the schema that now contains the Database Vault audit trail.

- a. Create the realm. For example:

```
BEGIN
  DBMS_MACADM.CREATE_REALM(
    realm_name     => 'DV Audit Trail Realm',
    description    => 'Realm to protect the DV audit trail',
    enabled        => DBMS_MACUTL.G_YES,
    audit_options  => DBMS_MACUTL.G_REALM_AUDIT_FAIL +
    DBMS_MACUTL.G_REALM_AUDIT_SUCCESS,
    realm_type     => 1);
END;
/
```

- b. Add the schema that contains to audit trail to this realm. For example:

```
BEGIN
  DBMS_MACADM.ADD_OBJECT_TO_REALM(
    realm_name     => 'DV Audit Trail Realm',
    object_owner   => 'psmith',
    object_name    => '%',
    object_type    => '%');
END;
/
```

- c. Authorize a trusted user for this realm.

```
BEGIN
  DBMS_MACADM.ADD_AUTH_TO_REALM(
    realm_name     => 'DV Audit Trail Realm',
    grantee        => 'PSMITH',
    auth_options   => DBMS_MACUTL.G_REALM_AUTH_OWNER);
END;
/
```

---

**See Also:**

- [Using Oracle Data Pump with Oracle Database Vault](#) (page 13-5) for more information about granting users Oracle Data Pump privileges in a Database Vault environment
  - *Oracle Database SQL Language Reference* for information about the CREATE DIRECTORY statement
  - *Oracle Database Utilities* for information about the Oracle Data Pump expdp utility
  - [Oracle Database Vault Realm APIs](#) (page 15-1), for information about the realm-related DBMS\_MACADM procedures
- 

### A.4.3 Purging the Oracle Database Vault Audit Trail

You can purge the Oracle Database Vault audit trail in SQL\*Plus.

1. Log into the database instance as a user who has been granted the DV\_OWNER role or the DV\_AUDIT\_CLEANUP role.

For example:

```
sqlplus psmith
Enter password: password
```



Note that the DV\_OWNER and DV\_AUDIT\_CLEANUP roles do not allow their grantees to truncate the DVSYS.AUDIT\_TRAIL\$ system table.

You can query the DBA\_ROLE\_PRIVS data dictionary view to find the roles that have been granted to a user.

**2. Purge the Database Vault audit trail.**

```
DELETE FROM DVSYS.AUDIT_TRAIL$;
```

**Related Topics:**

[DV\\_AUDIT\\_CLEANUP Audit Trail Cleanup Role](#) (page 14-13)

The DV\_AUDIT\_CLEANUP role is used for purge operations.

## A.5 Oracle Database Audit Settings Created for Oracle Database Vault

When you install Oracle Database Vault, it creates several AUDIT settings in the database.

However, in a non-unified auditing environment, in order for these audit settings to take place, auditing must be enabled in this database. You can check if auditing is enabled by using the SHOW PARAMETER command to find the value of the AUDIT\_TRAIL initialization parameter. By default, auditing is enabled in Oracle Database.

[Table A-2](#) (page A-10) lists the AUDIT settings that Oracle Database Vault adds to the database.

**Table A-2 Audit Policy Settings Oracle Database Vault Adds to Oracle Database**

Audit Setting Type	Audited Statements (BY ACCESS and on Success or Failure Unless Otherwise Noted)
User Audit Settings for DVSYS/DVF	ADMINISTER DATABASE TRIGGER
User Audit Settings for LBACSYS	ALTER <i>object</i>
See <a href="#">Table 14-2</a> (page 14-24) for more information about these accounts.	AUDIT SYSTEM
See also these sections for detailed information on the DVSYS and DVF schemas:	BECOME USER
• <a href="#">DVSYS Schema</a> (page 14-1)	CLUSTER
• <a href="#">DVF Schema</a> (page 14-2)	COMMENT
	CONTEXT
	CREATE <i>object</i>
	DATABASE LINK
	DEBUG
	DIRECTORY
	DROP <i>object</i>
	EXECUTE LIBRARY (WHENEVER NOT SUCCESSFUL)
	EXECUTE PROCEDURE (WHENEVER NOT SUCCESSFUL)
	EXEMPT ACCESS POLICY
	EXPORT FULL DATABASE
	GRANT <i>object</i>
	IMPORT FULL DATABASE
	INDEX
	MANAGE SCHEDULER
	MANAGE TABLESPACE
	MATERIALIZED VIEW (audits both accessing and creating materialized views)
	SELECT SEQUENCE (WHENEVER NOT SUCCESSFUL)
	SELECT TABLE (WHENEVER NOT SUCCESSFUL)
Object Audit Settings for DVF	AUDIT PACKAGE/PROCEDURE/FUNCTION/SEQUENCE/TABLE
	COMMENT TABLE/VIEW
	DELETE TABLE/VIEW
	EXECUTE PACKAGE/PROCEDURE/FUNCTION (WHENEVER NOT SUCCESSFUL)
	GRANT PACKAGE/PROCEDURE/FUNCTION/SEQUENCE/TABLE
	RENAME PACKAGE/PROCEDURE/FUNCTION/SEQUENCE/VIEW/TABLE
	SELECT SEQUENCE/TABLE/VIEW (WHENEVER NOT SUCCESSFUL)

**Table A-2 (Cont.) Audit Policy Settings Oracle Database Vault Adds to Oracle Database**

Audit Setting Type	Audited Statements (BY ACCESS and on Success or Failure Unless Otherwise Noted)
Object Audit Settings for DVSYS	AUDIT PACKAGE/PROCEDURE/FUNCTION/SEQUENCE/TABLE
Object Audit Settings for LBACSYS	COMMENT TABLE/VIEW
	DELETE TABLE/VIEW
	EXECUTE PACKAGE/PROCEDURE/FUNCTION (WHENEVER NOT SUCCESSFUL)
	GRANT PACKAGE/PROCEDURE/FUNCTION/SEQUENCE/TABLE
	INSERT TABLE/VIEW
	RENAME PACKAGE/PROCEDURE/FUNCTION/SEQUENCE/VIEW/TABLE
	SELECT SEQUENCE/TABLE/VIEW (WHENEVER NOT SUCCESSFUL)
	UPDATE TABLE/VIEW



---

## Disabling and Enabling Oracle Database Vault

Periodically you must disable and then re-enable Oracle Database Vault, for activities such as installing Oracle Database optional products or features.

[When You Must Disable Oracle Database Vault](#) (page B-1)

You may need to disable Oracle Database Vault to perform upgrade tasks or correct erroneous configurations.

[Step 1: Disable Oracle Database Vault](#) (page B-2)

Be aware that after you disable Oracle Database Vault, Oracle Label Security, which is required to run Database Vault, is still enabled.

[Step 2: Perform the Required Tasks](#) (page B-2)

At this stage, Oracle Database Vault is disabled and you can perform the required tasks.

[Step 3: Enable Oracle Database Vault](#) (page B-3)

You can enable Oracle Database Vault and Oracle Label Security from SQL\*Plus.

### B.1 When You Must Disable Oracle Database Vault

You may need to disable Oracle Database Vault to perform upgrade tasks or correct erroneous configurations.

You can reenable Oracle Database Vault after you complete the corrective tasks.

To find the enablement and configuration status of Oracle Database Vault, see [Verifying That Database Vault Is Configured and Enabled](#) (page 3-9).

The following situations require you to disable Oracle Database Vault:

- You must install any of the Oracle Database optional products or features, such as Oracle Spatial, or Oracle Multimedia, by using Database Configuration Assistant (DBCA).
- If you did not configure backup DV\_OWNER and DV\_ACCTMGR accounts when you registered Oracle Database Vault, and these accounts are inadvertently locked or their passwords forgotten. Note that if your site only has one DV\_OWNER user and this user has lost his or her password, you will be unable to disable Oracle Database Vault. However, if your site's only DV\_ACCTMGR user has lost the password, you can disable Database Vault. As a best practice, you should grant the DV\_OWNER and DV\_ACCTMGR roles to new or existing user accounts, and use the Database Vault Owner and Account Manager accounts that you created when you registered Database Vault as back-up accounts. (See [Backup Oracle Database Vault Accounts](#) (page 14-25) for a guideline for avoiding this problem in the future.)

- If you want to register Oracle Internet Directory (OID) using Oracle Database Configuration Assistant (DBCA).

---

---

**Note:**

- Be aware that if you disable Oracle Database Vault, the privileges that were revoked from existing users and roles during installation remain in effect. See [Privileges That Are Revoked from Existing Users and Roles](#) (page 2-3) for a listing of the revoked privileges.
  - When Oracle Database Vault is disabled, there are some Database Vault features that you can still use.
  - Oracle does not support the deinstallation of Oracle Database Vault.
- 
- 

## B.2 Step 1: Disable Oracle Database Vault

Be aware that after you disable Oracle Database Vault, Oracle Label Security, which is required to run Database Vault, is still enabled.

1. In SQL\*Plus, log in as the Oracle Database Owner (DV\_OWNER) account, and then disable Oracle Database Vault.

```
sqlplus psmith
Enter password: password

EXEC DBMS_MACADM.DISABLE_DV;
```

2. In a multitenant environment, connect to the appropriate pluggable database (PDB).

For example:

```
CONNECT psmith@hrpdb
Enter password: password
```

To find the available PDBs, query the DBA\_PDBS data dictionary view. To check the current PDB, run the `show con_name` command.

3. Restart the database.

```
CONNECT SYS AS SYSOPER -- Or, CONNECT SYS@hrpdb AS SYSOPER
Enter password: password
```

```
SHUTDOWN IMMEDIATE
STARTUP
```

4. For Oracle RAC installations, repeat these steps for each node on which the database is installed.

## B.3 Step 2: Perform the Required Tasks

At this stage, Oracle Database Vault is disabled and you can perform the required tasks.

You can perform the following types of activities:

- **Use the Oracle Database Vault PL/SQL packages and functions.** For example, to correct a login or CONNECT rule set error, use the DBMS\_MACADM PL/SQL package

or the Oracle Database Vault pages in Enterprise Manager Cloud Control. Note that a CONNECT command rule cannot prevent a user who has the DV\_OWNER or DV\_ADMIN role from connecting to the database. This enables a Database Vault administrator to correct a misconfigured protection without having to disable Database Vault.

- **Use the SYSTEM or SYS accounts to perform tasks such as creating or changing passwords, or locking and unlocking accounts.** In addition to modifying standard database and administrative user accounts, you can modify passwords and the lock status of any of the Oracle Database Vault-specific accounts, such as users who have been granted the DV\_ADMIN or DV\_ACCTMGR roles. (See the tip under [Oracle Database Vault Accounts Created During Registration](#) (page 14-23) for a guideline for avoiding this problem in the future.)
- **Perform the installation or other tasks that require security protections to be disabled.**

## B.4 Step 3: Enable Oracle Database Vault

You can enable Oracle Database Vault and Oracle Label Security from SQL\*Plus.

1. In SQL\*Plus, connect as the Oracle Database Owner (DV\_OWNER) account, and then enable Database Vault.

If you are enabling Database Vault from a non-multitenant environment or from a PDB:

```
CONNECT psmith -- Or, CONNECT psmith@hrpdb for a PDB
Enter password: password
```

```
EXEC DBMS_MACADM.ENABLE_DV;
```

If you are enabling Database Vault from the CDB root, for example:

```
CONNECT c##dbv_owner
Enter password: password
```

Select from one of the following settings:

```
EXEC DBMS_MACADM.ENABLE_DV (strict_mode => 'n');
-- For regular mode
EXEC DBMS_MACADM.ENABLE_DV (strict_mode => 'y');
-- For strict mode
```

2. Check if Oracle Label Security is enabled.

```
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Oracle Label Security';
```

Oracle Label security must be enabled before you can use Database Vault. If it is not enabled, then this query returns FALSE.

3. If Oracle Label Security is not enabled, then enable it.

```
CONNECT SYS AS SYSDBA -- Or, CONNECT SYS@hrpdb AS SYSDBA
Enter password: password
```

```
EXEC LBACSYS.CONFIGURE_OLS;
EXEC LBACSYS.OLS_ENFORCEMENT.ENABLE_OLS;
```

4. Restart the database.

```
CONNECT SYS AS SYSOPER -- Or, CONNECT SYS@hrpdb AS SYSOPER  
Enter password: password
```

```
SHUTDOWN IMMEDIATE  
STARTUP
```

5. For Oracle RAC installations, repeat these steps for each node on which the database is installed.



---

# Postinstallation Oracle Database Vault Procedures

After you register Oracle Database Vault, you can perform specialized tasks, such as configuring it on Oracle Real Application Clusters (Oracle RAC) nodes.

## [Configuring Oracle Database Vault on Oracle RAC Nodes](#) (page C-1)

After you configure Oracle Database Vault for an Oracle Real Application Clusters (Oracle RAC) instance, you must configure each Oracle RAC node.

## [Adding Languages to Oracle Database Vault](#) (page C-2)

By default, Oracle Database Vault loads only the English language tables.

## [Deinstalling Oracle Database Vault](#) (page C-2)

You can remove Oracle Database Vault from an Oracle Database installation, for both to both single-instance and Oracle RAC installations.

## [Reinstalling Oracle Database Vault](#) (page C-4)

You can reinstall Oracle Database Vault by using Database Configuration Assistant and afterward, register Database Vault.

### Related Topics:

## [Plugging a Database Vault-Enabled PDB to a CDB](#) (page 13-23)

You can plug a legacy Database Vault-enabled PDB to a multitenant container database (CDB).

## C.1 Configuring Oracle Database Vault on Oracle RAC Nodes

After you configure Oracle Database Vault for an Oracle Real Application Clusters (Oracle RAC) instance, you must configure each Oracle RAC node.

The following procedure assumes that you have a separate Oracle home for each node.

1. Log into the database instance as user `SYS` with the `SYSDBA` administrative privilege.

```
sqlplus sys as sysdba
Enter password: password
```

2. Run the following `ALTER SYSTEM` statements on each Oracle RAC node:

```
ALTER SYSTEM SET AUDIT_SYS_OPERATIONS=TRUE SCOPE=SPFILE; -- For non-unified
auditing environments
ALTER SYSTEM SET OS_ROLES=FALSE SCOPE=SPFILE;
ALTER SYSTEM SET RECYCLEBIN='OFF' SCOPE=SPFILE;
```

```
ALTER SYSTEM SET REMOTE_LOGIN_PASSWORDFILE='EXCLUSIVE' SCOPE=SPFILE;  
ALTER SYSTEM SET SQL92_SECURITY=TRUE SCOPE=SPFILE;
```

**3. Restart Oracle Database.**

```
CONNECT / AS SYSOPER  
Enter password: password
```

```
SHUTDOWN IMMEDIATE  
STARTUP
```

## C.2 Adding Languages to Oracle Database Vault

By default, Oracle Database Vault loads only the English language tables.

You can add more languages by running the `DBMS_MACADM.ADD-NLS_DATA` procedure for each new language that you want to add. You can add more than one language to Database Vault.

1. Log into the database instance as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role.
2. Run the following procedure:

```
EXEC DBMS_MACADM.ADD-NLS_DATA(' language');
```

You can specify the *language* setting using any case. For example:

```
EXEC DBMS_MACADM.ADD-NLS_DATA(' french');
```

```
EXEC DBMS_MACADM.ADD-NLS_DATA(' JAPANESE');
```

Replace *language* with one of the following supported languages:

- ENGLISH
- GERMAN
- SPANISH
- FRENCH
- ITALIAN
- JAPANESE
- KOREAN
- BRAZILIAN PORTUGUESE
- SIMPLIFIED CHINESE
- TRADITIONAL CHINESE

## C.3 Deinstalling Oracle Database Vault

You can remove Oracle Database Vault from an Oracle Database installation, for both to both single-instance and Oracle RAC installations.

The deinstallation process does not affect the initialization parameter settings, even those settings that were modified during the installation process, nor does it affect Oracle Label Security.

1. Log into the database instance as user `SYS` with the `SYSDBA` administrative privilege, or as user who has the `ALTER SYSTEM` system privilege.

For example:

```
sqlplus psmith -- Or, sqlplus psmith@hrpdb for a pluggable database (PDB)
Enter password: password
```

2. Ensure that the recycle bin is disabled.

```
SHOW PARAMETER RECYCLEBIN
```

3. If the recycle bin is on, then disable it using one of the following statements:

```
ALTER SYSTEM SET RECYCLEBIN = OFF;
```

```
ALTER SESSION SET recyclebin = OFF SCOPE = SPFILE;
```

4. Connect as a user who has been granted the `DV_OWNER` or `DV_ADMIN` role.

For example:

```
CONNECT leo_dvowner -- Or, CONNECT leo_dvowner@hrpdb
Enter password: password
```

5. Run the following procedure to disable Oracle Database Vault:

```
EXEC DBMS_MACADM.DISABLE_DV;
```

6. Connect as `SYS` with the `SYSOPER` privilege and then restart the database.

For example:

```
CONNECT SYS AS SYSOPER -- Or, CONNECT SYS@hrpdb AS SYSOPER
Enter password: password
```

```
SHUTDOWN IMMEDIATE
STARTUP
```

For Oracle RAC installations, shut down and then restart each database instance as follows:

```
$ srvctl stop database -db db_name
$ srvctl start database -db db_name
```

7. Run the `dvremov.sql` script to remove Oracle Database Vault.

For example:

```
$ORACLE_HOME/rdbms/admin/dvremov.sql
```

Afterward, you can double-check that Oracle Database Vault is truly deinstalled by logging in to SQL\*Plus and entering the following statement:

```
SELECT * FROM V$OPTION WHERE PARAMETER = 'Oracle Database Vault';
```

If Oracle Database Vault is deinstalled, the following output appears:

PARAMETER	VALUE
Oracle Database Vault	FALSE

## C.4 Reinstalling Oracle Database Vault

You can reinstall Oracle Database Vault by using Database Configuration Assistant and afterward, register Database Vault.

1. Log into the database instance as user SYS with the SYSDBA administrative privilege.

```
sqlplus sys as sysdba -- Or, sqlplus sys@hrpdb as sysdba
Enter password: password
```

2. Start Database Configuration Assistant (DBCA).

- **UNIX:** Enter the following command in a shell window:

```
dbca
```

- **Windows:** Use one of the following methods to start DBCA on Windows:

- Click **Start**, select **Programs** (or **All Programs**), then **Oracle - HOME\_NAME**, then **Configuration and Migration Tools**, and then **Database Configuration Assistant**.
- Enter the following command at a command prompt:

```
dbca
```

3. Use DBCA to configure Database Vault for either a new or an existing database.

See *Oracle Database 2 Day DBA* for detailed information about creating a database with DBCA.

4. Follow the instructions in [Registering Oracle Database Vault with an Oracle Database](#) (page 3-2) to register Database Vault.

---

# Oracle Database Vault Security Guidelines

As with all Oracle Database products, you should follow security guidelines to better secure your Oracle Database Vault installation.

## [Separation of Duty Guidelines](#) (page D-1)

Oracle Database Vault is designed to easily implement separation of duty guidelines.

## [Managing Oracle Database Administrative Accounts](#) (page D-5)

Oracle provides guidelines for managing security for administrative accounts such as SYSTEM or users who have the SYSDBA administrative privilege.

## [Accounts and Roles Trusted by Oracle Database Vault](#) (page D-7)

Oracle Database Vault restricts access to application data from many privileged users and roles in the database.

## [Accounts and Roles That Should be Limited to Trusted Individuals](#) (page D-8)

You should limit powerful accounts and roles only to trusted individuals.

## [Guidelines for Using Oracle Database Vault in a Production Environment](#) (page D-9)

You should follow special guidelines when you run Oracle Database Vault in a production environment.

## [Secure Configuration Guidelines](#) (page D-10)

You should be aware of security considerations for special PL/SQL packages, privileges, and the recycle bin.

## D.1 Separation of Duty Guidelines

Oracle Database Vault is designed to easily implement separation of duty guidelines.

### [How Oracle Database Vault Handles Separation of Duty](#) (page D-2)

Separation of duty is restricting each user's privileges *only* to the tasks he or she is responsible for, and *no more*.

### [Separation of Tasks in an Oracle Database Vault Environment](#) (page D-2)

Oracle Database Vault defines the several main responsibilities.

### [Separation of Duty Matrix for Oracle Database Vault](#) (page D-3)

Before applying separation of duty, you must understand who performs basic administration tasks in your environment and what these administration tasks are.

### [Identification and Documentation of the Tasks of Database Users](#) (page D-4)

You should document the areas of the tasks that your organization needs.

## D.1.1 How Oracle Database Vault Handles Separation of Duty

Separation of duty is restricting each user's privileges *only* to the tasks he or she is responsible for, and *no more*.

You should assign specific categories of privileges to specific users, rather than granting many privileges to one user. Simply put, separation of duty creates accountability for each task that your organization requires.

Separation of duty has taken on increased importance over the past 10 years. For many organizations, separation of duty is a new concept that continues to evolve. Database consolidation, regulatory compliance, and outsourcing are just a few of the drivers for increased separation of duty. Oracle Database Vault separation of duty strengthens security by separating security-related administration from day-to-day DBA operations. You can tailor your Database Vault separation of duty implementation to easily adapt to current and future business requirements. Small organizations, in particular, need flexibility as they attempt to increase their security profile with limited resources.

## D.1.2 Separation of Tasks in an Oracle Database Vault Environment

Oracle Database Vault defines the several main responsibilities.

These responsibilities are as follows:

- **Account management.** Account management entails creating, modifying, and dropping user accounts. The DV\_ACCTMGR role provides these privileges. A primary day-to-day DV\_ACCTMGR user and a backup DV\_ACCTMGR user are created during the Oracle Database Vault registration process. As a safety measure, you keep and maintain the backup account in case the primary DV\_ACCTMGR account owner forgets his or her password or leaves the company.
- **Security administration.** Security administration covers basic security tasks such as creating realms and command rules, setting security policies for database users' access, and authorizing database users for jobs they are allowed to perform. Security administrators also run security audit reports. The DV\_OWNER and DV\_ADMIN roles provide these privileges. A primary day-to-day DV\_OWNER user and a backup DV\_OWNER user are created during the Oracle Database Vault registration process. As a safety measure, you should keep and maintain the backup user account in case the primary DV\_OWNER account owner forgets his or her password or leaves the company.

Optionally, you can consolidate the account management and security administrative responsibilities.

- **Database management.** Database management refers to managing the database system but not accessing business data. It includes the following operations:
  - Backup operations require a predefined time to perform the backup using predefined tools.
  - Tuning and monitoring operations require ongoing performance monitoring and analysis.
  - Patching operations require temporary access only during the time the patching takes place

Oracle strongly recommends that you review database management accounts within the context of separation of duty. Different database administrators may have different responsibilities that require different privileges and roles. Similarly, more experienced database administrators may have more roles and privileges. Instead of granting users the default DBA role to users, consider tailoring database administrative roles for specific positions and for seniority in your organization. It is important to use only named accounts for day-to-day activities. Accounts such as SYS and accounts that use the SYSDBA administrative privilege should be managed with Privileged Account Management (PAM) systems and checked out (and audited) when they are used. You should also manage the backup Oracle Database Vault owner and account management accounts with a PAM system. Within the operating system, you should make the `root` and `oracle` accounts available only through a checkout system, because of the powerful privileges that these accounts have.

You should have separate accounts for database account management, database security administration, and additional named accounts for backup operations. Auditors check for separate database accounts for different responsibilities and being able to track the actions of each account. Less important is the number of users assigned to specific tasks. Remember that Oracle Database Vault audit events are protected and that the Database Vault reports show all attempted violations.

---

---

**See Also:**

- [Oracle Database Vault Roles](#) (page 14-3) for an in-depth look at how the Oracle Database Vault roles provide for separation of duty
  - [Oracle Database Vault Accounts Created During Registration](#) (page 14-23) for a full list of the default Oracle Database Vault accounts
  - [Backup Oracle Database Vault Accounts](#) (page 14-25) for more information about the importance of backup accounts
- 
- 

### D.1.3 Separation of Duty Matrix for Oracle Database Vault

Before applying separation of duty, you must understand who performs basic administration tasks in your environment and what these administration tasks are.

Even if a single database administrator is responsible for managing both new database account provisioning and application patching, it is important to document and plan for each of these tasks. Using separate administration accounts for these types of tasks provides increased accountability and reduces associated risks if and when a single account is compromised by a malicious user. In midsize to large organizations, database administrators typically must perform common administration tasks but they do not need access to business data managed by the application. Creating a matrix for your separation of duty can help you plan your Database Vault deployment. As needed, you can include additional tasks and associated users to this list. This information should become part of the overall enterprise security documentation for your organization.

[Table D-1](#) (page D-4) shows an example of a separation of duty matrix.

**Table D-1 Example Separation of Duty Matrix**

User, Process or Application	Account Creation	Database Administration					Security Administrator
		SYSDBA	Backup	Tuning	Patching	Monitoring	
JSMITH	Yes	No	No	No	No	No	No
SHARDY	No	No	No	No	No	No	Yes
PKESTNER	No	No	Yes	No	No	No	No
RTYLER	No	No	No	No	Yes	No	No
SANDERSON	No	No	No	Yes	No	Yes	No
SYSTEM	No	No	No	No	Yes, for EBS patching	No	No
RMAN	No	Yes	Yes	No	No	No	No

In some cases, system management tasks may require temporary access to data through specific tools and programs. When this happens, build provisions for this temporary or emergency access into the Oracle Database Vault rules and rule sets.

#### D.1.4 Identification and Documentation of the Tasks of Database Users

You should document the areas of the tasks that your organization needs.

These areas are as follows:

- The responsibilities of each administrative user
- The kind of access users need. For example, application owners should have data access and developers need access to development instances only.
- Who must manage the system without accessing business data (for example, users who perform backup, patching, tuning, and monitoring operations)
- The duties of each category of tasks (for example, the files that must be backed up, the applications that require patching, what exactly is monitored). Include the alternate user accounts for each of these tasks.
- The databases and applications that must be protected. This includes Oracle applications, partner applications, and custom applications.
- Who must be authorized to access business data, including the following:
  - Application owners through middle tier processes
  - Business users through an application interface
- Emergency "what if" scenarios, such as how to handle a security breach
- Reporting in a production environment, which should include the following:
  - Who runs the reports
  - Which reports must be run



- The frequency with which each report is run
- The users who must receive a copy of each report
- In addition to a separation of duty matrix, the creation of the following matrices:
  - An Oracle Database Vault-specific matrix, which can cover the names and tasks of users who have been granted Database Vault roles
  - An application protection matrix, which can cover the applications to be protected and the types of protections you have put in place.

Table D-2 (page D-5) shows an example of protections Oracle created for PeopleSoft Applications. SYSADM, PSFTDBA, SYSTEM, and DBA have all been authorized for the appropriate rule sets.

**Table D-2 Example Application Protection Maxtrix**

Protection Type	SYSADM	PSFTDBA	SYSTEM	DBA
PeopleSoft Realm	Owner	Owner	No Access	No Access
SELECT Command Rule	Not Restricted	Limit PSFTDB Rule Set	No Access	No Access
CONNECT Command Rule	PeopleSoftAccess Rule Set	Not Restricted	Not Restricted	Not Restricted
DROP TABLESPACE Command Rule	Disabled Rule Set	Disabled Rule Set	Disabled Rule Set	Disabled Rule Set

## D.2 Managing Oracle Database Administrative Accounts

Oracle provides guidelines for managing security for administrative accounts such as SYSTEM or users who have the SYSDBA administrative privilege.

### SYSTEM User Account for General Administrative Uses (page D-6)

Ideally, the SYSTEM account should only be available as a backup that is checked out and audited while being used.

### SYSTEM Schema for Application Tables (page D-6)

If you have application tables in the SYSTEM schema, then you should add the SYSTEM account to your realm authorizations for these tables.

### Limitation of the SYSDBA Administrative Privilege (page D-6)

Limit the SYSDBA administrative privilege to users who must connect using this privilege when absolutely necessary and for applications that still require SYSDBA access.

### Root and Operating System Access to Oracle Database Vault (page D-6)

For better security, you should carefully monitor root and operating system access to Oracle Database Vault.

## D.2.1 SYSTEM User Account for General Administrative Uses

Ideally, the `SYSTEM` account should only be available as a backup that is checked out and audited while being used.

Only named accounts should be used for normal database administration tasks - not shared accounts. Doing so increases accountability for administrative actions in the database.

## D.2.2 SYSTEM Schema for Application Tables

If you have application tables in the `SYSTEM` schema, then you should add the `SYSTEM` account to your realm authorizations for these tables.

This enables these applications to continue to work normally.

You can place restrictions on the `SYSTEM` account to increase or fine-tune security for these applications. For example, you can create a Database Vault rule set to restrict the `SYSTEM` user's access to specific IP addresses.

## D.2.3 Limitation of the SYSDBA Administrative Privilege

Limit the `SYSDBA` administrative privilege to users who must connect using this privilege when absolutely necessary and for applications that still require `SYSDBA` access.

For example, mandatory patching processes require `SYSDBA` access.

For all other cases, create named database accounts to perform daily database administration. Members of the `OSDBA` user group are also given the `SYSDBA` administrative privilege. The database `SYS` account and accounts with `SYSDBA` privilege along with the operating system `root` and `oracle` accounts should be managed in a Privileged Account Management (PAM) system and checked out only when required.

### Related Topics:

[Management of SYSDBA Access](#) (page D-9)

You should avoid using the `SYS` account and the `SYSDBA` privilege for normal database maintenance tasks.

## D.2.4 Root and Operating System Access to Oracle Database Vault

For better security, you should carefully monitor root and operating system access to Oracle Database Vault.

Oracle Database Vault prevents highly privileged database users from accessing sensitive data. In addition, if you are using Oracle Database itself, then you can use Transparent Data Encryption to prevent the most highly privileged operating system users from accessing sensitive data. Transparent data encryption enables you to encrypt tablespaces and table columns. This prevents operating system users from browsing through the operating system database files and finding sensitive data. As a best practice, always carefully review and restrict direct access to the operating system.

You should have personalized accounts access the operating system. These personalized accounts should, in the Linux or UNIX environments, login using `sudo` to the `oracle` software owner when needed. With `sudo`, you can control which

specific command each personalized user can execute. Be sure to prevent the use of the `make`, `relink`, `gdb`, or other commands that could potentially harm the database, for these users. However, if an administrative user must install a patch or perform some other emergency operation, you can enable the `make` and `relink` commands for a limited time, and audit their actions during this period.

---

**See Also:** *Oracle Database Advanced Security Guide* for more information about Transparent Data Encryption

---

## D.3 Accounts and Roles Trusted by Oracle Database Vault

Oracle Database Vault restricts access to application data from many privileged users and roles in the database.

However, in some cases, Oracle Database Vaults trusts certain roles and privileges.

[Table D-3](#) (page D-7) lists the trusted roles and privileges that are created when you install Oracle Database Vault.

**Table D-3 Trusted Oracle Database Vault Roles and Privileges**

Role or Privilege	Status	Description
DV_ACCTMGR role	Open	<p>Role created during registration and used for creating new database accounts. As a safety measure, maintain a backup user who has the DV_ACCTMGR role and manage this account using a Privileged Account Management (PAM) system.</p> <p>Users who have the DV_OWNER role cannot alter this user.</p> <p>Loss of all accounts with the DV_ACCTMGR role (such as due to lost passwords or people leaving the organization) is not recoverable. Ensure that a backup DV_ACCTMGR account is created for this purpose.</p>
DV_OWNER role	Open	<p>Role created during registration and used for managing realms, factors and command rules. This user can add himself or herself to realm authorizations. As a safety measure, maintain a backup user who has the DV_OWNER role and manage this account using a Privileged Account Management (PAM) system.</p> <p>Users who have the DV_OWNER role cannot alter this user.</p> <p>Loss of all accounts with the DV_OWNER role (such as due to lost passwords or people leaving the organization) is not recoverable. Ensure that a backup DV_OWNER account is created for this purpose.</p>
SYSDBA privilege	Enabled	Privilege created during Oracle Database installation. Required by some Oracle features.
SYSOPER privilege	Enabled	Privilege created during Oracle Database installation. Database startup and shutdown. Granted to SYS only by default.

### Related Topics:

[Backup Oracle Database Vault Accounts](#) (page 14-25)

As a best practice, you should maintain backup accounts for the DV\_OWNER and DV\_ACCTMGR roles.

[Management of SYSDBA Access](#) (page D-9)

You should avoid using the SYS account and the SYSDBA privilege for normal database maintenance tasks.

[Management of SYSOPER Access](#) (page D-9)

By default, Oracle Database limits SYSOPER access to operating system users in the OSOPER group and to the user SYS.

## D.4 Accounts and Roles That Should be Limited to Trusted Individuals

You should limit powerful accounts and roles only to trusted individuals.

[Management of Users with Root Access to the Operating System](#) (page D-8)

Users who have root user access have full control over the system.

[Management of the Oracle Software Owner](#) (page D-8)

Users who have access to a system as the Oracle software owner have control over the Oracle software.

[Management of SYSDBA Access](#) (page D-9)

You should avoid using the SYS account and the SYSDBA privilege for normal database maintenance tasks.

[Management of SYSOPER Access](#) (page D-9)

By default, Oracle Database limits SYSOPER access to operating system users in the OSOPER group and to the user SYS.

### D.4.1 Management of Users with Root Access to the Operating System

Users who have root user access have full control over the system.

Activities that these users can perform include the following:

- Reading unencrypted files
- Moving and deleting any files
- Starting or stopping any program on the system
- Logging in as any user, including the user who owns the Oracle Database installation

Oracle Database Vault does not provide protection against the operating system root access. Manage the root and oracle accounts in a Privileged Account Management (PAM) system. Only check these accounts out when they are required for certain tasks. Enhance audit levels when highly privileged operating system accounts are being used, up to an including keystroke capture and video capture.

### D.4.2 Management of the Oracle Software Owner

Users who have access to a system as the Oracle software owner have control over the Oracle software.

Activities these users can perform include the following:

- Reading unencrypted database files
- Moving and deleting database files
- Starting or stopping Oracle programs in the system

Oracle Database Vault does not provide protection against the operating system access of the Oracle software owner. Manage the Oracle software owner account in a Privileged Account Management (PAM) system. Only check this account out when it is required for certain tasks. Enhance audit levels when highly privileged operating system accounts are being used, up to an including keystroke capture and video capture.

### D.4.3 Management of SYSDBA Access

You should avoid using the `SYS` account and the `SYSDBA` privilege for normal database maintenance tasks.

Instead, use named accounts that have the required system privileges or a specific administrative privilege such as `SYSBACKUP`, `SYSDBG`, or `SYSKM`. However, there are cases where the `SYSDBA` privilege is required to perform a patch, upgrade of the database or troubleshoot issues (for example, connecting to a down database).

Because users with the `SYSDBA` privilege could have access to sensitive application data either directly or indirectly (for example, through diagnostics, database upgrades, and patching), use of the `SYSDBA` privilege and accounts must be highly restricted. The list of highly privileged accounts include `SYS` and user accounts with the `SYSDBA` privilege in the database, and the `root` and `oracle` accounts in the operating system. Access to highly privileged accounts in the database and the operating system should be on an exception basis and require the user to go through a process to unlock access to these accounts and privileges. Oracle recommends that you manage these accounts with a Privileged Account Management (PAM) system. Only check these accounts out when they are required for certain tasks. Enhance audit levels when highly privileged operating system accounts (`root` and `oracle`) and database accounts (`SYS` account and `SYSDBA` administrative privilege) are being used, up to an including keystroke capture and video capture. When these highly privileged accounts access the database, audit the `SYS` account to monitor their activities.

### D.4.4 Management of SYSOPER Access

By default, Oracle Database limits `SYSOPER` access to operating system users in the `OSOPER` group and to the user `SYS`.

This prevents `SYSOPER` from modifying the Oracle data dictionary directly. The `SYSOPER` privilege has limited privileges within the database, but individuals with this role can start and shut down the Oracle database. Only grant the `SYSOPER` privilege to trusted individuals.

## D.5 Guidelines for Using Oracle Database Vault in a Production Environment

You should follow special guidelines when you run Oracle Database Vault in a production environment.

These guidelines are as follows:

- Run a full test of your applications to ensure that the Database Vault policies you have created are working as expected

- Monitor the performance of your applications, and if necessary, tune your rule expressions
- Assign responsibilities to the appropriate production support and security groups, as follows:
  - Assign security responsibilities to the database security administrator.
  - Assign account management to the database account manager.
  - Assign resource management tasks to database administrators.
- Back up your Database Vault API scripts to a secure server.

## D.6 Secure Configuration Guidelines

You should be aware of security considerations for special PL/SQL packages, privileges, and the recycle bin.

### [General Secure Configuration Guidelines](#) (page D-10)

General secure configuration guidelines involved patches and revoke operations.

### [UTL\\_FILE and DBMS\\_FILE\\_TRANSFER Package Security Considerations](#) (page D-11)

You should carefully restrict access to the UTL\_FILE and DBMS\_FILE\_TRANSFER PL/SQL packages.

### [CREATE ANY JOB Privilege Security Considerations](#) (page D-14)

The CREATE ANY JOB privilege has been revoked from the DBA and the SCHEDULER\_ADMIN roles.

### [CREATE EXTERNAL JOB Privilege Security Considerations](#) (page D-14)

The CREATE EXTERNAL JOB privilege was introduced in Oracle Database 10g release 2 (10.2).

### [LogMiner Package Security Considerations](#) (page D-14)

The role EXECUTE\_CATALOG\_ROLE no longer has the EXECUTE privilege granted by default on the several LogMiner packages.

### [ALTER SYSTEM and ALTER SESSION Privilege Security Considerations](#) (page D-14)

You should be aware of ways to secure the powerful ALTER SYSTEM and ALTER SESSION system privileges.

### D.6.1 General Secure Configuration Guidelines

General secure configuration guidelines involved patches and revoke operations.

- Installing patches and new applications might re-grant some of the privileges that Oracle recommends that you revoke in this section. Check these privileges after you install patches and new applications to verify that they are still revoked.
- When you revoke EXECUTE privileges on packages, ensure that you grant EXECUTE on the packages to the owner, check the package dependencies, and recompile any invalid packages after the revoke.

To find users who have access to the package, log into the database instance as a named database administrator and issue the following query.

```
SELECT * FROM DBA_TAB_PRIVS WHERE TABLE_NAME = package_name;
```

*package\_name* is the name of the package you are looking for.

To find the users, packages, procedures, and functions that are dependent on the package, issue this query:

```
SELECT OWNER, NAME, TYPE FROM ALL_DEPENDENCIES
WHERE REFERENCED_NAME = package_name;
```

Note that these two queries do not identify references to packages made through dynamic SQL.

## D.6.2 UTL\_FILE and DBMS\_FILE\_TRANSFER Package Security Considerations

You should carefully restrict access to the UTL\_FILE and DBMS\_FILE\_TRANSFER PL/SQL packages.

[About Security Considerations for the UTL\\_FILE and DBMS\\_FILE\\_TRANSFER Packages](#) (page D-11)

The UTL\_FILE package is owned by SYS and granted to PUBLIC.

[Securing Access to the DBMS\\_FILE\\_TRANSFER Package](#) (page D-12)

You can secure access to the DBMS\_FILE\_TRANSFER PL/SQL package in a variety of ways.

[Example: Creating a Command Rule to Deny Access to CREATE DATABASE LINK](#) (page D-12)

The DBMS\_MACADM.CREATE\_COMMAND\_RULE enables you to create command rules to deny access to the CREATE DATABASE LINK SQL statement.

[Example: Creating a Command Rule to Enable Access to CREATE DATABASE LINK](#) (page D-13)

The DBMS\_MACADM.UPDATE\_COMMAND\_RULE procedure can be used to modify an existing command rule.

[Example: Command Rules to Disable and Enable Access to CREATE DIRECTORY](#) (page D-13)

### D.6.2.1 About Security Considerations for the UTL\_FILE and DBMS\_FILE\_TRANSFER Packages

The UTL\_FILE package is owned by SYS and granted to PUBLIC.

However, a user must have access to the directory object to manipulate the files in that operating system directory.

The DBMS\_FILE\_TRANSFER package is owned by SYS and granted to the EXECUTE\_CATALOG\_ROLE. Users with EXECUTE access on this package can move files from one location to another on the same file system. They also can move files between database instances, including databases on remote systems.

---

**See Also:** *Oracle Database PL/SQL Packages and Types Reference* for information about configuring the UTL\_FILE package securely

---

### D.6.2.2 Securing Access to the DBMS\_FILE\_TRANSFER Package

You can secure access to the DBMS\_FILE\_TRANSFER PL/SQL package in a variety of ways.

- Use any of the following methods to secure the DBMS\_FILE\_TRANSFER PL/SQL package:
  - Revoke the EXECUTE privilege from the DBMS\_FILE\_TRANSFER package and grant the EXECUTE privilege only to trusted users who need it.
  - Create command rules to control the CREATE DATABASE LINK and CREATE DIRECTORY SQL statements. See [Creating a Command Rule](#) (page 7-9) for information on creating command rules by using Oracle Database Vault Administrator.
  - Create Oracle Database Vault command rules to limit and enable access to the CREATE DATABASE LINK and CREATE DIRECTORY statements, which are used to establish connections to remote databases.

---

---

**See Also:**

The following sections for examples of command rules that you can create to protect use of the CREATE DATABASE LINK statement:

- [Example: Creating a Command Rule to Deny Access to CREATE DATABASE LINK](#) (page D-12)
  - [Example: Creating a Command Rule to Enable Access to CREATE DATABASE LINK](#) (page D-13)
  - [Example: Command Rules to Disable and Enable Access to CREATE DIRECTORY](#) (page D-13)
- 
- 

### D.6.2.3 Example: Creating a Command Rule to Deny Access to CREATE DATABASE LINK

The DBMS\_MACADM.CREATE\_COMMAND\_RULE enables you to create command rules to deny access to the CREATE DATABASE LINK SQL statement.

[Example D-1](#) (page D-12) shows how to create a command rule to deny access to the CREATE DATABASE LINK privilege.

#### **Example D-1** *Creating a Command Rule to Deny Access to CREATE DATABASE LINK*

```
BEGIN
  DBMS_MACADM.CREATE_COMMAND_RULE (
    command      => 'CREATE DATABASE LINK',
    rule_set_name => 'Disabled',
    object_owner  => '%',
    object_name   => '%',
    enabled       => DBMS_MACUTL.G_YES);
  END;
  /
  COMMIT;
```



### D.6.2.4 Example: Creating a Command Rule to Enable Access to CREATE DATABASE LINK

The DBMS\_MACADM.UPDATE\_COMMAND\_RULE procedure can be used to modify an existing command rule.

[Example D-2](#) (page D-13) shows how to create a command rule that enables access to the CREATE DATABASE LINK privilege.

When a valid user must use the CREATE DATABASE LINK statement, the Oracle Database Vault owner can reenale it from Oracle Database Vault Administrator or issue the following commands in SQL\*Plus.

#### **Example D-2 Creating a Command Rule to Enable Access to CREATE DATABASE LINK**

```
BEGIN
  DBMS_MACADM.UPDATE_COMMAND_RULE (
    command      => 'CREATE DATABASE LINK',
    rule_set_name => 'Enabled',
    object_owner  => '%',
    object_name   => '%',
    enabled       => DBMS_MACUTL.G_YES);
END;
/
COMMIT;
```

### D.6.2.5 Example: Command Rules to Disable and Enable Access to CREATE DIRECTORY

[Example D-3](#) (page D-13) shows command rules that disable and enable access to CREATE DIRECTORY.

#### **Example D-3 Command Rules to Disable and Enable Access to CREATE DIRECTORY**

```
-- Disable access to CREATE DIRECTORY
BEGIN
  DBMS_MACADM.CREATE_COMMAND_RULE (
    command      => 'CREATE DIRECTORY',
    rule_set_name => 'Disabled',
    object_owner  => '%',
    object_name   => '%',
    enabled       => dbms_macutl.g_yes);
END;
/
COMMIT;

-- Enable access to CREATE DIRECTORY
BEGIN
  dbms_macadm.update_command_rule (
    command      => 'CREATE DIRECTORY',
    rule_set_name => 'Enabled',
    object_owner  => '%',
    object_name   => '%',
    enabled       => dbms_macutl.g_yes);
END;
/
COMMIT;
```

### D.6.3 CREATE ANY JOB Privilege Security Considerations

The `CREATE ANY JOB` privilege has been revoked from the `DBA` and the `SCHEDULER_ADMIN` roles.

Ensure that this change does not affect your applications.

#### Related Topics:

[Using Oracle Scheduler with Oracle Database Vault](#) (page 13-14)

Users who are responsible for scheduling database jobs must have Oracle Database Vault-specific authorization.

### D.6.4 CREATE EXTERNAL JOB Privilege Security Considerations

The `CREATE EXTERNAL JOB` privilege was introduced in Oracle Database 10g release 2 (10.2).

This privilege is required for database users who want to execute jobs that run on the operating system outside the database. By default, the `CREATE EXTERNAL JOB` privilege is granted to all users who have been granted the `CREATE JOB` privilege. For greater security, revoke this privilege from users who do not need it and then grant it only to those users who do need it.

### D.6.5 LogMiner Package Security Considerations

The role `EXECUTE_CATALOG_ROLE` no longer has the `EXECUTE` privilege granted by default on the several LogMiner packages.

These packages are as follows:

- `DBMS_LOGMNR`
- `DBMS_LOGMNR_D`
- `DBMS_LOGMNR_LOGREP_DICT`
- `DBMS_LOGMNR_SESSION`

You should ensure that this change does not affect your applications.

### D.6.6 ALTER SYSTEM and ALTER SESSION Privilege Security Considerations

You should be aware of ways to secure the powerful `ALTER SYSTEM` and `ALTER SESSION` system privileges.

[About ALTER SYSTEM and ALTER SESSION Privilege Security Considerations](#) (page D-15)

Be aware that trace and debug commands have the potential to show Oracle database memory information.

[Example: Adding Rules to the Existing ALTER SYSTEM Command Rule](#) (page D-15)

You can create a rule that prevents users with the `ALTER SYSTEM` privilege from issuing `ALTER SYSTEM` statements.

### D.6.6.1 About ALTER SYSTEM and ALTER SESSION Privilege Security Considerations

Be aware that trace and debug commands have the potential to show Oracle database memory information.

Oracle Database Vault does not protect against these commands. To help secure the Oracle database memory information, Oracle recommends that you strictly control access to the ALTER SYSTEM and ALTER SESSION privileges. These privileges can be granted by the user SYS when connected as SYSDBA and by any user granted the DBA role.

Oracle also recommends that you add rules to the existing command rule for ALTER SYSTEM statement. You can use Oracle Database Vault Administrator to create a rule and add it to a rule set. You should grant the ALTER SESSION privilege only to trusted users. (For example, the ALTER SESSION statement can enable tracing.)

### D.6.6.2 Example: Adding Rules to the Existing ALTER SYSTEM Command Rule

You can create a rule that prevents users with the ALTER SYSTEM privilege from issuing ALTER SYSTEM statements.

[Example D-4](#) (page D-15) shows how to create a rule that prevents users with ALTER SYSTEM privilege from issuing the ALTER SYSTEM DUMP statement. Log into the database instance as the Oracle Database Vault Owner when you create this command rule.

Alternatively, you can use Oracle Database Vault Administrator to create and add this rule to the rule set. See [Creating a Rule to Add to a Rule Set](#) (page 6-8) for more information.

#### **Example D-4 Adding Rules to the Existing ALTER SYSTEM Command Rule**

```
CONNECT bea_dvacctmgr
Enter password: password

BEGIN
  DBMS_MACADM.CREATE_RULE('NO_SYSTEM_DUMP',
    '(INSTR(UPPER(DV_SQL_TEXT), 'DUMP') = 0)');
  END;
/
EXEC DBMS_MACADM.ADD_RULE_TO_RULE_SET
  ('Allow Fine Grained Control of System Parameters', 'NO_SYSTEM_DUMP');

COMMIT;
```



---

# Troubleshooting Oracle Database Vault

You can troubleshoot Oracle Database Vault by using tools such as trace files or checking certain Oracle Database Vault reports.

[Using Trace Files to Diagnose Oracle Database Vault Events](#) (page E-1)

Trace files, which the database generates, capture important information to help you debug errors.

[General Diagnostic Tips](#) (page E-11)

Oracle provides general tips for diagnosing problems in realms, factors, and rule sets.

[Configuration Problems with Oracle Database Vault Components](#) (page E-12)

Oracle Database Vault provides reports to check configuration problems with realms, command rules, factors, rule sets, or secure application roles.

[Resetting Oracle Database Vault Account Passwords](#) (page E-12)

Backup accounts can help you reset lost passwords for users who have been granted the DV\_OWNER and DV\_ACCTMGR roles.

## E.1 Using Trace Files to Diagnose Oracle Database Vault Events

Trace files, which the database generates, capture important information to help you debug errors.

[About Using Trace Files to Diagnose Oracle Database Vault Events](#) (page E-2)

You can monitor the Oracle Database Vault database instance for server and background process events by enabling and checking the database instance trace files.

[Types of Oracle Database Vault Trace Events That You Can and Cannot Track](#) (page E-2)

You can use trace files to track a variety of Oracle Database Vault activities.

[Levels of Oracle Database Vault Trace Events](#) (page E-3)

You can use the several levels for Oracle Database Vault trace events.

[Performance Effect of Enabling Oracle Database Vault Trace Files](#) (page E-3)

Be careful about enabling trace files.

[Enabling Oracle Database Vault Trace Events](#) (page E-3)

You can use the ALTER SESSION or ALTER SYSTEM SQL statements to enable Oracle Database Vault trace events.

[Finding Oracle Database Vault Trace File Data](#) (page E-5)

The Linux `grep` command and the ADR Command Interpreter (ADRCI) command-line utility can find Oracle Database Vault trace file data.

[Example: Low Level Oracle Database Vault Realm Violations in a Trace File](#)  
(page E-7)

You can use trace file data to track low level realm violations.

[Example: High Level Trace Enabled for Oracle Database Vault Authorization](#)  
(page E-8)

You can track Oracle Database Vault authorizations in a trace file with high level trace enabled.

[Example: Highest Level Traces on Violations on Realm-Protected Objects](#)  
(page E-9)

You can track high level violations using trace files.

[Disabling Oracle Database Vault Trace Events](#) (page E-10)

You can disable tracing for Oracle Database Vault events.

## E.1.1 About Using Trace Files to Diagnose Oracle Database Vault Events

You can monitor the Oracle Database Vault database instance for server and background process events by enabling and checking the database instance trace files.

Trace files reveal the Oracle Database Vault policy authorization success and failures. They are useful for providing information to help resolve bug and other issues that may occur.

To set tracing for Oracle Database Vault, you must have the DV\_ADMIN role. To perform the configuration, you use either of the ALTER SESSION SET EVENTS or ALTER SYSTEM SET EVENTS SQL statements.

---



---

### See Also:

*Oracle Database Administrator's Guide* for more information about how to manage trace files

---



---

## E.1.2 Types of Oracle Database Vault Trace Events That You Can and Cannot Track

You can use trace files to track a variety of Oracle Database Vault activities.

[Table E-1](#) (page E-2) describes these activities.

**Table E-1 Contents of Oracle Database Vault Trace Files**

Database Vault Feature	Description
Realm authorizations	The trace file tracks cases of realm authorization with a rule set and realm authorization to a role. See <a href="#">Example: Low Level Oracle Database Vault Realm Violations in a Trace File</a> (page E-7) for examples of this type of trace file.
Rule set evaluations	The trace file includes information about a rule set evaluation from a realm authorization, for a command rule, the CONNECT command rule, and from a factor.
Oracle Data Pump authorization	The trace file includes Database Vault Data Pump authorization results and other user, object, and SQL text information.

**Table E-1 (Cont.) Contents of Oracle Database Vault Trace Files**

Database Vault Feature	Description
Oracle Scheduler job authorization	The trace file includes the Database Vault Oracle Scheduler job authorization results, job name, job owner, current statement, and so on.
Object privilege bypass	The trace file tracks both direct grants and grants through a role. This type of trace is useful for cases where mandatory realms are not enabled, which enables users who have an object privilege to access realm protected objects.
Factor loading	The trace file tracks the expression and value for each factor loaded.
Others	Object owner bypassed realm protection and other Database Vault failed and succeeded operations

### E.1.3 Levels of Oracle Database Vault Trace Events

You can use the several levels for Oracle Database Vault trace events.

These levels are as follows:

- **Low** prints the information for all failed Oracle Database Vault authorizations to a trace file. This type of trace file includes failed realm authorizations, failed factor loading, failed rule set evaluating, and so on. It has a low impact on Oracle Database performance.
- **High** prints trace records that include both successful and failed authorizations. Because this type of tracing tracks all the authorizations, the overhead is larger than that of the low level tracing. In addition, the trace files are usually larger.
- **Highest** prints the PL/SQL stack and function call stack to a trace file, as well as what is traced at level high (as described in [Table E-1](#) (page E-2)). It has the highest impact on Oracle Database performance.

### E.1.4 Performance Effect of Enabling Oracle Database Vault Trace Files

Be careful about enabling trace files.

Doing so can increase the overhead of the database instance operation, which could decrease performance.

### E.1.5 Enabling Oracle Database Vault Trace Events

You can use the `ALTER SESSION` or `ALTER SYSTEM SQL` statements to enable Oracle Database Vault trace events.

#### [Enabling Trace Events for the Current Database Session](#) (page E-4)

You can use the `ALTER SESSION SET EVENTS SQL` statement to enable trace events for the current database session.

#### [Enabling Trace Events for All Database Sessions](#) (page E-4)

You can use the `ALTER SYSTEM SET EVENTS SQL` statement to enable Database Vault trace events for all database sessions.

### [Management of Trace Events in a Multitenant Environment](#) (page E-5)

You should be aware of how enabling trace events is affected in a multitenant environment.

#### **E.1.5.1 Enabling Trace Events for the Current Database Session**

You can use the `ALTER SESSION SET EVENTS SQL` statement to enable trace events for the current database session.

1. Log into the database instance as a user who has been granted the `DV_ADMIN` role and the `ALTER SESSION` system privilege.

For example:

```
sqlplus leo_dvowner
Enter password: password
Connected.
```

2. Enter the `ALTER SESSION SET EVENTS SQL` statement to set the tracing to low, high, or highest, as described in [Levels of Oracle Database Vault Trace Events](#) (page E-3).
  - To turn on tracing for failed operations that have a low impact, enter one of the following statements:

```
ALTER SESSION SET EVENTS 'TRACE[DV] DISK=LOW';
```

```
ALTER SESSION SET EVENTS '47998 TRACE NAME CONTEXT FOREVER, LEVEL 1';
```

- To turn on tracing for both failed and successful operations that have a high impact, enter one of the following statements:

```
ALTER SESSION SET EVENTS 'TRACE[DV] DISK=HIGH';
```

```
ALTER SESSION SET EVENTS '47998 TRACE NAME CONTEXT FOREVER, LEVEL 3';
```

- To turn on tracing for both failed and successful operations with a function and PL/SQL call stack that has the highest impact, enter one of the following statements:

```
ALTER SESSION SET EVENTS 'TRACE[DV] DISK=HIGHEST';
```

```
ALTER SESSION SET EVENTS '47998 TRACE NAME CONTEXT FOREVER, LEVEL 4';
```

#### **E.1.5.2 Enabling Trace Events for All Database Sessions**

You can use the `ALTER SYSTEM SET EVENTS SQL` statement to enable Database Vault trace events for all database sessions.

1. Log into the database instance as a user who has been granted the `DV_ADMIN` role and the `ALTER SYSTEM` system privilege.

For example:

```
sqlplus leo_dvowner
Enter password: password
Connected.
```

2. Enter the `ALTER SYSTEM SET EVENTS SQL` statement, using the syntax that is shown in Step 2 in [Enabling Trace Events for the Current Database Session](#) (page E-4).



For example:

```
ALTER SYSTEM SET EVENTS 'TRACE[DV] DISK=LOW';
```

### 3. Restart the database.

For example:

```
SHUTDOWN IMMEDIATE
STARTUP
```

Another way that you can enable trace events for all database sessions is to add the following line to the `init.ora` file, and then restart the database:

```
event="47998 trace name context forever, level [trace_level]"
```

Replace `trace_level` with one of the following values:

- 1 for the lowest level of tracing
- 3 for the high level
- 4 for the highest level

For example:

```
event="47998 trace name context forever, level [1]"
```

### E.1.5.3 Management of Trace Events in a Multitenant Environment

You should be aware of how enabling trace events is affected in a multitenant environment.

- **Trace events for the current session:** In a multitenant environment, running the `ALTER SESSION SET EVENTS SQL` statement from either the root or a pluggable database (PDB) enables tracing for the current user session. If you switch from one PDB to another PDB (by using the `ALTER SESSION SET CONTAINER` statement), then tracing is still enabled for the new PDB. You cannot enable tracing for a single PDB in a multitenant container database (CDB); it applies to all PDBs and the root. Remember that must have the `ALTER SESSION SET CONTAINER` system privilege to move from one PDB to another.
- **Trace events for all database sessions:** In a multitenant environment, running the `ALTER SYSTEM SET EVENTS` statement from either the root or a specific PDB enables tracing for all PDBs in the container database.

## E.1.6 Finding Oracle Database Vault Trace File Data

The Linux `grep` command and the ADR Command Interpreter (ADRCI) command-line utility can find Oracle Database Vault trace file data.

### [Finding the Database Vault Trace File Directory Location](#) (page E-6)

You can find the full directory location of trace files by querying the `$DIAG_INFO` dynamic view.

### [Using the Linux grep Command to Search Trace Files for Strings](#) (page E-6)

To query or process the trace files, you can use the Linux `grep` command to search for strings.

### Using the ADR Command Interpreter (ADRCI) Utility to Query Trace Files (page E-6)

You can query trace files by using the ADR Command Interpreter (ADRCI) command-line utility.

#### E.1.6.1 Finding the Database Vault Trace File Directory Location

You can find the full directory location of trace files by querying the `V$DIAG_INFO` dynamic view.

- Query the `V$DIAG_INFO` dynamic view as follows:

```
SELECT VALUE FROM V$DIAG_INFO WHERE NAME = 'Default Trace File';
```

Output similar to the following appears:

```
VALUE
-----
/u01/app/oracle/product/12.1.0/log/diag/rdbms/orcl/orcl/trace/orcl_ora_7174.trc
```

#### E.1.6.2 Using the Linux `grep` Command to Search Trace Files for Strings

To query or process the trace files, you can use the Linux `grep` command to search for strings.

- For example, to find the trace files that show realm authorization failures, enter the following command:

```
grep 'Result=Realm Authorization Failed' *.trc
```

#### E.1.6.3 Using the ADR Command Interpreter (ADRCI) Utility to Query Trace Files

You can query trace files by using the ADR Command Interpreter (ADRCI) command-line utility.

- To use the ADRCI utility to find trace file information, use the `SHOW` command.

For example, to use ADRCI to find the trace files, enter the `SHOW TRACEFILE` command:

```
adrci --To start ACRCI from the command line
adrci> show tracefile

diag/rdbms/orcl/orcl/trace/orcl_m002_14551.trc
diag/rdbms/orcl/orcl/trace/orcl_tmon_13450.trc
diag/rdbms/orcl/orcl/trace/orcl_vktm_963.trc
diag/rdbms/orcl/orcl/trace/alert_orcl.log
...
```

To find the number of all trace incidents:

```
adrci> show incident

ADR Home = /u01/app/oracle/product/12.1.0/log/diag/rdbms/orcl/orcl:
*****
234 rows fetched
```

The following ADRCI command returns a list of all trace files whose name contains the word `ora`:

```
adrci> show tracefile %ora%
```

```

/u01/app/oracle/product/12.1.0/log/diag/rdbms/orcl/orcl/trace/orcl_ora_18841.trc
/u01/app/oracle/product/12.1.0/log/diag/rdbms/orcl/orcl/trace/orcl_ora_12017.trc
/u01/app/oracle/product/12.1.0/log/diag/rdbms/orcl/orcl/trace/orcl_ora_19372.trc
/u01/app/oracle/product/12.1.0/log/diag/rdbms/orcl/orcl/trace/orcl_ora_12221.trc
/u01/app/oracle/product/12.1.0/log/diag/rdbms/orcl/orcl/trace/orcl_ora_1600.trc
...

```

The following ADRCI command searches for trace files that contain the phrase Realm Authorization Failed:

```
adrci> show trace %trc -xp "[payload like '%Realm Authorization Failed%']"
```

---



---

#### See Also:

- *Oracle Database Utilities* for detailed information about the ADRCI utility
  - *Oracle Database Administrator's Guide* for information about viewing reports with the ADRCI utility
- 
- 

## E.1.7 Example: Low Level Oracle Database Vault Realm Violations in a Trace File

You can use trace file data to track low level realm violations.

[Example E-1](#) (page E-7) shows an example of tracking low lever real violations.

### **Example E-1 Low Level Oracle Database Vault Realm Violations in a Trace File**

```

*** 2010-02-05 18:35:31.438
*** SESSION ID:(34.559) 2010-02-05 18:35:31.438
*** CLIENT ID:( ) 2010-02-05 18:35:31.438
*** SERVICE NAME:(SYS$USERS) 2010-02-05 18:35:31.438
*** MODULE NAME:(SQL*Plus) 2010-02-05 18:35:31.438
*** ACTION NAME:( ) 2010-02-05 18:35:31.438

Result=Realm Authorization Failed
  Realm_Name=realm 3      Required_Auth_Level=0
  Current_User=116
  Object_Owner=U1 Object_Name=T1 Object_Type=TABLE
  SQL_Text=INSERT INTO U1.T1 VALUES(30)

Result=Realm Authorization Failed
  Realm_Name=realm 3      Required_Auth_Level=0
  Current_User=116
  Object_Owner=U1 Object_Name=T1 Object_Type=TABLE
  SQL_Text=DELETE FROM U1.T1

Result=Realm Authorization Failed
  Realm_Name=realm 3      Required_Auth_Level=0
  Current_User=116
  Object_Owner=U1 Object_Name=T3 Object_Type=TABLE
  SQL_Text=CREATE TABLE U1.T3(C INT)

*** 2010-02-05 18:35:34.465

Result=Realm Authorization Failed
  Realm_Name=realm 3      Required_Auth_Level=0
  Current_User=116
  Object_Owner=U1 Object_Name=T1 Object_Type=TABLE
  SQL_Text=INSERT INTO U1.T1 VALUES(30)

```

```

Result=Realm Authorization Failed
  Realm_Name=realm 3      Required_Auth_Level=0
  Current_User=116
  Object_Owner=U1 Object_Name=T1 Object_Type=TABLE
  SQL_Text=DELETE FROM U1.T1

```

## E.1.8 Example: High Level Trace Enabled for Oracle Database Vault Authorization

You can track Oracle Database Vault authorizations in a trace file with high level trace enabled.

[Example E-2](#) (page E-8) shows an example of this type of trace file.

### **Example E-2 High Level Trace Enabled for Oracle Database Vault Authorization**

```

Result= Realm Authorization Passed
  Reason=Current user is the object owner
  Current_User=70 Command=SELECT
  Object_Owner=LBACSYS Object_Name=LBAC$AUDIT Object_Type=TABLE

Result= Realm Authorization Passed
  Reason=Current user is the object owner
  Current_User=70 Command=SELECT
  Object_Owner=LBACSYS Object_Name=LBAC$AUDIT Object_Type=TABLE

Result= Realm Authorization Passed
  Reason=Current user is the object owner
  Current_User=70 Command=SELECT
  Object_Owner=LBACSYS Object_Name=LBAC$POL Object_Type=TABLE

Result= Realm Authorization Passed
  Reason=Current user is the object owner
  Current_User=70 Command=SELECT
  Object_Owner=LBACSYS Object_Name=LBAC$USER_LOGON Object_Type=VIEW

.....

Result= Realm Authorization Passed
  Reason=Current user is the object owner
  Current_User=70 Command=SELECT
  Object_Owner=LBACSYS Object_Name=LBAC$POL Object_Type=TABLE

Result=Set Factor Value
  Factor_Name=Sensitive_Treatments Factor_Expression=/SURGERY/
  PSYCHOLOGICAL

Result=Set Factor Value
  Factor_Name=Database_Instance
  Factor_Expression=UPPER(SYS_CONTEXT('USERENV','INSTANCE')) Factor_Value=1

Result=Set Factor Value
  Factor_Name=Client_IP
  Factor_Expression=UPPER(SYS_CONTEXT('USERENV','IP_ADDRESS')) Factor_Value=

Result=Set Factor Value
  Factor_Name=Authentication_Method
  Factor_Expression=UPPER(SYS_CONTEXT('USERENV','AUTHENTICATION_METHOD'))
  Factor_Value=PASSWORD

.....

*** ACTION NAME:( ) 2010-02-05 18:47:19.540

```

```

Result=Rule Set Evaluation Failed
  Command=SELECT RuleSet_ID=2 RuleSet_Name=Disabled
  Current_User=SYSTEM
  Object_Owner=U1 Object_Name=T1 Object_Type=TABLE
  SQL_Text=SELECT * FROM U1.T1

Result=Rule Set Evaluation Succeeded
  Command=SELECT RuleSet_ID=1 RuleSet_Name=Enabled
  Current_User=SYSTEM
  Object_Owner=U1 Object_Name=T1 Object_Type=TABLE
  SQL_Text=SELECT * FROM U1.T1

```

## E.1.9 Example: Highest Level Traces on Violations on Realm-Protected Objects

You can track high level violations using trace files.

[Example E-3](#) (page E-9) shows how highest level violations that involve Oracle Scheduler jobs authorization can appear in a trace file when trace is enabled at the highest level.

### **Example E-3 Highest Level Traces on Violations on Realm-Protected Objects**

```

----- Call Stack Trace -----
kzvdvechk<-kzvdvegau<-kksfbc<-opiexe<-kpoal8<-opiodr<-ttcpip<-opitsk<-opiino<-
opiodr<-opidrv<-sou2o<-opimai_real<-ssthrdmain<-main<-__libc_start_main<-_start

Result=Object Privilege check passed
  Current_User=INVOKER2 Used_Role=1
  Object_Owner=SYSTEM Object_Name=PRODUCT_PRIVS Object_Type=VIEW
  SQL_Text=SELECT CHAR_VALUE FROM SYSTEM.PRODUCT_PRIVS WHERE
(UPPER('SQL*PLUS') LIKE UPPER(PRODUCT)) AND ((USER LIKE USERID) OR (USERID =
'PUBLIC')) AND (UPPER(ATTRIBUTE) = 'ROLES')
*** MODULE NAME:(SQL*Plus) 2010-02-05 18:57:53.973
*** ACTION NAME:( ) 2010-02-05 18:57:53.973

----- Current SQL Statement for this session (sql_id=2sr63rjm45yfh) -----
UPDATE INVOKER1.T1 SET A = 20
----- PL/SQL Stack -----
----- PL/SQL Call Stack -----
  object      line object
  handle      number name
0x26a00e34      1 anonymous block
0x2495b000     185 package body SYS.DBMS_ISCHED
0x24958fb8     486 package body SYS.DBMS_SCHEDULER
0x247bbb34      1 anonymous block

----- Call Stack Trace -----
kzvdvechk<-kzvdvegau<-kksfbc<-opiexe<-opipls<-opiodr<-__PGOSF151_rpidrus<-skgmstack<-
rpidru<-rplswu2<-rpidrv<-psddr0<-psdnal<-pevm_EXECC<-pfrinstr_EXECC<-pfrun_no_tool<-
pfrun<-plsqli_run<-peicnt<-kkxexe<-opiexe<-kpoal8<-opiodr<-kpoodr<-upirtrc<-kpurcsc<-
kpuexec
<-OCISmtExecute<-jslvec_execcb<-jslvswu<-jslve_execute0<-jskaJobRun<-jsiRunJob<-
jsaRunJob<-spefcmpa<-spefmccallstd<-pextproc<-__PGOSF495_peftrusted<-
__PGOSF522_psdexsp<-rplswu2<-psdextp<-pefccal<-pefcacal<-pevm_FCAL<-pfrinstr_FCAL<-
pfrun_no_tool<-pfrun<-plsqli_run
<-peicnt<-kkxexe<-opiexe<-kpoal8<-opiodr<-ttcpip<-opitsk<-opiino<-opiodr<-opidrv<-
sou2o<-opimai_real<-ssthrdmain<-main<-__libc_start_main<-_start

Result=Realm Authorization Succeeded
  Realm_Name=jobowner realm Used_Auth_Level=0
  Current_User=119
  Object_Owner=INVOKER1 Object_Name=T1 Object_Type=TABLE

```

```
SQL_Text=UPDATE INVOKER1.T1 SET A = 20
```

```
Result=Scheduler Job Authorization Succeeded
Current_User=JOBOWNER Logon_User=INVOKER2
Job_Owner=JOBOWNER Job_Name=DMLJOB1
Object_Owner=INVOKER1 Object_Name=T1 Object_Type=TABLE
SQL_Text=UPDATE INVOKER1.T1 SET A = 20
```

## E.1.10 Disabling Oracle Database Vault Trace Events

You can disable tracing for Oracle Database Vault events.

### [Disabling Trace Events for the Current Database Session](#) (page E-10)

You can use the `ALTER SESSION SET EVENTS SQL` statement to disable Database Vault tracing for the current database session.

### [Disabling Trace Events for All Database Sessions](#) (page E-10)

You can use the `ALTER SYSTEM SET EVENTS SQL` statement to disable Database Vault tracing for all database sessions.

### [Disabling Trace Events in a Multitenant Environment](#) (page E-11)

You should be aware of how enabling trace events is affected in a multitenant environment.

#### E.1.10.1 Disabling Trace Events for the Current Database Session

You can use the `ALTER SESSION SET EVENTS SQL` statement to disable Database Vault tracing for the current database session.

1. Log into the database instance as a user who has been granted the `DV_ADMIN` role and the `ALTER SESSION` system privilege.

For example:

```
sqlplus leo_dvowner
Enter password: password
Connected.
```

2. Enter both of the following SQL statements to disable tracing:

```
ALTER SESSION SET EVENTS 'TRACE[DV] OFF';
ALTER SESSION SET EVENTS '47998 trace name context off';
```

Alternatively, you can use the `ALTER SYSTEM` statement as well:

```
ALTER SYSTEM SET EVENTS 'TRACE[DV] OFF';
ALTER SYSTEM SET EVENTS '47998 trace name context off';
```

#### E.1.10.2 Disabling Trace Events for All Database Sessions

You can use the `ALTER SYSTEM SET EVENTS SQL` statement to disable Database Vault tracing for all database sessions.

1. Log into the database instance as a user who has been granted the `DV_ADMIN` role and the `ALTER SYSTEM` system privilege.

For example:

```
sqlplus leo_dvowner
Enter password: password
Connected.
```

2. Enter the `ALTER SYSTEM SET EVENTS SQL` statement, using the syntax that is shown in Step 2 (page E-10) in [Disabling Trace Events for the Current Database Session](#) (page E-10).

For example:

```
ALTER SYSTEM SET EVENTS 'TRACE[DV] OFF';
```

3. Restart the database.

For example:

```
SHUTDOWN IMMEDIATE
STARTUP
```

Another way that you can disable trace events for all database sessions is to add the following line to the `init.ora` file, and then restart the database:

```
event="47998 trace name context off"
```

Ensure that the `init.ora` file does not have any conflicting 47998 lines, such as `event="47998 trace name context forever, level [1]"`.

### E.1.10.3 Disabling Trace Events in a Multitenant Environment

You should be aware of how enabling trace events is affected in a multitenant environment.

- **Trace events for the current session:** In a multitenant environment, running the `ALTER SESSION SET EVENTS SQL` statement from either the root or a PDB disables tracing for the current user session. If you switch from one PDB to another PDB (by using the `ALTER SESSION SET CONTAINER` statement), then tracing is still disabled for the new PDB. You cannot disable tracing for a single PDB in a CDB; it applies to all PDBs and the root. Remember that must have the `ALTER SESSION SET CONTAINER` system privilege to move from one PDB to another.
- **Trace events for all database sessions:** In a multitenant environment, running the `ALTER SYSTEM SET EVENTS` statement from either the root or a specific PDB disables tracing for all PDBs in the CDB.

## E.2 General Diagnostic Tips

Oracle provides general tips for diagnosing problems in realms, factors, and rule sets.

These guidelines are as follows:

- For realm protections, verify that a user has the underlying system or object privileges (granted directly or through a role) that might affect the command.
- If a realm authorization is not working, verify that the account roles are set correctly.
- For PL/SQL expressions used in factors and rule sets, grant the `EXECUTE` privilege on the PL/SQL package functions used in these expressions directly to the account and determine if the results appear to be correct.
- Use the auditing reports to diagnose problems in general. See [Oracle Database Vault Auditing Reports](#) (page 27-5) for more information.

## E.3 Configuration Problems with Oracle Database Vault Components

Oracle Database Vault provides reports to check configuration problems with realms, command rules, factors, rule sets, or secure application roles.

See the following sections for more information:

- [Command Rule Configuration Issues Report](#) (page 27-3)
- [Factor Configuration Issues Report](#) (page 27-4)
- [Factor Without Identities Report](#) (page 27-4)
- [Identity Configuration Issues Report](#) (page 27-4)
- [Realm Authorization Configuration Issues Report](#) (page 27-4)
- [Rule Set Configuration Issues Report](#) (page 27-3)
- [Secure Application Configuration Issues Report](#) (page 27-5)

To run these reports, see [Running the Oracle Database Vault Reports](#) (page 27-2).

## E.4 Resetting Oracle Database Vault Account Passwords

Backup accounts can help you reset lost passwords for users who have been granted the DV\_OWNER and DV\_ACCTMGR roles.

### [Resetting the DV\\_OWNER User Password](#) (page E-12)

You can use the DV\_OWNER backup account to reset the DV\_OWNER user password.

### [Resetting the DV\\_ACCTMGR User Password](#) (page E-13)

You can use the DV\_ACCTMGR backup account to reset the DV\_ACCTMGR user password.

### E.4.1 Resetting the DV\_OWNER User Password

You can use the DV\_OWNER backup account to reset the DV\_OWNER user password.

To reset the DV\_OWNER user password, you must temporarily revoke the DV\_OWNER role from this user, reset the password, and then re-grant the role back to the user.

1. Log in to the database instance as the backup user for the DV\_OWNER user account.

For example:

```
sqlplus dbv_owner_backup
Enter password: password
```

2. Revoke the DV\_OWNER role from the DV\_OWNER user who has lost the password.

For example:

```
REVOKE DV_OWNER FROM dbv_owner;
```

3. Connect as a user who has been granted the DV\_ACCTMGR role.

For example:

```
CONNECT dbv_acctmgr
Enter password: password
```



4. Reset the password for the DV\_OWNER user.

```
ALTER USER dbv_owner IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace *password* with a password that is secure.

5. Connect as the backup DV\_OWNER user.

```
CONNECT dbv_owner_backup  
Enter password: password
```

6. Grant the DV\_OWNER role back to the DV\_OWNER user.

```
GRANT DV_OWNER TO dbv_owner;
```

---

---

**Note:**

Ensure that the backup DV\_OWNER account is safely stored in case it is needed again.

---

---

## E.4.2 Resetting the DV\_ACCTMGR User Password

You can use the DV\_ACCTMGR backup account to reset the DV\_ACCTMGR user password.

To reset the DV\_ACCTMGR user password, you can use the backup DV\_ACCTMGR account to reset this user's password.

1. Log in to the database instance as the backup user for the DV\_ACCTMGR user account.

For example:

```
sqlplus dbv_acctmgr_backup  
Enter password: password
```

2. Reset the password for the DV\_ACCTMGR user.

For example:

```
ALTER USER dbv_acctmgr IDENTIFIED BY password;
```

Follow the guidelines in *Oracle Database Security Guide* to replace *password* with a password that is secure.

---

---

**Note:**

Ensure that the backup DV\_ACCTMGR account is safely stored in case it is needed again.

---

---



## A

- access control policy
  - reports
    - Core Database Vault Audit Report, [27-6](#)
- Access to Sensitive Objects Report, [27-11](#)
- accounts
  - See database accounts
- Accounts With DBA Roles Report, [27-14](#)
- Accounts with SYSDBA/SYSOPER Privilege Report, [27-12](#)
- ad hoc tools
  - preventing use of, [8-23](#)
- administrators
  - DBA operations in Oracle Database Vault, [13-1](#)
  - restricting different types, [8-29](#)
- ADRCI utility
  - Database Vault, [E-6](#)
- alerts
  - email alert in rule set, [6-17](#)
  - Enterprise Manager Cloud Control, [13-4](#)
- ALTER ROLE statement
  - monitoring, [26-1](#)
- ALTER SESSION command rules
  - about, [7-5](#)
- ALTER SESSION event command rules
  - creating, [17-11](#)
  - updating, [17-22](#)
- ALTER SESSION privilege
  - enabling trace files, [E-3](#)
  - reports, ALTER SYSTEM or ALTER SESSION Report, [27-15](#)
- ALTER SESSION statement
  - guidelines on managing privileges, [D-15](#)
- ALTER SYSTEM command rules
  - deleting system event command rules, [17-17](#)
- ALTER SYSTEM event command rules
  - creating, [17-12](#)
  - updating, [17-24](#)
- ALTER SYSTEM or ALTER SESSION Report, [27-15](#)
- ALTER SYSTEM privilege
  - reports, ALTER SYSTEM or ALTER SESSION Report, [27-15](#)
- ALTER SYSTEM statement
  - ALTER SYSTEM statement (*continued*)
    - guidelines on managing privileges, [D-15](#)
  - ALTER USER statement
    - monitoring, [26-1](#)
  - ANY System Privileges for Database Accounts Report, [27-10](#)
  - application security
    - finding privilege use by users, [4-4](#)
  - audit policy change
    - monitoring, [26-1](#)
  - AUDIT privilege, [27-16](#)
  - AUDIT Privileges Report, [27-16](#)
  - AUDIT\_SYS\_OPERATIONS initialization parameter, [2-1](#)
  - AUDIT\_TRAIL\$ system table
    - affected by AUDIT\_TRAIL initialization parameter, [A-3](#)
    - archiving, [A-6](#)
    - format, [A-3](#)
    - purging, [A-8](#)
- auditing
  - about, [A-1](#)
  - archiving Database Vault audit trail
    - about, [A-6](#)
    - Core Database Audit Report, [27-17](#)
  - DBMS\_MACUTL fields, [21-1](#)
  - factors
    - options, [8-13](#)
  - intruders
    - using factors, [8-13](#)
  - Oracle Database audit settings, [A-9](#)
  - purging Database Vault audit trail
    - about, [A-6](#)
  - realms
    - DBMS\_MACUTL fields, [21-1](#)
    - options, [5-8](#)
  - reports, [27-5](#)
  - rule sets
    - DBMS\_MACUTL fields, [21-1](#)
    - options, [6-5](#)
  - secure application roles
    - audit records, [9-10](#)
- auditing policies
  - about, [A-1](#)

- auditing policies (*continued*)
  - audit events
    - about, [A-3](#)
  - custom events
    - audit trail, [A-3](#)
  - events that are tracked, [A-3](#)
  - monitoring changes to, [26-1](#)
- authentication
  - Authentication\_Method default factor, [8-2](#)
  - command rules, [7-2](#)
  - method, finding with DVF.F
    - \$AUTHENTICATION\_METHOD, [18-29](#)
  - realm procedures, [15-2](#)
- authorizations
  - Oracle Data Pump activities, [13-6](#)
  - realms, [5-13](#)
  - scheduling database jobs, [13-14](#)
- AUTHORIZE\_MAINTENANCE\_USER procedure, [22-5](#)

## B

---

- backup accounts, [14-25](#)
- BECOME USER Report, [27-14](#)
- BECOME USER system privilege
  - about, [27-14](#)
- break-glass accounts
  - See backup accounts

## C

---

- catalog-based roles, [27-15](#)
- CDB\_DV\_STATUS view, [25-5](#)
- CDBs
  - functionality in Oracle Database Vault, [1-10](#)
  - privilege profiles, [4-4](#)
  - realms
    - authorizations, [5-13](#)
  - rule sets, [6-2](#)
- clients
  - finding IP address with DVF.F\$CLIENT\_IP, [18-30](#)
- code groups
  - retrieving value with DBMS\_MACUTL functions, [21-7](#)
- Command Rule Audit Report, [27-6](#)
- Command Rule Configuration Issues Report, [27-3](#)
- command rules
  - about, [7-2](#)
  - creating, [7-9](#)
  - data dictionary view, [7-16](#)
  - data masking, [13-22](#)
  - default command rules, [7-7](#)
  - deleting, [7-11](#)
  - editing, [7-9](#)
  - functions
    - DBMS\_MACUTL (utility), [21-1](#)
  - guidelines, [7-15](#)

- command rules (*continued*)
  - how command rules work, [7-11](#)
  - modifying enablement status, [7-11](#)
  - objects
    - name, [7-9](#)
    - owner, [7-9](#)
  - performance effect, [7-16](#)
  - procedures
    - DBMS\_MACADM (configuration), [17-1](#)
  - process flow, [7-11](#)
  - propagating configuration to other databases, [13-2](#)
  - reports, [7-16](#)
  - rule sets
    - selecting, [7-9](#)
    - used with, [7-2](#)
  - simulation mode, [11-1](#)
  - troubleshooting
    - with auditing report, [27-6](#)
  - tutorial, [7-12](#)
  - views, [7-16](#), [25-8](#)
  - with PDBs, [7-3](#)
    - See also rule sets
- compliance
  - Oracle Database Vault addressing, [1-7](#)
- computer name
  - finding with DVF.F\$MACHINE, [18-35](#)
  - Machine default factor, [8-2](#)
- configuration
  - monitoring changes, [26-1](#)
  - views
    - DVSYSDV\$CONFIGURATION\_AUDIT, [25-38](#)
    - DVSYSDV\$ENFORCEMENT\_AUDIT, [25-43](#)
    - SYSDV\$CONFIGURATION\_AUDIT, [25-56](#)
- CONFIGURE\_DV procedure
  - about, [22-18](#)
  - registering Database Vault with, [3-3](#), [3-7](#)
- CONNECT command rules
  - about, [7-4](#)
  - example, [7-4](#)
- CONNECT events, controlling with command rules, [7-2](#)
- connection pooling
  - finding unnecessarily granted privileges, [4-4](#)
- context profiles
  - privilege analysis, [4-3](#)
- core database
  - troubleshooting with Core Database Vault Audit Report, [27-6](#)
- Core Database Audit Report, [27-17](#)
- Core Database Vault Audit Trail Report, [27-6](#)
- CPU\_PER\_SESSION resource profile, [27-16](#)
- CREATE ANY JOB privilege, [D-14](#)
- CREATE ANY JOB statement
  - guidelines on managing privileges, [D-14](#)
- CREATE EXTERNAL JOB privilege, [D-14](#)

- CREATE JOB privilege, [D-14](#)
- CREATE JOB statement
  - guidelines on managing privileges, [D-14](#)
- CREATE ROLE statement
  - monitoring, [26-1](#)
- CREATE USER statement
  - monitoring, [26-1](#)
- CTXSYS schema realm protection, [5-7](#)

## D

---

- data definition language (DDL)
  - statement
    - controlling with command rules, [7-2](#)
- Data Definition Language (DDL) statements
  - Database Vault authorization
    - DBA\_DV\_DDL\_AUTH view, [25-10](#)
    - granting, [22-4](#)
    - revoking, [22-9](#)
- Data Dictionary realm
  - data masking, [13-21](#)
- data manipulation language (DML)
  - statement
    - checking with
      - DBMS\_MACUTL.CHECK\_DVSYSDML\_ALLOWED function, [21-7](#)
    - controlling with command rules, [7-2](#)
- data masking
  - about, [13-21](#)
  - adding users to realms for, [13-22](#)
  - creating command rule for, [13-22](#)
  - errors that can appear, [13-21](#)
- data Oracle Database Vault recognizes
  - See factors
- Database Account Default Password Report, [27-17](#)
- Database Account Status Report, [27-17](#)
- database accounts
  - backup DV\_OWNER and DV\_ACCTMGR, [14-25](#)
  - configuring Database Vault accounts as enterprise users, [12-2](#)
  - counting privileges of, [27-13](#)
  - DBSNMP
    - changing password, [13-5](#)
    - granted DV\_MONITOR role, [14-12](#)
  - DVSYSDML, [14-23](#)
  - LBACSYS, [14-23](#)
  - monitoring, [26-1](#)
  - reports
    - Accounts With DBA Roles Report, [27-14](#)
    - ALTER SYSTEM or ALTER SESSION Report, [27-15](#)
    - ANY System Privileges for Database Accounts Report, [27-10](#)
    - AUDIT Privileges Report, [27-16](#)
    - BECOME USER Report, [27-14](#)
    - Database Account Default Password Report, [27-17](#)
    - Database Account Status Report, [27-17](#)

- database accounts (*continued*)
  - reports (*continued*)
    - Database Accounts With Catalog Roles Report, [27-15](#)
    - Direct and Indirect System Privileges By Database Account Report, [27-10](#)
    - Direct Object Privileges Report, [27-8](#)
    - Direct System Privileges By Database Account Report, [27-9](#)
    - Hierarchical System Privileges by Database Account Report, [27-10](#)
    - Object Access By PUBLIC Report, [27-8](#)
    - Object Access Not By PUBLIC Report, [27-8](#)
    - OS Security Vulnerability Privileges, [27-16](#)
    - Password History Access Report, [27-15](#)
    - Privileges Distribution By Grantee Report, [27-13](#)
    - Privileges Distribution By Grantee, Owner Report, [27-13](#)
    - Privileges Distribution By Grantee, Owner, Privilege Report, [27-13](#)
    - Roles/Accounts That Have a Given Role Report, [27-15](#)
    - Security Policy Exemption Report, [27-14](#)
    - WITH ADMIN Privilege Grants Report, [27-14](#)
    - WITH GRANT Privileges Report, [27-15](#)
  - solution for lockouts, [B-1](#)
  - suggested, [14-23](#)
- Database Accounts With Catalog Roles Report, [27-15](#)
- database administrative operations, [13-1](#)
- database domains, Database\_Domain default factor, [8-2](#)
- database objects
  - Oracle Database Vault, [14-1](#)
  - reports
    - Object Dependencies Report, [27-9](#)
  - See also objects
- database options, installing, [B-1](#)
- database roles
  - about, [14-4](#)
  - counting privileges of, [27-13](#)
  - default Oracle Database Vault, [14-4](#)
  - DV\_ACCTMGR
    - about, [14-19](#)
  - DV\_ADMIN, [14-11](#)
  - DV\_AUDIT\_CLEANUP, [14-13](#)
  - DV\_DATAPUMP\_NETWORK\_LINK, [14-14](#)
  - DV\_GOLDENGATE\_ADMIN, [14-17](#)
  - DV\_GOLDENGATE\_REDO\_ACCESS, [14-18](#)
  - DV\_MONITOR, [14-12](#)
  - DV\_OWNER, [14-9](#)
  - DV\_PATCH\_ADMIN, [14-18](#)
  - DV\_POLICY\_OWNER, [14-22](#)
  - DV\_PUBLIC, [14-23](#)
  - DV\_REALM\_OWNER, [14-21](#)
  - DV\_REALM\_RESOURCE, [14-21](#)

database roles (*continued*)

- DV\_SECANALYST, [14-13](#)
- DV\_STREAMS\_ADMIN, [14-15](#)
- DV\_XSTREAM\_ADMIN, [14-16](#)
- enabled, determining with ROLE\_IS\_ENABLED, [18-27](#)
- granting Database Vault roles to users, [14-8](#)
- monitoring, [26-1](#)
- Oracle Database Vault, default, [14-4](#)
- reports
  - Accounts With DBA Roles Report, [27-14](#)
  - ALTER SYSTEM or ALTER SESSION Report, [27-15](#)
  - AUDIT Privileges Report, [27-16](#)
  - BECOME USER Report, [27-14](#)
  - Database Accounts With Catalog Roles Report, [27-15](#)
  - OS Security Vulnerability Privileges, [27-16](#)
  - Privileges Distribution By Grantee Report, [27-13](#)
  - Roles/Accounts That Have a Given Role Report, [27-15](#)
  - Security Policy Exemption Report, [27-14](#)
  - WITH ADMIN Privilege Grants Report, [27-14](#)
- separation of duty enforcement, [2-3](#)

database sessions

- controlling with Allow Sessions default rule set, [6-3](#)
- factor evaluation, [8-20](#)
- session user name, Proxy\_User default factor, [8-2](#)

Database Vault

See Oracle Database Vault

- Database Vault Account Management realm, [5-7](#)
- Database Vault command rule protections, [7-2](#)
- Database Vault realm protection, [5-2](#)
- Database Vault realm protections, [5-2](#)

databases

- defined with factors, [8-1](#)
- domain, Domain default factor, [8-2](#)
- event monitoring, [E-2](#)
- grouped schemas
  - See realms, [5-2](#)
- host names, Database\_Hostname default factor, [8-2](#)
- instance, retrieving information with functions, [18-1](#)
- instances
  - Database\_Instance default factor, [8-2](#)
  - names, finding with DVF.F\$DATABASE\_INSTANCE, [18-31](#)
  - number, finding with DV\_INSTANCE\_NUM, [16-15](#)
- IP addresses
  - Database\_IP default factor, [8-2](#)
  - retrieving with DVF.F\$DATABASE\_IP, [18-32](#)
- monitoring events, [E-2](#)

databases (*continued*)

names

- Database\_Name default factor, [8-2](#)
- retrieving with DV\_DATABASE\_NAME, [16-16](#)
- retrieving with DVF.F\$DATABASE\_NAME, [18-32](#)

parameters

- Security Related Database Parameters Report, [27-16](#)

roles that do not exist, [27-5](#)

schema creation, finding with DVF.F

\$IDENTIFICATION\_TYPE, [18-34](#)

schema creation, Identification\_Type default factor, [8-2](#)

user name, Session\_User default factor, [8-2](#)

DBA role

impact of Oracle Database Vault installation, [2-3](#)

DBA\_DV\_CODE view, [25-6](#)

DBA\_DV\_COMMAND\_RULE view, [7-16](#), [25-8](#)

DBA\_DV\_DATAPUMP\_AUTH view, [25-10](#)

DBA\_DV\_DDL\_AUTH view, [25-10](#)

DBA\_DV\_DICTIONARY\_ACCTS view, [25-11](#)

DBA\_DV\_FACTOR view, [25-11](#)

DBA\_DV\_FACTOR\_LINK, [25-14](#)

DBA\_DV\_FACTOR\_LINK view, [25-14](#)

DBA\_DV\_FACTOR\_TYPE view, [25-13](#)

DBA\_DV\_IDENTITY view, [25-15](#)

DBA\_DV\_IDENTITY\_MAP view, [25-15](#)

DBA\_DV\_JOB\_AUTH view, [25-16](#)

DBA\_DV\_MAC\_POLICY view, [25-17](#)

DBA\_DV\_MAC\_POLICY\_FACTOR view, [25-17](#)

DBA\_DV\_MAINTENANCE\_AUTH view, [25-18](#)

DBA\_DV\_ORADEBUG view, [25-18](#)

DBA\_DV\_PATCH\_ADMIN\_AUDIT view, [25-19](#)

DBA\_DV\_POLICY view, [25-19](#)

DBA\_DV\_POLICY\_LABEL view, [25-20](#)

DBA\_DV\_POLICY\_OBJECT view, [25-21](#)

DBA\_DV\_POLICY\_OWNER view, [25-22](#)

DBA\_DV\_PROXY\_AUTH view, [25-23](#)

DBA\_DV\_PUB\_PRIVS view, [25-23](#)

DBA\_DV\_REALM view, [25-24](#)

DBA\_DV\_REALM\_AUTH view, [25-25](#)

DBA\_DV\_REALM\_OBJECT view, [25-27](#)

DBA\_DV\_ROLE view, [25-28](#)

DBA\_DV\_RULE view, [25-29](#)

DBA\_DV\_RULE\_SET view, [25-30](#)

DBA\_DV\_RULE\_SET\_RULE view, [25-32](#)

DBA\_DV\_SIMULATION\_LOG view, [25-34](#)

DBA\_DV\_STATUS view, [25-33](#)

DBA\_DV\_TTS\_AUTH view, [25-36](#)

DBA\_DV\_USER\_PRIVS view, [25-36](#)

DBA\_DV\_USER\_PRIVS\_ALL view, [25-37](#)

DBA\_USERS\_WITH\_DEFPWD data dictionary view  
access to in Oracle Database Vault, [2-3](#)

DBMS\_FILE\_TRANSFER package, guidelines on managing, [D-11](#)

DBMS\_MACADM package

- about, [24-1](#)
- command rule procedures, listed, [17-1](#)
- factor procedures, listed, [18-1](#)
- Oracle Label Security policy procedures, listed, [20-1](#)
- realm procedures, listed, [15-1](#)
- rule set procedures, listed, [16-1](#)
- secure application role procedures, listed, [19-1](#)

DBMS\_MACADM PL/SQL package contents, [24-1](#)

DBMS\_MACADM.ADD\_AUTH\_TO\_REALM procedure, [15-2](#)

DBMS\_MACADM.ADD\_CMD\_RULE\_TO\_POLICY procedure, [23-2](#), [23-6](#)

DBMS\_MACADM.ADD\_FACTOR\_LINK procedure, [18-3](#)

DBMS\_MACADM.ADD-NLS\_DATA procedure, [C-2](#)

DBMS\_MACADM.ADD-NLS\_DATA procedure, [22-3](#)

DBMS\_MACADM.ADD\_OBJECT\_TO\_REALM procedure, [15-4](#)

DBMS\_MACADM.ADD\_OWNER\_TO\_POLICY procedure, [23-4](#)

DBMS\_MACADM.ADD\_POLICY\_FACTOR procedure, [18-4](#)

DBMS\_MACADM.ADD\_REALM\_TO\_POLICY procedure, [23-4](#)

DBMS\_MACADM.ADD\_RULE\_TO\_RULE\_SET procedure, [16-2](#)

DBMS\_MACADM.ASSIGN\_ROLE procedure, [19-2](#)

DBMS\_MACADM.AUTHORIZE\_DATAPUMP\_USER procedure, [22-3](#), [22-8](#)

DBMS\_MACADM.AUTHORIZE\_DDL procedure, [22-4](#)

DBMS\_MACADM.AUTHORIZE\_PROXY\_USER procedure, [22-6](#)

DBMS\_MACADM.AUTHORIZE\_SCHEDULER\_USER procedure, [22-7](#)

DBMS\_MACADM.AUTHORIZE\_TTS\_USER procedure, [22-7](#)

DBMS\_MACADM.CHANGE\_IDENTITY\_FACTOR procedure, [18-4](#)

DBMS\_MACADM.CHANGE\_IDENTITY\_VALUE procedure, [18-5](#)

DBMS\_MACADM.CREATE\_COMMAND\_RULE procedure, [17-2](#)

DBMS\_MACADM.CREATE\_CONNECT\_COMMAND\_RULE procedure, [17-9](#)

DBMS\_MACADM.CREATE\_DOMAIN\_IDENTITY procedure, [18-6](#)

DBMS\_MACADM.CREATE\_FACTOR procedure, [18-7](#)

DBMS\_MACADM.CREATE\_FACTOR\_TYPE procedure, [18-9](#)

DBMS\_MACADM.CREATE\_IDENTITY procedure, [18-11](#)

DBMS\_MACADM.CREATE\_IDENTITY\_MAP procedure, [18-10](#)

DBMS\_MACADM.CREATE\_MAC\_POLICY procedure, [20-1](#)

DBMS\_MACADM.CREATE\_POLICY procedure, [23-5](#)

DBMS\_MACADM.CREATE\_POLICY\_LABEL procedure, [20-3](#)

DBMS\_MACADM.CREATE\_REALM procedure, [15-5](#)

DBMS\_MACADM.CREATE\_ROLE procedure, [19-2](#)

DBMS\_MACADM.CREATE\_RULE procedure, [16-3](#)

DBMS\_MACADM.CREATE\_RULE\_SET procedure, [16-5](#)

DBMS\_MACADM.CREATE\_SESSION\_EVENT\_CMD\_RULE procedure, [17-11](#)

DBMS\_MACADM.CREATE\_SYSTEM\_EVENT\_CMD\_RULE procedure, [17-12](#)

DBMS\_MACADM.DELETE\_AUTH\_FROM\_REALM procedure, [15-8](#)

DBMS\_MACADM.DELETE\_COMMAND\_RULE procedure, [17-14](#)

DBMS\_MACADM.DELETE\_CONNECT\_COMMAND\_RULE procedure, [17-16](#)

DBMS\_MACADM.DELETE\_FACTOR procedure, [18-12](#)

DBMS\_MACADM.DELETE\_FACTOR\_LINK procedure, [18-13](#)

DBMS\_MACADM.DELETE\_FACTOR\_TYPE procedure, [18-14](#)

DBMS\_MACADM.DELETE\_IDENTITY procedure, [18-13](#)

DBMS\_MACADM.DELETE\_IDENTITY\_MAP procedure, [18-14](#)

DBMS\_MACADM.DELETE\_MAC\_POLICY\_CASCADE procedure, [20-4](#)

DBMS\_MACADM.DELETE\_OBJECT\_FROM\_REALM procedure, [15-9](#)

DBMS\_MACADM.DELETE\_OWNER\_FROM\_POLICY procedure, [23-8](#)

DBMS\_MACADM.DELETE\_POLICY\_FACTOR procedure, [20-5](#)

DBMS\_MACADM.DELETE\_POLICY\_LABEL procedure, [20-5](#)

DBMS\_MACADM.DELETE\_REALM procedure, [15-9](#)

DBMS\_MACADM.DELETE\_REALM\_CASCADE procedure, [15-10](#)

DBMS\_MACADM.DELETE\_REALM\_FROM\_POLICY procedure, [23-9](#)

DBMS\_MACADM.DELETE\_ROLE procedure, [19-3](#)

DBMS\_MACADM.DELETE\_RULE procedure, [16-8](#)

DBMS\_MACADM.DELETE\_RULE\_FROM\_RULE\_SET procedure, [16-8](#)

DBMS\_MACADM.DELETE\_RULE\_SET procedure, [16-9](#)

DBMS\_MACADM.DELETE\_SESSION\_EVENT\_CMD\_RULE procedure, [17-17](#)

DBMS\_MACADM.DELETE\_SYSTEM\_EVENT\_CMD\_RULE procedure, [17-17](#)

DBMS\_MACADM.DISABLE\_DV procedure, [22-13](#)

DBMS\_MACADM.DISABLE\_DV\_DICTIONARY\_ACCTS procedure, [22-14](#)  
 DBMS\_MACADM.DISABLE\_DV\_PATCH\_ADMIN\_AUDIT procedure, [22-14](#)  
 DBMS\_MACADM.DISABLE\_ORADEBUG procedure, [22-15](#)  
 DBMS\_MACADM.DROP\_DOMAIN\_IDENTITY procedure, [18-15](#)  
 DBMS\_MACADM.DROP\_POLICY procedure, [23-10](#)  
 DBMS\_MACADM.ENABLE\_DV procedure  
   about, [22-15](#)  
   registering Database Vault with, [3-3](#), [3-5](#), [3-7](#)  
 DBMS\_MACADM.ENABLE\_DV\_DICTIONARY\_ACCESS procedure, [22-17](#)  
 DBMS\_MACADM.ENABLE\_ORADEBUG procedure, [22-17](#)  
 DBMS\_MACADM.ENABLE\_DV\_PATCH\_ADMIN\_AUDIT procedure, [22-16](#)  
 DBMS\_MACADM.GET\_INSTANCE\_INFO function, [18-17](#)  
 DBMS\_MACADM.GET\_SESSION\_INFO function, [18-16](#)  
 DBMS\_MACADM.RENAME\_FACTOR procedure, [18-17](#)  
 DBMS\_MACADM.RENAME\_FACTOR\_TYPE procedure, [18-18](#)  
 DBMS\_MACADM.RENAME\_POLICY procedure, [23-10](#)  
 DBMS\_MACADM.RENAME\_REALM procedure, [15-11](#)  
 DBMS\_MACADM.RENAME\_ROLE procedure, [19-4](#)  
 DBMS\_MACADM.RENAME\_RULE procedure, [16-9](#)  
 DBMS\_MACADM.RENAME\_RULE\_SET procedure, [16-10](#)  
 DBMS\_MACADM.UNASSIGN\_ROLE procedure, [19-5](#)  
 DBMS\_MACADM.UNAUTHORIZE\_DDL procedure, [22-9](#)  
 DBMS\_MACADM.UNAUTHORIZE\_PROXY\_USER procedure, [22-11](#)  
 DBMS\_MACADM.UNAUTHORIZE\_SCHEDULER\_USER procedure, [22-12](#)  
 DBMS\_MACADM.UNAUTHORIZE\_TTS\_USER procedure, [22-13](#)  
 DBMS\_MACADM.UPDATE\_COMMAND\_RULE procedure, [17-18](#)  
 DBMS\_MACADM.UPDATE\_CONNECT\_COMMAND\_RULE procedure, [17-21](#)  
 DBMS\_MACADM.UPDATE\_FACTOR procedure, [18-18](#)  
 DBMS\_MACADM.UPDATE\_FACTOR\_TYPE procedure, [18-21](#)  
 DBMS\_MACADM.UPDATE\_IDENTITY procedure, [18-21](#)  
 DBMS\_MACADM.UPDATE\_MAC\_POLICY procedure, [20-6](#)  
 DBMS\_MACADM.UPDATE\_POLICY\_DESCRIPTION procedure, [23-11](#)  
 DBMS\_MACADM.UPDATE\_POLICY\_STATE procedure, [23-11](#)  
 DBMS\_MACADM.UPDATE\_REALM procedure, [15-11](#)  
 DBMS\_MACADM.UPDATE\_REALM\_AUTH procedure, [15-13](#)  
 DBMS\_MACADM.UPDATE\_ROLE procedure, [19-4](#)  
 DBMS\_MACADM.UPDATE\_RULE procedure, [16-11](#)  
 DBMS\_MACADM.UPDATE\_RULE\_SET procedure, [16-12](#)  
 DBMS\_MACADM.UPDATE\_SESSION\_EVENT\_COMMAND\_RULE procedure, [17-22](#)  
 DBMS\_MACADM.UPDATE\_SYSTEM\_EVENT\_COMMAND\_RULE procedure, [17-24](#)  
 DBMS\_MACSEC\_ROLES package  
   about, [19-6](#)  
   functions, listed, [19-6](#)  
 DBMS\_MACSEC\_ROLES.CAN\_SET\_ROLE function, [19-6](#)  
 DBMS\_MACSEC\_ROLES.SET\_ROLE procedure, [19-7](#)  
 DBMS\_MACUTL package  
   about, [21-1](#)  
   constants (fields)  
     examples, [21-6](#)  
     listed, [21-1](#)  
   procedures and functions, listed, [21-7](#)  
 DBMS\_MACUTL PL/SQL package contents, [24-8](#)  
 DBMS\_MACUTL.CHECK\_DVSYSDML\_ALLOWED procedure, [21-8](#)  
 DBMS\_MACUTL.GET\_CODE\_VALUE function, [21-9](#)  
 DBMS\_MACUTL.GET\_DAY function, [21-12](#)  
 DBMS\_MACUTL.GET\_HOUR function, [21-11](#)  
 DBMS\_MACUTL.GET\_MINUTE function, [21-11](#)  
 DBMS\_MACUTL.GET\_MONTH function, [21-13](#)  
 DBMS\_MACUTL.GET\_SECOND function, [21-10](#)  
 DBMS\_MACUTL.GET\_YEAR function, [21-13](#)  
 DBMS\_MACUTL.IS\_ALPHA function, [21-14](#)  
 DBMS\_MACUTL.IS\_DIGIT function, [21-15](#)  
 DBMS\_MACUTL.IS\_DVSYSDML\_OWNER function, [21-15](#)  
 DBMS\_MACUTL.IS\_OLS\_INSTALLED function, [21-16](#)  
 DBMS\_MACUTL.IS\_OLS\_INSTALLED\_VARCHAR function, [21-16](#)  
 DBMS\_MACUTL.USER\_HAS\_OBJECT\_PRIVILEGE function, [21-17](#)  
 DBMS\_MACUTL.USER\_HAS\_ROLE function, [21-18](#)  
 DBMS\_MACUTL.USER\_HAS\_ROLE\_VARCHAR function, [21-19](#)  
 DBMS\_MACUTL.USER\_HAS\_SYSTEM\_PRIVILEGE function, [21-20](#)  
 DBMS\_PRIVILEGE\_CAPTURE PL/SQL package, [4-5](#)  
 DBSNMP schema realm protection, [5-7](#)  
 DBSNMP user account  
   changing password, [13-5](#)  
   granted DV\_MONITOR role, [14-12](#)  
 deinstallation, [B-1](#)  
 deinstalling Oracle Database Vault, [C-2](#)



DELETE\_CATALOG\_ROLE role, [27-15](#)

deleting event command rules, [17-17](#)

Denial of Service (DoS) attacks  
reports  
    System Resource Limits Report, [27-16](#)  
    Tablespace Quotas Report, [27-19](#)

Direct and Indirect System Privileges By Database  
    Account Report, [27-10](#)

Direct Object Privileges Report, [27-8](#)

direct system privileges, [27-10](#)

Direct System Privileges By Database Account Report, [27-9](#)

disabling system features with Disabled default rule set, [6-3](#)

domains  
    defined with factors, [8-1](#)  
    finding database domain with DVF.F  
        \$DATABASE\_DOMAIN, [18-31](#)  
    finding with DVF.F\$DOMAIN, [18-33](#)

DROP ROLE statement  
    monitoring, [26-1](#)

DROP USER statement  
    monitoring, [26-1](#)

dual key connection, dual key security  
    See two-person integrity (TPI)

DV\_ACCTMGR role  
    about, [14-19](#)  
    backup account, [14-25](#)  
    Database Vault disabled, [14-19](#)  
    GRANT and REVOKE operations affected by, [14-19](#)  
    privileges associated with, [14-19](#)  
    realm protection, [5-7](#)

DV\_ADMIN role  
    about, [14-11](#)  
    changing password for user granted DV\_ADMIN, [14-11](#)  
    Database Vault disabled, [14-9](#), [14-11](#)  
    GRANT and REVOKE operations affected by, [14-11](#)  
    privileges associated with, [14-11](#)

DV\_AUDIT\_CLEANUP role  
    about, [14-13](#)  
    Database Vault disabled, [14-12](#), [14-13](#)  
    GRANT and REVOKE operations affected by, [14-13](#)  
    privileges associated with, [14-13](#)

DV\_DATAPUMP\_NETWORK\_LINK role  
    about, [14-14](#)  
    Database Vault disabled, [14-14](#)  
    GRANT and REVOKE operations affected by, [14-14](#)  
    privileges associated with, [14-14](#)

DV\_GOLDENDATE\_REDO role  
    privileges associated with, [14-18](#)

DV\_GOLDENDGATE\_ADMIN role  
    Database Vault disabled, [14-17](#)

DV\_GOLDENGATE\_ADMIN role  
    Database Vault disabled, [14-17](#)  
    GRANT and REVOKE operations affected by, [14-17](#)  
    privileges associated with, [14-17](#)

DV\_GOLDENGATE\_REDO\_ACCESS role  
    Database Vault disabled, [14-18](#)  
    GRANT and REVOKE operations affected by, [14-18](#)

DV\_MONITOR role  
    about, [14-12](#)  
    Database Vault disabled, [14-12](#)  
    GRANT and REVOKE operations affected by, [14-12](#)  
    privileges associated with, [14-12](#)

DV\_OWNER role  
    about, [14-9](#)  
    backup account, [14-25](#)  
    changing password for user granted DV\_OWNER, [14-9](#)  
    Database Vault disabled, [14-9](#)  
    GRANT and REVOKE operations affected by, [14-9](#)  
    privileges associated with, [14-9](#)

DV\_PATCH\_ADMIN role  
    Database Vault disabled, [14-18](#)  
    GRANT and REVOKE operations affected by, [14-18](#)  
    privileges associated with, [14-18](#)

DV\_POLICY\_OWNER role  
    about, [14-22](#)  
    GRANT and REVOKE operations affected by, [14-22](#)  
    privileges associated with, [14-22](#)

DV\_PUBLIC role, [14-23](#)

DV\_REALM\_OWNER role  
    Database Vault disabled, [14-21](#)  
    GRANT and REVOKE operations affected by, [14-21](#)  
    privileges associated with, [14-21](#)

DV\_REALM\_RESOURCE role  
    Database Vault disabled, [14-21](#)  
    GRANT and REVOKE operations affected by, [14-21](#)  
    privileges associated with, [14-21](#)

DV\_SECANALYST role  
    about, [14-13](#)  
    Database Vault disabled, [14-13](#)  
    GRANT and REVOKE operations affected by, [14-13](#)  
    privileges associated with, [14-13](#)

DV\_STREAMS\_ADMIN role  
    Database Vault disabled, [14-15](#)  
    GRANT and REVOKE operations affected by, [14-15](#)  
    privileges associated with, [14-15](#)

DV\_XSTREAM\_ADMIN role  
    Database Vault disabled, [14-16](#)

- DV\_XSTREAM\_ADMIN role (*continued*)
  - GRANT and REVOKE operations affected by, [14-16](#)
  - privileges associated with, [14-16](#)
- DVF account
  - auditing policy, [A-9](#)
  - database accounts, [14-23](#)
- DVF PL/SQL interface contents, [24-9](#)
- DVF schema
  - about, [14-2](#)
  - auditing policy, [A-9](#)
  - DBA\_DV\_DICTIONARY\_ACCTS view, [25-11](#)
  - PDBs, [14-2](#)
  - protecting, [22-14](#)
  - realm protection, [5-6](#)
- DVSYSAccount, [14-23](#)
- DVSYSA schema
  - about, [14-1](#)
  - auditing policy, [A-9](#)
  - CDBs, [1-10](#)
  - DBA\_DV\_DICTIONARY\_ACCTS view, [25-11](#)
  - DV\_OWNER role, [14-9](#)
  - DV\_POLICY\_OWNER role, [14-22](#)
  - PDBs, [14-1](#), [14-4](#)
  - protecting, [22-14](#)
  - realm protection, [5-6](#)
- DVSYSA.DBA\_DV\_FACTOR\_LINK view, [25-14](#)
- DVSYSA.DV\$CONFIGURATION\_AUDIT view, [25-38](#)
- DVSYSA.DV\$ENFORCEMENT\_AUDIT view, [25-43](#)
- DVSYSA.DV\$REALM view, [25-46](#)
- DVSYSA.POLICY\_OWNER\_POLICY view, [25-49](#)
- DVSYSA.POLICY\_OWNER\_REALM view, [25-49](#)
- DVSYSA.POLICY\_OWNER\_REALM\_AUTH view, [25-51](#)
- DVSYSA.POLICY\_OWNER\_REALM\_OBJECT view, [25-52](#)
- DVSYSA.POLICY\_OWNER\_RULE view, [25-53](#)
- DVSYSA.POLICY\_OWNER\_RULE\_SET view, [25-54](#)
- DVSYSA.POLICY\_OWNER\_RULE\_SET\_RULE view, [25-56](#)

## E

---

- email alert in rule set, [6-17](#)
- enabling system features with Enabled default rule set, [6-3](#)
- encrypted information, [27-19](#)
- enterprise identities, Enterprise\_Identity default factor, [8-2](#)
- Enterprise Manager
  - See Oracle Enterprise Manager
- enterprise user security
  - configuring Database Vault accounts for, [12-2](#)
- errors
  - factor error options, [8-13](#)
- event handler
  - rule sets, [6-5](#)

- example, [7-5](#)
- examples
  - DBMS\_MACUTL constants, [21-6](#)
  - realms, [5-19](#)
  - separation of duty matrix, [D-3](#)
  - trace files, [E-7-E-9](#)
  - See also tutorials
- Execute Privileges to Strong SYS Packages Report, [27-10](#)
- EXECUTE\_CATALOG\_ROLE role
  - impact of Oracle Database Vault installation, [2-3](#)
- EXEMPT ACCESS POLICY system privilege, [27-14](#)
- exporting data
  - See Oracle Data Pump
- external network services, fine-grained access to
  - example using email alert, [6-17](#)

## F

---

- Factor Audit Report, [27-6](#)
- Factor Configuration Issues Report, [27-4](#)
- Factor Without Identities Report, [27-4](#)
- factors
  - about, [8-1](#)
  - assignment
    - disabled rule set, [27-4](#)
    - incomplete rule set, [27-4](#)
    - validate, [8-11](#)
  - assignment operation, [27-6](#)
  - audit events, custom, [A-3](#)
  - audit options, [8-13](#)
  - child factors
    - about, [8-7](#)
    - Factor Configuration Issues Report, [27-4](#)
    - mapping, [8-18](#)
  - creating, [8-5](#)
  - creating names, [8-6](#)
  - data dictionary views, [8-37](#)
  - DBA\_DV\_FACTOR view, [25-11](#)
  - DBA\_DV\_SIMULATION\_LOG view, [25-34](#)
  - DBMS\_MACUTL constants, example of, [21-7](#)
  - default factors, [8-2](#)
  - deleting, [8-19](#)
  - domain, finding with DVF.F\$DOMAIN, [18-33](#)
  - error options, [8-13](#)
  - evaluate, [8-9](#)
  - evaluation operation, [27-6](#)
  - factor type
    - about, [8-6](#)
    - selecting, [8-6](#)
  - factor-identity pair mapping, [8-18](#)
  - functionality, [8-20](#)
  - functions
    - DBMS\_MACUTL (utility), [21-1](#)
    - DBMS\_MACUTL constants (fields), [21-1](#)
  - guidelines, [8-36](#)
  - identifying using child factors, [8-18](#)

## factors (continued)

### identities

- about, [8-8, 8-14](#)
  - adding to factor, [8-14](#)
  - assigning, [8-9](#)
  - configuring, [8-16](#)
  - creating, [8-16](#)
  - data dictionary views, [8-37](#)
  - database session, [8-8](#)
  - deleting, [8-17](#)
  - enterprise-wide users, [18-33](#)
  - how factor identities work, [8-8](#)
  - labels, [8-9](#)
  - mapping, about, [8-18](#)
  - mapping, identified, [8-7](#)
  - mapping, procedure, [8-18](#)
  - mapping, tutorial, [8-29](#)
  - Oracle Label Security labels, [8-9](#)
  - reports, [8-37](#)
  - resolving, [8-7](#)
  - retrieval methods, [8-10](#)
  - setting dynamically, [18-23](#)
  - trust levels, [8-8, 8-16](#)
  - with Oracle Label Security, [8-8](#)
- initialization, command rules, [7-2](#)
- invalid audit options, [27-4](#)
- label, [27-4](#)
- naming conventions, [8-6](#)
- Oracle Virtual Private Database, attaching factors to, [12-5](#)
- parent factors, [8-7](#)
- performance effect, [8-37](#)
- procedures
- DBMS\_MACADM (configuration), [18-1](#)
- process flow, [8-20](#)
- reports, [8-37](#)
- retrieving, [8-21](#)
- retrieving with GET\_FACTOR, [18-24](#)
- rule sets
- selecting, [8-12](#)
- setting, [8-22](#)
- setting with SET\_FACTOR, [18-23](#)
- troubleshooting
- auditing report, [27-6](#)
  - configuration problems, [E-12](#)
  - tips, [E-11](#)
- type (category of factor), [8-6](#)
- validating, [8-11](#)
- values (identities), [8-1](#)
- views
- DBA\_DV\_FACTOR\_LINK, [25-14](#)
  - DBA\_DV\_FACTOR\_TYPE, [25-13](#)
  - DBA\_DV\_IDENTITY, [25-15](#)
  - DBA\_DV\_IDENTITY\_MAP, [25-15](#)
  - DBA\_DV\_MAC\_POLICY\_FACTOR, [25-17](#)
- ways to assign, [8-8](#)

## factors (continued)

See also rule sets

FLASHBACK TABLE SQL statement, [5-2](#)

### functions

#### command rules

DBMS\_MACUTL (utility), [21-1](#)

DVSYS schema enabling, [18-22](#)

#### factors

DBMS\_MACUTL (utility), [21-1](#)

Oracle Label Security policy

DBMS\_MACADM (configuration), [20-1](#)

#### realms

DBMS\_MACUTL (utility), [21-1](#)

#### rule sets

DBMS\_MACADM (configuration), [16-1](#)

DBMS\_MACUTL (utility), [21-1](#)

PL/SQL functions for inspecting SQL, [16-14](#)

#### secure application roles

DBMS\_MACADM (configuration), [19-1](#)

DBMS\_MACSEC\_ROLES (configuration),  
[19-6](#)

DBMS\_MACUTL (utility), [21-1](#)

## G

---

general security reports, [27-7](#)

GRANT statement

monitoring, [26-1](#)

### guidelines

ALTER SESSION privilege, [D-15](#)

ALTER SYSTEM privilege, [D-15](#)

backup DV\_OWNER and DV\_ACCTMGR  
accounts, [14-25](#)

command rules, [7-15](#)

CREATE ANY JOB privilege, [D-14](#)

CREATE EXTERNAL JOB privilege, [D-14](#)

CREATE JOB privilege, [D-14](#)

DBMS\_FILE\_TRANSFER package, [D-11](#)

factors, [8-36](#)

general security, [D-1](#)

LogMiner packages, [D-14](#)

managing DV\_OWNER and DV\_ACCTMGR  
accounts, [14-23](#)

operating system access, [D-6](#)

Oracle software owner, [D-8](#)

performance effect, [8-37](#)

realms, [5-20](#)

root access, [D-6](#)

root user access, [D-8](#)

rule sets, [6-30](#)

secure application roles, [9-4](#)

SYSDBA access, [D-9](#)

SYSDBA privilege, limiting, [D-6](#)

SYSOPER access, [D-9](#)

SYSTEM schema and application tables, [D-6](#)

SYSTEM user account, [D-6](#)

trusted accounts and roles, [D-7](#)

guidelines (*continued*)  
using Database Vault in a production  
environment, [D-9](#)  
UTL\_FILE package, [D-11](#)

---

## H

hackers  
See security attacks  
Hierarchical System Privileges by Database Account  
Report, [27-10](#)  
host names  
finding with DVF.F\$DATABASE\_HOSTNAME,  
[18-31](#)

---

## I

identities  
See factors, identities  
Identity Configuration Issues Report, [27-4](#)  
IDLE\_TIME resource profile, [27-16](#)  
IMP\_FULL\_DATABASE role  
impact of Oracle Database Vault installation, [2-3](#)  
importing data  
See Oracle Data Pump  
incomplete rule set  
role enablement, [27-5](#)  
Information Lifecycle Management  
authorizations, about, [13-17](#)  
granting users authorization for, [13-17](#)  
revoking authorization from users, [13-18](#)  
initialization parameters  
Allow System Parameters default rule set, [6-3](#)  
modified after installation, [2-1](#)  
modified by Oracle Database Vault, [2-1](#)  
reports, [27-16](#)  
insider threats  
See intruders  
installations  
Database Vault and Label Security in a  
multitenant environment, [3-1](#)  
security considerations, [D-10](#)  
intruders  
compromising privileged accounts, [1-8](#)  
See also security attacks  
IP addresses  
Client\_IP default factor, [8-2](#)  
defined with factors, [8-1](#)

---

## J

Java Policy Grants Report, [27-18](#)  
jobs, scheduling  
See Oracle Scheduler

---

## L

Label Security Integration Audit Report, [27-6](#)

labels  
about, [8-15](#)  
See also Oracle Label Security  
languages  
adding to Oracle Database Vault, [C-2](#)  
finding with DVF.F\$LANG, [18-34](#)  
finding with DVF.F\$LANGUAGE, [18-35](#)  
name  
Lang default factor, [8-2](#)  
Language default factor, [8-2](#)  
LBACSYS account  
about, [14-23](#)  
auditing policy, [A-9](#)  
See also Oracle Label Security  
LBACSYS schema  
auditing policy, [A-9](#)  
realm protection, [5-6](#)  
locked out accounts, solution for, [B-1](#)  
log files  
Database Vault log files, [A-3](#)  
logging on  
reports, Core Database Audit Report, [27-17](#)  
LogMiner packages  
guidelines, [D-14](#)

---

## M

managing user accounts and profiles  
Can Maintain Accounts/Profiles default rule set,  
[6-3](#)  
managing user accounts and profiles on own account,  
Can Maintain Own Accounts default rule set,  
[6-3](#)  
mandatory realms  
about, [5-3](#)  
mapping identities, [8-18](#)  
MDDATA schema realm protection, [5-7](#)  
MDSYS schema realm protection, [5-7](#)  
monitoring  
activities, [26-1](#)  
multitenant container databases  
See CDBs  
My Oracle Support  
about, [xxviii](#)

---

## N

naming conventions  
factors, [8-6](#)  
realms, [5-8](#)  
rule sets, [6-5](#)  
rules, [6-12](#)  
network protocol  
finding with DVF.F\$NETWORK\_PROTOCOL,  
[18-36](#)  
network protocol, Network\_Protocol default factor,  
[8-2](#)  
NOAUDIT statement

NOAUDIT statement (*continued*)  
monitoring, [26-1](#)

Non-Owner Object Trigger Report, [27-19](#)  
nonsystem database accounts, [27-8](#)

## O

Object Access By PUBLIC Report, [27-8](#)  
Object Access Not By PUBLIC Report, [27-8](#)  
Object Dependencies Report, [27-9](#)  
object owners  
nonexistent, [27-3](#)  
reports  
Command Rule Configuration Issues Report, [27-3](#)  
object privilege reports, [27-7](#)  
object types  
supported for Database Vault realm protection, [5-5](#)  
objects  
command rule objects  
name, [7-9](#)  
owner, [7-9](#)  
processing, [7-11](#)  
dynamic SQL use, [27-18](#)  
mandatory realms, [5-3](#)  
monitoring, [26-1](#)  
object names  
finding with DV\_DICT\_OBJ\_NAME, [16-17](#)  
object owners  
finding with DV\_DICT\_OBJ\_OWNER, [16-17](#)  
realms  
object name, [5-8](#)  
object owner, [5-8](#)  
object type, [5-8](#)  
procedures for registering, [15-4](#)  
reports  
Access to Sensitive Objects Report, [27-11](#)  
Accounts with SYSDBA/SYSOPER Privilege Report, [27-12](#)  
Direct Object Privileges Report, [27-8](#)  
Execute Privileges to Strong SYS Packages Report, [27-10](#)  
Non-Owner Object Trigger Report, [27-19](#)  
Object Access By PUBLIC Report, [27-8](#)  
Object Access Not By PUBLIC Report, [27-8](#)  
Object Dependencies Report, [27-9](#)  
Objects Dependent on Dynamic SQL Report, [27-18](#)  
OS Directory Objects Report, [27-18](#)  
privilege, [27-7](#)  
Public Execute Privilege To SYS PL/SQL Procedures Report, [27-12](#)  
sensitive, [27-10](#)  
System Privileges By Privilege Report, [27-10](#)  
restricting user access to using mandatory realms, [5-3](#)

objects (*continued*)  
types  
finding with DV\_DICT\_OBJ\_TYPE, [16-16](#)  
views, DBA\_DV\_REALM\_OBJECT, [25-27](#)  
*See also* database objects  
Objects Dependent on Dynamic SQL Report, [27-18](#)  
OEM  
*See* Oracle Enterprise Manager (OEM)  
OEM\_MONITOR schema realm protection, [5-7](#)  
OLS  
*See* Oracle Label Security  
operating system access  
guideline for using with Database Vault, [D-6](#)  
operating systems  
reports  
OS Directory Objects Report, [27-18](#)  
OS Security Vulnerability Privileges Report, [27-16](#)  
vulnerabilities, [27-16](#)  
ORA-00942 error, [9-8](#)  
ORA-01301 error, [13-21](#)  
ORA-06512 error, [6-20](#), [21-8](#)  
ORA-24247 error, [6-20](#)  
ORA-47305 error, [9-8](#)  
ORA-47400 error, [6-22](#), [13-21](#)  
ORA-47401 error, [5-18](#), [13-21](#)  
ORA-47408 error, [13-21](#)  
ORA-47409 error, [13-21](#)  
ORA-47500 error, [22-18](#)  
ORA-47503 error, [3-7](#)  
ORA-47920 error, [21-8](#)  
ORA\$DEPENDENCY profile, [4-2](#)  
Oracle Data Guard  
integrating Database Vault with, [12-15](#)  
Oracle Data Pump  
archiving the Oracle Database Vault audit trail with, [A-6](#)  
authorizing transportable tablespace operations for Database Vault, [13-11](#)  
DBA\_DV\_DATAPUMP\_AUTH view, [25-10](#)  
DBA\_DV\_TTS\_AUTH view, [25-36](#)  
DBMS\_MACADM.AUTHORIZE\_TTS\_USER, [22-7](#)  
DBMS\_MACADM.UNAUTHORIZE\_TTS\_USER, [22-13](#)  
granting authorization to use with Database Vault, [13-7](#)  
guidelines before performing an export or import, [13-13](#)  
levels of authorization required  
Oracle Data Pump only, [13-7](#)  
transportable tablespaces, [13-10](#)  
MACADM procedures for authorization, [22-3](#)  
realm protection, [5-8](#)  
revoking standard authorization, [13-8](#)  
revoking transportable tablespace authorization, [13-12](#)

- Oracle Data Pump (*continued*)
  - using with Oracle Database Vault, [13-6](#)
- Oracle Database Vault
  - about, [1-2](#)
  - components, [1-4](#)
  - deinstalling, [C-2](#)
  - disabling
    - procedures for, [B-1](#)
    - reasons for, [B-1](#)
  - enabling
    - procedures for, [B-1](#)
  - integrating with other Oracle products, [12-1](#)
  - Oracle Database installation, affect on, [2-1](#)
  - post-installation procedures, [C-1](#)
  - privileges to use, [1-3](#)
  - registering
    - using DBCA, [3-2](#)
  - reinstalling, [C-4](#)
  - roles
    - privileges of, [14-6](#)
- Oracle Database Vault Administrator (DVA)
  - logging on from Oracle Enterprise Manager Cloud Control, [3-10](#)
- Oracle Database Vault Administrator pages, [1-5](#)
- Oracle Database Vault policies
  - about, [10-1](#)
  - creating, [10-4](#)
  - data dictionary views, [10-6](#)
  - default, [10-3](#)
  - deleting, [10-6](#)
  - in multitenant environment, [10-3](#)
  - modifying, [10-6](#)
- Oracle Database Vault realm, [5-6](#)
- Oracle Database Vault registration
  - about, [3-2](#)
  - common user to manage CDB root, [3-5](#)
  - common users to manage specific PDBs, [3-7](#)
  - non-multitenant environment, [3-3](#)
  - plugging in a Database Vault-enabled database, [3-9](#)
  - verifying configuration and enablement, [3-9](#)
- Oracle Default Component Protection Realm, [5-8](#)
- Oracle Default Schema Protection Realm, [5-7](#)
- Oracle Enterprise Manager
  - DBSNMP account
    - changing password, [13-5](#)
    - granted DV\_MONITOR role, [14-12](#)
    - using Oracle Database Vault with, [13-2](#)
- Oracle Enterprise Manager Cloud Control
  - monitoring Database Vault for attempted violations, [14-12](#)
  - propagating Database Vault configurations to other databases, [13-2](#)
  - starting Oracle Database Vault from, [3-10](#)
- Oracle Enterprise Manager realm, [5-7](#)
- Oracle Enterprise User Security, integrating with Oracle Database Vault, [12-1](#)
- Oracle Flashback Technology, [5-2](#), [7-2](#)
- Oracle GoldenGate
  - Database Vault role used for
    - DV\_GOLDENGATE\_ADMIN, [14-17](#)
    - DV\_GOLDENGATE\_REDO\_ACCESS, [14-18](#)
  - in an Oracle Database Vault environment, [13-20](#)
- Oracle Internet Directory Distinguished Name, Proxy\_Enterprise\_Identity default factor, [8-2](#)
- Oracle Internet Directory, registering with DBCA, [12-17](#)
- Oracle Label Security
  - using OLS\_LABEL\_DOMINATES function in rule expressions, [16-3](#)
- Oracle Label Security (OLS)
  - audit events, custom, [A-3](#)
  - checking if installed using DBMS\_MACUTL functions, [21-7](#)
  - data dictionary views, [12-14](#)
  - functions
    - DBMS\_MACUTL (utility), [21-1](#)
  - how Database Vault integrates with, [12-6](#)
  - initialization, command rules, [7-2](#)
  - integration with Oracle Database Vault
    - example, [12-10](#)
    - Label Security Integration Audit Report, [27-6](#)
    - procedure, [12-8](#)
    - requirements, [12-7](#)
  - labels
    - about, [8-15](#)
    - determining with GET\_FACTOR\_LABEL, [18-24](#)
    - invalid label identities, [27-4](#)
  - policies
    - accounts that bypass, [27-14](#)
    - monitoring policy changes, [26-1](#)
    - nonexistent, [27-4](#)
  - procedures
    - DBMS\_MACADM (configuration), [20-1](#)
  - reports, [12-14](#)
  - views
    - DBA\_DV\_MAC\_POLICY, [25-17](#)
    - DBA\_DV\_MAC\_POLICY\_FACTOR, [25-17](#)
    - DBA\_DV\_POLICY\_LABEL, [25-20](#)
    - See also* LBACSYS account
- Oracle MetaLink
  - See* My Oracle Support
- Oracle OLAP realm protection, [5-7](#)
- Oracle Real Application Clusters
  - configuring Database Vault on RAC nodes, [C-1](#)
  - deinstalling Oracle Database Vault from, [C-2](#)
  - multiple factor identities, [8-8](#)
- Oracle Recovery Manager (RMAN)
  - in an Oracle Database Vault environment, [13-18](#)
- Oracle Scheduler
  - DBA\_DV\_JOB\_AUTH view, [25-16](#)
  - granting Oracle Database Vault authorization, [13-15](#)

- Oracle Scheduler (*continued*)
  - realm protection, [5-8](#)
  - revoking Oracle Database Vault authorization, [13-16](#)
  - SCHEDULER\_ADMIN role, impact of Oracle Database Vault installation, [2-3](#)
  - using with Oracle Database Vault, [13-14](#)
- Oracle software owner, guidelines on managing, [D-8](#)
- Oracle Spatial realm protection, [5-7](#)
- Oracle Streams
  - Database Vault role used for, [14-15](#)
- Oracle System Privilege and Role Management Realm, [5-8](#)
- Oracle Text realm protection, [5-7](#)
- Oracle Virtual Private Database (VPD)
  - accounts that bypass, [27-14](#)
  - factors, attaching to, [12-5](#)
  - GRANT EXECUTE privileges with Grant VPD Administration default rule set, [6-3](#)
  - using Database Vault factors with Oracle Label Security, [12-10](#)
- ORADEBUG utility
  - about, [13-26](#)
  - DBA\_DV\_ORADEBUG view, [25-18](#)
  - PL/SQL procedure for disabling in Database Vault, [22-15](#)
  - PL/SQL procedure for enabling in Database Vault, [22-17](#)
  - using with Database Vault, [13-26](#)
- OS Directory Objects Report, [27-18](#)
- OS Security Vulnerability Privileges Report, [27-16](#)
- OS\_ROLES initialization parameter, [2-1](#)
- OUTIN schema realm protection, [5-8](#)

## P

- parameters
  - modified after installation, [2-1](#)
  - reports
    - Security Related Database Parameters Report, [27-16](#)
- parent factors
  - See* factors
- Password History Access Report, [27-15](#)
- passwords
  - forgotten, solution for, [B-1](#)
  - reports
    - Database Account Default Password Report, [27-17](#)
    - Password History Access Report, [27-15](#)
    - Username/Password Tables Report, [27-19](#)
  - resetting for DV\_ACCTMGR user, [E-13](#)
  - resetting for DV\_OWNER user, [E-12](#)
- patches
  - auditing DV\_PATCH\_ADMIN user, [14-18](#)
  - DBMS\_MACADM.DISABLE\_DV\_PATCH\_ADMIN\_AUDIT procedure, [22-14](#)

- patches (*continued*)
  - DBMS\_MACADM.ENSABLE\_DV\_PATCH\_ADMIN\_AUDIT procedure, [22-16](#)
  - DV\_PATCH\_ADMIN requirement for, [14-18](#)
  - security consideration, [D-10](#)
  - two-person integrity used for, [6-25](#)
- PDBs
  - command rules in, [7-3](#)
  - disabling tracing
    - all database sessions, [E-11](#)
    - current database session, [E-11](#)
  - DVF schema, [14-2](#)
  - DVSYS schema, [14-1](#), [14-4](#)
  - enabling tracing
    - all database sessions, [E-5](#)
    - current database session, [E-4](#)
  - plugging Database Vault-enabled PDB to CDB, [13-23](#)
  - privilege analysis, [4-4](#)
- performance effect
  - command rules, [7-16](#)
  - realms, [5-21](#)
  - reports
    - Resource Profiles Report, [27-16](#)
    - System Resource Limits Report, [27-16](#)
  - rule sets, [6-30](#)
  - secure application roles, [9-10](#)
  - static evaluation for rule sets, [6-30](#)
- performance tools
  - Automatic Workload Repository (AWR)
    - command rules, [7-16](#)
    - factors, [8-37](#)
      - Oracle Enterprise Manager performance tools, [5-21](#)
      - performance tools
        - Cloud Control, realms, [5-21](#)
        - Oracle Enterprise Manager realms, [5-21](#)
  - realms, [5-21](#)
  - rule sets, [6-30](#)
  - secure application roles, [9-10](#)
- Oracle Enterprise Manager
  - command rules, [7-16](#)
  - factors, [8-37](#)
    - performance tools
      - Oracle Enterprise Manager Cloud Control command rules, [7-16](#)
  - rule sets, [6-30](#)
  - secure application roles, [9-10](#)
- Oracle Enterprise Manager Cloud Control
  - factors, [8-37](#)
  - rule sets, [6-30](#)

- performance tools (*continued*)
  - Oracle Enterprise Manager Cloud Control (*continued*)
    - secure application roles, [9-10](#)
  - TKPROF utility
    - command rules, [7-16](#)
    - factors, [8-37](#)
    - realms, [5-21](#)
    - rule sets, [6-30](#)
    - secure application roles, [9-10](#)
- PL/SQL
  - packages
    - unwrapped bodies, [27-19](#)
    - Unwrapped PL/SQL Package Bodies Report, [27-19](#)
  - PL/SQL factor functions, [18-27](#)
- pluggable databases
  - See PDBs
- policies
  - See Oracle Database Vault policies
- policy changes, monitoring, [26-1](#)
- POLICY\_OWNER\_COMMAND\_RULE view, [25-48](#)
- post-installation procedures, [C-1](#)
- privilege analysis
  - about, [4-2](#)
  - accessing reports in Cloud Control, [4-16](#)
  - benefits, [4-3](#)
  - CDBs, [4-4](#)
  - creating
    - about, [4-6](#)
    - in Cloud Control, [4-7](#)
    - using DBMS\_PRIVILEGE\_CAPTURE.CREATE\_CAPTURE, [4-9](#)
  - creating role in Cloud Control, [4-19](#)
  - data dictionary views, [4-33](#)
  - DBMS\_PRIVILEGE\_CAPTURE PL/SQL package, [4-5](#)
  - disabling
    - about, [4-15](#)
    - in Cloud Control, [4-15](#)
    - using DBMS\_PRIVILEGE\_CAPTURE.DISABLE\_CAPTURE, [4-15](#)
  - dropping
    - about, [4-18](#)
    - in Cloud Control, [4-18](#)
    - using DBMS\_PRIVILEGE\_CAPTURE.DROP\_CAPTURE, [4-18](#)
  - enabling
    - about, [4-13](#)
    - in Cloud Control, [4-13](#)
    - using DBMS\_PRIVILEGE\_CAPTURE.ENABLE\_CAPTURE, [4-14](#)
  - examples of creating and enabling, [4-11](#)
  - general steps for managing, [4-6](#)
  - generating regrant scripts, [4-22](#)
  - generating reports
    - about, [4-16](#)
    - in Cloud Control, [4-16](#)
    - using DBMS\_PRIVILEGE\_CAPTURE.GENERATE\_REPORT, [4-17](#)
  - generating revoke scripts, [4-21](#)
- privilege analysis (*continued*)
  - logon users, [4-3](#)
  - pre-compiled database objects, [4-2](#)
  - privilege uses captured, [4-3](#)
  - requirements for using, [4-3](#)
  - restrictions, [4-3](#)
  - revoking and re-granting in Cloud Control, [4-20](#)
  - revoking and regranting using scripts, [4-21](#)
  - tutorial, [4-28](#)
  - tutorial for ANY privileges, [4-23](#)
  - use cases
    - finding application pool privileges, [4-4](#)
    - finding overly privileged users, [4-4](#)
- privileges
  - checking with
    - DBMS\_MACUTL.USER\_HAS\_OBJECT\_PRIVILEGE function, [21-7](#)
  - existing users and roles, Database Vault affect on, [2-3](#)
  - least privilege principle
    - violations to, [27-18](#)
  - monitoring
    - GRANT statement, [26-1](#)
    - REVOKE statement, [26-1](#)
  - Oracle Database Vault restricting, [2-3](#)
  - prevented from existing users and roles, [2-5](#)
  - reports
    - Accounts With DBA Roles Report, [27-14](#)
    - ALTER SYSTEM or ALTER SESSION Report, [27-15](#)
    - ANY System Privileges for Database Accounts Report, [27-10](#)
    - AUDIT Privileges Report, [27-16](#)
    - Database Accounts With Catalog Roles Report, [27-15](#)
    - Direct and Indirect System Privileges By Database Account Report, [27-10](#)
    - Direct System Privileges By Database Account Report, [27-9](#)
    - Hierarchical System Privileges By Database Account Report, [27-10](#)
    - listed, [27-12](#)
    - OS Directory Objects Report, [27-18](#)
    - Privileges Distribution By Grantee Report, [27-13](#)
    - Privileges Distribution By Grantee, Owner Report, [27-13](#)
    - Privileges Distribution By Grantee, Owner, Privilege Report, [27-13](#)
    - WITH GRANT Privileges Report, [27-15](#)
  - restricting access using mandatory realms, [5-3](#)
  - roles
    - checking with
      - DBMS\_MACUTL.USER\_HAS\_ROLE\_VARCHAR function, [21-7](#)
  - system
    - checking with
      - DBMS\_MACUTL.USER\_HAS\_SYSTEM\_PRIVILEGE function, [21-7](#)
  - views
    - DBA\_DV\_PUB\_PRIVS, [25-23](#)
    - DBA\_DV\_USER\_PRIVS, [25-36](#)
    - DBA\_DV\_USER\_PRIVS\_ALL, [25-37](#)
    - Privileges Distribution By Grantee Report, [27-13](#)



- Privileges Distribution By Grantee, Owner Report, [27-13](#)
- Privileges Distribution By Grantee, Owner, Privilege Report, [27-13](#)
- privileges using external password, [27-12](#)
- problems, diagnosing, [E-2](#)
- procedures
  - command rules
    - .DBMS\_MACADM (configuration), [17-1](#)
  - factors
    - DBMS\_MACADM (configuration), [18-1](#)
  - realms
    - DBMS\_MACADM (configuration), [15-1](#)
- production environments
  - guidelines for securing, [D-9](#)
- profiles, [27-16](#)
- proxy user authorization
  - Database Vault authorization
    - DBA\_DV\_PROXY\_AUTH view, [25-23](#)
    - granting, [22-6](#)
    - revoking, [22-11](#)
- PUBLIC access to realms, [5-15](#)
- Public Execute Privilege To SYS PL/SQL Procedures Report, [27-12](#)
- PUBLIC user account
  - impact of Oracle Database Vault installation, [2-3](#)

## Q

---

- quotas
  - tablespace, [27-19](#)

## R

---

- Realm Audit Report, [27-5](#)
- Realm Authorization Configuration Issues Report, [27-4](#)
- realm authorizations:multitenant environment, [5-13](#)
- realms
  - about, [5-2](#)
  - adding roles to as grantees, [5-20](#)
  - audit events, custom, [A-3](#)
  - authentication-related procedures, [15-2](#)
  - authorization
    - enabling access to realm-protected objects, [5-19](#)
    - how realm authorizations work, [5-17](#)
    - process flow, [5-17](#)
    - troubleshooting, [E-11](#)
  - authorizations
    - grantee, [5-8](#)
    - rule set, [5-8](#)
  - authorizations in multitenant environment, [5-13](#)
  - creating, [5-8](#)
  - creating names, [5-8](#)
  - data dictionary views, [5-22](#)
  - data masking, [13-22](#)

- realms (*continued*)
  - Database Vault Account Management realm, [5-7](#)
  - DBMS\_MACUTL constants, example of, [21-6](#)
  - default realms
    - listed, [5-5](#)
  - deleting, [5-15](#)
  - disabling, [5-14](#)
  - DV\_REALM\_OWNER role, [14-21](#)
  - DV\_REALM\_RESOURCE role, [14-21](#)
  - effect on other Oracle Database Vault components, [5-20](#)
  - enabling, [5-14](#)
  - enabling access to realm-protected objects, [5-19](#)
  - example, [5-19](#)
  - functions
    - DBMS\_MACUTL (utility), [21-1](#)
    - DBMS\_MACUTL constants (fields), [21-1](#)
  - guidelines, [5-20](#)
  - how realms work, [5-15](#)
  - mandatory realms, [5-3](#)
  - multitenant environment
    - about, [5-5](#)
  - naming conventions, [5-8](#)
  - object types, supported, [5-5](#)
  - object-related procedures, [15-4](#)
  - Oracle Database Vault realm, [5-6](#)
  - Oracle Default Component Protection Realm, [5-8](#)
  - Oracle Default Schema Protection Realm, [5-7](#)
  - Oracle Enterprise Manager realm, [5-7](#)
  - Oracle System Privilege and Role Management Realm, [5-8](#)
  - performance effect, [5-21](#)
  - procedures
    - DBMS\_MACADM (configuration), [15-1](#)
  - process flow, [5-15](#)
  - propagating configuration to other databases, [13-2](#)
  - protection after object is dropped, [5-20](#)
  - PUBLIC access, [5-15](#)
  - realm authorizations
    - about, [5-13](#)
  - realm secured objects
    - object name, [5-8](#)
    - object owner, [5-8](#)
    - object type, [5-8](#)
  - realm-secured objects, [5-12](#)
  - reports, [5-22](#)
  - roles
    - DV\_REALM\_OWNER, [14-21](#)
    - DV\_REALM\_RESOURCE, [14-21](#)
  - secured object, [27-4](#)
  - simulation mode, [11-1](#)
  - territory a realm protects, [5-12](#)
  - troubleshooting, [E-11](#), [E-12](#)
  - tutorial, [3-12](#)
  - views
    - DBA\_DV\_CODE, [25-6](#)

realms (continued)

views (continued)

DBA\_DV\_MAINTENANCE\_AUTH, [25-18](#)  
DBA\_DV\_POLICY, [25-19](#)  
DBA\_DV\_POLICY\_OBJECT, [25-21](#)  
DBA\_DV\_POLICY\_OWNER, [25-22](#)  
DBA\_DV\_REALM, [25-24](#)  
DBA\_DV\_REALM\_OBJECT, [25-27](#)  
DBS\_DV\_REALM\_AUTH, [25-25](#)  
DVSYS.POLICY\_OWNER\_COMMAND\_RULE,  
[25-48](#)  
DVSYS.POLICY\_OWNER\_POLICY, [25-49](#)  
DVSYS.POLICY\_OWNER\_REALM, [25-49](#)  
DVSYS.POLICY\_OWNER\_REALM\_AUTH,  
[25-51](#)  
DVSYS.POLICY\_OWNER\_REALM\_OBJECT,  
[25-52](#)  
DVSYS.POLICY\_OWNER\_RULE, [25-53](#)  
DVSYS.POLICY\_OWNER\_RULE\_SET, [25-54](#)  
DVSYS.POLICY\_OWNER\_RULE\_SET\_RULE,  
[25-56](#)

See also rule sets

recovering lost password, [E-12](#), [E-13](#)

RECOVERY\_CATALOG\_OWNER role, [27-15](#)

RECYCLEBIN initialization parameter

default setting in Oracle Database Vault, [2-1](#)

registering Oracle Database Vault, [3-2](#)

reinstalling Oracle Database Vault, [C-4](#)

REMOTE\_LOGIN\_PASSWORDFILE initialization  
parameter, [2-1](#)

reports

about, [27-1](#)

Access to Sensitive Objects Report, [27-11](#)

Accounts With DBA Roles Report, [27-14](#)

Accounts with SYSDBA/SYSOPER Privilege  
Report, [27-12](#)

ALTER SYSTEM or ALTER SESSION Report,  
[27-15](#)

ANY System Privileges for Database Accounts  
Report, [27-10](#)

AUDIT Privileges Report, [27-16](#)

auditing, [27-5](#)

BECOME USER Report, [27-14](#)

categories of, [27-1](#)

Command Rule Audit Report, [27-6](#)

Command Rule Configuration Issues Report, [27-3](#)

Core Database Audit Report, [27-17](#)

Core Database Vault Audit Trail Report, [27-6](#)

Database Account Default Password Report,  
[27-17](#)

Database Account Status Report, [27-17](#)

Database Accounts With Catalog Roles Report,  
[27-15](#)

Direct and Indirect System Privileges By Database  
Account Report, [27-10](#)

Direct Object Privileges Report, [27-8](#)

reports (continued)

Direct System Privileges By Database Account  
Report, [27-9](#)

Enterprise Manager Cloud Control, [13-4](#)

Execute Privileges to Strong SYS Packages Report,  
[27-10](#)

Factor Audit Report, [27-6](#)

Factor Configuration Issues Report, [27-4](#)

Factor Without Identities, [27-4](#)

general security, [27-7](#)

Hierarchical System Privileges by Database  
Account Report, [27-10](#)

Identity Configuration Issues Report, [27-4](#)

Java Policy Grants Report, [27-18](#)

Label Security Integration Audit Report, [27-6](#)

Non-Owner Object Trigger Report, [27-19](#)

Object Access By PUBLIC Report, [27-8](#)

Object Access Not By PUBLIC Report, [27-8](#)

Object Dependencies Report, [27-9](#)

Objects Dependent on Dynamic SQL Report,  
[27-18](#)

OS Directory Objects Report, [27-18](#)

OS Security Vulnerability Privileges, [27-16](#)

Password History Access Report, [27-15](#)

permissions for running, [27-2](#)

privilege management, [27-12](#)

Privileges Distribution By Grantee Report, [27-13](#)

Privileges Distribution By Grantee, Owner Report,  
[27-13](#)

Privileges Distribution By Grantee, Owner,  
Privilege Report, [27-13](#)

Public Execute Privilege To SYS PL/SQL  
Procedures Report, [27-12](#)

Realm Audit Report, [27-5](#)

Realm Authorization Configuration Issues Report,  
[27-4](#)

Resource Profiles Report, [27-16](#)

Roles/Accounts That Have a Given Role Report,  
[27-15](#)

Rule Set Configuration Issues Report, [27-3](#)

running, [27-2](#)

Secure Application Configuration Issues Report,  
[27-5](#)

Secure Application Role Audit Report, [27-6](#)

Security Policy Exemption Report, [27-14](#)

Security Related Database Parameters, [27-16](#)

security vulnerability, [27-17](#)

System Privileges By Privilege Report, [27-10](#)

System Resource Limits Report, [27-16](#)

Tablespace Quotas Report, [27-19](#)

Unwrapped PL/SQL Package Bodies Report,  
[27-19](#)

Username /Password Tables Report, [27-19](#)

WITH ADMIN Privileges Grants Report, [27-14](#)

WITH GRANT Privileges Report, [27-15](#)

Resource Profiles Report, [27-16](#)

resources

- resources (*continued*)
  - reports
    - Resource Profiles Report, [27-16](#)
    - System Resource Limits Report, [27-16](#)
- REVOKE statement
  - monitoring, [26-1](#)
- roles
  - adding to realms as grantees, [5-20](#)
  - catalog-based, [27-15](#)
  - Database Vault default roles, [14-4](#)
  - privilege analysis, [4-3](#)
  - privileges, checking with
    - DBMS\_MACUTL.USER\_HAS\_ROLE\_VARCHAR function, [21-7](#)
  - role enablement in incomplete rule set, [27-5](#)
  - role-based system privileges, [27-10](#)
    - See also* secure application roles
- Roles/Accounts That Have a Given Role Report, [27-15](#)
- root access
  - guideline for using with Database Vault, [D-6](#)
  - guidelines on managing, [D-8](#)
- Rule Set Configuration Issues Report, [27-3](#)
- rule sets
  - about, [6-2](#)
  - adding existing rules, [6-14](#)
  - audit options, [6-5](#)
  - auditing
    - intruders
      - using rule sets, [6-5](#)
  - command rules
    - disabled, [27-3](#)
    - selecting for, [7-9](#)
    - used with, [7-2](#)
  - creating
    - rules in, [6-12](#)
  - creating names, [6-5](#)
  - data dictionary views, [6-31](#)
  - DBMS\_MACUTL constants, example of, [21-6](#)
  - default rule sets, [6-3](#)
  - default rules, [6-9](#)
  - deleting
    - rules from, [6-14](#)
  - disabled for
    - factor assignment, [27-4](#)
    - realm authorization, [27-4](#)
  - evaluation of rules, [6-8](#)
  - event handlers, [6-5](#)
  - events firing, finding with DV\_SYSEVENT, [16-15](#)
  - factors, selecting for, [8-12](#)
  - fail code, [6-5](#)
  - fail message, [6-5](#)
  - functions
    - DBMS\_MACADM (configuration), [16-1](#)
    - DBMS\_MACUTL (utility), [21-1](#)
    - DBMS\_MACUTL constants (fields), [21-1](#)
    - PL/SQL functions for rule sets, [16-14](#)
  - guidelines, [6-30](#)
- rule sets (*continued*)
  - how rule sets work, [6-16](#)
  - incomplete, [27-3](#)
  - multitenant environment
    - about, [6-2](#)
  - naming conventions, [6-5](#)
  - nested rules, [6-16](#)
  - performance effect, [6-30](#)
  - procedures
    - DBMS\_MACADM (configuration), [16-1](#)
  - process flow, [6-16](#)
  - propagating configuration to other databases, [13-2](#)
  - removing references to objects, [6-15](#)
  - reports, [6-31](#)
  - rule sets
    - evaluation options, [6-5](#)
  - rules that exclude one user, [6-17](#)
  - security attacks
    - tracking
      - with rule set auditing, [6-5](#)
  - static evaluation, [6-30](#)
  - troubleshooting, [E-11](#), [E-12](#)
  - views
    - DBA\_DV\_RULE, [25-29](#)
    - DBA\_DV\_RULE\_SET, [25-30](#)
    - DBA\_DV\_RULE\_SET\_RULE, [25-32](#)
    - See also* command rules, factors, realms, rules, secure application roles
- rules
  - about, [6-8](#)
  - creating, [6-12](#)
  - creating names, [6-12](#)
  - data dictionary views, [6-31](#)
  - default, [6-9](#)
  - deleting, [6-14](#)
  - deleting from rule set, [6-14](#)
  - existing rules, adding to rule set, [6-14](#)
  - naming conventions, [6-12](#)
  - nested within a rule set, [6-16](#)
  - removing from rule set, [6-14](#)
  - reports, [6-31](#)
  - troubleshooting, [E-11](#)
  - views
    - DBA\_DV\_RULE, [25-29](#)
    - DBA\_DV\_RULE\_SET\_RULE, [25-32](#)
    - See also* rule sets
- rules sets
  - audit event, custom, [A-3](#)

## S

- SCHEDULER\_ADMIN role
  - impact of Oracle Database Vault installation, [2-3](#)
- scheduling database jobs
  - CREATE EXTERNAL JOB privilege security consideration, [D-14](#)

- scheduling jobs
  - See Oracle Scheduler
- schemas
  - DVF, [14-2](#)
  - DVSY, [14-1](#)
- Secure Application Configuration Issues Report, [27-5](#)
- secure application role, [9-1](#)
- Secure Application Role Audit Report, [27-6](#)
- secure application roles
  - audit event, custom, [A-3](#)
  - creating, [9-2](#)
  - data dictionary view, [9-10](#)
  - DBMS\_MACSEC\_ROLES.SET\_ROLE function, [9-2](#)
  - deleting, [9-4](#)
  - functionality, [9-4](#)
  - functions
    - DBMS\_MACADM (configuration), [19-1](#)
    - DBMS\_MACSEC\_ROLES (configuration), [19-6](#)
    - DBMS\_MACSEC\_ROLES package, [19-6](#)
    - DBMS\_MACUTL (utility), [21-1](#)
    - DBMS\_MACUTL constants (fields), [21-1](#)
  - guidelines on managing, [9-4](#)
  - modifying, [9-3](#)
  - performance effect, [9-10](#)
  - procedure
    - DBMS\_MACADM (configuration), [19-1](#)
  - procedures and functions
    - DBMS\_MACUTL (utility), [21-7](#)
  - propagating configuration to other databases, [13-2](#)
  - reports
    - Rule Set Configuration Issues Report, [27-3](#)
  - troubleshooting, [E-12](#)
  - troubleshooting with auditing report, [27-6](#)
  - tutorial, [9-5](#)
  - views
    - DBA\_DV\_ROLE, [25-28](#)
    - See also roles, rule sets
- security attacks
  - Denial of Service (DoS) attacks
    - finding system resource limits, [27-16](#)
  - Denial of Service attacks
    - finding tablespace quotas, [27-19](#)
  - eliminating audit trail, [27-16](#)
  - monitoring security violations, [26-1](#)
  - Oracle Database Vault addressing compromised privileged user accounts, [1-8](#)
  - reports
    - AUDIT Privileges Report, [27-16](#)
    - Objects Dependent on Dynamic SQL Report, [27-18](#)
    - Privileges Distribution By Grantee, Owner Report, [27-13](#)
    - Unwrapped PL/SQL Package Bodies Report, [27-19](#)
- security attacks (*continued*)
  - SQL injection attacks, [27-18](#)
  - tracking
    - with factor auditing, [8-13](#)
- security policies, Oracle Database Vault addressing, [1-8](#)
- Security Policy Exemption Report, [27-14](#)
- Security Related Database Parameters Report, [27-16](#)
- security violations
  - monitoring attempts, [26-1](#)
- security vulnerabilities
  - how Database Vault addresses, [1-9](#)
  - operating systems, [27-16](#)
  - reports
    - Security Related Database Parameters Report, [27-16](#)
    - root operating system directory, [27-18](#)
- SELECT\_CATALOG\_ROLE role, [27-15](#)
- sensitive objects reports, [27-10](#)
- separation of duty concept
  - about, [D-2](#)
  - command rules, [7-7](#)
  - database accounts, [14-23](#)
  - database accounts, suggested, [14-23](#)
  - database roles, [2-3](#)
  - Database Vault Account Manager role, [14-23](#)
  - documenting tasks, [D-4](#)
  - example matrix, [D-3](#)
  - how Oracle Database Vault addresses, [2-3](#)
  - realms, [1-9](#)
  - restricting privileges, [2-3](#)
  - roles, [14-4](#)
  - tasks in Oracle Database Vault environment, [D-2](#)
- session event command rule
  - updating, [17-22](#)
- session event command rules
  - creating for events, [17-11](#)
  - deleting, [17-17](#)
- sessions
  - audit events, custom, [A-3](#)
  - DBMS\_MACUTL fields, [21-1](#)
  - finding session user with DVF.F\$SESSION\_USER, [18-37](#)
  - restricting data based on, [8-29](#)
  - retrieving information with functions, [18-1](#)
- simulation mode
  - about, [11-1](#)
  - use cases, [11-2](#)
- SQL injection attacks, detecting with Object Dependent on Dynamic SQL Report, [27-18](#)
- SQL statements
  - default command rules that protect, [7-7](#)
  - SQL statements protected by, [7-8](#)
  - SQL text, finding with DV\_SQL\_TEXT, [16-18](#)
  - SQL92\_SECURITY initialization parameter, [2-1](#)
- subfactors
  - See child factors under factors topic

- SYS account
  - privilege analysis, [4-3](#)
- SYS user account
  - adding to realm authorization, [5-20](#)
- SYS\_CONTEXT function
  - Boolean expressions used in privilege analysis, [4-9](#)
- SYS.DV\$CONFIGURATION\_AUDIT view, [25-56](#)
- SYS.DV\$ENFORCEMENT\_AUDIT view, [25-57](#)
- SYSDBA access
  - guidelines on managing, [D-9](#)
- SYSDBA privilege
  - limiting, importance of, [D-6](#)
- SYSOPER access
  - guidelines on managing, [D-9](#)
- system event command rule
  - updating, [17-24](#)
- system event command rules
  - creating, [17-12](#)
  - deleting, [17-17](#)
- system features
  - disabling with Disabled rule set, [6-3](#)
  - enabling with Enabled rule set, [6-3](#)
- system privileges
  - checking with
    - DBMS\_MACUTL.USER\_HAS\_SYSTEM\_PRIVILEGE function, [21-7](#)
  - reports
    - System Privileges By Privileges Report, [27-10](#)
- System Privileges By Privilege Report, [27-10](#)
- System Resource Limits Report, [27-16](#)
- system root access, guideline on managing, [D-8](#)
- SYSTEM schema
  - application tables in, [D-6](#)
  - realm protection, [5-8](#)
- SYSTEM user account
  - guidelines for using with Database Vault, [D-6](#)
- trace files, Oracle Database Vault (*continued*)
  - examples (*continued*)
    - highest level on realm violations, [E-9](#)
    - low level realm violations, [E-7](#)
  - finding trace file directory, [E-6](#)
  - levels of trace events, [E-3](#)
  - performance effect, [E-3](#)
  - querying
    - ADRCI utility, [E-6](#)
    - Linux grep command, [E-6](#)
- traisimulationning mode
  - tutorial, [11-3](#)
- Transparent Data Encryption, used with Oracle Database Vault, [12-4](#)
- transportable tablespaces
  - authorizing for Oracle Data Pump operations in Database Vault, [13-11](#)
  - DBA\_DV\_TTS\_AUTH view, [25-36](#)
  - DBMS\_MACADM.AUTHORIZE\_TTS\_USER procedure, [22-7](#)
  - DBMS\_MACADM.UNAUTHORIZE\_TTS\_USER procedure, [22-13](#)
- triggers
  - different from object owner account, [27-19](#)
  - reports, Non-Owner Object Trigger Report, [27-19](#)
- troubleshooting
  - access security sessions, [27-6](#)
  - auditing reports, using, [27-5](#)
  - factors, [E-11](#)
  - general diagnostic tips, [E-11](#)
  - locked out accounts, [B-1](#)
  - passwords, forgotten, [B-1](#)
  - realms, [E-11](#)
  - rule sets, [E-11](#)
  - rules, [E-11](#)
  - secure application roles, [27-6](#)
- trust levels
  - about, [8-15](#)
  - determining for identities with
    - GET\_TRUST\_LEVEL\_FOR\_IDENTITY, [18-26](#)
  - determining with GET\_TRUST\_LEVEL, [18-25](#)
  - factor identity, [8-15](#)
  - factors, [8-16](#)
  - for factor and identity requested, [18-26](#)
  - identities, [8-8](#)
  - of current session identity, [18-25](#)
- trusted users
  - accounts and roles that should be limited, [D-8](#)
  - default for Oracle Database Vault, [D-7](#)
- tutorials
  - access, granting with secure application roles, [9-5](#)
  - ad hoc tool access, preventing, [8-23](#)
  - configuring two-person integrity (TPI), [6-25](#)
  - Database Vault factors with Virtual Private Database and Oracle Label Security, [12-10](#)

## T

---

- tablespace quotas, [27-19](#)
- Tablespace Quotas Report, [27-19](#)
- time data
  - DBMS\_MACUTL functions, [21-7](#)
- trace files
  - about, [E-2](#)
- trace files, Oracle Database Vault
  - about, [E-2](#)
  - activities that can be traced, [E-2](#)
  - ADRCI utility, [E-6](#)
  - directory location for trace files, [E-6](#)
  - disabling for all sessions, [E-10](#)
  - disabling for current session, [E-10](#)
  - enabling for all sessions, [E-4](#)
  - enabling for current session, [E-4](#)
  - examples
    - high level authorization, [E-8](#)

tutorials (*continued*)

- email alert in rule set, [6-17](#)
- factors, mapping identities, [8-29](#)
- Oracle Label Security integration with Oracle Database Vault, [12-10](#)
- privilege analysis, [4-28](#)
- privilege analysis for ANY privileges, [4-23](#)
- restricting access based on session data, [8-29](#)
- restricting user activities with command rules, [7-12](#)
- schema, protecting with a realm, [3-12](#)
- simulation mode, [11-3](#)
  - See also* examples
- two-man rule security
  - See* two-person integrity (TPI)
- two-person integrity (TPI)
  - about, [6-25](#)
  - configuring with a rule set, [6-25](#)

## U

- UNAUTHORIZE\_MAINTENANCE\_USER procedure, [22-10](#)
- unified audit trail
  - how it works with Database Vault, [A-1](#)
  - protecting with a realm, [A-2](#)
- Unwrapped PL/SQL Package Bodies Report, [27-19](#)
- user authorization
  - Database Vault authorization for ILM
    - granting, [22-5](#)
    - revoking, [22-10](#)
  - Database Vault authorization for Information Lifecycle Management
    - granting, [22-5](#)
    - revoking, [22-10](#)
- user names
  - reports, Username/Password Tables Report, [27-19](#)
- USER\_HISTORY\$ table, [27-15](#)
- Username/Password Tables Report, [27-19](#)
- users
  - enterprise identities, finding with DVF.F\$PROXY\_ENTERPRISE\_IDENTITY, [18-36](#)
  - enterprise-wide identities, finding with DVF.F\$ENTERPRISE\_IDENTITY, [18-33](#)
  - finding session user with DVF.F\$SESSION\_USER, [18-37](#)
  - login user name, finding with DV\_LOGIN\_USER, [16-15](#)
  - restricting access by factor identity, [8-29](#)
- utility functions
  - See* .DBMS\_MACUTL package
- UTL\_FILE object, [27-9](#)
- UTL\_FILE package, guidelines on managing, [D-11](#)

## V

views

- CDB\_DV\_STATUS, [25-5](#)
- DBA\_DV\_CODE, [25-6](#)
- DBA\_DV\_COMMAND\_RULE, [25-8](#)
- DBA\_DV\_DATAPUMP\_AUTH, [25-10](#)
- DBA\_DV\_DDL\_AUTH, [25-10](#)
- DBA\_DV\_DICTIONARY\_ACCTS, [25-11](#)
- DBA\_DV\_FACTOR, [25-11](#)
- DBA\_DV\_FACTOR\_TYPE, [25-13](#)
- DBA\_DV\_IDENTITY, [25-15](#)
- DBA\_DV\_IDENTITY\_MAP, [25-15](#)
- DBA\_DV\_JOB\_AUTH, [25-16](#)
- DBA\_DV\_MAINTENANCE\_AUTH, [25-18](#)
- DBA\_DV\_ORADEBUG, [25-18](#)
- DBA\_DV\_PATCH\_ADMIN\_AUDIT, [25-19](#)
- DBA\_DV\_POLICY, [25-19](#)
- DBA\_DV\_POLICY\_LABEL, [25-20](#)
- DBA\_DV\_POLICY\_OBJECT, [25-21](#)
- DBA\_DV\_POLICY\_OWNER, [25-22](#)
- DBA\_DV\_PROXY\_AUTH, [25-23](#)
- DBA\_DV\_PUB\_PRIVS, [25-23](#)
- DBA\_DV\_REALM, [25-24](#)
- DBA\_DV\_REALM\_AUTH, [25-25](#)
- DBA\_DV\_REALM\_OBJECT, [25-27](#)
- DBA\_DV\_ROLE, [25-28](#)
- DBA\_DV\_RULE\_SET, [25-30](#)
- DBA\_DV\_RULE\_SET\_RULE, [25-32](#)
- DBA\_DV\_SIMULATION\_LOG, [25-34](#)
- DBA\_DV\_STATUS, [25-33](#)
- DBA\_DV\_TTS\_AUTH, [25-36](#)
- DBA\_DV\_USER\_PRIVS, [25-36](#)
- DBA\_DV\_USER\_PRIVS\_ALL, [25-37](#)
- DVSYSDV\$CONFIGURATION\_AUDIT, [25-38](#)
- DVSYSDV\$ENFORCEMENT\_AUDIT, [25-43](#)
- DVSYSDV\$REALM, [25-46](#)
- DVSYSPOLICY\_OWNER\_COMMAND\_RULE, [25-48](#)
- DVSYSPOLICY\_OWNER\_POLICY, [25-49](#)
- DVSYSPOLICY\_OWNER\_REALM, [25-49](#)
- DVSYSPOLICY\_OWNER\_REALM\_AUTH, [25-51](#)
- DVSYSPOLICY\_OWNER\_REALM\_OBJECT, [25-52](#)
- DVSYSPOLICY\_OWNER\_RULE, [25-53](#)
- DVSYSPOLICY\_OWNER\_RULE\_SET, [25-54](#)
- DVSYSPOLICY\_OWNER\_RULE\_SET\_RULE, [25-56](#)
- SYS.DV\$CONFIGURATION\_AUDIT, [25-56](#)
- SYS.DV\$ENFORCEMENT\_AUDIT, [25-57](#)
  - See also* names beginning with DVSYSDBA\_DV

VPD

*See* Oracle Virtual Private Database (VPD)

## **W**

---

WITH ADMIN Privileges Grants Report, [27-14](#)  
WITH ADMIN status, [27-9](#), [27-10](#)  
WITH GRANT clause, [27-15](#)  
WITH GRANT Privileges Report, [27-15](#)

## **X**

---

XStream  
Database Vault role used for, [14-16](#)  
in an Oracle Database Vault environment, [13-19](#)

