

Oracle® Enterprise Manager Cloud Control Security Guide



13c Release 2

E74859-06

May 2018

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2011, 2017, Oracle and/or its affiliates. All rights reserved.

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

Audience	ix
Documentation Accessibility	ix
Related Documents	ix
Conventions	ix

1 Security Overview

1.1 Security Threats	1-1
1.2 Security Principles	1-4
1.2.1 Separation of Duties and Principle of Least Privilege	1-4
1.2.2 Encryption	1-4
1.2.3 Monitoring for Suspicious Activity (Auditing)	1-5
1.2.4 Non-repudiation	1-5

2 Security Features

2.1 Configuring Authentication	2-1
2.1.1 Supported Authentication Schemes	2-1
2.1.2 Creating a New Administrator	2-3
2.1.2.1 Repository Based Authentication	2-3
2.1.2.2 Restoring to the Default Authentication Method	2-4
2.1.3 Deleting an Administrator	2-5
2.1.4 Enterprise User Security Based Authentication	2-6
2.1.4.1 Registering Enterprise Users (EUS Users) as Enterprise Manager Users	2-7
2.1.5 Oracle Internet Directory (OID)	2-8
2.1.5.1 Prerequisites	2-8
2.1.5.2 Testing the OID Configuration	2-10
2.1.6 Microsoft Active Directory Based Authentication	2-10
2.1.6.1 Testing the Microsoft Active Directory Configuration	2-11
2.1.7 External Authorization using External Roles	2-11
2.1.7.1 Auto Provisioning	2-11

2.1.7.2	Using a Different Name to the External Users Display Name	2-12
2.1.8	Mapping LDAP User Attributes to Enterprise Manager User Attributes	2-14
2.1.9	Changing User Display Names in Enterprise Manager	2-16
2.1.10	Configuring Other LDAP/SSO Providers	2-17
2.1.10.1	Configuring Single Sign-on based Authentication	2-18
2.1.11	Configuring Enterprise User Security based Authentication	2-24
2.1.12	Restoring to the Default Authentication Method	2-24
2.1.12.1	Bypassing the Single Sign-On Logon Page	2-24
2.1.12.2	Restoring the Default Authentication Method	2-24
2.2	Configuring Privileges and Role Authorization	2-24
2.2.1	Understanding Users, Privileges, and Roles	2-25
2.2.1.1	Classes of Users	2-26
2.2.1.2	Reassigning Objects	2-27
2.2.1.3	Aggregate Target Privileges	2-28
2.2.2	Privileges and Roles	2-28
2.2.2.1	Administrators and Database Privileges	2-29
2.2.2.2	Granting Privileges	2-29
2.2.2.3	Fine-grained Access Control	2-30
2.2.2.4	Creating Roles	2-31
2.2.2.5	Private Roles	2-31
2.2.2.6	Using Roles to Manage Privileges	2-32
2.2.3	Managing Privileges with Privilege Propagating Groups	2-33
2.2.3.1	Example1: Granting various teams different levels of access to target groups	2-35
2.2.3.2	Example 2: Granting developers view access to target database instances.	2-36
2.2.3.3	Entitlement Summary	2-39
2.3	Configuring Secure Communication	2-39
2.3.1	About Secure Communication	2-40
2.3.2	Enabling Security for the Oracle Management Service	2-40
2.3.2.1	Configuring the OMS with Server Load Balancer	2-42
2.3.2.2	Creating a New Certificate Authority	2-43
2.3.2.3	Viewing the Security Status and OMS Port Information	2-44
2.3.2.4	Configuring Transport Layer Security	2-44
2.3.3	Securing the Oracle Management Agent	2-45
2.3.4	Managing Agent Registration Passwords	2-46
2.3.4.1	Using the Cloud Control Console to Manage Agent Registration Passwords	2-46
2.3.4.2	Using emctl to Add a New Agent Registration Password	2-47
2.3.5	Restricting HTTP Access to the Management Service	2-47
2.3.6	Enabling Security for the Management Repository Database	2-49

2.3.6.1	About Oracle Advanced Security and the sqlnet.ora Configuration File	2-49
2.3.6.2	Configuring the Management Service to Connect to a Secure Management Repository Database	2-50
2.3.6.3	Enabling Oracle Advanced Security for the Management Repository	2-52
2.3.6.4	Enabling Security for a Management Agent Monitoring a Secure Management Repository or Database	2-53
2.3.7	Custom Configurations	2-53
2.3.7.1	Configuring Custom Certificates for WebLogic Server	2-53
2.3.7.2	Configuring Custom Certificates for OMS Console Access	2-56
2.3.7.3	Configuring Custom Certificates for OMS Upload Access	2-56
2.3.8	Secure Communication Setup Tools	2-57
2.3.8.1	emctl secure oms	2-58
2.3.8.2	emctl secure agent	2-59
2.3.8.3	emctl secure wls	2-59
2.3.8.4	emctl status oms -details	2-59
2.3.9	Configuring Third Party Certificates	2-60
2.3.9.1	Configuring a Third Party Certificate for HTTPS Console Users	2-60
2.3.9.2	Configuring Third Party Certificate for HTTPS Upload Virtual Host	2-60
2.4	Configuring and Using Target Credentials	2-61
2.4.1	Credential Subsystem	2-61
2.4.1.1	Named Credentials	2-63
2.4.1.2	Privileged Credentials	2-68
2.4.1.3	Monitoring Credentials	2-69
2.4.1.4	Preferred Credentials	2-69
2.4.1.5	Saving Preferred Credentials for Hosts and Oracle Homes	2-72
2.4.1.6	Saving Preferred Credentials to Access My Oracle Support	2-72
2.4.1.7	Managing Credentials Using EM CLI	2-73
2.4.1.8	Host Authentication Features	2-73
2.5	Configuring and Using Cryptographic Keys	2-89
2.5.1	Configuring the emkey	2-90
2.5.2	emctl Commands	2-90
2.5.2.1	emctl status emkey	2-91
2.5.2.2	emctl config emkey -copy_to_credstore	2-91
2.5.2.3	emctl config emkey -copy_to_file_from_credstore	2-92
2.5.2.4	emctl config emkey -copy_to_file_from_repos	2-92
2.5.2.5	emctl config emkey -copy_to_credstore_from_file	2-92
2.5.2.6	emctl config emkey -copy_to_repos_from_file	2-92
2.5.2.7	emctl config emkey -remove_from_repos	2-93
2.5.3	Install and Upgrade Scenarios	2-93
2.5.3.1	Installing the Management Repository	2-93

2.5.3.2	Installing the First Oracle Management Service	2-93
2.5.3.3	Upgrading from 10.2 or 11.1 to 12.1	2-93
2.5.3.4	Recreating the Management Repository	2-94
2.6	Configuring and Managing Audit	2-94
2.6.1	Auditing Credentials	2-94
2.6.2	Default Audit Actions	2-95
2.6.3	Configuring the Enterprise Manager Audit System	2-95
2.6.4	Configuring the Audit Data Export Service	2-96
2.6.5	Updating the Audit Settings	2-96
2.6.6	Searching the Audit Data	2-97
2.6.7	List of Operations Audited	2-97
2.6.8	Auditing the Infrastructure	2-97
2.6.8.1	WebLogic Server Auditable Events	2-102
2.7	Additional Security Considerations	2-103
2.7.1	Changing the SYSMAN and MGMT_VIEW Passwords	2-103
2.7.1.1	Changing the SYSMAN User Password	2-103
2.7.1.2	Changing the MGMT_VIEW User Password	2-105
2.7.2	Responding to Browser-Specific Security Certificate Alerts	2-106
2.7.2.1	Third Party Certificate Workflow	2-106
2.7.2.2	Responding to the Internet Explorer Security Alert Dialog Box	2-107
2.7.2.3	Responding to the Mozilla Firefox New Site Certificate Dialog Box	2-108
2.7.2.4	Responding to the Google Chrome Security Alert Dialog Box	2-110
2.7.2.5	Responding to Safari Security Dialog Box	2-114

3 Keeping Enterprise Manager Secure

3.1	Guidelines for Secure Infrastructure and Installations	3-1
3.1.1	Secure the Infrastructure and Operating System	3-1
3.1.1.1	Best Practices for Securing the Infrastructure and Operating System	3-2
3.1.2	Securing the Oracle Management Repository	3-2
3.1.2.1	Enable Advanced Security Option	3-2
3.1.3	Securing the Oracle Management Agent	3-5
3.1.4	Secure Communication	3-5
3.1.4.1	Best Practices for Securing the Oracle Management Agent	3-5
3.1.4.2	Enable ICMP	3-6
3.1.4.3	Configure Oracle Management Agent for Firewalls	3-6
3.1.4.4	Configure Oracle Management Service for Firewalls	3-6
3.1.5	Security Console	3-7
3.1.5.1	Overview	3-8
3.1.5.2	Pluggable Authentication	3-8
3.1.5.3	Fine-grained Access Control	3-9

3.1.5.4	Secure Communication	3-12
3.1.5.5	Credentials Management	3-14
3.1.5.6	Comprehensive Auditing	3-14
3.1.5.7	Active User Session Count	3-15
3.1.5.8	Best Practices Analysis	3-15
3.2	Guidelines for SSL Communication	3-15
3.2.1	Ensure TLSv1.2 Protocol is Enabled	3-15
3.2.2	Leave Communication in Secure-Lock Mode	3-17
3.2.2.1	Secure and Lock the OMS and Agents	3-17
3.2.3	Modify Cipher Configuration if Required	3-18
3.2.3.1	Third Party Certificates	3-21
3.2.3.2	Oracle Wallets	3-21
3.2.4	Best Practices for Securing Communication	3-22
3.3	Guidelines for Authentication	3-22
3.3.1	Enable External Authentication	3-22
3.3.1.1	Best Practices for Authentication	3-23
3.4	Guidelines for Authorization	3-23
3.4.1	Best Practices for Privilege and Role Management	3-25
3.4.2	Use Principle of Least Privileges for Defining Roles/Privileges	3-25
3.4.3	Use Privilege Propagation Groups	3-25
3.4.3.1	Best Practices for Groups and Systems	3-25
3.5	Guidelines for Auditing	3-26
3.5.1	Best Practices for Auditing	3-27
3.6	Guidelines for Managing Target Credentials	3-27
3.6.1	Best Practices for Credentials	3-28

4 Security Best Practices for Database Management in Enterprise Manager

4.1	Flexible Database Access Control	4-1
4.1.1	Database Management Roles and Responsibilities	4-2
4.1.2	Application DBA Access	4-2
4.1.2.1	Creating an Application DBA Account	4-2
4.1.2.2	Creating Named Credentials	4-3
4.1.3	Application Developer Access	4-3
4.1.3.1	Granting Application Developer Access on the Database	4-3
4.1.3.2	Granting Application Developer Access to the Database Named Credentials	4-3
4.1.4	Database Monitoring User Access	4-3
4.1.4.1	Granting View Database Performance Access on the Database	4-4
4.1.4.2	Sharing credentials with the Database Monitoring User	4-4

4.1.5	Database Administrator Access	4-4
4.1.5.1	Creating a Database Administrator Account	4-4
4.1.5.2	Creating Named Credentials	4-4
4.1.5.3	Granting Privileges Through Roles and Privilege Propagating Groups	4-5
4.1.6	Privilege Groups	4-5
4.1.6.1	Database Application DBA	4-6
4.1.6.2	Database Application Developer	4-6
4.1.6.3	Manage Database High Availability Privilege Group	4-6
4.1.6.4	View Database High Availability Privilege Group	4-6
4.1.6.5	Manage Database Performance Privilege Group	4-7
4.1.6.6	View Database Performance Privilege Group	4-7
4.1.6.7	Manage Database Schema Privilege Group	4-8
4.1.6.8	View Database Schema Privilege Group	4-9
4.1.6.9	Manage Database Security Privilege Group	4-10
4.1.6.10	View Database Security Privilege Group	4-11
4.1.6.11	Manage Database Storage Privilege Group	4-12
4.2	Secured Communication (TCPS) Access to Databases	4-12
4.2.1	Configuring TCPS	4-13
4.2.2	Configuring Third Party CA Certificates for Communication With Target Databases	4-13
4.3	Account Management	4-14

5 Troubleshooting

5.1	Troubleshooting Authentication Issues in Enterprise Manager	5-1
5.1.1	Enabling the WebLogic Debug Flag	5-1
5.1.2	Debugging errors in ldap_trace.logATN file	5-1
5.1.3	Invalid Credentials	5-2
5.1.4	Timeout in LDAP Server'	5-3
5.1.5	Errors Outside ldap_trace.logATN'	5-3

6 References

Index

Preface

This guide describes how to set up Enterprise Manager Cloud Control 13c security.

The preface covers the following:

- [Audience](#)
- [Documentation Accessibility](#)
- [Related Documents](#)
- [Conventions](#)

Audience

This document is intended for administrators who want to set up and manage Enterprise Manager security.

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 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 the latest releases of these and other Oracle documentation, check the Oracle Technology Network at:

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

Oracle Enterprise Manager also provides extensive Online Help. Click **Help** at the top of any Enterprise Manager page to display the online help window.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	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.

1

Security Overview

This chapter provides a brief overview of security concepts and concerns. The following topics are discussed:

- [Security Threats](#)
- [Security Principles](#)

The dynamic and complex nature of today's IT environments, the potential fallout of security breaches in terms of the financial implications and loss of goodwill coupled with stringent regulatory requirements make security a critical area of consideration for both business and IT managers. While security considerations are important for standalone applications, the introduction of distributed system management applications can make it yet more challenging. While standardized security best practices are available for databases and application servers, there aren't any standardized security benchmarks specifically for system management products. However, Enterprise Manager has been evaluated and in the past, has received a third party security certification, by the Common Criteria Recognition Arrangement.

Securing Enterprise Manager requires working closely with System Administrators, Network Administrators, Database Administrators, Application Administrators and the Security team. This document can be used by all concerned parties to identify various security considerations and the best practices for securing Oracle Enterprise Manager deployments. The recommendations in this document are based on our experience with both customer deployments and Oracle's own internal usage of Enterprise Manager.

1.1 Security Threats

The following table briefly summarizes the primary security threats to your Enterprise Manager Cloud Control environment.

Table 1-1 Security Threats

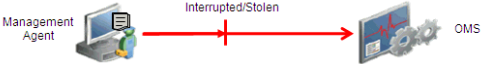

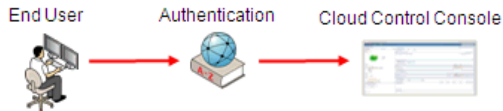
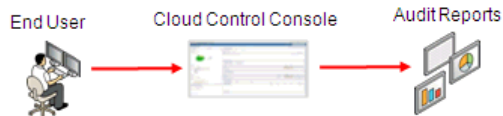
Threats	Security Consideration	Resolution/Best Practice
Man-in-the-middle attacks	Data confidentiality and integrity	<p>Data Confidentiality and Integrity</p> <ul style="list-style-type: none"> Not disclosed to any entities unless they are authorized to access Not changed, destroyed, or lost in unauthorized or accidental manner <p>Man-in-the-Middle Attacks</p> <ul style="list-style-type: none"> Interrupts, intercepts, modifies or fabricates data in transit  <p>Best Practice: Secure communication between Enterprise Manager components.</p>
Denial-of-service attacks	Data availability	<p>Data Availability</p> <ul style="list-style-type: none"> Available and usable upon demand by an authorized entity <p>Denial-of-Service attacks</p> <ul style="list-style-type: none"> Makes Management Repository or OMS unavailable to intended users by flooding them with more requests than they can handle.  <p>Best Practice: Secure individual Enterprise Manager components</p>

Table 1-1 (Cont.) Security Threats

Threats	Security Consideration	Resolution/Best Practice
Password crack attacks	Authentication	<p>Authentication</p> <ul style="list-style-type: none"> The process to verify the identity, usually username and password, claimed by a user <p>Password Crack Attacks</p> <ul style="list-style-type: none"> Obtains password from an authentication exchange, then uses the password to log on to Enterprise Manager Cloud Control <p>Examples: guessing, dictionary and brute force attacks</p> <div style="text-align: center;">  <pre> graph LR A[End User] --> B[Authentication] B --> C[Cloud Control Console] </pre> </div> <p>Best Practice: Change passwords and enable password profiles</p>
Exploitation of authorization	Segregation of duties	<p>Exploitation of Authorization</p> <ul style="list-style-type: none"> Accesses resources (targets, jobs, templates and so on) not authorized to you <p>Segregation of Duties</p> <ul style="list-style-type: none"> No person should be given responsibility for more than one related function <p>Best Practice: Follow principle of least privileges</p>
Repudiation	Non-repudiation	<p>Accountability of Actions</p> <ul style="list-style-type: none"> Network security: Neither sender nor recipient can later deny having processed the information Web Application security: No one can later deny the actions he/she has taken in the application <p>Repudiation</p> <ul style="list-style-type: none"> Refuses authoring of something that happened <div style="text-align: center;">  <pre> graph LR A[End User] --> B[Cloud Control Console] B --> C[Audit Reports] </pre> </div> <p>Best Practice: Audit Enterprise Manager actions</p>

1.2 Security Principles

Underlying all strategies to implement effective system security are the following basic principles:

- [Separation of Duties and Principle of Least Privilege](#)
- [Encryption](#)
- [Monitoring for Suspicious Activity \(Auditing\)](#)
- [Non-repudiation](#)

1.2.1 Separation of Duties and Principle of Least Privilege

The *principle of least privilege* and *separation of duties* are concepts that, although semantically different, are intrinsically related from the standpoint of security. The intent behind both is to **prevent people from having higher privilege levels than they actually need**. Now that their relationship has been framed, let us define the concepts.

- **Principle of Least Privilege:** Users should only have the least amount of privileges required to perform their job and no more. This reduces authorization exploitation by limiting access to Enterprise Manager resources such as targets, jobs, or monitoring templates for which they are not authorized.

Example: A user whose sole responsibility is to monitor and maintain a human resources database does not need privileges to access and manage Enterprise Manager plug-ins on the Oracle Management Services (OMS).

- **Separation of Duties:** Beyond limiting user privilege level, you also limit user duties, or the specific jobs they can perform with Enterprise Manager. No user should be given responsibility for more than one related function. This limits the ability of a user to perform a malicious action and then cover up that action.

Example: You have an Enterprise Manager administrator who is responsible for creating user accounts. However, that administrator may create unnecessary accounts, perhaps for unauthorized colleagues to access confidential systems. If that administrator also has the ability to view and erase the audit logs, then there is a potential problem in that it prevents a wayward administrator from being caught. In this situation, you want to separate the account creation duties from the security administration duties. The person who is the account administrator, in this case, should also not be the security administrator.

In order to be effective, the principle of least privilege and separation of duties should be enforced for all Enterprise Manager users in your organization.

1.2.2 Encryption

Encryption is the process of transforming data into an unreadable format using a secret key and an encryption algorithm. For Enterprise Manager, *emkey* is the key to encrypting and decrypting sensitive data within your Enterprise Manager environment. It is important that *emkey* be accessible only to authorized users.

1.2.3 Monitoring for Suspicious Activity (Auditing)

Whenever an Enterprise Manager administrator makes use of higher-level privileges, such as creating new Super Administrator accounts, you should be able to look at the Enterprise Manager audit logs and tell whether those account creation actions were warranted. Enterprise Manager's audit capabilities allow you to monitor and record all administrator actions that take place. You can perform activities such as:

- Investigating suspicious activity. For example, if a user is frequently accessing systems outside their job responsibilities, then a security administrator might decide to track access to those machines.
- Notify a supervisor of the actions of an unauthorized user. For example, an unauthorized user could be changing or deleting data, or the user has more privileges than expected, which can lead to reassessing user authorizations.

1.2.4 Non-repudiation

Non-repudiation is a method of establishing user action accountability by "proving" that a user performed a specific action: Users cannot falsely deny that they performed that action. Conversely, non-repudiation also protects users from later being accused of having performed a specific action.

With regard to data, non-repudiation, is a way to prove that a given sender actually sent a particular message. Non-repudiation is typically achieved through the use of digital signatures. The originator of a message uses a cryptographic tool to convert plain, readable messages or plaintext into encrypted ciphertext. While the original text is present, its appearance changes into a form that is unintelligible if intercepted. The message recipient likewise uses a cryptographic tool to decrypt the ciphertext into its original readable format.

2

Security Features

This chapter covers the following topics:

- [Configuring Authentication](#)
- [Configuring Privileges and Role Authorization](#)
- [Configuring Secure Communication](#)
- [Configuring and Using Target Credentials](#)
- [Configuring and Using Cryptographic Keys](#)
- [Configuring and Managing Audit](#)
- [Additional Security Considerations](#)

2.1 Configuring Authentication

Enterprise Manager authentication is the process of determining the validity of the user accessing Enterprise Manager. The authentication feature is available across the different interfaces such as Enterprise Manager console and Enterprise Manager Command Line Interface (EM CLI).

Enterprise Manager's authentication framework consists of pluggable authentication schemes that let you use the type of authentication protocol best suited to your environment.

Note:

Oracle Enterprise Manager 13c relies on the underlying WebLogic Server that is part of the OMS stack for external Authentication methods. For this reason, Enterprise Manager 12c can be authenticated using any authentication method that is supported by Oracle WebLogic Server. Note that only some providers have been certified so far although theoretically it should be possible to configure for all.

2.1.1 Supported Authentication Schemes

Enterprise Manager supports the following authentication schemes:

- **Repository-Based Authentication:**

This scheme involves saving the administrator's username and password in the Enterprise Manager repository and performing validation against these saved values whenever a user logs on to the Enterprise Manager console. An Enterprise Manager user created is also a repository (database) user. By using this option, you can take advantage of all the benefits of Oracle database user management that this authentication method provides such as password control through the

password profile, enforced password complexity, password life time, and number of failed attempts allowed. During the password grace period, the administrator is prompted to change the password but when the password has expired, it must be changed. For more details, refer to [Creating a New Administrator](#).

- **Oracle Access Manager (OAM) Single Sign-On (SSO) Based Authentication:** Oracle Access Manager is the Oracle Fusion Middleware single sign-on solution. The underlying identity stores will be the Enterprise Directory Identity Stores being supported by Oracle Access Manager. This authentication scheme is used for data centers that have standardized on Oracle Access Manager as the central tool for authentication across all enterprise applications. If you want to support protocols such as Kerberos for authentication, you must configure OAM for this. For more information about OAM, see *Oracle® Fusion Middleware Administrator's Guide for Oracle Access Manager 13c Release 1 (11.1.1)*.
- **Enterprise User Security Based Authentication:** The Enterprise User Security (EUS) option enables you to create and store enterprise users and roles for the Oracle database in an LDAP-compliant directory server. After the Enterprise Manager repository is configured with EUS, you can configure Enterprise Manager to use EUS as its authentication mechanism as described in [Enterprise User Security Based Authentication](#). You can register any EUS user as an Enterprise Manager administrator.

In addition to using EUS to authenticate Enterprise Manager administrators, it can also be used to simplify management of database target credentials. EUS helps centralize the administration of users and roles across multiple databases. If the managed databases are configured with EUS, the process of logging into these databases is simplified. When you drill down to a managed database, Enterprise Manager will attempt to connect to the database using Enterprise Manager credentials. If successful, Enterprise Manager will directly connect you to the database without displaying a logon page.

- **LDAP Authentication Options: Oracle Internet Directory and Microsoft Active Directory**
 - *Oracle Internet Directory (OID) Based Authentication* - Oracle Internet Directory is a LDAP v3 compliant directory built on the Oracle database and is fully integrated into Oracle Fusion Middleware and Oracle Applications. Therefore, it is ideally suited for Oracle environments or enterprises with Oracle database expertise. When using an authentication scheme based on OID as the identity store, you can have your applications authenticate users against the OID.
 - *Microsoft Active Directory Based Authentication* - Microsoft Active Directory is a directory service that provides authentication and authorization functionality in a Windows network. When using a Microsoft Active Directory as an identity store, you can plug in this scheme to have your applications authenticate users against the Microsoft Active Directory.

 **Note:**

Enterprise Manager will support external authentication as long as the specific authentication scheme is supported and integrated with the WebLogic Server.

These authentication schemes have been tested in house and some of the external authentication schemes mentioned below can be configured using the `emctl config auth` utility command, which configures the required WebLogic providers as well as set the required OMS properties.

Authenticating schemes where the `emctl` utility command configures the WebLogic authentication providers, the command sets the required configuration parameters and leaves most of the other parameters to the default values. Administrators should ensure the configuration parameters of the WebLogic providers are tuned for performance suited to their environment before going into production. This can be done through the WebLogic Administration Console.

2.1.2 Creating a New Administrator

Enterprise Manager allows you to create and manage new administrator accounts. Each administrator account includes its own logon credentials as well as a set of roles and privileges that are assigned to the account. You can also assign a password profile to the administrator. You will need to have Enterprise Manager Super Administrator privileges to create and manage new administrator accounts.

To create, edit, or view an administrator account:

1. From the **Setup** menu, select **Security**, then select **Administrators**. The Administrators page is displayed.
2. Click the appropriate task button on the Administrators page. The Authentication page is displayed.

Repository Based Authentication is selected as the default authentication method.

2.1.2.1 Repository Based Authentication

Repository Based Authentication is the default method of Enterprise Manager Authentication. With this authentication method, a new administrator is created in the repository.

Note:

Repository-based authentication is the default authentication method.

On this page, you can specify the type of administrator account being created and select the password profile. The password cannot be changed by the administrator if the **Prevent Password Change** check box is selected.

If you select the **Expire Password Now** check box, the password for the new administrator account will be set to an expired state. If the password has expired, when the new administrator logs in, the Change Password page is displayed and the administrator is prompted to change the password.

The administrator should enter his current password and the new password and click **Apply**. He can now start using Enterprise Manager.

2.1.2.1.1 Creating a New User (Command Line)

The following examples make User1 an Enterprise Manager user, provide a description for the user, and prevent the password from being changed. Only another Super Administrator can change the password. The profile is set as MGMT_ADMIN_USER_PROFILE.

Example 2-1 Command Line

```
emcli create_user
  -name="User1"
  -desc="This is temp hire."
  -prevent_change_password="true"
  -profile="MGMT_ADMIN_USER_PROFILE"
```

Example 2-2 Scripting and Interactive

```
create_user
  (name="User1"
  ,desc="This is temp hire."
  ,prevent_change_password="true"
  ,profile="MGMT_ADMIN_USER_PROFILE")
```

2.1.2.2 Restoring to the Default Authentication Method

The following sections detail how to restore the default Enterprise Manager authentication methods.

2.1.2.2.1 Bypassing the Single Sign-On Logon Page

If the OMS is configured with SSO or OAM or some other authentication method, you may want to by-pass the Single Sign-On or OAM authentication under certain circumstances. To bypass the SSO logon page, connect to the following URL:

1. Connect to `https://ms_host:ms_https_port/em`
`ms_host` & `ms_https_port` are WLS-managed server's hostname & port#. These parameters can be found in the `EM_INSTANCE_HOME/emgc.properties` file. They are listed as `EM_INSTANCE_HOST` & `MS_HTTPS_PORT` in this file.
2. Log in using a repository user's credentials.

2.1.2.2.2 Restoring the Default Authentication Method

1. Run the following command on each OMS:

```
emctl config auth repos [-sysman_pwd <pwd>]
```

Sample command output:

```
Oracle Enterprise Manager Cloud Control 13c Release 2
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
Configuring Repos Authentication ... Started
Configuring Repos Authentication ... Successful
If you have updated files like httpd.conf (for example, while installing
WebGate), rollback them.
If this is a multi-OMS environment, execute this command on remaining servers.
After that, restart OMS(s) using: 'emctl stop oms -all' and 'emctl start oms'
```

2. Run the following commands on each OMS:

```
emctl stop oms -all  
  
emctl start oms
```

If you have configured OAM SSO, you need to manually un-install Webgate and remove the Webgate directives from Apache `httpd.conf`.

If you have configured with OSSO, you need to manually remove the OSSO directives from `httpd.conf`.

2.1.3 Deleting an Administrator

To delete an administrator account:

1. From the **Setup** menu, select **Security**, then select **Administrators**. The Administrators page is displayed.
2. Select the administrator that you want to delete, then click **Delete**.
3. On the confirmation page, click **Yes**.

If the administrator has resources assigned the Delete Administrator page appears. Use the Delete Administrator page to specify what happens to administrator-owned objects when removing an administrator from Enterprise Manager. On this page, you can:

- Delete all administrator-owned objects along with the Enterprise Manager administrator. This will delete the administrator and associated job types, jobs, corrective actions, report definitions, reports, and templates. Blackouts will not be deleted.
- Reassign objects to another Enterprise Manager administrator. This will assign the administrator's objects to another administrator. The credentials belonging to the administrator will be deleted from the repository before any reassignment takes place.

Usage Tips

Click **View Objects** to see all objects currently owned by the Enterprise Manager administrator to be deleted.

To reassign the objects to another administrator, enter the name of the new administrator in the **New Owner** text box, or click the flashlight icon to view a list of available administrators.

Only a super administrator can delete other Enterprise Manager administrators. Enterprise Manager will not allow administrators to:

- Delete themselves.
- Delete the management repository owner.

Administrator object reassignments can be handled as follows:

- **Blackouts** can be reassigned to any user who has OPERATOR privileges on all targets affected by the blackout.
- **Jobs** can be reassigned to any administrator. However, ALL credentials associated with the job will be removed, leaving the job in a Suspended state. This requires the new job owner to explicitly set new credentials. Currently running jobs are allowed to continue running. Once the new job owner sets the credentials, the job will revert to a SCHEDULED state.

- **Corrective Actions** can be reassigned to any administrator who has OPERATOR privileges for targets on which the corrective action can operate.
- **Report Definitions** can be reassigned to any administrator.
- **Reports** can be reassigned to any administrator.
- **Monitoring Templates** can be reassigned to any administrator.

2.1.4 Enterprise User Security Based Authentication

Enterprise User Security enables you to create and store Oracle database information as directory objects in an LDAP-compliant directory server such as Oracle Internet Directory (OID) or Microsoft Active Directory. For example, an administrator can create and store enterprise users and roles for the Oracle database in the directory, which helps centralize the administration of users and roles across multiple databases.



See Also:

Database Enterprise User Security Administrator's Guide.

If you currently use Enterprise User Security to manage Oracle users and roles for all your Oracle databases, you can also extend this feature to manage Enterprise Manager administrator accounts. Configuring Enterprise Manager for use with Enterprise User Security simplifies the process of logging in to database targets you are managing with the Oracle Enterprise Manager console.

To configure Enterprise Manager for use with Enterprise User Security:

1. Ensure that you have enabled Enterprise User Security for your Oracle Management Repository database, as well as the database targets you will be managing with the Cloud Control console. Refer to *Oracle Database Advanced Security Administrator's Guide* for details.
2. Using the `emctl set property` command, set the following property:

```
oracle.sysman.emSDK.sec.DirectoryAuthenticationType=EnterpriseUser
```



Note:

For multiple OMS configurations, the command must be run on each OMS.

For example:

```
emctl set property -name oracle.sysman.emSDK.sec.DirectoryAuthenticationType -  
value EnterpriseUser
```

3. Stop the Oracle Management Service.

```
emctl stop oms -all
```

 **See Also:**

Controlling the Oracle Management Service on page 24-4

4. Start the Management Service.

```
emctl start oms
```

The next time you use the Oracle Enterprise Manager console to drill down to a managed database, Enterprise Manager will attempt to connect to the database using Enterprise User Security. If successful, Enterprise Manager will connect you to the database without displaying a logon page. If the attempt to use Enterprise User Security fails, Enterprise Manager will prompt you for the database credentials.

2.1.4.1 Registering Enterprise Users (EUS Users) as Enterprise Manager Users

After you have configured Enterprise Manager to use Enterprise Users (EUS), you can register existing enterprise users as Enterprise Manager Users and grant them the necessary privileges so that they can manage Enterprise Manager effectively.

You can register existing enterprise users by using:

- Enterprise Manager Console
- Enterprise Manager Command Line Interface (EM CLI)

2.1.4.1.1 Registering Enterprise Users Using the Enterprise Manager Console

You can use the Enterprise Manager console to register enterprise users by following these steps:

1. Log in to Enterprise Manager as a Super Administrator.
2. From the **Setup** menu, select **Security** then select **Administrators** to display the Administrators page. Since Enterprise Manager has been configured to use Enterprise Users, the first page of the Create Administrator wizard will provide the option to create an administrator based on a registered Oracle Internet Directory user or a normal database user.
3. Select Oracle Internet Directory and click **Continue** to go to the next page in the wizard.
4. Enter the name and e-mail address of the Oracle Internet Directory user or click the flashlight icon to search for a user name in the Oracle Internet Directory.
5. Use the rest of the wizard pages to define the roles, system privileges, and other characteristics of the Enterprise Manager administrator and then click **Finish**. Enterprise Manager displays a summary page that lists the characteristics of the administrator account.
6. Click **Finish** to create the new Enterprise Manager administrator.

The OID user is now included in the list of Enterprise Manager administrators. You can now verify the account by logging out of the Cloud Control console and logging back in using the OID user credentials on the Single Sign-On logon page.

2.1.4.1.2 Registering Enterprise Users Using the Command Line Interface

To register Enterprise Users as Enterprise Manager users using EM CLI, enter the following command:

```
emcli create_user -name=eususer -type=DB_EXTERNAL_USER
```

This command registers the `eususer` as an Enterprise Manager user where `eususer` is an existing Enterprise User.

2.1.5 Oracle Internet Directory (OID)

You can implement an OID-based authentication scheme to have Enterprise Manager authenticate users against the OID.

Running the `emctl config auth oid` command on the OMS creates a WebLogic authentication provider of type `OracleInternetDirectoryAuthenticator` that uses the configuration parameter values specified by the command. Any configuration values not specified retain the default values. Tuning and modification of advanced OID configuration parameters is carried out through the WebLogic Server Administration Console and not the `emctl config auth oid` command.

Note:

In the event you need to perform LDAP troubleshooting, enable LDAP tracing log file (`ldap_trace.log`ATN) generation from the WebLogic Server Console. For more information, see "[Troubleshooting Authentication Issues in Enterprise Manager](#)".

2.1.5.1 Prerequisites

Oracle Internet Directory LDAP server is set up and running.

WebLogic Administration Server is up and running.

1. Run the `emctl config auth oid` command on each OMS.

```
emctl config auth ad -ldap_host <ldap host> -ldap_port <ldap port>
  -ldap_principal <ldap principal> [-ldap_credential <ldap credential>] [-
sysman_pwd <pwd>]
  -user_base_dn <user base DN> -group_base_dn <group base DN> [-user_dn <dn>]
[-group_dn <dn>]
  [-enable_auto_provisioning] [-auto_provisioning_minimum_role <min_role>] [-
minimum_privilege <min_priv>]
  [-use_ssl] [-cert_file <cert>] [-trust_cacerts] [-use_anonymous_bind] [-
keystore_pwd <passwd>]
```

where:

- `ldap_host`: LDAP host name
- `ldap_port`: LDAP port

- `ldap_principal`: The distinguished name (DN) of the LDAP user the WebLogic server should use to connect to the LDAP server.
- `ldap_credential`: Password for the user specified by `ldap_principal`.
- `user_base_dn`: The base distinguished name (DN) of the tree in the LDAP directory that contains users.
- `group_base_dn` - The base distinguished name (DN) of the tree in the LDAP directory that contains groups.
- `enable_auto_provisioning`: If specified, turns on auto provisioning in Enterprise Manager, where external LDAP users do not have to be provisioned manually in Enterprise Manager
- `auto_provisioning_minimum_role <min_role>`: if specified, auto provisions only those external users in Enterprise Manager who have the `min_role` granted to them in LDAP
- `minimum_privilege <min_priv>`: If specified, prevents access to Enterprise Manager to users who do not have the `min_priv` granted to them.
- `use_ssl`: Use SSL to connect to the LDAP server
- `cert_file <cert>`: Use the passed in LDAP server certificate to establish trust while connecting to LDAP server over ssl. Specify this option if the LDAP server has certificate signed by not well-known (or trusted) Certificate Authority. Note: This expects a single certificate. We do not support importing certificate chains. Please import using keytool utility before running this command.
- `trust_cacerts`: Trust the LDAP server's certificate while connecting to LDAP server. This is typically used if certificate is signed by well known CA
- `keystore_pwd <passwd>`: The password for the default DemoTrust.jks keystore (if default password has changed) or any custom keystore to which the LDAP server's certificate will be imported as part of validation.
- `use_anonymous_bind`: If specified, uses anonymous bind to connect to LDAP server

Example:

```
emctl config auth oid -ldap_host "ldaphost" -ldap_port "3060" -ldap_principal
"cn=orcladmin,cn=users,dc=us,dc=oracle,dc=com" -user_base_dn
"cn=users,dc=us,dc=oracle,dc=com" -group_base_dn
"cn=groups,dc=us,dc=oracle,dc=com" -ldap_credential "my_ldap_password" -
sysman_pwd "my_sysman_password"
```

2. Stop the OMS.

```
emctl stop oms -all
```

3. Restart the OMS.

```
emctl start oms
```

 **Note:**

For Enterprise Manager deployments consisting of multiple OMS instances, `emctl config auth oid` must be run on each OMS. Each OMS must be restarted in order for changes to take effect.

2.1.5.2 Testing the OID Configuration

Use the WebLogic Server Administration Console (**Users and Groups** tab) to check whether the OID configuration has been successful. To navigate to this tab, select **Home/Summary of Security Realms/myrealm/Users and Groups**. From the **Users and Groups** tab, you should see users and groups showing up from the OID.

2.1.6 Microsoft Active Directory Based Authentication

You can implement Microsoft AD-based authentication scheme to have Enterprise Manager authenticate users against the Active Directory.

Running the `emctl config auth ad` command on the OMS creates a WebLogic authentication provider of type `ActiveDirectoryAuthenticator` that uses the configuration parameter values specified by the command. Any configuration values not specified retain the default values. Tuning and modification of advanced AD configuration parameters is carried out through the WebLogic Server Administration Console and not the `emctl config auth ad` command.

Before running the following procedure, ensure the Active Directory LDAP server is up and running.

1. Run the `emctl config auth oid` command on each OMS.

```
emctl config auth ad -ldap_host <ldap host> -ldap_port <ldap port> -  
ldap_principal <ldap principal> [-ldap_credential <ldap credential>] [-  
sysman_pwd <pwd>] -user_base_dn <user base DN> -group_base_dn <group base DN>
```

where:

- `ldap_host`: Name of the machine name where Active Directory has been installed.
- `ldap_port`: Active port where Active Directory is listening for requests.
- `ldap_principal`: The distinguished name (DN) of the Active Directory user the WebLogic server should use to connect to the LDAP server to ensure the user's validity.
- `ldap_credential`: Password for the user specified by `ldap_principal`.
- `sysman_pwd`: SYSMAN password. This password is required to set the necessary property value changes to Enterprise Manager
- `user_base_dn`: The users specified as the `ldap_principal` must have read access to this directory. If the users are located in multiple base DNS, enter the highest, most common DN in this field. This field does not accept multiple entries.
- `group_base_dn` - The users specified as the `ldap_principal` must have read access to this directory.

Example:

```
emctl config auth ad -ldap_host "ldaphost" -ldap_port "3060" -ldap_principal  
"cn=orcladmin" -user_base_dn "cn=users,dc=us,dc=oracle,dc=com" -group_base_dn  
"cn=groups,dc=us,dc=oracle,dc=com" -ldap_credential "my_ldap_password" -  
sysman_pwd "my_sysman_password"
```

2. Stop the OMS.

```
emctl stop oms -all
```

3. Restart the OMS.

```
emctl start oms
```

Note:

For Enterprise Manager deployments consisting of multiple OMS instances, *emctl config auth ad* must be run on each OMS. Each OMS must be restarted in order for changes to take effect.

2.1.6.1 Testing the Microsoft Active Directory Configuration

Use the WebLogic Server Administration Console (**Users and Groups** tab) to check whether the Microsoft Active Directory configuration has been successful. To navigate to this tab, select **Home/Summary of Security Realms/myrealm/Users and Groups**. From the **Users and Groups** tab, you should see users and groups showing up from the Microsoft Active Directory.

2.1.7 External Authorization using External Roles

When configuring Enterprise Manager for external authentication of users, you can also configure it to work with the external authentication provider to manage authorization as well. This is done using external roles. This is useful in many scenarios including, but not limited to, auto-provisioned users where the auto-provisioned user will not have any Enterprise Manager roles granted to them. The idea behind external roles is to create a role in Enterprise Manager with the relevant privileges and have the name of the role match the name of a LDAP group. Users who are part of the LDAP group will automatically be granted privileges in the role once they log on to Enterprise Manager.

To set up external roles, create a role in Enterprise Manager and mark it as external. The name of this role should be the same as an external LDAP group. Set up this role with the necessary roles and privileges. For example, in Enterprise Manager you can create a role called `EM_ADMIN` that is marked external. The `EM_ADMIN` name matches an LDAP group called `EM_ADMIN`. Assume JohnDoe is a member of the `EM_ADMIN` LDAP group and is also an Enterprise Manager user. When JohnDoe logs on to Enterprise Manager, he will be granted all the privileges defined in the Enterprise Manager role `EM_ADMIN`.

2.1.7.1 Auto Provisioning

Typically the external LDAP users must be created in Enterprise Manager before they can log in to the Enterprise Manager console. Auto provisioning removes that requirement by automatically creating the Enterprise Manager user account upon successful authentication of the user the first time he logs on to Enterprise Manager.

To enable auto provisioning, set the OMS property *oracle.sysman.core.security.auth.autoprovisioning* to *true*.

This parameter can be set using `emctl` or the console.

This allows the external users to login without being first created as an Enterprise Manager user in the Enterprise Manager repository. Their user account gets created automatically upon the first login. Once this property is set, all external LDAP users will be able to login to Enterprise Manager console. If you want to further restrict the auto provisioning feature to a subset of users, such as only to members of certain LDAP groups, then set another OMS property "oracle.sysman.core.security.auth.autoprovisioning_minimum_role". This property should be set to the LDAP group name whose members should be auto-provisioned. For example, if set to "EM_ADMIN", only members of that LDAP group called EM_ADMIN will be able to login to Enterprise Manager and have user accounts automatically created in Enterprise Manager.

2.1.7.2 Using a Different Name to the External Users Display Name

By default, you must log in to Oracle Enterprise Manager with the user name that is displayed in the Weblogic Console >Security Realms >myrealms >Users and Groups >Users list. After authenticating Oracle Enterprise Manager with external providers, the cn values of the external users are listed in Weblogic Console Users list.

In some environments, the cn value is in the form 'FIRST NAME LAST NAME'. If you prefer to use the sAMAccountName or user ID (UID) to login to Oracle Enterprise Manager you must update the provider configurations.

For example, there is a user with the user name 'TEST USER' displayed in the Weblogic Console, but the user wants to login to Oracle Enterprise Manager as 'tuser' which is the sAMAccountName of that user.



Note:

The sAMAccountName is used in this example. To use a UID, replace sAMAccountName with uid in the steps that follow.

1. In the external provider, check the parameter/properties configured for the external user.
2. The value of parameter 'cn' is 'TEST USER'.
3. In the same file, find the parameter that has the value for user as 'tuser' . That parameter may be 'sAMAccountName'.

To use the sAMAccountName of the external users (tuser) to log in to Oracle Enterprise Manager:

1. Back up the <GC DOMAIN>/config/config.xml file.
2. On the Weblogic Console, navigate to Security Realms>myrealms>Providers>External Authenticator.
3. Click **Lock and Edit** to edit this page.
4. Click the Provider Specific tab.
5. Look for the **User From Name** filter.
6. Change the value of User From Name from (&(cn=%u)(objectclass=person)) to (&(sAMAccountName=%u)(objectclass=person)).
7. Look for **User Name Attribute**.

8. Change the value of **User Name Attribute** from cn to sAMAccountName.
9. Click **Save** then click **Activate Changes**.
10. Restart Oracle Management Server with the `-all` option:


```
<OMS_HOME>/bin>./emctl stop oms -all -force

<OMS_HOME>/bin>./emctl start oms
```
11. Log in to the Weblogic Console >Security Realms >myrealms >Users and Groups >Users list and confirm that the user 'tuser' exist in Users list. Now you can use the user name 'tuser' to log in to Oracle Enterprise Manager.

2.1.7.2.1 Updating the Oracle Virtual Directory with User Name Changes

With Oracle Enterprise Manager release 12.1.0.4 and higher, you must perform the following additional steps to update the user name changes in the Oracle Virtual Directory layer:

1. Backup the `<MW_HOME>/oracle_common/common/bin/wlst.sh` and `<GCDomain>/config/fmwconfig/ovd/default/adaptor.os_xml` file.
2. Open the `<MW_HOME>/oracle_common/common/bin/wlst.sh` file in a text editor and add the following parameter to `WLST_PROPERTIES`:

```
-Dweblogic.ssl.JSSEEnabled=true -Djavax.net.ssl.keyStore=<MW_HOME>/wlserver_10.3/
server/lib/DemoIdentity.jks
-Djavax.net.ssl.keyStorePassword=DemoIdentityKeyStorePassPhrase
-Djavax.net.ssl.trustStore=<MW_HOME>/wlserver_10.3/server/lib/DemoTrust.jks
-Djavax.net.ssl.trustStorePassword=DemoTrustKeyStorePassPhrase
-Dweblogic.security.SSL.trustedCAKeyStore=<MW_HOME>/wlserver_10.3/server/lib/
DemoTrust.jks
-Dweblogic.security.SSL.ignoreHostnameVerification=true
```

For example:

```
WLST_PROPERTIES="-Dweblogic.ssl.JSSEEnabled=true
-Djavax.net.ssl.keyStore=/u01/mwr/wlserver_10.3/server/lib/DemoIdentity.jks
-Djavax.net.ssl.keyStorePassword=DemoIdentityKeyStorePassPhrase
-Djavax.net.ssl.trustStore=/u01/mwr/wlserver_10.3/server/lib/DemoTrust.jks
-Djavax.net.ssl.trustStorePassword=DemoTrustKeyStorePassPhrase
-Dweblogic.security.SSL.trustedCAKeyStore=/u01/mwr/wlserver_10.3/server/lib/
DemoTrust.jks
-Dweblogic.security.SSL.ignoreHostnameVerification=true ${WLST_PROPERTIES}
-DORACLE_HOME='${ORACLE_HOME}' -DCOMMON_COMPONENTS_HOME='${
COMMON_COMPONENTS_HOME}' "
export WLST_PROPERTIES
```

Note:

If third party or custom certificates are imported to WebLogic Server, you must replace the path in the preceding example with the respective keystores. The custom path is available in the `config.xml` file.

3. Launch `<MW_HOME>/oracle_common/common/bin/wlst.sh`.
4. Enter the following command to connect to the admin server:

```
connect('weblogic','<weblogic password>','t3s://<ADMIN SERVER HOSTNAME>:<ADMIN
SERVER PORT>')
```

For example:

```
connect('weblogic','<weblogic password>','t3s://hostname.domain.com:7102')
```

5. Enter the following command:

```
$addPlugin(adapterName='ADAPTER_NAME',pluginName='changerdn',pluginClass='oracle.
ods.virtualization.engine.chain.plugins.changeuserRdn.ChangeUserRDN',paramKeys='r
eplaceValue|fromRDN|toRDN',paramValues='true|cn|sAMAccountName')
```

 **Note:**

The name of the LDAP provider on the admin server console must be specified for adapterName parameter in the preceding command.

6. Enter the following command to stop the OMS:

```
<OMS HOME>/bin>./emctl stop oms -all -force
```

7. Ensure no process is running from OMS path.

8. Enter the following commands to start the admin server and the OMS:

```
<OMS HOME>/bin>./emctl start oms -admin_only<OMS HOME>/bin>./emctl start oms
```

2.1.8 Mapping LDAP User Attributes to Enterprise Manager User Attributes

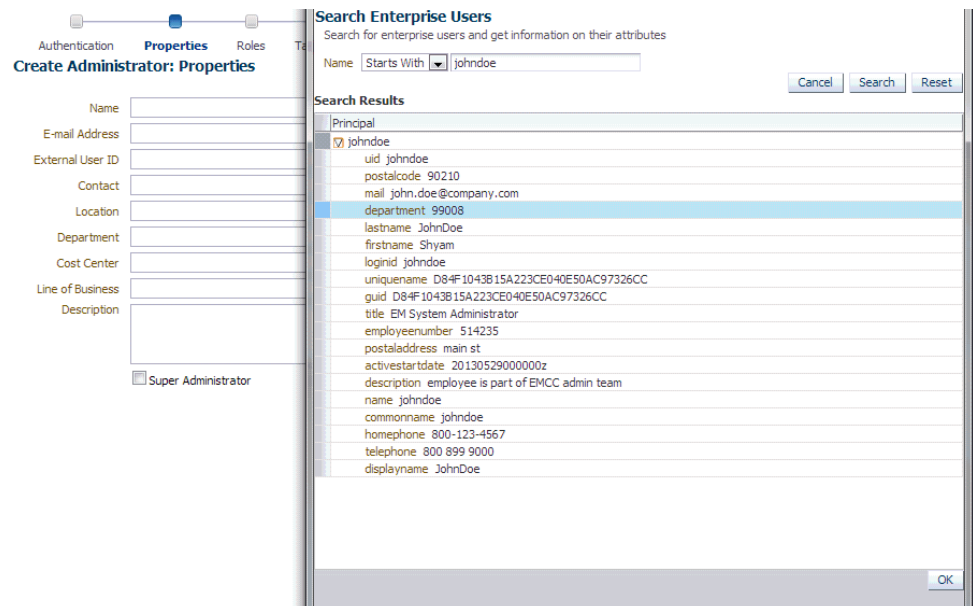
When external authentication is enabled, a flashlight icon appears next to the name field in the *Create User* flow.

 **Note:**

External authentication is enabled when an administrator is first created in Enterprise Manager.

Clicking on the flashlight displays a popup window, giving Enterprise Manager administrators the ability to search for enterprise users in the external LDAP server (for example AD/OID) that have been configured. The user's LDAP attributes are shown as well. This helps the Enterprise Manager administrator to verify external user's attributes before creating them in Enterprise Manager. The screen shot below gives an example of the popup with external LDAP user 'johndoe' and all his LDAP account attributes displayed.

Figure 2-1 User Account Attributes



When external authentication has been configured, it is often desirable to automatically propagate user information such as email address, department, that is defined for the user in LDAP to the corresponding Enterprise Manager user account. This can be done by setting the OMS property `oracle.sysman.core.security.auth.Idapuserattributes_emuserattributes_mappings`. This property will contain the mapping between the Enterprise Manager user properties and the corresponding LDAP user attributes that will be used to populate the user properties. The mapping between an Enterprise Manager property and an LDAP attribute is expressed in the format `<key>={%attribute%}` where:

- **key** - An Enterprise Manager user property. Values for user properties are:
 USERNAME
 EMAIL
 CONTACT
 LOCATION
 DEPARTMENT
 COSTCENTER
 LINEOFBUSINESS
 DESCRIPTION
 Any other values specified for keys will be ignored.
- **attribute** - A user attribute that needs to be fetched from LDAP and is used to set the properties of the user in Enterprise Manager. The attribute should be specified using the following format `{%attribute%}`, for example `{%mail%}`

The value between % should be a valid attribute in the LDAP server. You can also specify literal strings when specifying attribute values, for example:

```
DESCRIPTION={%firstname% %lastname% employee}
```

In this example, only *firstname* and *lastname* will be fetched from LDAP but the description for the user will be "firstname lastname employee". For example, "John Doe employee".

Another example is `CONTACT={telephone number %phone%}`. If a comma needs to be specified in the literal string value, it needs to be escaped with "\". For example,

```
DESCRIPTION={%lastname% \, %firstname% \, %phone%}
```

This will result in a user with description "Doe, John, 212-454-0000". The other characters that need to be escaped with backslash (\), if specified in the literal string, are ':' and '=', so they should be entered as \: or \=.

The OMS property

`oracle.sysman.core.security.auth.ldapuserattributes_emuserattributes_mappings` should thus be set to a set of comma separated key-attribute pairs.

As an example, let us assume user JOHNDOE exists in LDAP and has the following attributes:

```
uid=johndoe,mail=johndoe@company.com,description=EM LDAP
Admin,postalcode=90210,department=EnterpriseAdmin,telephone=2124540000,displayName=JohnDoe
```

If you set OMS property:

```
oracle.sysman.core.security.auth.ldapuserattributes_emuserattributes_mappings to
"USERNAME={%uid%},EMAIL={%mail%},CONTACT={%telephone%},DEPARTMENT={%department
%},DESCRIPTION={%description%},LOCATION={%postalcode%}"
```

then when you select the user from the popup window and hit Ok, the user's attributes are automatically populated in the appropriate fields of the 'Create User' page.

2.1.9 Changing User Display Names in Enterprise Manager

In some LDAP environments, users may have numeric login IDs. Enterprise Manager has the ability to display user-friendly username in when a user logs in using a numeric ID. When they log on to the Enterprise Manager console, the numeric ID is displayed and used everywhere the user's name is shown including audit records. In order to show a more user-friendly name, you can use the OMS property `oracle.sysman.core.security.auth.enable_username_mapping` to enable the mapping of an external, more intuitive name than the name shown in Enterprise Manager. You can use `emctl` to change this property.

```
emctl set property -name "oracle.sysman.core.security.auth.enable_username_mapping" -
value "true"
```

You can also set this using the Enterprise Manager console as well. These are dynamic properties and do not require bouncing the Management Service.

Once enabled, an External User ID field will be added that will contain the name or ID used by the user to log on to Enterprise Manager (this name/ID exists as a valid user in LDAP). The Create Administrator page appears.

For example, if external user 123456 wants to log in and johndoe needs to be shown as logged in user, specify 'johndoe' in the Name field. The Create Administrator page will appear as follows:

User 123456 will still log in as that ID as that user exists in the LDAP server as 123456 but the name 'johndoe' will be shown as his user name in the Enterprise Manager console.

The OMS property

`oracle.sysman.core.security.auth.ldapuserattributes_emuserattributes_mappings` can also be used in this environment to automatically populate the user's name and external ID. An extra field called EXTERNALUSERID needs to be set. Using the example above, set the OMS property to the following:

```
"USERNAME={%displayname%},EXTERNALUSERID={%uid%},EMAIL={%mail%},CONTACT="{%telephone%},DEPARTMENT={%department%},DESCRIPTION={%description%},LOCATION={%postalcode%}"
```

The features described above are available in EM CLI as well. With the OMS properties set, the EM CLI `create_user verb` can be used to create users with their LDAP attributes automatically populated.

2.1.10 Configuring Other LDAP/SSO Providers

Oracle Enterprise Manager currently offers native support for Oracle Internet Directory, Oracle Access Manager, Active Directory and Single Sign-On. Native support allows WebLogic Server and Enterprise Manager to be configured for external authentication using the EMCTL command. For more information on configuring Enterprise with Oracle Internet Directory, see "[Oracle Internet Directory \(OID\)](#)", with Active Directory see "[Microsoft Active Directory Based Authentication](#)".

LDAP providers need to be marked 'SUFFICIENT' and should be ahead of the Enterprise Manager Repository authenticator in the list of providers.

For SSO providers, please refer to the requirements of the specific SSO provider configuration. Along with configuring the appropriate authentication providers, certain OMS properties have to be set as well in order for Enterprise Manager to work.

For configuring Enterprise Manager with any other type of LDAP server, the following OMS properties need to be set. You can use `emctl` or the console to set these properties. The properties need to be set for each OMS.

```
emctl set property -name
"oracle.sysman.core.security.auth.is_external_authentication_enabled" -value
"true"
```

- `oracle.sysman.core.security.auth.is_external_authentication_enabled=true.`
- `oracle.sysman.emSDK.sec.DirectoryAuthenticationType` to LDAP

For configuring Enterprise Manager with any other type of SSO solution, along with configuring the weblogic authentication/identity assertion providers, the following OMS properties need to be set.

- `oracle.sysman.core.security.auth.is_external_authentication_enabled=true`
- `oracle.sysman.core.security.sso.type=OTHERSSO`
- `oracle.sysman.core.security.sso.logout_url=<whatever value was provided for configuring logout on SSO server>`
- `oracle.sysman.emSDK.sec.DirectoryAuthenticationType=SSO`

2.1.10.1 Configuring Single Sign-on based Authentication

This section covers the following topics:

- [Configuring Single-Sign-on with Oracle Access Manager 10g](#)
- [Configuring Single-Sign-on with Oracle AS SSO 10g](#)

2.1.10.1.1 Configuring Single-Sign-on with Oracle Access Manager 10g

When using an Oracle Access Manager Single Sign-On authentication scheme, the underlying identity stores will consist of Enterprise Directory Identity Stores supported by Oracle Access Manager. This section provides instructions on how to configure OAM SSO-based authentication schemes.

Prerequisites

Oracle Access Manager is installed.

The Oracle Access Manager Single Sign-On server is configured with Oracle HTTP server, Web Gate, and the Oracle Access Manager Identity Store.

1. Run the `emctl config auth` command.

```
emctl config auth oam [-sysman_pwd <pwd>] -oid_host <host> -oid_port <port>
-oid_principal <principal> [-oid_credential <credential>]
-user_base_dn <dn> -group_base_dn <dn>
-oam_host <host> -oam_port <port> [-logout_url <url>] [-is_oam10g] [-user_dn
<dn>] [-group_dn <dn>]
```

Note: Use the `-is_oam10g` option only if the OAM version is 10g.

2. Stop each OMS.

```
emctl stop oms -all
```

3. Restart each OMS.

```
emctl start oms
```

2.1.10.1.2 Configuring Single-Sign-on with Oracle AS SSO 10g

If you are currently using Oracle Application Server Single Sign-On to control access and authorization for your enterprise, you can extend those capabilities to the Enterprise Manager console.

By default, Enterprise Manager displays the main logon page. However, you can configure Enterprise Manager so it uses Oracle Application Server Single Sign-On to

authenticate your Enterprise Manager users. Instead of seeing the Enterprise Manager logon page, users will see the standard Oracle Application Server Single Sign-On logon page. From the logon page, administrators can use their Oracle Application Server Single Sign-On credentials to access the Oracle Enterprise Manager 13c Cloud Control console.

 **Note:**

- You can configure Enterprise Manager to use one of the default Oracle Application Server Single Sign-On or Enterprise User Security features, but not both.
- When Enterprise Manager is configured to use Single Sign-On with Server Load Balancer (SLB), make sure that the correct monitoring settings have been defined.

Partner applications are applications that are designed to delegate authentication to the OracleAS Single Sign-On server. The following sections describe how to configure Enterprise Manager as an OracleAS Single Sign-On Partner Application:

- [Registering Enterprise Manager as a Partner Application](#)
- [Removing Single Sign-On Configuration](#)
- [Registering Single Sign-On Users as Enterprise Manager Administrators](#)
- [Registering Single Sign-On Users Using EM CLI](#)
- [Bypassing the Single Sign-On Logon Page](#)
- [Restoring the Default Authentication Method](#)

2.1.10.1.2.1 Registering Enterprise Manager as a Partner Application

To register Enterprise Manager as a partner application manually, follow these steps:

1. Stop all OMSs by running `emctl stop oms` on each OMS.
2. Enter the following URL to navigate to the SSO Administration page.
`https://sso_host:sso_port/pls/orasso`
3. Log in as `orcladmin` user and click on **SSO Server Administration**.
4. Click **Administer Partner Applications** and then click **Add Partner Application**.
5. Enter the following information on the Add Partner Application page.

```
Name: <EMPartnerName>
Home URL: protocol://em_host:em_port
Success URL: protocol://em_host:em_port/osso_login_success
Logout URL: protocol://em_host:em_port/osso_logout_success
Administrator Email: user@host.com
```

Note1: `host`, `port`, and `protocol` refer to the Enterprise Manager host, port and the protocol (`http` or `https`) used.

Note2: The `em_host`, `em_port`, `email` and Enterprise Manager Partner Name must be replaced with the appropriate values and not typed as shown in this example.

- Go back to Administer Partner Applications page and click on the **Edit** icon for <EMPartnerName>.

Record the values of ID, Token, Encryption Key, Login URL, Single Sign-Off URL, Home URL and write the following in a file `osso.txt`:

```
sso_server_version= v1.2
cipher_key=<value of EncryptionKey>
site_id=<value of ID>
site_token=<value of Token>
login_url=<value of Login URL>
logout_url=<value of Single Sign-Off URL>
cancel_url=<value of Home URL>
sso_timeout_cookie_name=SSO_ID_TIMEOUT
sso_timeout_cookie_key=9E231B3C1A3A808A
```

- Set the `ORACLE_HOME` environment variable to WebTier Oracle Home location.

```
setenv ORACLE_HOME /scratch/13c/MWHome/Oracle_WT
```

Then, run the following:

```
$ORACLE_HOME/ohs/bin/iasobf <location of osso.txt> <location of osso.conf>
```

- Run the following command on each OMS:

```
emctl config auth sso -ossoconf <osso.conf file loc> -dasurl <DAS URL> [-
unsecure] [-sysman_pwd <pwd>] [-domain <domain>]-ldap_host <ldap host> -
ldap_port <ldap port> -ldap_principal <ldap principal> [-ldap_credential <ldap
credential>] -user_base_dn <user base DN> -group_base_dn <group base DN> [-
logout_url <sso logout url>]
```

where `ldap_host`, `ldap_port`, `ldap_principal` and `ldap_credential` are the details of SSO's LDAP.

The sample output for this command is shown below:

```
Oracle Enterprise Manager Cloud Control 13c Release 12.1.0.3.0
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
SSO Configuration done successfully. Please restart Admin & Managed Servers.
```

- Run the following commands on each OMS:

```
emctl stop oms -all
emctl start oms
```

2.1.10.1.2.2 Removing Single Sign-On Configuration

To remove the single sign-on configuration, perform the following:

- Run the following command on each OMS:

```
emctl config auth repos [-sysman_pwd <pwd>]
```

Sample command output:

```
Oracle Enterprise Manager Cloud Control 13c Release 2
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
Configuring Repos Authentication ... Started
Configuring Repos Authentication ... Successful
```

If you have updated files such as, for example, `httpd.conf` (when installing WebGate) or any other required files should be backed up prior in order to rolled

back during this step. If you are using multi-OMS environment, you must execute `emctl config auth repos` on the remaining servers.

2. Bounce all OMSs by issuing the following on each OMS:

```
emctl stop oms -all
emctl start oms
```

2.1.10.1.2.3 Registering Single Sign-On Users as Enterprise Manager Administrators

After you have configured Enterprise Manager to use the Single Sign-On logon page, you can register any Single Sign-On user as an Enterprise Manager administrator. You can register single sign-on users using:

- Enterprise Manager Graphical User Interface
- Enterprise Manager Command Line Interface

2.1.10.1.2.3.1 Registering Single Sign-On Users Using the Graphical User Interface

You can use the graphical user interface to register single sign-on users by following these steps:

1. Go to the Enterprise Manager Console URL.

The browser is redirected to the standard Single Sign-On Logon page.

2. Enter the credentials for a valid Single Sign-On user. Note: This step requires that an SSO user is already registered with Enterprise Manager.

If no SSO user is yet registered as Enterprise Manager user, you can create them using the following procedure:

1. Navigate to Enterprise Manager by connecting to the OMS directly. For example, `https://oms_host:oms_https_port/em`.

2. Log in as a Repository user.

3. From the **Setup** menu, select **Security** then select **Administrator**

4. Create SSO users.

3. Log in to Enterprise Manager as a Super Administrator.

4. From the **Setup** menu, select **Security**, then select **Administrators** to display the Administrators page.

Because Enterprise Manager has been configured to use Single Sign-On, the first page in the Create Administrator wizard now offers you the option of creating an administrator either as an External User or as Repository User.

5. Select **External User Identity Store** and advance to the next page in the wizard.
6. Enter the name and e-mail address of the External User Identity Store user, or click the flashlight icon to search for a user name in the Oracle Internet Directory.
7. Use the rest of the wizard pages to define the roles, system privileges, and other characteristics of the Enterprise Manager administrator and then click **Finish**.

Enterprise Manager displays a summary page that lists the characteristics of the administrator account.

8. Click **Finish** to create the new Enterprise Manager administrator.

The External User Identity Store user is now included in the list of Enterprise Manager administrators. You can now verify the account by logging out of the

Cloud Control console and logging back in using the External User Identity Store user credentials on the Single Sign-On logon page.

2.1.10.1.2.3.2 Registering Single Sign-On Users Using EM CLI

You can use the following EM CLI command to create Single Sign-On users:

```
emcli create_user -name=ssouser -type=EXTERNAL_USER
```

This command creates a user with the name **ssouser** who is authenticated against the single sign-on user.

Argument	Description
-name	Name of the administrator.
-type	The type of user. The default value for this parameter is EM_USER. The other possible values are: <ul style="list-style-type: none"> EXTERNAL_USER: Used for single-sign-on based authentication. DB_EXTERNAL_USER: Used for enterprise user based security authentication.
-password	The password for the newly created administrator.
-roles	The list of roles that can be granted to this administrator.
-email	The list of email addresses for this administrator.
-privilege	The system privileges that can be granted to the administrator. This option can be specified more than once.
-profile	The name of the database profile. This is an optional parameter. The default profile used is DEFAULT.
-desc	The description of the user being added.
-expired	This parameter is used to set the password to "expired" status. This is an optional parameter and is set to False by default.
-prevent_change_password	When this parameter is set to True, the user cannot change the password. This is an optional parameter and is set to False by default.
-input_file	This parameter allows the administrator to provide the values for any of these arguments in an input file. The format of value is name_of_argument:file_path_with_file_name.

Example 1

```
emcli create_user
  -name="new_admin"
  -email="first.last@mycompany.com; joe.shmoe@shmoeshop.com"
  -roles="public"
  -privilege="view_job;923470234ABCDFE23018494753091111"
  -privilege="view_target;<host>.com:host"
```

This example creates an Enterprise Manager administrator named `new_admin`. This administrator has two privileges: the ability to view the job with ID `923470234ABCDFE23018494753091111` and the ability to view the target `<host>.com:host`. The administrator `new_admin` is granted the PUBLIC role.

Example 2

```
emcli create_user
-name="User1"
-type="EXTERNAL_USER"
-input_file="privilege:/home/user1/priv_file"

Contents of priv_file are:
view_target;<host>.com:host
```

This example makes `user1` which has been created externally as an Enterprise Manager user. `user1` will have view privileges on `<host>.com:host`.

Example 3

```
emcli create_user
-name="User1"
-desc="This is temp hire."
-prevent_change_password="true"
-profile="MGMT_ADMIN_USER_PROFILE"
```

This example sets `user1` as an Enterprise Manager user with some description. The `prevent_change_password` is set to `true` to indicate that the password cannot be changed by `user1` and the profile is set to `MGMT_ADMIN_USER_PROFILE`.

Example 4

```
emcli create_user
-name="User1"
-desc="This is temp hire."
-expire="true"
```

This example sets `user1` as an Enterprise Manager with some description. Since the password is set to expire immediately, when the user logs in for the first time, he is prompted to change the password.

2.1.10.1.2.4 Bypassing the Single Sign-On Logon Page

If the OMS is configured with SSO or OAM or some other authentication method, you may want to by-pass the Single Sign-On or OAM authentication under certain circumstances. To bypass the SSO logon page, connect to the following URL:

1. Connect to `https://ms_host:ms_https_port/em`

`ms_host` & `ms_https_port` are WLS-managed server's hostname & port#. These parameters can be found in the `EM_INSTANCE_HOME/emgc.properties` file. They are listed as `EM_INSTANCE_HOST` & `MS_HTTPS_PORT` in this file.

2. Log in using a repository user's credentials.

2.1.10.1.2.5 Restoring the Default Authentication Method

1. Run the following command on each OMS:

```
emctl config auth repos [-sysman_pwd <pwd>]
```

Sample command output:

```
Oracle Enterprise Manager Cloud Control 13c Release 2
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
Configuring Repos Authentication ... Started
Configuring Repos Authentication ... Successful
If you have updated files like httpd.conf (for example, while installing
```

WebGate), rollback them.

If this is a multi-OMS environment, execute this command on remaining servers.
After that, restart OMS(s) using: 'emctl stop oms -all' and 'emctl start oms'

2. Run the following commands on each OMS:

```
emctl stop oms -all  
emctl start oms
```

2.1.11 Configuring Enterprise User Security based Authentication

For instructions on configuring Enterprise Manager for use with Enterprise User Security, see "[Enterprise User Security Based Authentication](#)".

2.1.12 Restoring to the Default Authentication Method

The following sections provide instructions on restoring the default authentication method used by Enterprise Manager.

2.1.12.1 Bypassing the Single Sign-On Logon Page

If the OMS is configured with SSO or OAM or some other authentication method, you may want to by-pass the Single Sign-On or OAM authentication under certain circumstances. To bypass the SSO logon page, connect to the following URL:

1. Connect to `https://ms_host:ms_https_port/em`

`ms_host` & `ms_https_port` are WLS-managed server's hostname & port#. These parameters can be found in the `EM_INSTANCE_HOME/emgc.properties` file. They are listed as `EM_INSTANCE_HOST` & `MS_HTTPS_PORT` in this file.

2. Log in using a repository user's credentials.

2.1.12.2 Restoring the Default Authentication Method

1. Run the following command on each OMS:

```
emctl config auth repos [-sysman_pwd <pwd>]
```

Sample command output:

```
Oracle Enterprise Manager Cloud Control 13c Release 2  
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.  
Configuring Repos Authentication ... Started  
Configuring Repos Authentication ... Successful  
If you have updated files like httpd.conf (for example, while installing  
WebGate), rollback them.  
If this is a multi-OMS environment, execute this command on remaining servers.  
After that, restart OMS(s) using: 'emctl stop oms -all' and 'emctl start oms'
```

2. Run the following commands on each OMS:

```
emctl stop oms -all  
emctl start oms
```

2.2 Configuring Privileges and Role Authorization

Giving the same level of access to all targets to all administrators is dangerous. Also, individually granting access to tens, hundreds, or even thousands of targets to every

new member of the group is time consuming. With Enterprise Manager's administrator privileges and roles feature, these tasks can be streamlined and can easily scale as the enterprise grows. Authorization controls the access to the secure resources managed by Enterprise Manager via system, target, and object level privileges and roles. This section describes Enterprise Manager's Authorization model including roles and privileges assigned to each user class.

 **Note:**

An administrator without any privileges or assigned targets should not be able to see monitored targets from within Enterprise Manager. When logging in to Enterprise Manager as a new administrator without any roles or privileges assigned, all targets will be displayed (security issue) unless the EXEMPT ACCESS POLICY privilege is revoked for the Enterprise Manager Super Administrator SYSMAN.

The system privilege EXEMPT ACCESS POLICY allows a user to be exempted from all fine-grained access control policies on any SELECT or DML operation (INSERT, UPDATE, and DELETE). This provides ease of use for administrative activities such as installation and import and export of the database through a non-SYS schema.

Also, regardless of the utility or application that is being used, if a user is granted the EXEMPT ACCESS POLICY privilege, then the user is exempt from VPD and Oracle Label Security policy enforcement. That is, the user will not have any VPD or Oracle Label Security policies applied to their data access.

To resolve the issue:

Connect to the Enterprise Manager Repository database as SYS or SYSTEM user and execute the following SQL statement:

```
SQL> revoke EXEMPT ACCESS POLICY from sysman;
```

2.2.1 Understanding Users, Privileges, and Roles

When an Enterprise Manager administrator adds a user to the system, the primary consideration must be what does this person need to do in order to perform his job? Once the job for this new user is defined and understood, appropriate privileges must be assigned to this user and access granted to the required systems required to complete the job.

Privileges are ultimately granted to administrators to enable them to manage targets in Enterprise Manager. While you can grant specific privileges to individual administrators, tracking and granting privileges on many targets across many administrators easily becomes error-prone and an administrative burden in itself. Our recommendation is to define and use roles to manage the granting of privileges to administrators.

A role is a user-defined set of privileges typically containing the set of privileges that you want to grant to a team of users. A role can contain other roles as well. For example, you can create a First Line Support role containing the privileges needed for the administrators to view and manage incidents on targets. Once this role is created,

you can grant this role to the appropriate administrators who will manage these incidents as part of their job responsibility. If you need to change the set of privileges for your administrators, e.g. add new privileges or remove privileges, then all you need to do is update the role. The updated set of privileges in the role is automatically enabled for the administrators to whom the role has been granted. Likewise if new administrators are added, all you need to do is grant them the appropriate role(s) instead of granting them individual privileges. See "[Classes of Users](#)" for more information.

Using roles is one big step towards managing privileges. However, there is still the challenge of having to keep the role updated with privileges on new targets as they are added to Enterprise Manager.

2.2.1.1 Classes of Users

Oracle Enterprise Manager supports different classes of Oracle users, depending upon the environment you are managing and the context in which you are using Oracle Enterprise Manager.

The Enterprise Manager administrators you create and manage in the Enterprise Manager console are granted privileges and roles to log in to the Enterprise Manager console and to manage specific target types and to perform specific management tasks. The default super administrator for the Enterprise Manager console is the SYSMAN user, which is a database user associated with the Oracle Management Repository. You define the password for the SYSMAN account during the Enterprise Manager installation procedure.

By restricting access to privileged users and providing tools to secure communications between Oracle Enterprise Manager 13c components, Enterprise Manager protects critical information in the Oracle Management Repository.

The Management Repository contains management data that Enterprise Manager uses to help you monitor the performance and availability of your entire enterprise. This data provides you with information about the types of hardware and software you have deployed, as well as the historical performance and specific characteristics of the applications, databases, applications servers, and other targets that you manage. The Management Repository also contains information about the Enterprise Manager administrators who have the privileges to access the management data.

You can create and manage Enterprise Manager administrator accounts. Each administrator account includes its own login credentials, as well as a set of roles and privileges that are assigned to the account. There are three classes of users:

- **Super Administrator:** Super Administrators are users having Super Administrator privilege. Users with this privilege are powerful users who can create/edit/delete users/roles. They can manage all the resources in the system with the following restrictions:

- Do not have access to Named credentials created by other users - Cannot manage jobs, deployment procedures created by other users.

The Super Administrator, SYSMAN is created by default when Enterprise Manager is installed. The Super Administrator can create other administrator accounts.

- **Administrator:** Regular Enterprise Manager administrator.
- **Repository Owner:** Database administrator for the Management Repository. This account cannot be modified, duplicated, or deleted.

The types of management tasks that the administrator can perform and targets that he can access depends on the roles, system privileges, resource privileges, and target privileges that he is granted. The Super Administrator can choose to let certain administrators perform only certain management tasks, or access only certain targets, or perform certain management tasks on certain targets. In this way, the Super Administrator can assign the minimum level of privileges that administrators need to do their job.

2.2.1.2 Reassigning Objects

To reassign objects from one Enterprise Manager administrator to another in preparation for deleting an administrator:

1. Navigate to the Setup > Security > Administrators page.e.
2. Select the administrator to be deleted, then click **View** to see all objects currently owned by the selected administrator.
3. To reassign the objects to another administrator, enter the name of the new administrator in the New Owner text box, or click the flashlight icon to view a list of available administrators.
4. Choose the desired Administrator to whom the objects must be reassigned then complete the operation.

Note:

A super administrator can use the Delete Administrator page to specify what happens to administrator-owned objects when removing an administrator from Enterprise Manager. On this page, a super administrator can:

- Delete all administrator-owned objects along with the Enterprise Manager administrator
- Reassign objects to another Enterprise Manager administrator

Note:

Only a Super Administrator can delete other Enterprise Manager administrators. Enterprise Manager will not allow administrators to:

- Delete themselves
- Delete the Management Repository owner

Administrator object reassignments can be handled as follows:

- Blackouts can be reassigned to any user who has OPERATOR privileges on all targets affected by the blackout.
- Jobs can be reassigned to any administrator. However, ALL credentials associated with the job will be removed, leaving the job in a Suspended state. This requires the new job owner to explicitly set new credentials. Currently running jobs

are allowed to continue running. After the new job owner sets the credentials, the job will revert to a SCHEDULED state.

- Corrective Actions can be reassigned to any administrator who has OPERATOR privileges for targets on which the corrective action can operate.
- Report Definitions can be reassigned to any administrator.
- Reports can be reassigned to any administrator.
- BIP Reports can not be reassigned. Only Information Publisher reports can be reassigned.
- Monitoring Templates can be reassigned to any administrator.

2.2.1.3 Aggregate Target Privileges

An Aggregate Target type is a target that has one or more member targets, for example groups, systems, or Real Application Cluster. Aggregate target privileges allows an Administrator to grant different levels of privileges to the member targets and to the Aggregate target. For example, an Administrator may want to grant VIEW privilege on the aggregate group level and FULL to each member target within the group. If the administrator does not grant specific privileges on the aggregate and its members, the default is the same privilege for the aggregate and its members.

For example, you can grant VIEW privilege at a group (Aggregate level) and FULL at the member target level. This allows a DBA granted FULL on a member target to perform full life cycle tasks including delete of the target. The DBA has VIEW privilege on the group, preventing him from deleting the group.

You can view/modify these privilege settings when creating or editing an Enterprise Manager administrator. From the **Setup** menu, select **Security**, and then select **Administrators**. Navigate to the Target Privilege page.

At the bottom of the Target Privileges page, you will find the Target Privileges region.

Check the **Advanced Privilege Settings** option to view settings for the aggregate target types that have been added to the user.

Two additional columns are displayed:

- Manage Aggregate Only Privilege Grants
- Manage Member Only Privilege Grants

Click the **Edit** (pencil) icon to change the privilege grant properties.

2.2.2 Privileges and Roles

Granting users specific privileges provide a basic level of security in Enterprise Manager. They are designed to control access to data and limit the management operations you can perform in Enterprise Manager such as changing monitoring settings or patching targets.

When Enterprise Manager is installed, the SYSMAN user (Super Administrator) is created by default. The SYSMAN Super Administrator can then create other administrator accounts for daily administration work. The SYSMAN account should only be used to perform infrequent system-wide, global configuration tasks.

The Super Administrator should grant the minimum level of privileges required to allow administrators to perform their tasks within Enterprise Manager. For example, the Super Administrator can allow some administrators to view any target and to add any target in the enterprise and other administrators to only perform specific operations such as maintaining and cloning on a target for which they are responsible.

2.2.2.1 Administrators and Database Privileges

Having DBA privileges on a database allows users to delete other database users, drop tables and perform other administrative operations. Hence, having DBA privileges on a repository database allows an administrator to perform all operations that can be performed as an Enterprise Manager Super Administrator: The administrator is implicitly treated as a Super Administrator. This is similar to OS authentication supported by the database where OS users with "DBA" privileges can connect to the Oracle server and exercise SYSDBA privileges.

If this level of access is not the intended behavior, Oracle recommends using one of the following:

- The Enterprise Manager repository database needs to be considered as a special database. Do not grant DBA privileges to any users on that database other than to users who have Super Administrator privileges in Enterprise Manager.
- Set up external authentication and migrate Enterprise Manager users to Active Directory or LDAP. This ensures that there are no *shadow* database users for Enterprise Manager application users being created and so DBA privileges cannot be granted to Enterprise Manager users.

Note:

Enterprise Manager administrators should not be given DBA privileges.

In situations where an Enterprise Manager Super Administrator has DBA privileges, SYSMAN will NOT be able to convert that user into a regular (non-Super Administrator) administrator until DBA privileges have been removed.

2.2.2.2 Granting Privileges

A privilege is a right to perform management actions within Enterprise Manager. Privileges can be divided into two categories:

- Target Privileges
- Resource Privileges

Target Privileges: These privileges allow an administrator to perform operations on a target. As such, there is a defined hierarchy that categorizes target privileges into the following levels:

- FULL: Highest level that includes OPERATOR and VIEW
- OPERATOR: Medium level that permits specific management actions. OPERATOR privilege is also an example of a privilege that can include other privileges. For example, OPERATOR privileges include blackout privileges, and

any user granted an OPERATOR target privilege is automatically granted the Blackout Target privilege. See [Table 3](#) for more information.

- VIEW: Lowest level permitting only view access to targets.

There are two categories of target privileges:

- Privileges applicable to all targets. These privileges allow administrators to perform operations on all components with the Enterprise Manager infrastructure.
- Privileges applicable to a specific target instance. These privileges allow Administrators to perform operations on specific targets in the Enterprise Manager infrastructure.

The Target Privileges page shows a list of privileges granted to all targets. For a detailed list of target privileges, see [Privileges](#).

Resource Privileges: These privileges grant administrator access to a specific functionality within Enterprise Manager. Examples of resource privileges include Backup Configurations, Cloud Policy, Compliance Framework, Enterprise Manager Plug-in, Job System, Patch Plan, Self Update and Template Collection. For a complete list refer to the Privileges and Roles section of Oracle Enterprise Manager Cloud Control Security Guide.

For example, to grant an administrator the ability to create new named credentials:

1. From the **Setup** menu, select **Security** and then **Administrators**. The *Administrators* page displays.
2. Either edit an existing administrator or create a new administrator to access the *Administrator* wizard.
3. Proceed to the **Resource Privileges** page.
4. From the *Resource Type* column, scroll down to **Named Credential**.
5. From the *Manage Privilege Grants* column, click on the corresponding pencil icon. The *Resource Type Privileges* page displays.
6. Select the privilege **Create new named credential** and click **Continue** to proceed with the administrator creation/edit processes

2.2.2.3 Fine-grained Access Control

Enterprise Manager implements granular privileges to control access to targets and other resources, enabling administrators to better segregate their duties. For example, consider the provisioning designer and provisioning operator job responsibilities. The former has greater responsibilities (creates components in the Software Library) than the latter (submits deployments). From the Security Console, you can view:

- The list of super administrators
- Administrators with highest number of direct privileges
- Target privileges
- Resource privileges
- The top five Administrators with the highest number of roles
- Roles with the highest number of nested roles

2.2.2.4 Creating Roles

A role is a collection of Enterprise Manager resource privileges, or target privileges, or both, which you can grant to administrators or to other roles. These roles can be based upon geographic location (for example, a role for Canadian administrators to manage Canadian systems), line of business (for example, a role for administrators of the human resource systems or the sales systems), or any other model.

Administrators do not want to perform the task of individually granting access to tens, hundreds, or even thousands of targets to every new member of their group. By creating roles, an administrator needs only to assign the role that includes all the appropriate privileges to his team members instead of having to grant many individual privileges. He can divide workload among his administrators by filtering target access, or filtering access to management tasks, or both. You can also configure Enterprise Manager to work with an external authentication provider to manage authorization as well by using external roles. For more information, see "[External Authorization using External Roles](#)".

Out-of-Box Roles: Enterprise Manager Cloud Control 13c comes with predefined roles to manage a wide variety of resource and target types. The following table lists some of the roles along with their function. The number and type of roles displayed depend on the number and type of installed plug-ins. For a complete list of out-of-box roles, see [Out-of-Box Roles](#).

Public Roles: Enterprise Manager creates one role by default called **Public**. This role is unique in that it is automatically assigned to all new non-super administrators when they are created. By default it has no privileges assigned to it. The Public role should be used to define default privileges you expect to assign to a majority of non-super administrators you create. Privileges need not be assigned to Public initially - they can be added at any time. The role may be deleted if your enterprise does not wish to use it. If deleted, it can be added back in later if you later decide to implement it.

2.2.2.5 Private Roles

Private Roles are a new role type introduced in Enterprise Manager Release 12.1.0.4 and are used to control the granting of sensitive/powerful privileges to administrators or roles. There are certain sensitive privileges which Enterprise Manager does not make available to Super Administrators. Specifically, they are:

- LAUNCH_DP
- FULL_DP
- GET_CREDENTIAL
- EDIT_CREDENTIAL
- FULL_CREDENTIAL
- FULL_JOB

These privileges are particularly sensitive and powerful, which is the reason Enterprise Manager does not grant these privileges to roles. Granting these privileges to roles would also make them available to other Administrators.

To accommodate the granting of these types of privileges in a more secure manner, roles are divided into two categories - system roles and private roles.

- Private roles are managed by administrators with the "create_role" privilege. Administrators granted the "create_role" privilege (Private Role) will maintain the lifecycle of the named credential and job roles, and will allow an administrator to grant these *full job* and *full credential* privileges to other administrators and to roles.
- System roles define all roles accessible to all Administrators with the "manage_system_role" privilege.

A private role can be granted to other administrators and roles via the Enterprise Manager console and EM CLI using the `emcli create_role verb`, and made grantable via `emcli grant_privs verb`.

Example 1:

```
emcli create_role
  -name="my_private_role"
  -type="EM_ROLE"
  -desc="This is a new private role called my_private_role"
  -roles="role1;role2;role3"
  -privilege="full_job;923470234ABCDFE23018494753091111"
  -privilege="FULL_CREDENTIAL;CRED_NAME=cred1:CRED_OWNER=user2"
  -users="USER1;USER2:WITH_ADMIN"
  -private_role[ Optional ]
```

This will create *my_private_role* owned by the logged-in user.

USER1 will be granted this role as WITHOUT_ADMIN option and USER2 will be granted this role as WITH_ADMIN option.

This role will consists FULL_JOB and FULL_CREDENTIAL privileges on respective objects.

The owner of a private role can grant this role to an administrator, and can specify if the other administrator has the right to further grant this private role to another administrator (by using the `-WITH_ADMIN` option) or to another private role. In effect, the role owner is privately administering access to this role, hence the name "private role." A system role can be granted to a private role, but a private role cannot be granted to a system role.

Verbs where the `-WITH_ADMIN` option is supported:

`create_role -users`

`modify_role -users`

`create_user -roles`

`modify_user -roles`

`grant_roles -roles`

2.2.2.6 Using Roles to Manage Privileges

Privileges are ultimately granted to administrators to enable them to manage targets in Enterprise Manager. While you can grant specific privileges to individual administrators, tracking and granting privileges on many targets across many administrators easily becomes error-prone and an administrative burden in itself. Our recommendation is to define and use roles to manage the granting of privileges to administrators. A role is a user-defined set of privileges typically containing the set of

privileges that you want to grant to a team of users. A role can contain other roles as well. For example, you can create a First Line Support role containing the privileges needed for the administrators to view and manage incidents on targets. Once this role is created, you can grant this role to the appropriate administrators who will manage these incidents as part of their job responsibility. If you need to change the set of privileges for your administrators, e.g. add new privileges or remove privileges, then all you need to do is update the role. The updated set of privileges in the role is automatically enabled for the administrators to whom the role has been granted. Likewise if new administrators are added, all you need to do is grant them the appropriate role(s) instead of granting them individual privileges.

Using roles is one big step towards managing privileges. However, there is still the challenge of having to keep the role updated with privileges on new targets as they are added to Enterprise Manager. Privilege-propagating groups are meant to address this challenge and will be discussed next.

2.2.3 Managing Privileges with Privilege Propagating Groups

To manage the granting of privileges across potentially hundreds or thousands of targets to a large set of administrators, use privilege propagating groups in conjunction with roles. A group is a user-defined collection of targets that you can create in order to manage and monitor the targets collectively as a unit. A privilege propagating group is a special type of group where a privilege that is granted on the group to a user automatically gives him that same privilege to all existing and new members of the group.

Leverage the privilege-propagating nature of Administration Groups

Enterprise Manager administration groups are privilege-propagating in nature. This means that a privilege on the administration group that is granted to a user or a role automatically *propagates* to all members of the group including any subgroups. If a new target is added to an administration group, then because the administration group is privilege-propagating, the user or role that has privileges on the administration group automatically gets privileges on the newly added target by virtue of it joining the group. No additional work is needed for granting privileges on the new target. Thus granting target privileges is much simpler because all you need to do is a one-time setup of granting privileges on the group to a role.

Create Roles for Different Job Responsibilities

After you have planned the various job responsibilities and mapped these to the corresponding privileges in Enterprise Manager, the next step is to create roles in Enterprise Manager containing privileges required for each job responsibility. In our example below, here are the various roles that need to be created for each job responsibility. Note that when it comes to privileges on targets in the administration group, the recommendation is to grant the privilege on the administration group and not on individual targets in order to leverage the privilege propagating nature of administration groups.

Table 2-1 EXAMPLES OF ROLES YOU CAN CREATE FOR DIFFERENT JOB RESPONSIBILITIES*

JOB RESPONSIBILITY	ROLE IN ENTERPRISE MANAGER	PRIVILEGES IN THE ROLE (MINIMUM SET)
Group Administrator Responsible for defining group membership and for granting privileges on the group to other administrators.	GROUP_ADMIN_ROLE	Group Administration on the group
Senior Administrator Responsible for adding and removing targets in Enterprise Manager, and for planning and setting up monitoring settings for targets. He is also responsible for setting up rules related to creating incidents for events and sending notifications.	SENIOR_ADMIN_ROLE	Add Any Target Create Enterprise Rule Set Operator on the group Create on Job System EM_TC_DESIGNER role
Target Owner For the targets he owns, he is responsible for setting monitoring settings, responding to events/incidents, and for performing maintenance operations	TARGET_OWNER_ROLE	Operator on the Administration Group(s) that he is managing Create on Job System View Any Monitoring Template View on the Template Collection(s) associated with the group(s) he is managing
First Level Support Responsible for responding to events/incidents on targets. As part of operational procedures, he is allowed to blackout a target that is down.	FIRST_LEVEL_SUPPORT	Manage Target Events on the appropriate Administration Group(s) Blackout Target on the appropriate Administration Group(s)

The privileges listed in the table represent the minimum set of privileges in the role. Additional privileges can be added based on other responsibilities. Also note that you will need to have Super Administrator privileges to create roles. Once roles have been defined, you can now grant these roles to your Enterprise Manager administrators. This can be done in several ways:

- Assign roles while creating/editing an Enterprise Manager administrator.
- As part of creating/editing a role, you to choose administrators to whom you would like to grant the role.
- When creating/editing administrators using the Enterprise Manager Command Line tool (EM CLI), you can specify the roles granted to the user. You can also use EM CLI to grant roles directly to an existing user.

As an example, say you want to grant Operator privileges on host targets used by the development team to all members of the development team. You can first create a privilege propagating group (Devt-Group) containing the relevant host targets. Then create a role (Devt-Role) and in this role include Operator privileges on Devt-Group. Finally grant the Devt-Role to all members of the development team. This will result in providing all members of the development team Operator privileges on all targets in

Devt-Group. As new host targets are added, you can simply add these new targets to Devt-Group and all members of the development team automatically obtain Operator privileges on the newly added targets. The following scenarios provide additional examples of using privilege propagating groups with roles.

We shall step through two use cases which outline when best to use privilege propagating groups, how to create target groups, add member to this group, and assign roles and Administrators to these target groups.

2.2.3.1 Example1: Granting various teams different levels of access to target groups

Consider a collection of Database Instances and WebLogic Servers within an organization are managed by separate teams within the organization. Both teams are using Enterprise Manager to manage their targets. The DBAs want full access privileges to their Database Instances and view privileges on the WebLogic Servers. Similarly, the WebLogic Server administrators want full privileges on the WebLogic Servers and view privileges on the Database Instances.

To manage privileges across the two teams, first create two privilege propagating groups containing the targets of the respective teams. For example, you can create a target group called DBAGroup containing the database Instances and another target group called WLSGroup containing the Oracle WebLogic Servers. DBAGroup contains the Database Instances that can be modified and managed by DBAs. While the WLSGroup is a group of Web Logic Servers modified and managed by the Web Logic Server administrators. Additionally, the DBAs want to view the Web Logic Server targets and the Web Logic Server technicians want to view the Database Instances. The following steps will show how to set up these target groups, privileges and roles, and how to grant the appropriate roles to the correct Administrator.

Here are the steps to follow:

1. Create a target group. On the console go to Targets->Groups from the drop down menu.
2. Click "Create" from the menu and select "Group" from the drop down menu.
3. Enter the name DBAGroup.
Enable "Privilege Propagation" group, by checking the box. This allows Administrators to do a one-time grant of privileges on a group to a user and that privilege will automatically be propagated (or applied) to each member of that group.
4. Add the database targets you want to add to the new database group, DBAGroup. This is done by hitting the "Add" button, selecting the Database Instance targets from the list. Click the "Select" button.
5. Select "OK".
6. Your new group, DBAGroup, should be displayed in the list of available groups.
7. Now create a second privilege propagating group, by repeating the steps 1-6, calling it WLSGroup, and adding the appropriate WebLogic Server targets to this group.
8. Your second group, WLSGroup, should be displayed in the list of available groups.
9. Next, create the Roles. A role contains privileges that can be granted to an administrator. Proceed to the Roles page. Go to the Setup->Security->Roles page.

10. Click **Create**.
11. On the Properties page, type the name of your role. In this example we have named it DBA-ROLE. This Role will contain privileges for the DBA team. It will contain Full privilege on all database Instances in the DBAGroup and view privilege on all Web Logic Server Instances in the WLSGroup. Click the "Next" button.
12. On the Roles page, click **Next**.
13. On the "Target Privileges" page, scroll down to the "Target Privileges" section, at the bottom of the page. Click the "Add" button. The list of available targets is displayed. Select the "Group" Target Type, to improve the search. Select the two groups we just created, DBAGroup and WLSGroup.
14. Our two groups will be displayed. For this role, DBA-ROLE, we want to grant "Full" on all databases in the DBAGroup and grant "View" on all WebLogic server targets in the WLSGroup. As the default privilege is "View" we need only modify the DBAGroup privilege for this Role, leaving the WLSGroup, with the default "View" privilege. This is done by selecting the pencil icon, to the right of "View" in the "Manage Target Privilege Grants" column. Click the "Continue" button.
15. Click the privilege "Full", select the "Continue" button.
16. The new privilege will be displayed. Select the "Next" button.
17. Select the "Next" button on the Resource Privilege page.
18. Select the Administrators you want to grant this role, DBA-ROLE too. Select the "Next" button.
19. Review the setting of your new role DBA-ROLE.
20. Next we create our second Role, WLS-ROLE. This Role will allow users granted this role full privilege on all the WebLogic Servers in WLSGroup and view privilege on all Database Instances in the DBAGroup. Repeat Steps 10-19, naming our second Role WLS-ROLE. Proceed to the review page, as displayed below.

2.2.3.2 Example 2: Granting developers view access to target database instances.

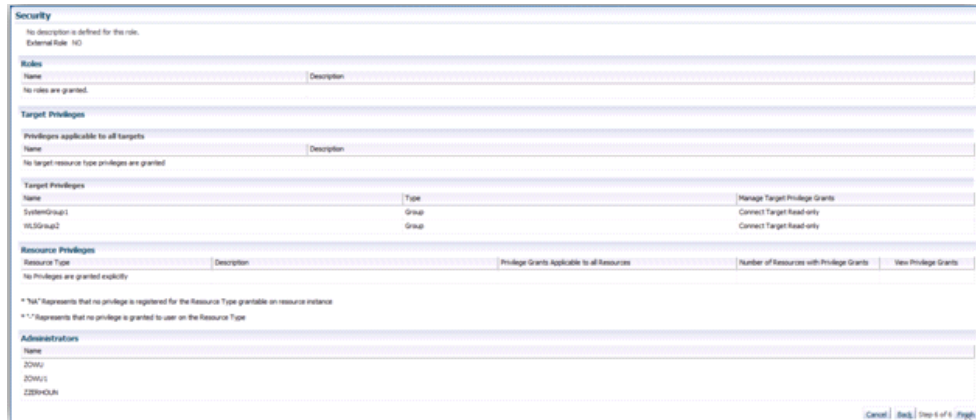
DBAs within data centers typically provide application developers read-only access to database performance pages in Enterprise Manager in order for them to view firsthand information on the impact of their applications on the underlying database and restrict them from performing any write operations on the database. The DBAs may not want to share database user account information with the developers nor create individual user accounts on every Database Instance.

You can use the 'Connect Target Read-Only' privilege to enable read-only access to a target. To manage the granting of this privilege across many databases to a team of developers, you can create a privilege propagating group, and add the Database Instances to this target group, calling it, for example DevGroup. You create a role, for example DEV-ROLE and grant the privilege, "Connect Target Read-Only" on his Role, in doing so, you assign this Role to each Developer, granting him access to the performance data in those Database Instances. As these engineers do not have individual user accounts on each Database Instance we will create a Named Credential, call it DevCred which contains database user credentials and we will assign this Named Credential to each Developer needing access to the performance

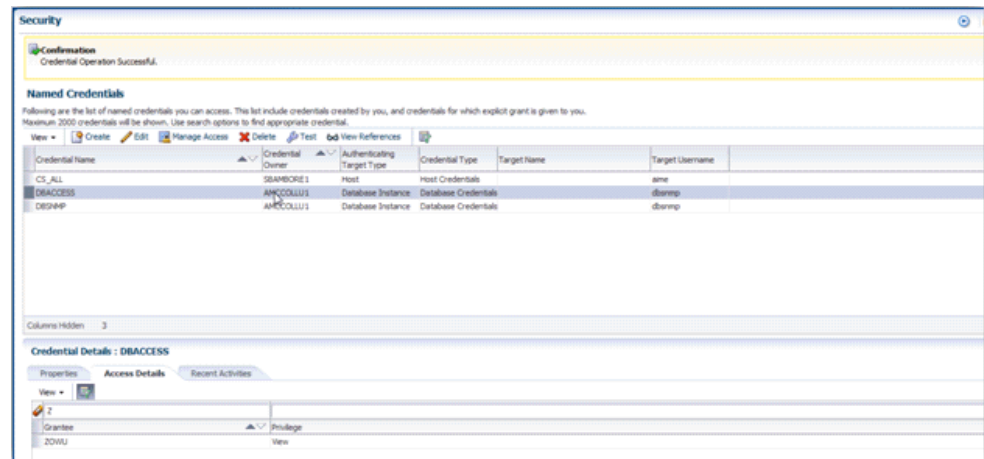
data in the Database Instances. The following steps will show you how to set up the target group and assign Roles and Named Credentials to this group.

Here are the steps to follow:

1. Create a group of targets. On the console go to Targets->Groups from the drop down menu.
2. Click "Create" and select "Group" from the drop down menu.
3. Enter the name of your new target group, for this User Case we shall call it DevGroup.
4. Enable "Privilege Propagation" group, by checking the box. This allows Administrators to do a one-time grant privileges on a group to a user and have that privilege be automatically propagated (or applied) to each member of that group. Add the database Targets you want to add to the group. This is done by hitting the "Add" button and selecting the Targets from the list.
5. Select "OK".
6. The new target group, DevGroup, is displayed in the list of available groups.
7. Next, create a view only Role for the Target DevGroup. A Role is a privilege that is granted to an Administrator. Proceed to the Roles page, go to the Setup->Security->Roles page.
8. Click "Create" button.
9. On the properties page, type the name of the new Role, DEV-ROLE, click the "Next" button.
10. Click "Next" on the "Roles" page.
11. On the "Target Privileges" page, scroll down to the "Target Privileges" section, at the bottom of the page. Click the "Add" button. The available targets are displayed. Select the "Group" Target Type, to improve the search. Select the group we just created, DevGroup. Click the "Select" button.
12. The target group is displayed. For this role, DEV-ROLE, we want to grant "Connect Target Read-Only" on all databases in the DevGroup. This is done by selecting the pencil icon, to the right of "View" in the "Manage Target Privilege Grants" column.
13. Click the privilege "Connect Target Read-Only", scroll to the bottom of the page. Select the "Continue" button.
14. The new privilege is displayed. Select the "Next" button
15. Select the "Next" button on the Resource Privilege page.
16. Select the Administrators you want to grant this role, DEV-ROLE too. Select the "Next" button.
17. Review the setting of your new role DEV-ROLE.



18. Next we will create a Named Credential. In this case a Named Credential contains the database credentials used to log on to the database. It will be used by the developer to access the database performance pages in Enterprise Manager. Follow the link "Setup"->"Security"->"Named Credential".
19. Click the "Create" button.
20. Enter the Username and Password information that this Named Credential will use to log onto the database. We have selected the following information:
 Credential name: DevCred
 Authenticating Target Type: Database Instance -For this Use Case, we are interested in granting access to the development engineers the database Instances in the DevGroup.
 Credential Type: Database Credentials - For this Use Case, we are supplying the username and password for the target Type specified above.
 Scope: Global - For this User Case, this username and password will apply to every Database. Click the "Test and Save" button.
21. Enter a valid "Test Target Name", and click **Test and Save**.
22. Our new Named Credential will be displayed. To Grant this Named Credential to a one of the development Engineers, click **Manage Access**.
23. Click the "Add Grant" button.
24. Select the Development Engineers you wish to use this Named Credential. Click the "Select" button.
25. The User information is displayed at the bottom of the page. More users may be added, if desired.



26. When this Development Engineer logs into Enterprise Manager they will have access to view necessary data, such as performance information. However, as expected, they are unable to perform any write operation to the databases. If the user does attempt to perform a write operation on any database, the following error is displayed in Enterprise Manager:

Failed to commit: Enterprise Manager has blocked you from performing the task as you are performing this operation using a READONLY connection.

2.2.3.3 Entitlement Summary

The Administrators Entitlement page displays all the privileges and roles granted to that Administrator. This page also summarizes an Administrator's access to targets as well as displaying the named credentials and secure resources owned by that Administrator. The following figure shows an example of the Enterprise Manager Administrator Entitlement page. You can access this page by clicking on the dropdown menu, beside the Administrator's name, and clicking Entitlement Summary.

2.3 Configuring Secure Communication

This section contains the following topics:

- [About Secure Communication](#)
- [Enabling Security for the Oracle Management Service](#)
- [Securing the Oracle Management Agent](#)
- [Managing Agent Registration Passwords](#)
- [Restricting HTTP Access to the Management Service](#)
- [Enabling Security for the Management Repository Database](#)
- [Custom Configurations](#)
- [Secure Communication Setup Tools](#)
- [Configuring Third Party Certificates](#)

2.3.1 About Secure Communication

Enterprise Manager Framework Security provides safe and secure communication channels between the components of Enterprise Manager. For example, Framework Security provides secure connections between your Oracle Management Service and its Management Agents. Secure communication also protects against network threats such as eavesdropping and ensures confidentiality/integrity by utilizing technologies such as public-key cryptography.

 **See Also:**

Oracle Enterprise Manager Concepts for an overview of Enterprise Manager components.

Enterprise Manager Framework Security implements the following types of secure connections between the Enterprise Manager components:

- HTTPS and Public Key Infrastructure (PKI) components, including signed digital certificates, for communications between the Management Service and the Management Agents.

 **See Also:**

For an overview of Public Key Infrastructure features, such as digital certificates and public keys, see the *Oracle® Database 2 Day Security Guide*.

- Oracle Advanced Security for communications between the Management Service and the Management Repository.

 **See Also:**

Oracle Database Advanced Security Administrator's Guide

2.3.2 Enabling Security for the Oracle Management Service

To enable Enterprise Manager Framework Security for the Management Service, you use the `emctl secure oms` utility, which is located in the following subdirectory of the Management Service home directory:

```
<OMS_ORACLE_HOME>/bin
```

The `emctl secure oms` utility performs the following actions:

- Generates a Root Key within your Management Repository. The Root Key is used during distribution of Oracle Wallets containing unique digital certificates for your Management Services & Management Agents. An Oracle Wallet is used to store

security credentials on Oracle Clients and servers, see Oracle Advanced Security Administrators Guide for more information on Oracle Wallets.

- Modifies your WebTier to enable an HTTPS channel between your Management Service and Management Agents, independent from any existing HTTPS configuration that may be present in your WebTier.
- Enables your Management Service to accept requests from Management Agents using Enterprise Manager Framework Security.

To run the `emctl secure oms` utility you must first choose an Agent Registration Password. The Agent Registration password is used to validate that future installation of Oracle Management Agents are authorized to load their data into this Enterprise Manager installation.

To enable Enterprise Manager Framework Security for the Oracle Management Service:

1. Stop the Management Service, the WebTier using the following command:

```
<OMS_ORACLE_HOME>/bin/emctl stop oms
```

2. Enter the following command:

```
<OMS_ORACLE_HOME>/bin/emctl secure oms
```

3. You will be prompted for the Enterprise Manager Root Password. Enter the `SYSMAN` password.
4. You will be prompted for the Agent Registration Password, which is the password required for any Management Agent attempting to establish secure communication with the Management Service. Specify an Agent Registration Password for the Management Service.
5. Restart the OMS.
6. After the Management Service restarts, test the secure connection to the Management Service by browsing to the following secure URL using the HTTPS protocol:

```
https://hostname.domain:https_console_port/em
```

Note: The Enterprise Manager console URL can be found by running the "emctl status oms -details" command.

For example:

```
$ emctl status oms -details
Oracle Enterprise Manager Cloud Control 13c Release 2
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
Enter Enterprise Manager Root (SYSMAN) Password :
...
Console URL: https://omshost.mydomain.com:5416/em
```

If the Management Service security has been enabled successfully, your browser displays the Enterprise Manager login page.

Example 2-3 Sample Output of the emctl secure oms Command

```
$ emctl secure oms
Oracle Enterprise Manager Cloud Control 13c Release 2
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
Securing OMS... Started.
Enter Enterprise Manager Root (SYSMAN) Password :
```



```
Enter Agent Registration Password :
Securing OMS... Successful
Restart OMS
```

2.3.2.1 Configuring the OMS with Server Load Balancer

When you deploy a Management Service that is available behind a Server Load Balancer (SLB), special attention must be given to the DNS host name through which the Management Service will be available. Although the Management Service may run on a particular local host, for example `myhost.mycompany.com`, your Management Agents will access the Management Service using the host name that has been assigned to the Server Load Balancer. For example, `oracleoms.mycompany.com`.

As a result, when you enable Enterprise Manager Framework Security for the Management Service, it is important to ensure that the Server Load Balancer host name is embedded into the Certificate that the Management Service uses for SSL communications. This may be done by using `emctl secure oms` and specifying the host name using an extra `-host` parameter as shown below.

Note:

Before running the commands, you must first identify the SLB hostname, port, and ensure that the SLB is configured.

- Enable security on the Management Service by entering the following command:


```
emctl secure oms -host <slb_hostname> [-slb_console_port <slb UI port>] [-slb_port <slb upload port>] [other params]
```

Run this command on each OMS. You will need to restart each OMS after running the 'emctl secure oms' command.
 - Create virtual servers and pools on the Server Load Balancer.
 - Verify that the console can be accessed using the following URL:


```
https://slb_hostname:slb_console_port/em
```
 - Re-secure the Agents with Server Load Balancer by using the following command:


```
emctl secure agent -emdWalletSrcUrl <SLB Upload or UI URL>
```

For example:

```
Agent_Home/bin/emctl secure agent -emdWalletSrcUrl https://slb_hostname:slb_upload_port/em
```
- It is possible to configure Oracle Enterprise Manager with one load balancer for upload operations and one for console operations. To do this, the pools at both of the SLBs must be configured with respective ports and the OMS must be secured separately for console and upload operations, using the following commands:
- ```
$emctl secure oms -host <slb_hostname>[-slb_port <slb upload port>] [other params]
$emctl secure console -host <slb_hostname> other params
```

### 2.3.2.1.1 Removing a Server Load Balancer Configuration

If you had previously configured the OMS with an SLB using `emctl secure oms -host` and now want to remove the SLB configuration, run the following command:

```
emctl secure oms -no_slb
```

If you had secured Agents using the SLB hostname they will need to be re-secured using the OMS hostname. To re-secure the Agents, run the following command:

```
emctl secure agent -emdWalletSrcUrl <Upload URL>
```

### 2.3.2.2 Creating a New Certificate Authority

You may need to create a new Certificate Authority (CA) if the current CA is expiring, if you want to change the key strength, or if you want to change the signature algorithm. A unique identifier is assigned to each CA. For instance, the CA created during installation may have an identifier as ID 1, subsequent CAs will have the IDs 2,3, and so on. At any given time, the last created CA is active and issues certificates for OMSs and Agents.

1. Run the `emctl secure createca` command on one of the OMS machines.
2. If there are multiple OMSs in your environment, copy `<EM_Instance_Home>/sysman/config/b64LocalCertificate.txt` from the machine on which `emctl secure createca` was run to all other OMS machines at the same location i.e `<EM_Instance_Home>/sysman/config/b64LocalCertificate.txt`
3. Restart all the OMSs.

#### Example 2-4 Creating a New Certificate Authority

```
emctl secure createca [-sysman_pwd <pwd>] [-host <hostname>] [-key_strength
<strength>] [-cert_validity <validity>] [-root_dc <root_dc>] [-root_country
<root_country>] [-root_email <root_email>] [-root_state <root_state>] [-root_loc
<root_loc>] [-root_org <root_org>] [-root_unit <root_unit>] [-sign_alg <md5|sha1|
sha256|sha384|sha512>] [-cert_validity <validity>]
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
Creating CA... Started.
Successfully created CA with ID 2
```

#### Example 2-5 Viewing Information about a Certificate Authority

```
emcli get_ca_info -ca_id="1;2" -details
Info about CA with ID: 1
CA is not configured
DN: CN=myhost.example.com, C=US
Serial# : 3423643907115516586
Valid From: Tue Mar 16 11:06:20 PDT 2011
Valid Till: Sat Mar 14 11:06:20 PDT 2020
Number of Agents registered with CA ID 1 is 1
myhost.mydomain.com:3872

Info about CA with ID: 2
CA is configured
DN: CN=myhost.example.com, C=US, ST=CA
Serial# : 1182646629511862286
Valid From: Fri Mar 19 05:17:15 PDT 2011
```

```
Valid Till: Tue Mar 17 05:17:15 PDT 2020
There are no Agents registered with CA ID 2
```

### 2.3.2.2.1 Administration Credentials Wallet

The WebLogic Administrator and Node Manager passwords are stored in the Administration Credentials Wallet. This is present in the `EM_INSTANCE_HOME/sysman/config/adminCredsWallet` directory. To recreate Administrator Credentials wallet, run the following command on each machine on which the Management Service is running:

```
emctl secure create_admin_creds_wallet [-admin_pwd <pwd>] [-nodemgr_pwd <pwd>]
```

### 2.3.2.3 Viewing the Security Status and OMS Port Information

To view the security status and OMS port information, use the following command

#### Example 2-6 `emctl status oms -details`

```
Oracle Enterprise Manager Cloud Control 13c Release 2
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
Console Server Host : mymachine.mycompany.com
HTTP Console Port : 7802
HTTPS Console Port : 5416
HTTP Upload Port : 7654
HTTPS Upload Port : 4473
EM Instance Home : /ade/myadmin_txn48/oracle/work/em/EMGC_OMS1
OMS Log Directory Location : /ade/myadmin_txn48/oracle/work/em/EMGC_OMS1/sysman/log
OMS is not configured with SLB or virtual hostname
Agent Upload is locked.
OMS Console is unlocked.
Active CA ID: 2
Console URL: https://mymachine.mycompany.com:5416/em
Upload URL: https://mymachine.mycompany.com:4473/empbs/upload

WLS Domain Information
Domain Name : EMGC_DOMAIN
Admin Server Host : mymachine.mycompany.com
Admin Server HTTPS Port: 7022
Admin Server is RUNNING

Managed Server Information
Managed Server Instance Name: EMGC_OMS1
Managed Server Instance Host: mymachine.mycompany.com
WebTier is Up
Oracle Management Server is Up
```

### 2.3.2.4 Configuring Transport Layer Security

The Oracle Management Service can be configured in TLSv1, TLSv1.1, and TLSv1.2 modes. By default, all three modes are enabled. To configure the OMS to use only one or two modes, do the following:

1. Stop the OMS by entering the following command:

```
<OMS_ORACLE_HOME>/bin/emctl stop oms
```

2. Enter a command similar to one of the following commands:

To restrict the OMS to one particular mode, enter:

```
emctl secure -protocol "TLSv1"
```

To enable more than one mode, use a space delimited list, for example:

```
emctl secure oms -protocol "TLSv1.1 TLSv1.2"
```

3. Restart the OMS with the following command:

```
<OMS_ORACLE_HOME>/bin/emctl start oms
```

## 2.3.3 Securing the Oracle Management Agent

When you install the Management Agent on a host, you must identify the Management Service that will be used by the Management Agent. To enable Enterprise Manager Framework Security for the Management Agent, use the `emctl secure agent` utility, which is located in the following directory of the Management Agent home directory:

```
<AGENT_INSTANCE_HOME>/bin (UNIX)
<AGENT_INSTANCE_HOME>\bin (Windows)
```

The `emctl secure agent` utility performs the following actions:

- Obtains an Oracle Wallet from the Management Service that contains a unique digital certificate for the Management Agent. This certificate is required in order for the Management Agent to conduct SSL communication with the secure Management Service.
- Obtains an Agent Key for the Management Agent that is registered with the Management Service.
- Configures the Management Agent so it is available on your network over HTTPS and so it uses the Management Service HTTPS upload URL for all its communication with the Management Service.

To enable Enterprise Manager Framework Security for the Management Agent:

1. Ensure that your Management Service and the Management Repository are up and running.
2. Stop the Management Agent:

```
emctl stop agent
```

3. Enter the following command:

```
emctl secure agent
```

The `emctl secure agent` utility prompts you for the Agent Registration Password, authenticates the password against the Management Service, and reconfigures the Management Agent to use Enterprise Manager Framework Security.

[Example 2-7](#) shows sample output of the `emctl secure agent` utility.

4. Restart the Management Agent:

```
emctl start agent
```

5. Confirm that the Management Agent is secure by checking the Management Agent home page.

 **Note:**

You can also check if the Agent Management is secure by running the `emctl status agent -secure` command, or by checking the Agent and Repository HTTPS URLs in the output of the `emctl status agent` command.

In the Management Agent home page, the **Secure Upload** field indicates whether or not Enterprise Manager Framework Security has been enabled for the Management Agent.

**Example 2-7 Sample Output of the `emctl secure agent` Utility**

```
emctl secure agent
Oracle Enterprise Manager 13c Release 2 Cloud Control.
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
Securing agent... Started
Securing agent... Successful.
```

**Example 2-8 Sample Output of the `emctl status agent secure` Command**

```
$ emctl status agent -secure
Oracle Enterprise Manager Cloud Control 13c Release 2
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
Checking the security status of the Agent at location set in /ade/pchebrol_emkey/
oracle/work/agentStateDir/sysman/config/emd.properties... Done.
Agent is secure at HTTPS Port 1838.
Checking the security status of the OMS at http://adc4110148.us.mycompany.com:7654/
empbs/upload/... Done.
OMS is secure on HTTPS Port 4473
```

## 2.3.4 Managing Agent Registration Passwords

Enterprise Manager uses the Agent Registration password to validate that installations of Oracle Management Agents are authorized to load their data into the Oracle Management Service.

The Agent Registration password is created during installation when security is enabled for the Oracle Management Service. You can add/edit/delete registration passwords directly from the Enterprise Manager console.

 **Note:**

If you want to avoid new Agents from being registered with the OMS, delete all registration passwords.'

### 2.3.4.1 Using the Cloud Control Console to Manage Agent Registration Passwords

You can use the Cloud Control Console to manage your existing registration passwords or create additional registration passwords:

1. From the **Setup** menu, select **Security**, then select **Registration Passwords**.
2. Enterprise Manager displays the Registration Passwords page. Registration password specified during install appears in the Registration Passwords table with description *<Initial Agent Registration Password>*.
3. Use the Registration Passwords page to change your registration password, create additional registration passwords, or remove registration passwords associated with the current Management Repository.

When you create or edit an Agent Registration Password on the Registration Passwords page, you can determine whether the password is persistent and available for multiple Management Agents or to be used only once or for a predefined period of time.

For example, if an administrator requests to install a Management Agent on a particular host, you can create a one-time-only password that the administrator can use to install and configure one Management Agent.

On the other hand, you can create a persistent password that an administrator can use for the next two weeks before it expires and the administrator must ask for a new password.

### 2.3.4.2 Using emctl to Add a New Agent Registration Password

To add a new Agent Registration Password, use the following `emctl` command on the machine on which the Management Service has been installed:

```
emctl secure setpwd [sysman pwd] [new registration pwd]
```

The `emctl secure setpwd` command requires that you provide the password of the Enterprise Manager super administrator user, `sysman`, to authorize the addition of the Agent Registration Password.

As with other security passwords, you should change the Agent Registration Password on a regular and frequent basis to prevent it from becoming too widespread.

### 2.3.5 Restricting HTTP Access to the Management Service

It is important that only secure Management Agent installations that use the Management Service HTTPS channel are able to upload data to your Management Repository and Cloud Control console is accessible via HTTPS only.

To restrict access so Management Agents can upload data to the Management Service only over HTTPS:

1. Stop the Management Service, the WebTier:

```
cd <OMS_ORACLE_HOME>/bin
emctl stop oms
```

2. Enter the following command to prevent Management Agents from uploading data to the Management Service over HTTP:

```
emctl secure lock -upload
```

To lock the console and prevent HTTP access to the console, enter the following command:

```
emctl secure lock -console
```

To lock both, enter either of the following commands:

```
emctl secure lock or
emctl secure lock -upload -console
```

To lock both the console access and uploads from Agents while enabling security on the Management Service, enter the following command:

```
emctl secure oms -lock [other options]
```

3. Restart the Management Service, the WebTier, and the other application server components:

```
emctl start oms
```

4. Verify that you cannot access the OMS upload URL using the HTTP protocol:

For example, navigate to the following URL:

```
http://hostname.domain:4889/empbs/upload
```

You should receive an error message similar to the following:

```
Forbidden
You are not authorised to access this resource on the server.
```

**Note:** The HTTP upload port number can be found using the `emctl status oms - details` command. Search for "HTTP Upload Port"

5. Verify that you can access the OMS Upload URL using the HTTPS protocol:

For example, navigate to the following URL:

```
https://hostname.domain:4888/empbs/upload
```

You should receive the following message, which confirms the secure upload port is available to secure Management Agents:

```
Http XML File receiver
Http Recceiver Servlet active!
```

### Example 2-9 Sample Output of the `emctl secure lock` Command

```
emctl secure lock
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
OMS Console is locked. Access the console over HTTPS ports.
Agent Upload is locked. Agents must be secure and upload over HTTPS port.
Restart OMS
```

### Example 2-10 Sample Output of the `emctl secure unlock` Command

```
emctl secure unlock
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
OMS Console is unlocked. HTTP ports too can be used to access console.
Agent Upload is unlocked. Unsecure Agents may upload over HTTP.
Restart OMS
```

To allow the Management Service to accept uploads from unsecure Management Agents, use the following command:

```
emctl secure unlock -upload
```

 **Note:**

- The OMS need to be stopped before running 'secure unlock', and then restarted afterwards.
- To unlock the console and allow HTTP access to the console, enter the following command:

```
emctl secure unlock -console
```

- To unlock both, enter either of the following command:

```
emctl secure unlock
emctl secure unlock -console -upload
```

 **Note:**

The Oracle Management Service is locked (both console & upload) by default beginning with Enterprise Manager 13c.

## 2.3.6 Enabling Security for the Management Repository Database

This section describes how to enable Security for the Oracle Management Repository. This section includes the following topics:

- [About Oracle Advanced Security and the sqlnet.ora Configuration File](#)
- [Configuring the Management Service to Connect to a Secure Management Repository Database](#)
- [Enabling Oracle Advanced Security for the Management Repository](#)
- [Enabling Security for a Management Agent Monitoring a Secure Management Repository or Database](#)

### 2.3.6.1 About Oracle Advanced Security and the sqlnet.ora Configuration File

You enable security for the Management Repository by using Oracle Advanced Security. Oracle Advanced Security ensures the security of data transferred to and from an Oracle database.

 **See Also:**

*Oracle Database Advanced Security Administrator's Guide*

To enable Oracle Advanced Security for the Management Repository database, you must make modifications to the `sqlnet.ora` configuration file. The `sqlnet.ora` configuration file is used to define various database connection properties, including Oracle Advanced Security parameters.



The `sqlnet.ora` file is located in the following subdirectory of the Database home:

```
<OMS_ORACLE_HOME>/network/admin
```

After you have enabled Security for the Management Repository and the Management Services that communicate with the Management Repository, you must also configure Oracle Advanced Security for the Management Agent by modifying the `sqlnet.ora` configuration file in the Management Agent home directory.

 **See Also:**

["Enabling Security for a Management Agent Monitoring a Secure Management Repository or Database"](#)

It is important that both the Management Service and the Management Repository are configured to use Oracle Advanced Security. Otherwise, errors will occur when the Management Service attempts to connect to the Management Repository. For example, the Management Service might receive the following error:

```
ORA-12645: Parameter does not exist
```

To correct this problem, be sure both the Management Service and the Management Repository are configured as described in the following sections.

 **Note:**

The procedures in this section describe how to manually modify the `sqlnet.ora` configuration file to enable Oracle Advanced Security. Alternatively, you can make these modifications using the administration tools described in the *Oracle Database Advanced Security Administrator's Guide*.

## 2.3.6.2 Configuring the Management Service to Connect to a Secure Management Repository Database

If you have enabled Oracle Advanced Security for the Management Service database—or if you plan to enable Oracle Advanced Security for the Management Repository database—use the following procedure to enable Oracle Advanced Security for the Management Service:

1. Stop the Management Service:

```
<OMS_ORACLE_HOME>/bin/emctl stop oms
```

2. Set Enterprise Manager operational properties by using the `emctl set property` command. The following table shows the `emoms` properties that must be set.

**Table 2-2 Oracle Advanced Security Properties in the Enterprise Manager Properties**

| Property                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| oracle.sysman.emRep.dbConn.enableEncryption | <p>Defines whether or not Enterprise Manager will use encryption between the Management Services and Management Repository. Possible values are TRUE and FALSE. The default value is TRUE. For example:</p> <pre>emctl set property -name 'oracle.sysman.emrep.dbConn.enableEncryption' -value 'true'</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| oracle.net.encryption_client                | <p>Defines the Management Service encryption requirement. Possible values are REJECTED, ACCEPTED, REQUESTED, and REQUIRED.</p> <p><b>IMPORTANT:</b> DO NOT set the encryption_client property to REQUIRED as this prevents Enterprise Manager from receiving notifications from server generated alerts (such as <i>tablespace full</i>). Currently, Enterprise Manager does not support server generated alerts with the REQUIRED setting; Only the REQUESTED setting is supported.</p> <p>The default value is REQUESTED. If the database supports secure connections, then the Management Service uses secure connections, otherwise the Management Service uses insecure connections.</p> <p>For example:</p> <pre>oracle.net.encryption_client=REQUESTED</pre> |
| oracle.net.encryption_types_client          | <p>Defines the different types of encryption algorithms the client supports. Possible values should be listed within parenthesis. The default value is ( DES40C ).</p> <p>For example:</p> <pre>oracle.net.encryption_types_client=( DES40C )</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| oracle.net.crypto_checksum_client           | <p>Defines the Client's checksum requirements.</p> <p>Possible values are REJECTED, ACCEPTED, REQUESTED, and REQUIRED.</p> <p>The default value is REQUESTED. In other words, if the server supports checksum enabled connections, then the Management Service uses them, otherwise it uses normal connections.</p> <p>For example:</p> <pre>oracle.net.crypto_checksum_client=REQUESTED</pre>                                                                                                                                                                                                                                                                                                                                                                      |

**Table 2-2 (Cont.) Oracle Advanced Security Properties in the Enterprise Manager Properties**

| Property                                | Description                                                                                                                                                                                                                                          |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| oracle.net.crypto_checksum_types_client | This property defines the different types of checksums algorithms the client supports. Possible values should be listed within parentheses. The default value is ( MD5 ).<br>For example:<br>oracle.net.<br>crypto_checksum_types_client=<br>( MD5 ) |

- Restart the Management Service.

```
<OMS_ORACLE_HOME>/bin/emctl start oms
```

### 2.3.6.3 Enabling Oracle Advanced Security for the Management Repository

To ensure your database is secure and that only encrypted data is transferred between your database server and other sources, review the security documentation available in the Oracle Database documentation library.



#### See Also:

*Oracle Database Advanced Security Administrator's Guide*

The following instructions provide an example of how you can confirm that Oracle Advanced Security is enabled for your Management Repository database and its connections with the Management Service:

- Locate the `sqlnet.ora` configuration file in the following directory of the database Oracle Home:

```
<OMS_ORACLE_HOME>/network/admin
```

- Using a text editor, look for the following entries (or similar entries) in the `sqlnet.ora` file:

```
SQLNET.ENCRYPTION_SERVER = REQUESTED
SQLNET.CRYPTO_SEED = "abcdefg123456789"
```



#### See Also:

"Configuring Network Data Encryption and Integrity for Oracle Servers and Clients in the *Oracle Application Server 10g Administrator's Guide*.

- Save your changes and exit the text editor.

## 2.3.6.4 Enabling Security for a Management Agent Monitoring a Secure Management Repository or Database

After you have enabled Oracle Advanced Security for the Management Repository, you must also enable Advanced Security for the Management Agent that is monitoring the Management Repository:

1. Locate the `sqlnet.ora` configuration file in the following directory inside the home directory for the Management Agent that is monitoring the Management Repository:

```
AGENT_HOME/network/admin (UNIX)
AGENT_HOME\network\admin (Windows)
```

2. Using a text editor, add the following entry to the `sqlnet.ora` configuration file:

```
SQLNET.CRYPTO_SEED = "abcdefg123456789"
```

The `SQLNET.CRYPTO_SEED` can be any string between 10 to 70 characters.

### See Also:

"Configuring Network Data Encryption and Integrity for Oracle Servers and Clients in the *Oracle Application Server Administrator's Guide*.

3. Save your changes and exit the text editor.
4. Restart the Management Agent.

## 2.3.7 Custom Configurations

### 2.3.7.1 Configuring Custom Certificates for WebLogic Server

WebLogic Servers installed as part of Enterprise Manager Cloud control (Administration Server and Managed Servers) are configured with a default identity keystore ( `Demoidentity.jks`) and a default trust keystore ( `DemoTrust.jks`). In addition, WebLogic Server trusts the CA certificates in the JDK cacerts file. This default keystore configuration is appropriate for testing and development purposes. However, these keystores should not be used in a production environment.

Default Demo Certificate configured for WLS has a key length of 512 bits. If Microsoft's Security update for minimum certificate key length (KB2661254) has been applied on the browser m/c, the WebLogic Admin Console will not be accessible on Internet Explorer. If you want to access WebLogic Admin Console using Internet Explorer, please configure custom certificate for WLS.

The following sections step you through configuring custom Weblogic Server certificates:

1. [Create a Java KeyStore or Wallet for each OMS](#)
2. [Import Custom CA Certificates into the Agents Monitoring Trust Store](#)
3. [Configure the Custom Certificate for each WLS](#)

 **Note:**

This procedure is applicable to Enterprise Manager 12c Cloud Control (12.1.0.2) and higher.

### 2.3.7.1.1 Create a Java KeyStore or Wallet for each OMS

1. Create a java keystore (JKS) for each OMS in the environment.

Regardless of whether the OMS is configured with a server load balancer or not, specify the OMS machine name for CN (Example: CN=myoms.mydomain.com) while generating the Certificate Signing Request (CSR). The OMS machine name can be found from the value of EM\_INSTANCE\_HOST property in <EM\_Instance\_Home>/emgc.properties.

Make a note of the keystore password, private key entry's alias, and private key password of each keystore.

Note: Use only the signature algorithms supported by WLS.

2. Copy the keystores to corresponding OMS machines or place them in a location accessible from OMS machines.

Example: The keystores are /scratch/oms1.jks, /scratch/oms2.jks , /scratch/oms3.jks

3. Write the CA certificates to individual files (one CA certificate per file). Either copy these certificate files to the OMS machines or place them in a location accessible from the OMS machines.

Example: The filenames are /scratch/calcert.cer, /scratch/ca2cert.cer, /scratch/ca3cert.cer

Use the Subject Alternative Name (SAN) field when configuring custom certificates in OMS to specify multiple host names in a certificate so the certificate can be used in more than one host. You can have a trusted certificate for all SSL end-points in Enterprise Manager without buying and managing several individual certificates. Using SAN enables you to have one certificate that can be used for all hosts, the SLB, OHS, and WLS. You can use the \* wildcard in the SAN field or in the Subject CN field, for example: Subject: CN=\*.mydomain.com O=My Org L=Redwood Shores S=California C=US Certificate Extensions: 9 Subject Alternative Name DNS Name=\*.mydomain.com DNS Name=mydomain.com DNS Name=mydomain2.com

### 2.3.7.1.2 Import Custom CA Certificates into the Agents Monitoring Trust Store

Execute the following steps on Management Agents running on the OMS machines which are installed along with the OMS.

 **Note:**

Only required on Agents installed along with OMS and not on any other Agents.

**1. Stop the Agent**

```
<Agent_Instance_Home>/bin/emctl stop agent
```

**2. Import the custom CA certificate into Agent:**

```
<Agent_Instance_Home>/bin/emctl secure add_trust_cert_to_jks
-trust_certs_loc <ca_cert_file>
-alias <certalias> [-password <montrust_jks_pwd>]
```

**Example:**

```
<Agent_Instance_Home>/bin/emctl secure add_trust_cert_to_jks -trust_certs_loc /
scratch/calcert.cer
-alias calcertalias [-password welcome]
```

Repeat this step for each CA involved in issuing the custom certificate.

Specify different alias each time.

**3. Start the Agent.**

```
<Agent_Instance_Home>/bin/emctl
```

### 2.3.7.1.3 Configure the Custom Certificate for each WLS

Execute the following steps on each OMS:

**1. Stop the OMS.**

```
<OMS_Home>/bin/emctl stop oms
```

**2. Run the following cmd:**

```
emctl secure wls
(-jks_loc <loc> -jks_pvtkey_alias <alias> [-jks_pwd <pwd>] [-jks_pvtkey_pwd
<pwd>] | -wallet <loc>)
Specify jks_loc, jks_pvtkey_alias or wallet
```

**Example:**

```
<OMS_OH>/bin/emctl secure wls
-jks_loc /scratch/oms1.jks -jks_pvtkey_alias pvtkey1alias

<OMS_OH>/bin/emctl secure wls -wallet /scratch/omswallet
```

**3. Stop the OMS.**

```
<OMS_Home>/bin/emctl stop oms -all
```

**4. Start the OMS.** **Note:**

Above steps need to be repeated on all the Management Services.

```
<OMS_Home>/bin/emctl start oms
```

### 2.3.7.1.4 Rolling back the WebLogic Servers to Demonstration Certificate

If you need to switch to using the default WebLogic demonstration certificates, execute the following steps on each OMS.

1. Stop the OMS.

```
<OMS_Home>/bin/emctl stop oms
```

2. Run the following command:

```
<OMS_Home>/bin/emctl secure wls -use_demo_cert
```

3. Stop the OMS.

```
<OMS_Home>/bin/emctl stop oms -all
```

4. Start the OMS.

```
<OMS_Home>/bin/emctl start oms
```

 **Note:**

The above steps need to be executed on all Management Services.

### 2.3.7.2 Configuring Custom Certificates for OMS Console Access

To configure the third party certificate for HTTPS WebTier Virtual Host:

1. Create a wallet for each OMS in the Cloud. Specify the host name of the machine where the OMS is installed or the Load Balancer Name if the OMS is behind the Server Load Balancer for Common Name.
2. Run the following command on each OMS and the restart that OMS:

```
emctl secure console -wallet <location of custom wallets> -self_signed [-host]
```

 **Note:**

One of the arguments `-wallet` or `-self_signed` is mandatory.

 **Note:**

Only Single-Sign-On (SSO) wallets are supported.

### 2.3.7.3 Configuring Custom Certificates for OMS Upload Access

You can configure the third party certificate for the HTTPS Upload Virtual Host in two ways:

#### Method I

1. Create a wallet for each OMS in the Cloud.
2. While creating the wallet, specify the host name of the machine where the OMS is installed or the Load Balancer Name if the OMS is behind the Load Balancer for Common Name.
3. Write the certificates of all the Certificate Authorities in the certificate chain (like the Root Certificate Authority, Intermediate Certificate Authority) into a file named `trusted_certs.txt`.
4. Download or copy the `trusted_certs.txt` file to the host machines on which each Agent that is communicating with the OMS is running.
5. Import the custom CA certificate(s) as trust certificate(s) for Agent by running the following command:

```
emctl secure add_trust_cert -trust_certs_loc <location of the trusted_certs.txt file>
```

6. Restart the Agent.
7. Secure the OMS and restart it.

```
emctl secure oms -wallet <location of wallet> -trust_certs_loc <loc of trusted_certs.txt> [any other options]
```

### Method 2

1. Create a wallet for each OMS in the Cloud.
2. Specify the host name of the machine where the OMS is installed or the Load Balancer Name if the OMS is behind the Server Load Balancer for Common Name (CN).
3. Write the certificates of all the Certificate Authorities in the certificate chain (like the Root Certificate Authority, Intermediate Certificate Authority) into a file named `trusted_certs.txt`.
4. Secure the OMS.  

```
emctl secure oms -wallet <location of wallet> -trust_certs_loc <loc of trusted_certs.txt> [any other options]
```
5. Restart the OMS.
6. Either re-secure the Agent by running the `emctl secure agent` command (should be run on all Agents) or import the trust points by running the `emctl secure` command.

#### Note:

The trusted certs file (`trusted_certs.txt`) should contain only certificates in base64 format and not any special characters or comments..

## 2.3.8 Secure Communication Setup Tools

The following `emctl` commands are used to secure various components of the Enterprise Manager infrastructure.



### 2.3.8.1 emctl secure oms

```
emctl secure oms [-sysman_pwd <sysman password>] [-reg_pwd <registration password>]
 [-host <hostname>] [-ms_hostname <Managed Server hostname>]
 [-slb_port <SLB HTTPS upload port>] [-slb_console_port <ty6 HTTPS console
port>] [-no_slb]
 [-secure_port <OHS HTTPS upload Port>] [-upload_http_port <OHS HTTP upload
port>]
 [-reset] [-console] [-force_newca]
 [-lock_upload] [-lock_console] [-unlock_upload] [-unlock_console]
 [-wallet <wallet_loc> -trust_certs_loc <certs_loc>]
 [-key_strength <strength>] [-sign_alg <md5|sha1|sha256|sha384|sha512>]
 [-cert_validity <validity>] [-protocol <protocol>]
 [-root_dc <root_dc>] [-root_country <root_country>] [-root_email
<root_email>]
 [-root_state <root_state>] [-root_loc <root_loc>] [-root_org <root_org>] [-
root_unit <root_unit>]
```

| Parameter        | Description                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sysman_pwd       | Oracle Management Repository user password.                                                                                                                                |
| reg_pwd          | The Management Agent registration password.                                                                                                                                |
| host             | The host name to be used in the certificate used by the Oracle Management Service. You may need to use the SLB host name if there is an SLB before the Management Service. |
| reset            | A new certificate authority will be created. All the Agents and Oracle Management Services need to be resecured.                                                           |
| secure_port      | Specify this to change HTTPS Upload port on WebTier.                                                                                                                       |
| upload_http_port | Specify this to change HTTP Upload port on WebTier                                                                                                                         |
| slb_port         | This parameter is required when Server Load Balancer is used. It specifies the secure upload port configured in the Server Load Balancer.                                  |
| slb_console_port | This parameter is required when Server Load Balancer is used. It specifies the secure console port configured in the Server Load Balancer.                                 |
| no_slb           | Remove SLB configuration.                                                                                                                                                  |
| root_dc          | The domain component used in the root certificate. The default value is com.                                                                                               |
| root_country     | The country to be used in the root certificate. The default value is US.                                                                                                   |
| root_state       | The state to be used in the root certificate. The default value is CA.                                                                                                     |
| root_loc         | The location to be used in the root certificate. The default value is EnterpriseManager on <hostname>.                                                                     |
| root_org         | The organization name to be used in the root certificate. The default value is EnterpriseManager on <hostname>.                                                            |
| root_unit        | The organizational unit to be used in the root certificate. The default value is EnterpriseManager on <hostname>.                                                          |
| root_email       | The email address to be used in the root certificate. The default value is EnterpriseManager@<hostname>.                                                                   |

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wallet          | This is the location of the wallet containing the third party certificate. This parameter should be specified while configuring third party certificates.                                                                                                                                                                                                   |
| trust_certs_loc | The location of the <code>trusted_certs.txt</code> (required when third party certificates are used).                                                                                                                                                                                                                                                       |
| key_strength    | The strength of the key to be used. Valid values are 512, 1024, 2048, and 4096.<br><b>Note:</b> For the IBM AIX Platform, the maximum allowed <code>key_strength</code> is 2048 bits.                                                                                                                                                                       |
| cert_validity   | The number of days for which the self-signed certificate is valid. The valid range is between 1 to 3650.                                                                                                                                                                                                                                                    |
| protocol        | This parameter is used to configure Oracle Management Service in TLSv1-only or SSLv3-only or mixed mode (default). Valid values are the allowed values as per <b>Apache's SSLProtocol</b> directive.<br>Note: The <code>key_strength</code> and <code>cert_validity</code> parameters are applicable only when the <code>-wallet</code> option is not used. |
| force_newca     | If specified, any Agents that are still configured with an older Certificate Authority are ignored.                                                                                                                                                                                                                                                         |
| ms_hostname     | Managed Server's hostname.                                                                                                                                                                                                                                                                                                                                  |
| sign_alg        | Signature algorithm.                                                                                                                                                                                                                                                                                                                                        |
| lock            | Locks the Upload                                                                                                                                                                                                                                                                                                                                            |
| lock_console    | Locks the Console                                                                                                                                                                                                                                                                                                                                           |
| console         | If specified, the certificate is recreated for the HTTPS console port as well.                                                                                                                                                                                                                                                                              |

### 2.3.8.2 emctl secure agent

Secures the agent against an OMS. The registration password (or password file) must be provided.

```
emctl secure agent <registration password> [-passwd_file <absolute path to file>]
```

### 2.3.8.3 emctl secure wls

```
emctl secure wls (-jks_loc <loc> -jks_pvtkey_alias <alias> | -wallet <loc> | -
use_demo_cert)
Specify jks_loc, jks_pvtkey_alias or wallet or use_demo_cert
[-jks_pwd <pwd>] [-jks_pvtkey_pwd <pwd>]
-jks_loc : Location of JKS containing the custom cert for Admin & Managed
Servers
-jks_pvtkey_alias : JKS's private key alias
-jks_pwd : JKS's keystore password
-jks_pvtkey_pwd : JKS's private key password
-wallet : Location of wallet containing the custom cert for Admin & Managed
Servers
-use_demo_cert: Configure the demo cert for Admin & Managed Servers
```

### 2.3.8.4 emctl status oms -details

```
emctl status oms -details [-sysman_pwd <pwd>]
```

## 2.3.9 Configuring Third Party Certificates

You can configure third party certificates for:

- HTTPS Console Users
- HTTPS Upload Virtual Host



### Note:

Only Single Sign-On wallets are supported.

### 2.3.9.1 Configuring a Third Party Certificate for HTTPS Console Users

To configure the third party certificate for HTTPS WebTier Virtual Host:

1. Create a wallet for each OMS. Specify the host name of the machine where the OMS is installed or the Load Balancer Name if the OMS is behind the Server Load Balancer for Common Name.
2. Run the following command on each OMS and the restart that OMS:

```
emctl secure console -wallet <location of custom wallets> -self_signed [-host]
```



### Note:

One of the arguments `-wallet` or `-self_signed` is mandatory.



### Note:

Only single-sign-on wallets are supported.

### 2.3.9.2 Configuring Third Party Certificate for HTTPS Upload Virtual Host

You can configure the third party certificate for the HTTPS Upload Virtual Host in two ways:

#### Method I

1. Create a wallet for each OMS.
2. While creating the wallet, specify the host name of the machine where the OMS is installed or the Load Balancer Name if the OMS is behind the Load Balancer for Common Name.
3. Write the certificates of all the Certificate Authorities in the certificate chain (like the Root Certificate Authority, Intermediate Certificate Authority) into a file named `trusted_certs.txt`.

4. Download or copy the `trusted_certs.txt` file to the host machines on which each Agent that is communicating with the OMS is running.
5. Run the `add_trust_cert` command on each Agent and then restart that Agent.

```
emctl secure add_trust_cert -trust_certs_loc <location of the trusted_certs.txt file>
```

6. Secure the OMS and restart it.

```
emctl secure oms -wallet <location of wallet> -trust_certs_loc <loc of trusted_certs.txt> [any other options]
```

### Method 2

1. Create a wallet for each OMS in the Cloud.
2. Specify the host name of the machine where the OMS is installed or the Load Balancer Name if the OMS is behind the Server Load Balancer for Common Name (CN).
3. Write the certificates of all the Certificate Authorities in the certificate chain (like the Root Certificate Authority, Intermediate Certificate Authority) into a file named `trusted_certs.txt`.

4. Restart the OMS after it has been secured.

```
emctl secure oms -wallet <location of wallet> -trust_certs_loc <loc of trusted_certs.txt> [any other options]
```

5. Either re-secure the Agent by running the `emctl secure agent` command (should be run on all Agents) or import the trust points by running the `emctl secure add_trust_cert -trust_certs_loc <location of the trusted_certs.txt file>` command. The `-trust_certs_loc` parameter must contain the path and the filename of the `trusted_certs.txt` file.

#### Note:

This file must only contain certificates in base64 format and no special characters or empty lines.

## 2.4 Configuring and Using Target Credentials

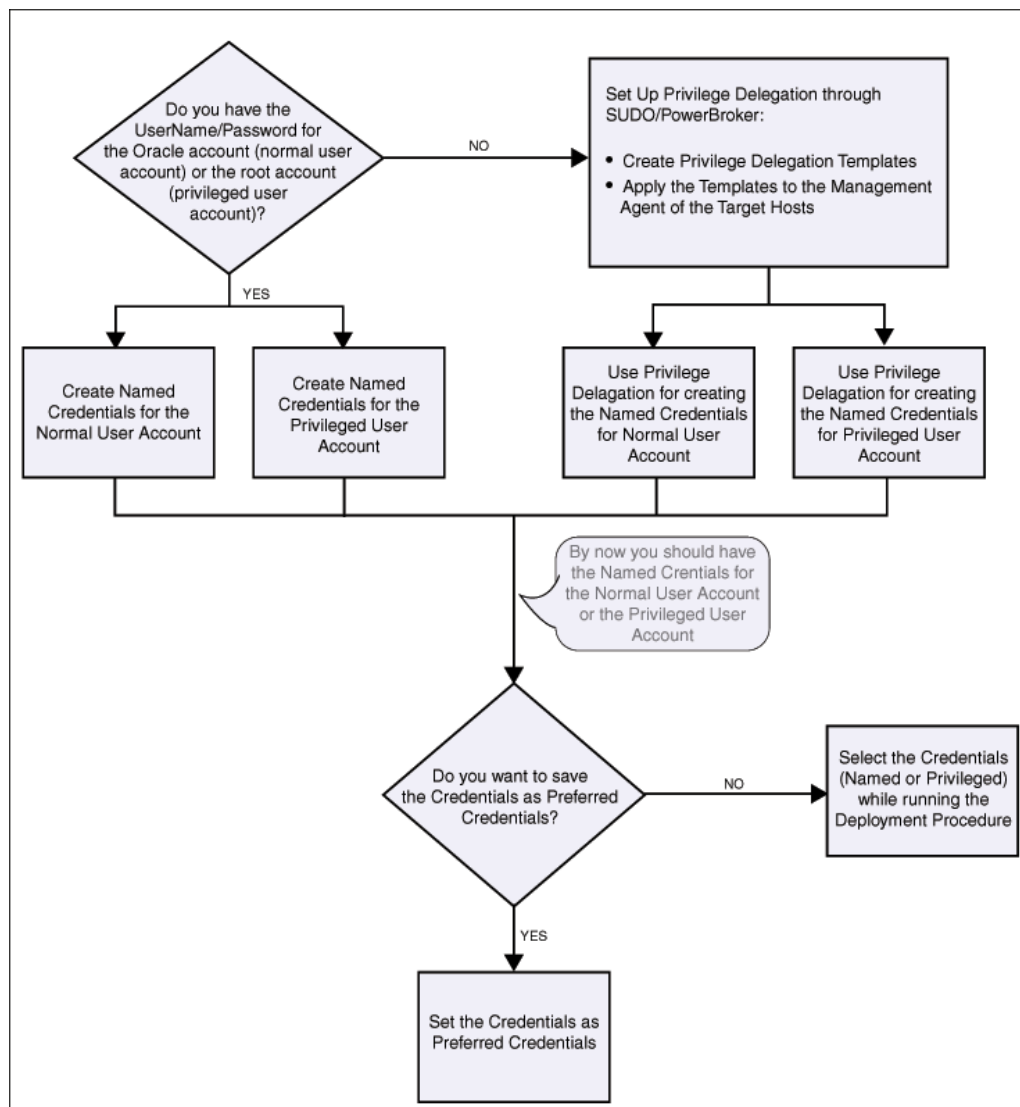
The following topics are discussed in this section:

- Credential Subsystem
- Pluggable Authentication Modules (PAM) Support
- Sudo and Powerbroker Support

### 2.4.1 Credential Subsystem

Credentials like user names and passwords are typically required to access targets such as databases, application servers, and hosts. The following flow chart illustrates the typical credential setup workflow.

**Figure 2-2 Credential Setup Workflow**



Credentials are encrypted and stored in Enterprise Manager. Beginning with Enterprise Manager 13c, the credential subsystem supports, in addition to basic username-password, strong authentication schemes such as PKI, SSH keys and Kerberos. SSH key based host authentication, used by jobs, deployment procedures and other Enterprise Manager subsystems, is now supported.

By using appropriate credentials, you can:

- Collect metrics in the background as well as real-time
- Perform jobs such as backup, patching, and cloning
- Perform real-time target administration such as start, and stop
- Connect to My Oracle Support

Based on their usage, credentials can be classified into the following categories:

- **Named Credentials**

- [Privileged Credentials](#)
- [Monitoring Credentials](#)
- [Preferred Credentials](#)

### 2.4.1.1 Named Credentials

Credentials are stored within Enterprise Manager as "named" entities. Administrators define and store credentials within Enterprise Manager and refer to the credential by a credential name. The advantages of saving the credentials are:

- You do not have to expose the credential details to all the users.
- It saves your time and effort as you do not have to specify the user name and password every time for each Oracle home or host machine, you can instead select a named profile that has used the saved credentials.

Named Credentials can be a username/password pair like the operating system login credentials, or Oracle home owner credentials primarily used for performing operations such as running jobs, patching and other system management tasks. For example, an administrator can store the username and password they want to use for patching as "MyPatchingCreds". He can later submit a patching job that uses "MyPatchingCreds" to patch a production databases.

#### 2.4.1.1.1 Typical Scenarios for Using Named Credentials

- In data centers where only senior DBAs have knowledge of higher privileged credential, sys credentials for database, for example, they can store these credentials in named credential and share these with the junior administrators. Junior administrators can perform their jobs using the named credentials without knowing what the actual credentials are.
- In data centers where administrators have the same credentials for a target. They can create one named credential containing those credentials and share the named credential with appropriate personnel. This simplifies credential maintenance (changing passwords, for example) by eliminating the need to several copies of named credentials containing the same credentials.

 **Note:**

For a video tutorial on using named credentials, see:

[Oracle Enterprise Manager 13c: Create and Use Named Credentials](#)

[https://apex.oracle.com/pls/apex/f?p=44785:24:0::NO:24:P24\\_CONTENT\\_ID,P24\\_PREV\\_PAGE:5460,1](https://apex.oracle.com/pls/apex/f?p=44785:24:0::NO:24:P24_CONTENT_ID,P24_PREV_PAGE:5460,1)

There are two category scopes of named credentials:

- **Global Named Credential**

A global named credential is an entity, containing authentication information for a target type. A global named credential can be applied to any Enterprise Manager target type at the time of its creation or, at a later time. Global named credentials

consist of the credential type (also known as the authentication scheme) and the credential properties (also known as the authentication parameters).

Each target type may have one or more credential types,

For example:

*hostA* has password based (requiring username/password) and SSH key (requiring public/private key pair) credential type and database *instanceA* has password based and Kerberos based credential type.

Credential properties consist of the information needed for the credential type and may also contain parameters, if being used for Privilege Delegation, PDP, for more information about PDP, see the section on Privilege Delegation, for possible commands and parameters.

As global named credentials are initially set up as independent entities, an Enterprise Manager administrator can associate this type of credential with a target type at a later time.

- **Target Named Credentials**

A target named credential is an entity, containing credential information applied to a specific target. A target named credential can be applied to an Enterprise Manager target and is applied at the time of creation. This entity will also contain a credential type (whether it is username/password or public/private key pair) along with credential parameters (In the case of PDP settings, the location of the PDP utility being used and the parameters and command to be run) for a target type.

#### 2.4.1.1.2 Access Control

In order to create a named credential an administrator must have the `CREATE_CREDENTIAL` privilege. Once the administrator with the `CREATE_CREDENTIAL` privilege creates a named credential, he is considered the owner of that named credential. The owner of a named credential can share access to the named credential at any time. He is considered the grantor administrator. The administrator granted access to the named credential is the grantee administrator. The owner can share access to the named credential by granting the appropriate level of privilege to one or many grantee administrators. The type of privilege granted by the owner of the named credential depends on the level of access needed by the grantee administrator. The following privilege levels are available for all named credentials:

- **VIEW:** The VIEW privilege is the default privilege level. Grantee administrators with VIEW privilege on a named credential will be able to use that named credential to run jobs, patching operations and other system management activities within Enterprise Manager. The grantee administrator will also be able to view the non-sensitive details (for example, SUDO or PowerBroker and the commands being used) and username of the named credential. The grantee administrator will not be able to view any sensitive information of the named credential such as the password and public/private key.
- **EDIT:** The EDIT privilege level also contains VIEW level privileges. Grantee administrators with EDIT privilege on a named credential can use that named credential to run jobs, patch operations and other management activities within Enterprise Manager. The grantee administrator will also be able to change the sensitive information such as the password, or the public/private key pair of that named credential. The grantee administrator can change both the Credential Type (such as Host or SSH key) of the named credential as well as the username for the credential. The authenticating target type cannot be changed.

- **FULL:** The FULL privilege contains both VIEW and EDIT. Grantee administrators with FULL privilege on a named credential will be able to use that named credential for running jobs, patching operations and other management activities within Enterprise Manager. The grantee administrator will also be able to change the named credential username, sensitive information such as the password or the public/private key pair, and Credential Type (Host, SSH key etc). An administrator with FULL privilege on a named credential will also be able to delete that named credential.

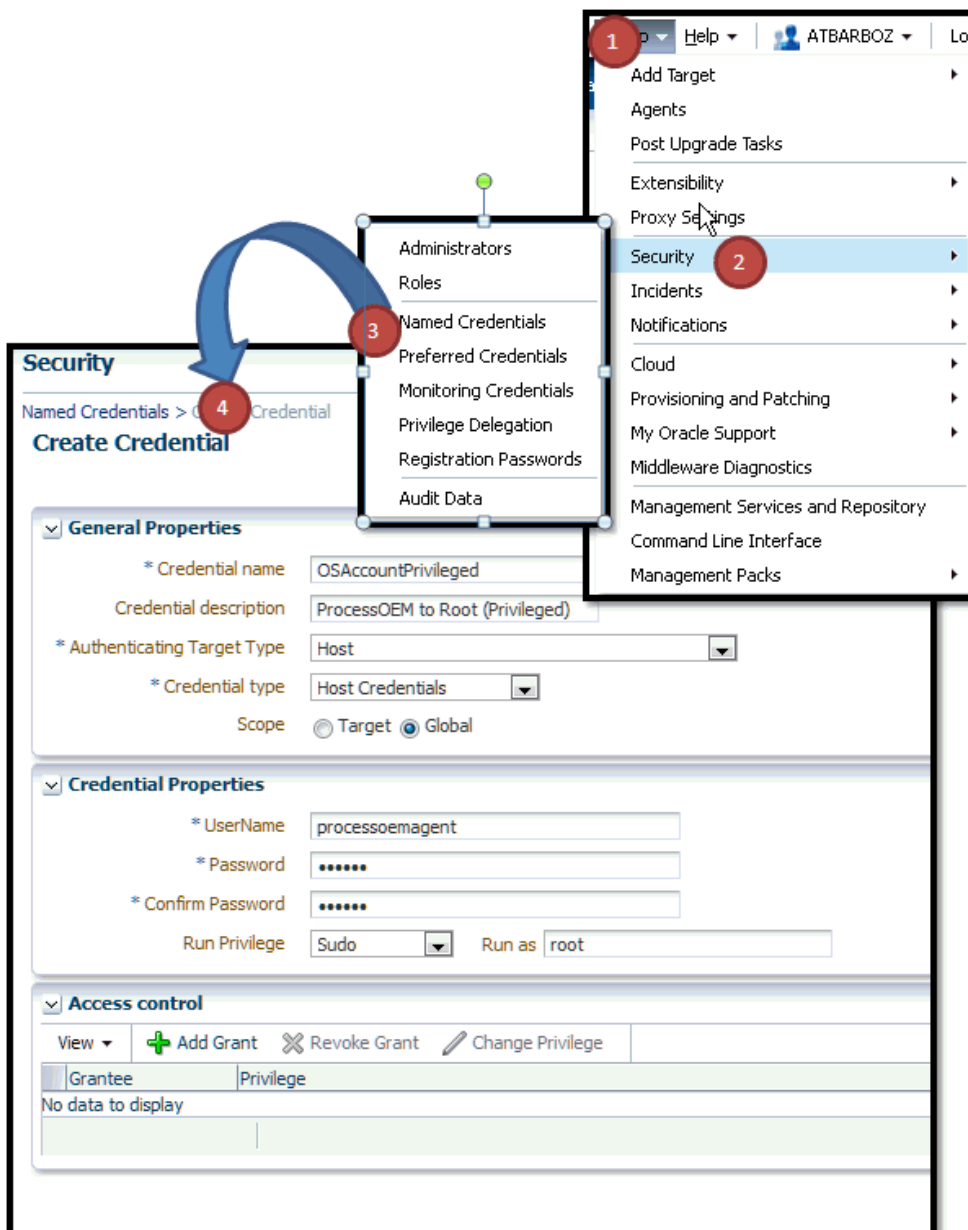
### 2.4.1.1.3 Creating Named Credentials

You must have the *Named Credential* resource privilege to create named credentials.

To create named credentials, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Security**, then select **Named Credentials**.
2. On the Named Credentials page, click **Create**.
3. On the Create Credentials page, in the General Properties section, provide the following details:
  - a. Enter a unique **Credential Name**, and provide a description.
  - b. Select **Host** as the Authentication Target Type, and **Host Credentials** as the Credential type
  - c. Select **Global** to use the same credentials for all the targets.
4. On the Create Credentials page, in the Credential Properties section, enter the **UserName** and **Password** required to access the host machine, and from the Run Privilege drop down list, do one of the following:
  - Select **None**, if you are using operating system host credentials (like *Oracle*) or the Oracle Home Owner credentials.
  - When you do not have access to the operating system host credentials or the `root` credentials of the host machine, then select **Sudo** or **PowerBroker** to `SUDO` (or `pbrun`) to the host machine using the credentials of another operating system user. To use the credentials of other users, in the **Run As** field, you need to enter operating system host credentials (like *Oracle*) or Oracle Home owner credentials of the host user.





5. On the Create Credentials page, in the Access Control section, click **Add Grant** to grant privileges on the named profile to the selected Administrators or roles. By default the selected Administrator is granted View privilege.

 **Note:**

To enable Administrators (or users) to access, and leverage an OMS Agent Filesystem Software Library Location, the owner of the Named Credential must ensure that an explicit View privilege is granted to all the Administrators accessing the OMS Agent location. To do so, you can either click **Add Grant** and add the names of the administrators while creating the Named Credential as mentioned in this section, or edit an existing Named Credential to grant privileges to other Administrators (or users) by following these steps:

- a. In Cloud Control, from the **Setup** menu, select **Security**, then select **Named Credentials**.
- b. On the Named Credentials page, click **Manage Access**.
- c. On the Manage Access page, click **Add Grant** to add a user, or **Change Privilege** to edit the privileges of an existing user.
- d. Click **Save**.

For example, if you have a Cloud Plug-in installed, and are using the Cloud features in Enterprise Manager, then ensure that the `CLOUD_ENGINE_USER` is also granted **View** privileges on credentials associated with Software Library. Since the `CLOUD_ENGINE_USER` is a hidden user account, the owner of the named credential will not be able to grant him View privileges from the Enterprise Manager UI. To handle this situation, (especially on a Windows host where OMS Agent Filesystem is the recommended approach for setting up Software Library) you can run the following EMCLI commands:

```
emcli login -username=<username> -password=<password>
emcli grant_privs -name=CLOUD_ENGINE_USER -
privilege="GET_CREDENTIAL;CRED_NAME=<>:CRDED_OWNER=<>"
```

To change the privilege, select the administrator, and click **Change Privilege**. In the Select Privilege dialog box, change the privilege to **Edit** or **Full**, and then click **OK**.

6. After entering all the details, click **Test and Save**. If the host credentials are correct, then the test is successful and the credentials get saved.

Enterprise Manager Administrators will be able to grant privileges to other administrators while creating the credential or by granting the privileges when editing the credential.

From the Named Credential page, you can **Create** a new named credential, **Edit** an existing credential, **Manage Access** (grant/revoke privileges), **Delete**, **Test**, **View References**, or click the *Query by Example* icon to filter the list of named credentials.

Only the credential owner can manage access their credentials. When a credential owner views references, he can see all references even if not owned by him. Whereas a user who does not own the credential, will see only their own references.

#### 2.4.1.1.4 Access Control for Named Credentials

 **Note:**

You must have the Named Credentials resource privileges in order to create a named credential.

The access control model for named credentials adhere to the following rules:

- Only named credential owners can grant privileges on named credentials they have created to other Enterprise Manager grantee administrators.
- Enterprise Manager Super Administrators cannot obtain any privileges on a newly created named credential until he is explicitly granted privileges on the named credential.
- Enterprise Manager administrators regardless of privilege level, cannot see the sensitive fields such as passwords and private keys from the console UI. This is achieved by replacing password with "\*" characters.
- Named credential privileges cannot be assigned to a role. This eliminates back door entry by Enterprise Manager Super Administrators to grant themselves privileges on the credentials for which they do not have explicit access.
- An Enterprise Manager grantee administrator cannot view other administrators' credentials unless an explicit grant is provided by the owner. Even Enterprise Manager Super Administrators cannot view other users' named credentials by default.
- Any Enterprise Manager administrator can create his own named credentials and, by default, has FULL privileges on the named credentials owned.

#### 2.4.1.1.5 Authentication Scheme

An authentication scheme is the type of authentication supported by a target type. For example, a host can support a username/password-based authentication, Public Key authentication or Kerberos authentication. In fact, each target type in an enterprise may support different authentication schemes. To accommodate the many authentication schemes that can exist in a managed environment, Enterprise Manger allows you to configure the credentials for these authentication schemes.

 **Note:**

All the credentials owned by an Enterprise Manager administrator will be deleted if that administrator is deleted from Enterprise Manager. All references and grants to grantee administrators of that named credential will also be deleted. Since access to a named credential is not granted to a Super Administrator, by default, a super administrator cannot re-assign a named credential owned by another administrator, by default.

#### 2.4.1.2 Privileged Credentials

Privileged Credentials specify root users' authentication information on a system. Privileged credentials are the root account details used to perform privileged actions

like executing root scripts. Privileged credentials are intended for privileged or power users. In Enterprise Manager 11g, each provisioning user required SUDO privileges that had to be explicitly granted. However, in Enterprise Manager 13c, you must set up privileged credentials to perform typical root user actions with SUDO privileges.

### 2.4.1.2.1 Creating Privileged Credentials

To create privileged credentials, follow these steps:

1. Create the Named credentials using the steps mentioned in "[Creating Named Credentials](#)".
2. On the Named Credentials page, select the credential, and then click **Edit**.
3. On the Edit Credential Properties page, in the Credential Properties section, edit the existing **UserName** and **Password** required to access the host machine, and from the Run Privilege drop down list, do one of the following:
  - Select **None**, if you are using operating system host credentials (like *Oracle*) or the Oracle Home Owner credentials.
  - When you do not have access to the operating system host credentials or the `root` credentials of the host machine, then select **Sudo** or **PowerBroker** to `sudo` (or `pbrun`) to the host machine using the credentials of another operating system user. To use the credentials of other users, in the **Run As** field, you need to enter operating system host credentials (like *Oracle*) or Oracle Home owner credentials of the host user.

### 2.4.1.3 Monitoring Credentials

Monitoring credentials are used only by the Management Agent during the monitoring of specific types of targets. Targets requiring monitoring credentials will be displayed in the console. When targets are added to Enterprise Manager an administrator with the correct privilege will set up the monitoring credentials. An administrator must have the `ADD_TARGET` privilege to discover a target, and to enter the credentials for that target, he needs the `CONFIGURE_TARGET` privilege. Monitoring credentials are stored in the repository and propagated to the Agent. If the credentials are not set, the target will appear in the broken or down state, there will also be Metric Collection errors as the Agents will be unable to monitor without credentials.

To create or edit a monitoring credentials, from the **Setup** menu, choose **Security** and then **Monitoring Credentials**.

To modify monitoring credentials, select the desired target type and click **Manage Monitoring Credentials**. The monitoring credentials page for the selected target type displays. Alternatively, you can also modify monitoring credentials using EM CLI, as shown in the following example.

```
./emcli set_monitoring_credential -target_name=mytarget.myco.com
-target_type=host -cred_type=HostCreds -set_name=Bob
-attributes="HostUserName:dwwolf;HostPassword:xxxxx:PDPTYPE:SUDO;RUNAS:root"
```

### 2.4.1.4 Preferred Credentials

Preferred credentials are used to simplify access to managed targets by storing the login information for those targets in the Management Repository. For example, for a database target one may have multiple logins, but store a preferred username/password credential to log in to perform specific operations. With preferred credentials,

administrators can access an Enterprise Manager target that recognizes those credentials without being prompted to log in to the target, as the login happens automatically with those preferred credentials. Preferred credentials can also be used to carry out administrative operations using the job system. Unlike named credentials, which defines an independent entity, containing the username/password or public/private key, along with a Credential Type and optional parameters, which can be granted to grantee administrators by a named credential owner, a preferred credential is set up by each administrator for any target that they wish to access in a more convenient way.

To create a preferred credential:

1. From the Setup menu, select **Security** and then **Preferred Credentials**. The Preferred Credentials page displays.
2. Choose a target type from the list.
3. Click **Manage Preferred Credentials**. The Preferred Credentials page for the selected target type displays.

**Example:** An Enterprise Manager target owner defines two preferred credential sets for a host target: One named *HostCredNormal* and the other is named *HostCredPriv*. For simple operations he uses *HostCredNormal* as it uses a regular user (*myusername/password*) such as *oracle/oracle123*. However, he uses *HostCredPriv* for more privileged operations on that host as it uses the root user (*root/rootpasswd*). When submitting jobs, depending on the job, he could use either of these credential sets.

- **Default Preferred Credentials:** Default credentials are configured for a specific target type and is available for all the targets of that target type. It will be overridden by target preferred credentials.
- **Normal Host Credentials** (*HostCredNormal* in the example). Perform normal administrative operations.
- **Privileged Host Credentials** (*HostCredPriv* in the example). Perform privileged operations requiring root access.
- **Target Preferred Credentials:** Target preferred credentials are credentials set for a specific target. Target preferred credentials could be used by applications such as the job system, notifications, or patching. For example, if the administrator chooses to use target preferred credentials while submitting a job, then that target preferred credential set for the target (target credentials) will be used. If the target preferred credential is not present, then the default preferred credential (for the target type) will be used. If the default preferred credentials are not present, the job will fail. If not specified preferred credentials refer to preferred target credentials.

For example, to set the host preferred credentials, from the **Setup** menu, choose **Security** and then **Preferred Credential**. In the Preferred Credentials page, select the **Host** target type from the table and click **Manage Preferred Credentials**. The Host Preferred Credentials are displayed.

On this page, you can set both default and explicit preferred credentials for the host target types.

#### 2.4.1.4.1 Global Preferred Credentials

Beginning with Enterprise Manager Release 12.1.0.4, preferred credentials can be globally scoped. Global preferred credentials provide a convenient way to implement

system-wide credentials by allowing an administrator (with required privileges) to apply these credentials to all users for a specific target or to apply them to all users for a target type.

The following graphic shows the Host Preferred Credentials page. Settings on the *My Preferences* tab refer to the preferred credentials set by an administrator to apply to a specific target or target type.

Settings on the *Global Preferences* tab refer to the preferred credentials set by an Administrator (with required privileges) to apply to all users for a specific target or to apply to all users for all target types.

#### 2.4.1.4.1.1 Required Privileges

The following privileges are required to use Global Preferred Credentials:

- *OPERATOR\_TARGET*: Required to use a Global Preferred Credential.
- *FULL\_TARGET*: Required to set target-specific scope at the Global Preferences level.
- *FULL\_ANY\_TARGET*: Required to set target type scope at the Global Preferences level.

#### 2.4.1.4.1.2 Hierarchy of Credential Preference

Preferred credentials are resolved in specific order. User-scoped preferences will always takes precedence. Enterprise Manager first searches at the target level, searching first for the preferred credential for that target name. If not found, it then searches for the target type (default) preferred credential. If these user-scoped preferences are not found, Enterprise Manager then repeats the same search at the Global scope, searching first for the target name preferred credential then target type (default) preferred credential.

Enterprise Manager provides a Credential Hierarchy table that depicts the hierarchy determining which preferred credential is used by the system.

The credential search order is always the same and continues until a preferred credential is found: If credentials are not found at one level, Enterprise Manager moves to the next level in the sequence as shown in the following table.

**Table 2-3 Hierarchy of Credential Preference**

| User/Target | User 1 | User 2  | User 3 | ... | All Users |
|-------------|--------|---------|--------|-----|-----------|
| Target 1    |        |         |        |     |           |
| Target 2    |        |         |        |     |           |
| Target 3    |        | Level 1 |        |     | Level 3   |
| .           |        |         |        |     |           |
| .           |        |         |        |     |           |
| .           |        |         |        |     |           |
| All Targets |        | Level 2 |        |     | Level 4   |

This example illustrates the hierarchy of preferred credentials chosen to complete a job if none is explicitly chosen during job execution. The order in which the preferred credential is chosen is always the same. In this example we will assume the job is

running as User 2. The following order is always observed until a preferred credential is set at that level.

- **Level 1** - My Preferences, Target Preferred Credential
- Level 2 - My Preferences, Default (Target Type) Preferred Credential
- Level 3 - Global Preferences Target Preferred Credential
- Level 4 - Global Preferences, Default (Target Type) Preferred Credential

It is assumed that the credential has been tested during setup. If a credential is not set at a specific level, the credential sub-system moves on to the next level (checking from level 1 to level 4) until a credential is found. The first credential found is the credential used for the job. Credentials set at subsequent levels are ignored.

*Users preferences (preferred credentials), if set, always override global preferences.*

### 2.4.1.5 Saving Preferred Credentials for Hosts and Oracle Homes

To save the credentials as preferred credentials in Cloud Control, follow these steps:

1. In Cloud Control, from the Setup menu, select **Security**, then select **Preferred Credentials**. The Preferred Credentials page displays.
2. On the Preferred Credentials page, select either **Host** or **Oracle Home** from the list of target types, and click **Manage Preferred Credentials**.

**Note:** For setting up preferred credentials for virtual server targets, select **Oracle VM Server** as the target type and click the **Set Credentials**.

- If you select **Host** for provisioning tasks, then the **Host Preferred Credentials** page appears.
  - On the Host Preferred Credentials page, in the Target Preferred Credentials section, select the host target on which you want to provision, and click **Set**.
3. On the Preferred Credentials page, from the table, select either **Host** or **Oracle Home**, and click **Manage Preferred Credentials**.
    - If you select Oracle Home for patching tasks, then the Oracle Home Preferred Credentials page appears.
    - On the Oracle Home Preferred Credentials page, in the Target Preferred Credentials section, select the Oracle home you want to patch. Ensure that you set both Normal and Privileged credentials for the targets selected, and click **Set**.

### 2.4.1.6 Saving Preferred Credentials to Access My Oracle Support

To register the My Oracle Support credentials as preferred credentials in Cloud Control, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **My Oracle Support**, and then, click **Set Credentials**.
2. On the My Oracle Support page, provide the My Oracle Support credentials, and click **Apply**.

Oracle recommends you to register the My Oracle Support credentials as preferred credentials in Cloud Control so that you do not have to explicitly provide the

credentials every time you access the My Oracle Support console, which is integrated within the Cloud Control console.

### 2.4.1.7 Managing Credentials Using EM CLI

You can manage passwords using EM CLI verbs. Using EM CLI, you can perform such actions as:

- Change the database user password in both the target database and Enterprise Manager.

```
emcli update_db_password -change_at_target=Yes|No -change_all_reference=Yes|No
```

- Update a password which has already been changed at the host target.

```
emcli update_host_password -change_all_reference=Yes|No
```

- Set preferred credentials for given users.

```
emcli set_preferred_credential
-set_name="set_name"
-target_name="target_name"
-target_type="ttype"
-credential_name="cred_name"
[-credential_owner ="owner"]
```

And

```
emcli set_preferred_credential
-set_name="set_name"
-target_name="target_name"
-target_type="ttype"
-credential_name="cred_name"
[-credential_owner ="owner"]
```

- Determine if a specific target type has preferred credentials configured for it..

```
bin/emcli list -res=PreferredCredentials -bind="TargetType = 'host'
```

For a complete list of credential management verbs, refer to the *Enterprise Manager Command Line Interface* guide.

### 2.4.1.8 Host Authentication Features

This section covers the following topics:

- [Setting Up SSH Key-based Host Authentication](#)
- [Setup Example Session](#)
- [Setting Up Host Preferred Credentials Using SSH Key Credentials](#)
- [Setting Up Host Preferred Credentials Using SSH Key Credentials \(pre-12.1.0.4\)](#)
- [Authenticating host credentials](#)
- [Configuring the PAM "emagent" Service](#)
- [Sudo and PowerBroker Support](#)
- [Creating a Privilege Delegation Setting](#)



### 2.4.1.8.1 Setting Up SSH Key-based Host Authentication

Secure Shell or SSH allows data to be exchanged over the network using a secure channel between two devices. SSH is used primarily on Linux and Unix based systems. SSH was designed as a replacement for FTP, telnet and other unsecure remote shells, which send information, notably passwords in plaintext, leaving them open for interception. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. SSH also protects the system against DNS spoofing attacks. This makes SSH a better choice in production environments over telnet/FTP and other username/password based authentications.

You can configure Enterprise Manager to use SSH while performing management operations, thus allowing Enterprise Manager administrators to leverage the security features provided by SSH along with the management capabilities of Enterprise Manager. When authenticating in this mode, the Agent acts as a Java SSH client and connect to the host using the username/password provided in the credential.

Enterprise Manager allows you to store a public-private key pair for administrators and allows them to view and install the public key on the hosts. Administrators can then submit jobs/patching operations in which they specify the credential that refers to the private key to perform the operation. The OMS passes the private key to the Agent along with the commands and the command parameters. Agent invokes the Java SSH client and attempts to connect to the host using the private key. Since the host already has the public key installed, it identifies the private key and successfully authenticates the Agent's Java SSH client. The Agent can now run the commands through the SSH client on the host to perform the requested operations. The username used in the communication must be a valid OS user on both the host and the OMS. This is the username used in the named credential and not the username of the administrator invoking the operation.

 **Note:**

For Enterprise Manager Grid Control release 12.1.0.3 and earlier, to use SSH credentials with privilege delegation you must add the following parameter and value to the `emd.properties` file:

```
EMDPD_PASSWORD_PROMPT_SUDO=FALSE
```

From release 12.1.0.4 this is handled automatically.

### 2.4.1.8.2 Setup Example Session

To generate, manage, or convert SSH authentication keys, you use the *SSH-keygen* utility available on UNIX systems. This utility SSH-keygen tool provides different options to create with different strengths RSA keys for SSH protocol version 1 and RSA or DSA keys for use by SSH protocol version 2.

 **Note:**

The procedure shown in this example assumes that you have a firm understanding of SSH setup procedures and user and host equivalence using public private key pair using SSH.

You are now ready to add the credential to Enterprise Manager.

1. From the **Setup** menu, select **Security**, then select **Named Credentials**.
2. On the Named Credentials page, click **Create**. The Create Credential page displays.
3. Enter a Credential Name. For example, SSHCRED1.  
Note: The SSHCRED1 credential set will be used in [Setting Up Host Preferred Credentials Using SSH Key Credentials \(pre-12.1.0.4\)](#)
4. Select **Host** from the **Authenticating Target Type** drop-down menu.
5. Select **SSH Key Credentials** from the **Credential Type** drop-down menu.
6. Ensure that the SSH private key/public key files have been copied to the host on which the browser is running. Doing so makes navigating to the files from within the console easier when you click **Browse** in the next step.
7. From the **Credential Properties** region, enter a **UserName**. This username is a valid OS user that resides on both the Host and the OMS.
8. From the **Credential Properties** region, click **Browse** for **Public Key** and **Private Key** to upload the generated public key/private key files.
9. Click **Test and Save** to verify the credentials and save them. The new named credential will appear.

### Example 2-11 Setting Up SSH key-based Authentication

```
$ ssh-keygen -t rsa
```

*The command options instruct the utility to generate SSH keys (RSA key pair).*

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/myhome/.ssh/id_rsa):
```

*The path specified is the standard path to the location where SSH keys are stored (\$HOME/.ssh).*

```
Enter passphrase (empty for no passphrase)
```

*Important: passphrase is not supported for use with SSH keys in named credentials.*

```
Enter same passphrase again: (empty for no passphrase)
Your identification has been saved in /home/admin1/.ssh/id_rsa.
Your public key has been saved in /home/admin1/.ssh/id_rsa.pub.
The key fingerprint is:
bb:da:59:7a:fc:24:c6:9a:ee:dd:af:da:1b:1b:ed:7f admin1@myhost2170474
```

The ssh-keygen utility has now generated two files in the .ssh directory.

```
$ ls id_rsa id_rsa.pub
```

To permit access to the host without having SSH prompt for a password, copy the public key to the `authorized_keys` file on that system.

```
$ cp id_rsa.pub authorized_keys
```

From this point, all keys listed in that file are allowed access.

Next, perform a remote logon using SSH. The system will not prompt you for a password.

```
$ ssh myhost
The authenticity of host 'myhost (10.229.147.184)' can't be established.
RSA key fingerprint is de:a0:2a:d5:23:f0:8a:72:98:74:2c:6f:bf:ad:5b:2b.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'myhost,10.229.147.184' (RSA) to the list of known hosts.
Last login: Mon Aug 29 16:48:45 2012 from anotherhost.example.com
$
```

**Note:**

To view an instructional video [Oracle Enterprise Manager 13c: Create SSH Key Named Credentials](#), go to:

[https://apex.oracle.com/pls/apex/f?p=44785:24:0::NO:24:P24\\_CONTENT\\_ID,P24\\_PREV\\_PAGE:5724,1](https://apex.oracle.com/pls/apex/f?p=44785:24:0::NO:24:P24_CONTENT_ID,P24_PREV_PAGE:5724,1)

### 2.4.1.8.3 Setting Up Host Preferred Credentials Using SSH Key Credentials

Enterprise Manager provides out-of-box support (12.1.0.4) for the use of SSH key credentials to be available and used as preferred credentials. SSH key credential sets are used to authenticate against targets. The introduction of SSH key credential sets is useful when a username and password credential is unknown or when considering alternative security options. SSH keys use encryption methods which provide more confidentiality and integrity of data over an otherwise potentially insecure network. Providing this support out of the box, eliminates the Administrator from creating a custom SSH key credential and facilitates ease of use.

**Note:**

SSH Credentials are not supported for Windows operating systems.

To set SSH credentials as preferred credential:

1. From the **Setup** menu, select **Security** and then select **Preferred Credentials**.
2. Select the 'Agent' or 'Host' target type and then click **Manage Preferred Credential**.

The Agent Preferred Credentials Setting page displays. For more information see the "[Preferred Credentials](#)".

This page will default to the page that was last referenced by the administrator. To set the preferred credential, click the **My Preferences** tab, as shown in the image below.

- Under the Default Preferred Credential region, which sets the preferred credential for all targets of the selected target type, an Agent Target Type was chosen. See above graphic.

Select **Host Credentials** and then click **Set**.

A dialog displays listing the current choice of available Name Credentials most appropriate for this Agent Target Type. For this Administrator. Select the **SSH Credential**, and click **Save**.

The Default Preferred Credential will then display the credential which will be used for all targets of type Host for this Administrator. The below image shows that the Credential Set = Host Credential; the Target Username = test, which indicates the OS user who is used in the Named Credential.

The screenshot shows the 'Host Preferred Credentials' configuration page in the Oracle Enterprise Manager Security console. The page includes a navigation bar with 'Enterprise', 'Targets', 'Favorites', and 'History'. Below the navigation bar, there is a 'Security' section with an 'Information' box stating 'Named credential association completed successfully.' The main content area is titled 'Host Preferred Credentials' and includes a 'My Preferences' tab. A table of default preferred credentials is displayed, with the following data:

| Credential Set              | Target Username | Credential Name | Credential Owner |
|-----------------------------|-----------------|-----------------|------------------|
| Normal Host Credentials     | maubyrne        | SSHCREDS        | AMCCOLLU1        |
| Privileged Host Credentials | aime            | CS_ALL          | SBAMBORE1        |

The 'Rows Selected' count is 1.

This setting means that all Agent connections, by this administrator, will use this credential set to authenticate with all Agents.

#### 2.4.1.8.4 Setting Up Host Preferred Credentials Using SSH Key Credentials (pre-12.1.0.4)

##### Note:

The method outlined below is a work-around to be used for pre-12.1.0.4 versions of Enterprise Manager.

You can set up host *preferred credentials* to use SSH keys by creating a new credential set that uses the *HostSSHCreds* credential type. Enterprise Manager administrators then set up *preferred credentials* that use this credential set. Each

Enterprise Manager target type can have one or more preferred credential sets of pre-defined credential types.

The following steps use EM CLI to create a host preferred credential set which supports SSH key credentials. This example assumes the existence of the *named credential SSHCRED1* of type *SSH Key Credentials* created in the previous section.

1. Log into EM CLI as an Enterprise Manager Super Administrator.
2. Create a new credential set of type *HostSSHCreds*.

```
$ emcli create_credential_set -set_name=HostSSHCredSet -target_type=host -
supported_cred_types=HostSSHCreds
```

Credential set "HostSSHCredSet" created successfully.

Once the credential set is created, Enterprise Manger administrators can set up preferred credentials for this newly created credential set using either EM CLI or the Enterprise Manager console.

3. Set up *Preferred Credentials* for the newly created credential set. You can use EM CLI or the Enterprise Manger console. The following EM CLI example assumes a named credential called SSHCRED1 of type SSH Key Credentials has already been created.

```
$ emcli set_preferred_credential -target_type=host -
target_name=myhost.mycompany.com -set_name=HostSSHCredSet -
credential_name=SSHCRED1
```

Successfully set preferred credentials for target myhost.mycompany.com:host.

Once the credential set is created and preferred credentials have been set up, whenever the HostSSHCredSet credential set is used for any of the Enterprise Manager operation, that operation will use SSH credentials as defined in the named credential SSHCRED1. The following graphic shows the HostSSHCredSet credential set listed as a default preferred credential for host targets.

| Credential Set              | Target Username | Credential Name | Credential Owner |
|-----------------------------|-----------------|-----------------|------------------|
| Normal Host Credentials     |                 |                 |                  |
| Privileged Host Credentials |                 |                 |                  |
| HostSSHCredSet              |                 |                 |                  |

You can now set the preferred credentials of regular regular Enterprise Manager administrators to use the SSHCRED1 named credential by editing/creating an administrator and granting *Named Credential* resource privileges.

#### 2.4.1.8.5 Authenticating host credentials

The Enterprise Manager Agent can use two methods to authenticate OS credentials:

- Traditional Authentication
- PAM Authentication

With *traditional authentication*, credentials submitted by users are compared with entries in the system's password database -- that is, against entries found in */etc/*

`passwd` and related files, and in remote extensions to those files as defined by OS-specific configuration such as `/etc/nsswitch.conf` or `/etc/netssvc.conf`.

With *PAM authentication*, the Agent uses a feature of the operating system called PAM, or Pluggable Authentication Modules, to validate the credentials submitted by users. PAM is a framework that allows administrators to specify which of a wide range of authentication mechanisms (such as LDAP, Kerberos, RADIUS) should be used by PAM-aware applications. An application identifies itself to PAM using a service-name. If the administrator has configured a PAM definition for that service-name, then the rules in that definition are applied for that application's authentication requests. If not, then the rules for a special default service-name, "other", are used.

The Enterprise Manager Agent identifies itself to PAM using the service name "emagent". If the administrator has explicitly defined an "emagent" PAM service, then the agent will attempt only PAM authentication -- if the method or methods defined for the "emagent" service do not accept a set of credentials, then the operation associated with those credentials will fail.

If the administrator has **not** explicitly defined an "emagent" PAM service, then the Agent will first attempt traditional authentication; if that attempt fails, then it will attempt PAM authentication, using the "other" service definition. If either the traditional or PAM authentication attempt succeeds, then the operation associated with the credentials will proceed.

#### 2.4.1.8.6 Configuring the PAM "emagent" Service

PAM is a complex and open-ended framework, and general advice on configuring it is beyond the scope of this document. Typically, though, a customer who wants Enterprise Manager to authenticate host credentials using PAM will already have some other service defined to use the same PAM rules, and that other service's definition can form the basis for the emagent one.

For example, suppose a customer's Oracle Enterprise Linux host has already been configured for its SSH daemon to use a mix of Kerberos and local authentication when accepting connections. The SSHD service definition file, `/etc/pam.d/sshd`, might have the following set of authentication rules:

```
auth sufficient pam_fprintd.so
auth sufficient pam_unix.so nullok
auth requisite pam_succeed_if.so uid >= 500 quiet
auth sufficient pam_krb5.so use_first_pass
auth required pam_deny.so
```

Here, if the customer has access to a fingerprint scanner attached to the host, authenticate based on that. If finger print authentication does not work, try traditional authentication. If that fails, **and** if the user's UID is 500 or higher, try kerberos authentication. If that fails, too, then fail the entire authentication.")

The customer might decide that Enterprise Manager should follow the same authentication process, but exclude the fingerprint-scanner check, since Enterprise Manager will not generally have access to the user's finger when it needs to run a job or collect an authenticated metric. So she would create a new service definition file, `/etc/pam.d/emagent`, and include all the same "auth" lines as in the SSHD definition above, except for the `pam_fprintd.so` one:

```
auth sufficient pam_unix.so nullok
auth requisite pam_succeed_if.so uid >= 500 quiet
```

```
auth sufficient pam_krb5.so use_first_pass
auth required pam_deny.so
```

Details of the authentication methods to be used will vary from customer to customer, and the exact method of configuration will vary from platform to platform. But this general approach to defining an Agent PAM service definition should generally be useful: identify an existing service to use as your base, copy that service's definition, and remove any rules that are not appropriate for Enterprise Manager's use.

### 2.4.1.8.7 Sudo and PowerBroker Support

Privilege Delegation, PDP, allows an administrator to perform privileged activities with the privileges of another user. Enterprise Manager uses two authentication utility tools to achieve Privilege Delegation, they are Sudo and PowerBroker.

**Sudo:** Sudo allows a permitted user to execute a command as the super user or another user, as specified in the sudoers file. If the invoking user is root or if the target user is the same as the invoking user, no password is required. Otherwise, sudo requires that users authenticate themselves with a password by default. Once a user has been authenticated, a timestamp is updated and the user may then use sudo without a password for a short period of time (5 minutes unless overridden in sudoers). sudo determines who is an authorized user by consulting the `/etc/sudoers` file. For more information, see the manual page on sudo (`man sudo`) on Unix. Enterprise Manager authenticates the user using sudo, and executes the script as sudo. For example, if the command to be executed is `foo -arg1 -arg2`, it will be executed as `sudo -S foo -arg1 -arg2`.



#### Note:

The certified SUDO versions are 1.6.7 to 1.6.9. Also, note that SUDO 1.7.2 and higher versions are also supported. The certified PBRUN versions are 4.0.8 and 5.x. Higher versions of these utilities may continue to work unless some fundamental changes have been introduced to their behavior.

**PowerBroker:** BeyondTrust PowerBroker enables UNIX system administrators to specify the circumstances under which other people may run certain programs such as root (or other important accounts). The result is that responsibility for such actions as adding user accounts, fixing line printer queues, and so on, can be safely assigned to the appropriate people, without disclosing the root password. The full power of root is thus protected from potential misuse or abuse—for example, modifying databases or file permissions, erasing disks, or more subtle damage. BeyondTrust PowerBroker can access existing programs as well as its own set of utilities that execute common system administration tasks. Utilities being developed to run on top of BeyondTrust PowerBroker can manage passwords, accounts, backups, line printers, file ownership or removal, rebooting, logging people out, killing their programs, deciding who can log in to where from where, and so on. They can also provide TCP/IP, Load Balancer, cron, NIS, NFS, FTP, rlogin, and accounting subsystem management. Users can work from within a restricted shell or editor to access certain programs or files as root. See your PowerBroker documentation for detailed setup and configuration information.



 **Note:**

PowerBroker 7.1.1 has been tested and is the recommended minimum version.

Enterprise Manager Privilege Delegation uses these tools (Sudo and PowerBroker), together with the use of Named Credentials, to provide a framework to allow Administrators to perform privileged activities.

There are many operations within an organization, where an administrator will need elevated privileges to perform specific tasks. For example, for all the provisioning and patching tasks in Cloud Control, Named Credentials must be set up for normal operating system user account (oracle) and Named credentials for privileged user accounts (root). If you do not have access to either of these accounts, then you can use SUDO or PowerBroker access to switch users to perform the tasks. Privilege

Delegation offers the following advantages:

- You have the flexibility to use either SUDO or PowerBroker within the same framework.
- Using the framework, you can now run PowerBroker in a password-less or password-protected mode.
- You can create a template with these Privilege Delegation settings and reuse that template for multiple hosts. This not only allows you to standardize Privilege Delegation setting across your enterprise, but also facilitates and simplifies the process of configuring and management of Privilege Delegation Settings.
- You can use the Privilege Delegation settings not only for deployment procedures, but also for jobs in Cloud Control.

The following example explains the different users in the Privilege Delegation process:

**Example:** Consider three users:

*User1* – called EMUSER, is an Enterprise Manager Admin logged into either Cloud Control or EM CLI

*User2* – called OSUSER1, is a target host OS user.

*User3* – called OSUSER2, is a target host OS user.

EMUSER has a Named Credential for OSUSER1. In which sudo is configured. The Named credential says run as OSUSER2.

The Internal steps for the Privilege Delegation would be as follows:

1. Log in to a system as OSUSER1
2. Authenticate using OSUSER1's password
3. Launch sudo to become OSUSER2
4. Run the specified command as OSUSER2.

When the command specified is run. It's as if OSUSER2 has logged in. For example if the "id" command is run, it would display as OSUSER2.



### 2.4.1.8.7.1 Authentication Utility Tools Configuration

The authentication utility tools supported by Enterprise Manager are `sudo` and `pbrun`. These tools reside on the target host with the management Agent and before correct operation, must be configured appropriately. The following section outlines these tools and their associated configuration file.

Administrators can set up `sudo` or `pbrun`, based on their configuration file entries to assign specific Enterprise Manager functional privileges to their OS users. The Management Agent uses a trusted executable called `nmosudo`, using the `nmosudo` executable the Agent verifies, via a cryptographic handshake, the source of the request. Then based on the configuration files of `sudo` or `pbrun`, allows a less privileged user to run `nmosudo` as a more privileged user.

Enterprise Manager guarantees that the `nmosudo` executable only honors requests to run remote operation requests from the OMS via the Agent. `nmosudo` will not run the remote operation if it cannot validate that the request came from the Agent. Thus, it will not be possible for user 'johndoe' to invoke `nmosudo` directly from the command line and run a Perl script as user 'oracle'.

In Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1) [with or without Bundle Patch 1], `nmosudo` was located in the agent instance directory. For example, `/u01/oracle/agent/agent_inst/bin/nmosudo`.

In Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) and subsequent releases, this location has changed. Now, `nmosudo` is present in the `sbin` directory, which is in the agent base directory. For example, `/u01/oracle/agent/sbin/nmosudo`.

Therefore, when you install or upgrade to Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2), you must modify the PDP configuration files to include the new location of `nmosudo`.

### 2.4.1.8.7.2 Sudo Configuration



#### Note:

The certified SUDO versions are 1.6.7 to 1.6.9. Also, note that SUDO 1.7.2 and higher versions are also supported.

For more information, see the man page on `sudo` (`man sudo`) on Unix.

Sample entries for the `sudo` configuration file (`/etc/sudoers`) are shown below. The general format for the files is as follows:

```
root ALL=(ALL) ALL
```

This means that the root user can execute from ALL terminals, acting as ALL users, and run ALL commands.

#### Sample 1

```
Sample /etc/sudoers file should have following entry
If you do not have access to oracle and root accounts,
then add the following entries into the file:
```

```
#usage:
#[user] [terminal]=[as other user] [command]

#where: user = the user
terminal = terminal from where user can run sudo # cmd
as other user = which user the first user may act # as
command = which commands can be run which using # sudo

johndoe ALL=(oracle) /u01/oracle/agent/sbin/nmosudo *
johndoe ALL=(root) /u01/oracle/agent/sbin/nmosudo *

#Where, the user johndoe can access sudo from any terminal #to run as oracle the
nmosudo executable with all commands, #passed from the console.
```

### Sample 2

```
If you have access to the oracle account,
but not to the root account,
then only add the following entry into the file:
johndoe ALL=(root) /u01/oracle/agent/sbin/nmosudo *

#Where, the user johndoe can access sudo from any terminal #to run as root the
nmosudo executable with all commands, #passed from the console.
```

#### Note:

This example illustrates how the SUDOERS file can be configured to allow users to restrict only a subset of commands.

All commands that are executed thru Enterprise Manager using SUDO will be prefixed with the following:

```
<AGENT_HOME>/sbin/nmosudo DEFAULT_PLUGIN DEFAULT_FUNCTIONALITY
DEFAULT_SUBACTION DEFAULT_ACTION <Command-to-executed-with-args>
```

Customers can use this to restrict the list of commands they want users to use.

For example, if *johndoe* is allowed to execute only `root.sh` as root, the following can be added to the SUDOERS file

```
johndoe ALL=(root) <AGENT_HOME>/sbin/nmosudo DEFAULT_PLUGIN
DEFAULT_FUNCTIONALITY DEFAULT_SUBACTION DEFAULT_ACTION root.sh
```

### Sample 3

```
ALL=(ALL)/u01/oracle/agent/sbin/nmosudo DEFAULT_PLUGIN DEFAULT_FUNCTIONALITY
DEFAULT_SUBACTION DEFAULT_ACTION perl -e exit 0,/u01/oracle/agent/sbin/nmosudo
DEFAULT_PLUGIN DEFAULT_FUNCTIONALITY DEFAULT_SUBACTION DEFAULT_ACTION id
```

This example allows the user to perform a basic PERL test, and run only `id` command.

#### 2.4.1.8.7.3 Powerbroker Configuration

BeyondTrust PowerBroker enables UNIX system administrators to specify the circumstances under which other users may run certain programs such as `root` (or

other important accounts). The result is that responsibility for such actions as adding user accounts, fixing line printer queues, and so on, can be safely assigned to the appropriate people, without disclosing the root password. The full power of root is thus protected from potential misuse or abuse—for example, modifying databases or file permissions, erasing disks, or more subtle damage. BeyondTrust PowerBroker can access existing programs as well as its own set of utilities that execute common system administration tasks. Utilities being developed to run on top of BeyondTrust PowerBroker can manage passwords, accounts, backups, line printers, file ownership or removal, rebooting, logging people out, killing their programs, deciding who can log in to where from where, and so on. They can also provide TCP/IP, Load Balancer, cron, NIS, NFS, FTP, rlogin, and accounting subsystem management. Users can work from within a restricted shell or editor to access certain programs or files as root. See your PowerBroker documentation for detailed setup and configuration information.



#### Note:

PowerBroker 7.1.1 has been tested and is the recommended minimum version.

If you want to use pbrun authentication utility, then before editing a Deployment Procedure, update the `/etc/pb.conf` file to allow a normal user to switch to another user who has the privileges to run the Deployment Procedure. A sample PowerBroker configuration file (`/etc/pb.conf`) would contain:

#### Sample:

```
if(user=="johndoe") if(command=="u01/oracle/agent/sbin/nmosudo *")
// /u01/oracle/agent/ Agent Home location
```

```
{
 switch (requestuser)
 {
 case "root":
 runuser="root";
 break;
 case "oracle":
 runuser="oracle";
 break;
 default:
 reject;
 }
 accept;
}
```

The above example allows user johndoe to execute all commands passed from the console via nmosudo as root and as oracle. Refer to sudo/PowerBroker documentation for detailed configuration information.

#### 2.4.1.8.7.4 Privilege Needed for Creating a Privilege Delegation

Enterprise Manager allows you to create Privilege Delegation settings either by creating the setting directly on a host target, or by creating a Privilege Delegation Setting Template that you can apply to multiple hosts.

- **VIEW:** Administrators with View privileges on these host targets will be able to view those privilege delegation settings.
- **FULL:** Administrators with Full privileges on host targets can create privilege delegation settings for that host.

Enterprise Manager Super Administrators can configure privilege delegation settings for any host target.

#### 2.4.1.8.7.5 Creating a Privilege Delegation

The use of Privilege Delegation can be invoked using any of the following methods:

- Cloud Control console
- EM CLI
- Privilege Delegation template

*Privilege Delegation Templates:* Enterprise Manager allows for a default Privilege Delegation template to be set and also for that template to be applied to multiple hosts. This prevents an Administrator from having to apply a Privilege Delegation setting on a host-by-host basis, especially when the same Privilege Delegation setting is being applied to all host targets. This feature is particularly useful when many host targets have been simultaneously added to Enterprise Manager. This feature is also available via EM CLI by using the `set_default_privilege_delegation_setting` verb.

##### Setting Privilege Delegation from Cloud Control

To set Privilege Delegation from the Cloud Control console:

1. From the **Setup** menu, select **Security**, then select **Privilege Delegation**.
2. On the Manage Privilege Delegation Settings page, select the host name, and then click **Edit**. This Edit Host Privilege Delegation dialog displays.
3. Select **Sudo** or **PowerBroker**, and specify the location where SUDO or PowerBroker is located (for PowerBroker, you can optionally provide the password prompt) to configure the host with a Privilege Delegation setting.
4. Click **Save**.

#### 2.4.1.8.7.6 Setting Privilege Delegation Templates from Cloud Control

You can apply Privilege Delegation settings on a per host basis or to multiple hosts simultaneously. Enterprise Manager allows you to define a default Privilege Delegation template that applies Privilege Delegation settings to multiple hosts. Templates are particularly useful when many host targets have been added simultaneously to Enterprise Manager. This functionality is also available via EM CLI by using the `set_default_privilege_delegation_setting` verb. See "[Setting Privilege Delegation via EM CLI](#)" for more information.

1. In Cloud Control, from the **Setup** menu, select **Security**, then select **Privilege Delegation**. The Manage Privilege Delegation page displays.
2. Click the **Templates** tab to display the Manage Privilege Delegation Templates page.
3. Click **Create**. The **Create Template** dialog displays.
4. Select a privilege delegation type, either **Sudo** or **PowerBroker**.

5. Enter a name for the template and specify the location where SUDO or PowerBroker is located (for PowerBroker, you can optionally provide the password prompt), and click Save.

For example, if you select SUDO, and if sudo is located in the /usr/sbin/directory, then in the Sudo Command field you need to enter /usr/sbin/sudo -E -u %RUNAS% %COMMAND%.

 **Note:**

If you do not apply the privilege delegation template to a target, and if you configure a step in the deployment procedure to run in Privilege Delegation mode, then the deployment procedure for that target runs the step in normal mode instead.

Once you have created a privilege delegation setting, you must apply this setting to selected targets. This setting can be applied to one more hosts or to a composite (Group) target (the group must contain at least one host target). You can apply a Privilege Delegation setting using the Cloud Control console. From the **Setup** menu, choose **Security** and then **Privilege Delegation**.

#### 2.4.1.8.7.7 Setting Privilege Delegation via EM CLI

The following examples create a setting named *sudo\_setting*. The setting is of type SUDO, and the Sudo path used is /usr/local/bin/sudo. Sudo arguments are:

```
-S -u %RUNAS%%COMMAND%
```

##### Example 1 - Command-Line

```
emcli create_privilege_delegation_setting
 -setting_name=sudo_setting
 -setting_type=SUDO
 -settings="SETTINGS:/usr/local/bin/sudo -S -u %RUNAS% %COMMAND%"
```

##### Example 2 - Scripting and Interactive

```
create_privilege_delegation_setting
 (setting_name="sudo_setting",
 setting_type="SUDO",
 settings="SETTINGS:/usr/local/bin/sudo -S -u %RUNAS% %COMMAND%")
```

The following examples create a setting named *pb\_setting*. The setting is of type POWERBROKER, and the PowerBroker path used is /etc/pbrun. Arguments are:

```
%RUNAS%%PROFILE%%COMMAND%
```

##### Example 3 - Command-Line

```
emcli create_privilege_delegation_setting
 -setting_name="pb_setting"
 -setting_type="POWERBROKER"
 -settings="SETTINGS,/etc/pbrun %RUNAS% %PROFILE% %COMMAND%"
 -separator="settings;"
 -subseparator="settings=, "
```

##### Example 4 - Scripting and Interactive

```
create_privilege_delegation_setting
(setting_name=pb_setting
,setting_type=POWERBROKER
,settings="SETTINGS,/etc/pbrun %RUNAS% %PROFILE% %COMMAND%"
,separator="settings="
,subseparator="settings=,")
```

The following examples are similar to examples 3 and 4, except that they also add arguments `PASSWORD_PROMPT_STRING` and `Password`.

#### Example 5 - Command-Line

```
emcli create_privilege_delegation_setting
-setting_name="pb_setting"
-setting_type="POWERBROKER"
-settings="SETTINGS,/etc/pbrun %RUNAS% %PROFILE% %COMMAND%";
PASSWORD_PROMPT_STRING,password:"
-separator="settings="
-subseparator="settings=,"
```

#### Example 6 - Scripting and Interactive

```
create_privilege_delegation_setting
(setting_name=pb_setting
,setting_type=POWERBROKER
,settings="SETTINGS,/etc/pbrun %RUNAS% %PROFILE% %COMMAND%";
PASSWORD_PROMPT_STRING,password:"
,separator="settings="
,subseparator="settings=,")
```

### 2.4.1.8.7.8 Testing Privilege Delegation Settings

After creating a privilege delegation template and before applying it to a *deployment procedure*, Oracle recommends you to test the privilege delegation setting.

The following is an example that describes how you can register your credentials as preferred credentials, and also choose to run as another user, and then test the settings by creating a job that checks whether a command is being as normal user or as another user using privilege delegation mechanism.

1. In Cloud Control, from the **Setup** menu, select **Security**, then select **Preferred Credentials**. The Preferred Credentials page displays.
2. On the Manage Privilege Delegation Settings page, from the Related Links section, click **Preferred Credentials**.
3. Select **Host** from the **Target Type** list and click **Manage Preferred Credentials**. The Host Preferred Credentials page displays.
4. From the Target Preferred Credentials region, select the **host**, and then click **Set**.
5. In the Select Named Credential dialog box, specify the normal user name, the normal password, and the Run as user name that you want to switch over to using the privilege delegation mechanism. Then click **Test and Save**.
6. After registering the credentials as preferred credentials, from the Enterprise menu, select **Jobs**, and then click **Job Activity**.
7. On the Job Activity page, from the Create Job list, select OS Command, and click **Go**.

8. On the Create OS Command Job page, in the General tab, specify a name for the job. Then, from the Target section, click **Add** to add the host on which you want to run the OS command.
9. In the Parameters tab, for Command, specify the command id.
10. Click **Submit**.
11. On the Job Activity page, click the job name you just created. Cloud Control displays the status of the job. Click the status column to view its results.

Cloud Control performs the command as the user referenced in the preferred credential.

#### 2.4.1.8.7.9 Agent Support for PowerBroker

The Enterprise Manager Agent supports privilege delegation using Powerbroker as long as pbrun can be invoked with its STDIN, STDOUT and STDERR not on the TTY. You can verify this by executing the pbrun command configured with the Agent, with its STDIN, STDOUT and STDER redirected to files.

In some PowerBroker configurations with this restriction, you will see pbrun errors with the text:"Cannot read ConfirmUser oracle password: no tty" This error may vary with the version of PowerBroker you are using. In Enterprise Manager, you will see errors from any operations performed through the Agent that require PowerBroker (Jobs, secure fetchlet invocations, credential verification operations etc.). You can find the pbrun command configured with the Agent in the following directory:

```
/agent_inst/sysman/config/emd.properties
```

The property name that will hold this command template is: EMPDP\_SETTINGS\_POWERBROKER. In the following example, the above property defines the following template:

```
EMDPD_SETTINGS_POWERBROKER=/usr/local/bin/pbrun -u %RUNAS% %COMMAND%
```

#### 2.4.1.8.7.10 Starting an Agent Using Sudo or PowerBroker Credentials

When performing Agent control operations (such as starting or stopping the Agent) from the Cloud Control console, Enterprise Manager makes a secure shell (SSH) connection to the machine where the Agent is installed in order to carry out the operation. Beginning with Enterprise Manager Release 12.1.0.4, Agent control operations can be performed using Sudo or PowerBroker credentials. For example, an administrator can navigate to the Agent home page and, from the **Agent** menu, perform Agent control operations.

Using sudo allows a permitted user to execute a command as the super user or another user, as specified by the security policy, which is defined in the config file for sudo, typically located at /etc/sudoers. If the invoking user is root or if the target user is the same as the invoking user, no password is required. Otherwise, sudo requires that users authenticate themselves with a password by default. Once a user has been authenticated, a timestamp is updated and the user may then use sudo without a password for a short period of time (5 minutes unless overridden in /etc/sudoers). sudo determines who is an authorized user by consulting the /etc/sudoers file, this file can also be configured to specify sudo access to certain commands.

### 2.4.1.8.8 Creating a Privilege Delegation Setting

Enterprise Manager allows you to create privilege delegation settings either by creating the setting directly on a host target, or by creating a Privilege Delegation Setting Template that you can apply to multiple hosts.

Administrators with Full privileges on host targets can create privilege delegation settings for that host. Administrators with View privileges on these host targets will be able to view those privilege delegation settings. Enterprise Manager Super Administrators can configure privilege delegation settings for any host target.

To create a privilege delegation setting directly on a host:

1. From the **Setup** menu, select **Security**, then select **Privilege Delegation**. The Manage Privilege Delegation screen is displayed
2. Select a host from the table and click **Edit**. The Edit Host Privilege Delegation Settings dialog displays.
3. Select a privilege delegation type (Sudo or PowerBroker).
4. Enter the privilege delegation command to be used and, in the case of PowerBroker, the optional Password Prompt.
5. Click **Save** to apply the settings to the host.

Once you have created a privilege delegation setting, you must apply this setting to selected targets. This setting can be applied to one more hosts or to a composite (Group) target (the group must contain at least one host target). You can apply a Privilege Delegation setting using the Cloud Control console. From the **Setup** menu, choose **Security** and then **Privilege Delegation**.

## 2.5 Configuring and Using Cryptographic Keys

To protect the integrity of sensitive data in Enterprise Manager, a signing or verification method known as the `emkey` is used. Encryption key is the master key that is used to encrypt/decrypt sensitive data, such as passwords and preferred credentials that are stored in the Repository. The `emkey` is generated during repository creation time and is originally stored in repository database. During installation of the first OMS, `emkey` is copied to the Credential Store and removed from the repository database, that is `emkey` is secured out-of-the-box. A backup is created in `OMS_ORACLE_HOME/sysman/config/emkey.ora`.

If the `emkey` is corrupted and the backup `emkey.ora` file is lost, all the encrypted information in repository becomes useless. Hence, it is strongly recommended to create a backup of this file on some other machine, so that in case the OMS machine crashes or `emkey` gets corrupted, the backed up file can be used for recovering the environment.

When starting up, OMS reads the `emkey` from Credential Store and repository. If the `emkey` is not found or is corrupted, it fails to start. By storing the key separately from Enterprise Manager schema, we ensure that the sensitive data such as Named Credentials in the Repository remain inaccessible to the schema owner and other SYSDBA users (Privileged users who can perform maintenance tasks on the database) in the Repository. Moreover, keeping the key separate from the schema will ensure that sensitive data remain inaccessible while Repository backups are



accessed. Further, the schema owner should not have access to the OMS/Repository Oracle homes.

### Repository Encryption Algorithm

Beginning with Enterprise Manager Cloud Control Release 12.1.0.2, the Advanced Encryption Standard (AES) algorithm is used to encrypt data in the Enterprise Manager Repository. The encryption key size is 256 bits.

Prior to release 12.1.0.2, Triple Data Encryption Standard (3DES) was the encryption algorithm used to encrypt repository data.

## 2.5.1 Configuring the emkey

The `emkey` is an encryption key that is used to encrypt and decrypt sensitive data in Enterprise Manager such as host passwords, database passwords and others. The `emkey.ora` file is a copy of `emkey` should be kept in a safe location for restoration purposes.

During startup, the Oracle Management Service checks the status of the `emkey`. If the `emkey` has been properly configured, the OMS uses it for encrypting and decrypting data. If the `emkey` has not been configured properly, the following error message is displayed.

### Example 2-12 `emctl start oms` Command

```
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
emctl start oms
Starting HTTP Server ...
Starting Oracle Management Server ...
Checking Oracle Management Server Status ...
Oracle Management Server is not functioning because of the following reason:
The Em Key is not configured properly. Run "emctl status emkey" for more details.
```

## 2.5.2 `emctl` Commands

The `emctl` commands related to `emkey` are given below:

- `emctl status emkey [-sysman_pwd <pwd>]`
- `emctl config emkey -copy_to_credstore [-sysman_pwd <pwd>]`
- `emctl config emkey -remove_from_repos [-sysman_pwd <pwd>]`
- `emctl config emkey -copy_to_file_from_credstore -admin_host <host> -admin_port <port> -admin_user <username> [-admin_pwd <pwd>] [-repos_pwd <pwd>] -emkey_file <emkey file>`
- `emctl config emkey -copy_to_file_from_repos (-repos_host <host> -repos_port <port> -repos_sid <sid> | -repos_conndesc <conn desc>) -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd <pwd>] -emkey_file <emkey file>`
- `emctl config emkey -copy_to_credstore_from_file -admin_host <host> -admin_port <port> -admin_user <username> [-admin_pwd <pwd>] [-repos_pwd <pwd>] -emkey_file <emkey file>`
- `emctl config emkey -copy_to_repos_from_file (-repos_host <host> -repos_port <port> -repos_sid <sid> | -repos_conndesc <conn desc>) -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd <pwd>] -emkey_file <emkey file>`

Examples: Use example 1 if your environment is configured with a service name. for all else use example 2.

Example 1

```
emctl config emkey -copy_to_repos_from_file -repos_connDESC
'"(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<>)(PORT=<>)))
(CONNECT_DATA=(SERVICE_NAME=<>)))"' -repos_user <> [-repos_pwd <pwd>] [-
admin_pwd <pwd>] -emkey_file < emkey file>
```

Example 2

```
emctl config emkey -copy_to_repos_from_file -repos_host <host> -repos_port
<port> -repos_sid <sid> -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd
<pwd>] -emkey_file <emkey file>
```

## 2.5.2.1 emctl status emkey

This command shows the health or status of the `emkey`. Depending on the status of the `emkey`, the following messages are displayed:

- When the `emkey` has been correctly configured in the Credential Store and Repository, the following message is displayed.
- When the `emkey` has been correctly configured in the Credential Store and has been removed from the Management Repository, the following message is displayed.
- When the `emkey` is corrupted in the Credential Store and removed from the Management Repository, the following message is displayed.

### Example 2-13 emctl status emkey - Example 1

```
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
The EmKey is configured properly, but is not secure. Secure the EMKey by running
"emctl config emkey -remove_from_repos"
```

### Example 2-14 emctl status emkey - Example 2

```
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
The EMKey is configured properly.
```

### Example 2-15 emctl status emkey - Example 3

```
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
The EMKey is not configured properly or is corrupted in the credential store and
does not exist in the Management Repository. To correct the problem:
1) Get the backed up emkey.ora file.
2) Configure the emkey by running "emctl config emkey -copy_to_credstore_from_file"
```

## 2.5.2.2 emctl config emkey -copy\_to\_credstore

This command copies the `emkey` from the Management Repository to the Credential Store.

### Example 2-16 Sample Output of the emctl config emkey -copy\_to\_credstore Command

```
emctl config emkey -copy_to_credstore [-sysman_pwd <pwd>]
Oracle Enterprise Manager 13c Release 2 Cloud Control
```

Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.  
The EMKey has been copied to the Credential Store.

### 2.5.2.3 emctl config emkey -copy\_to\_file\_from\_credstore

This command copies the emkey from the Credential Store to a specified file.

#### Example 2-17 Sample Output of the emctl config emkey -copy\_to\_file\_from\_credstore Command

```
emctl config emkey -copy_to_file_from_credstore -admin_host <host> -admin_port
<port> -admin_user <username> [-admin_pwd <pwd>] [-repos_pwd <pwd>] -emkey_file
<emkey file>
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
The EMKey has been copied to file.
```

### 2.5.2.4 emctl config emkey -copy\_to\_file\_from\_repos

This command copies the emkey from the Management Repository to a specified file.

#### Example 2-18 Sample Output of the emctl config emkey -copy\_to\_file\_from\_repos Command

```
emctl config emkey -copy_to_file_from_repos (-repos_host <host> -repos_port <port>
-repos_sid <sid> | -repos_conndesc <conn desc>) -repos_user <username> [-repos_pwd
<pwd>] [-admin_pwd <pwd>] -emkey_file <emkey file>
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
The EMKey has been copied to file.
```

Note: Either repos\_host, repos\_port, repos\_sid OR repos\_conndesc needs to be specified.

### 2.5.2.5 emctl config emkey -copy\_to\_credstore\_from\_file

The command removes the emkey from the repository: It secures the emkey, which is the out-of-the-box configuration.

#### Example 2-19 Sample Output of the emctl config emkey -copy\_to\_credstore\_from\_file Command

```
emctl config emkey -copy_to_credstore_from_file -admin_host <host> -admin_port
<port> -admin_user <username> [-admin_pwd <pwd>] [-repos_pwd <pwd>] -emkey_file
<emkey file>
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
The EMKey has been copied to the Credential Store.
```

### 2.5.2.6 emctl config emkey -copy\_to\_repos\_from\_file

This command copies the emkey from a specified file to the repository.

#### Example 2-20 Sample Output of the emctl config emkey -copy\_to\_repos\_from\_file Command

```
emctl config emkey -copy_to_repos_from_file (-repos_host <host> -repos_port <port>
-repos_sid <sid> | -repos_conndesc <conn desc>) -repos_user <username> [-repos_pwd
<pwd>] [-admin_pwd <pwd>] -emkey_file <emkey file>
```

```
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
The EMKey has been copied to the Management Repository. This operation will cause
the EMKey to become unsecure.
After the required operation has been completed, secure the EMKey by running "emctl
config emkey -remove_from_repos".
```

### 2.5.2.7 emctl config emkey -remove\_from\_repos

This command removes the emkey from the repository.

#### **Example 2-21 Sample Output of emctl config emkey -remove\_from\_repos Command**

```
emctl config emkey -remove_from_repos [-sysman_pwd <pwd>]
Oracle Enterprise Manager 13c Release 2 Cloud Control
Copyright (c) 1996, 2016 Oracle Corporation. All rights reserved.
The EMKey has been removed from the Management Repository.
```

#### **Note:**

If the emkey is corrupted in the Credential Store, you will not be able to remove it from the Management Repository.

## 2.5.3 Install and Upgrade Scenarios

This section explains the install and upgrade scenarios for emkey.

### 2.5.3.1 Installing the Management Repository

A new emkey is generated as a strong random number when the Management Repository is created.

### 2.5.3.2 Installing the First Oracle Management Service

When the Oracle Management Service is installed, the Installer copies the emkey to Credential Store and removes it from repository (emkey is secured out-of-box).

### 2.5.3.3 Upgrading from 10.2 or 11.1 to 12.1

The Management Repository is upgraded as usual. When upgrading the OMS, the `omsca` (OMS Configuration Assistant) copies the emkey to Credential Store and removes from repository. `omsca` reads the emkey from `emkey.ora` file present in the old OMS Oracle Home and copies it to Credential Store.

•

 **Note:**

In versions prior to 12.1 the emkey needs to be copied to the Management Repository before starting the upgrade. After the Oracle Management Service has been upgraded, you can secure the emkey, that is, remove it from the Management Repository by running the following command:

```
emctl config emkey -remove_from_repos
```

From version 12.1 on, there is a re-install check, during Upgrade, which takes care of this step.

### 2.5.3.4 Recreating the Management Repository

When the Management Repository is recreated, a new emkey is generated. This new key will not be in synchronization with the emkey existing in the Credential Store. Follow these steps to synchronize the key:

1. Copy the new emkey to Credential Store by using the `emctl config emkey -copy_to_credstore` command.
2. Take a backup by entering the `emctl config emkey -copy_to_file_from_repos` command or the `emctl config emkey -copy_to_file_from_credstore` command.
3. Secure the emkey by using the `emctl config emkey -remove_from_repos` command.

## 2.6 Configuring and Managing Audit

All operations performed by Enterprise Manager users such as creating users, granting privileges, starting a remote job like patching or cloning, need to be audited to ensure compliance with the Sarbanes-Oxley Act of 2002 (SAS 70). This act defines standards an auditor must use to assess the contracted internal controls of a service organization. Auditing an operation enables an administrator to monitor, detect, and investigate problems and enforce enterprise wide security policies.

Irrespective of how the user has logged into Enterprise Manager, when auditing is enabled, each user action is audited and the audit details are stored in a record.

### 2.6.1 Auditing Credentials

For Enterprise Manager 13c, BASIC auditing is enabled by default, thus creating an audit trail of credentials being created, edited, accessed, associated and deleted. Named credentials are first-class security objects on which privileges can be granted or revoked. This means that multiple Enterprise Manager administrators will be able to use and modify the credential objects. Because credentials are sensitive data that can be used to perform various operations on the systems, there is a need to audit the operations on credentials.

Enterprise Manger supports auditing all credential operation, but first needs to be enabled. The auditing information includes, but is not limited to, the current username, credential name, operation performed, operation status success or failure. The audit logs contain information about the credential owner, action initiator, credential name,

user name, and target name, job names along with the date time of the operation. Credential fields like password, private keys are never logged.

The following operations are audited:

- **Creating a Named Credential:** Creating new Enterprise Manager credentials will be audited.
- **Editing a Named Credential:** Editing a credential may consist of changing the username and/or the sensitive credential attributes. Credential edits may also include changing the authentication scheme for the credential.
- **Delete a Named Credential:** Deleting a credential from Enterprise Manager will be audited.
- **Associating a Named Credential:** A named credential can be set as a preferred credential for a credential set at the target level or at target type level. The named credential can also be reference directly from a job. All operations involving the setting of the named credentials as preferred credentials and using it in a job or deployment procedure will be audited.
- **Accessing a Named Credential:** Enterprise Manager subsystems request credentials from the credential store to perform various system management tasks

## 2.6.2 Default Audit Actions

By default, whenever a user logs in or out of Enterprise Manager, the action is audited. The following list shows the Enterprise Manager infrastructure operations that are also audited by default.

- Apply Update
- Change MGMT\_VIEW User Password
- Change Repository Password
- Configure Authentication
- Copy EM Key to Repository
- Remove EM Key from Repository
- Create Custom CA
- Remove Update
- Secure Console
- Secure Lock
- Secure OMS

## 2.6.3 Configuring the Enterprise Manager Audit System

You can configure the Enterprise Manager Audit System by using the following EM CLI commands:

- `enable_audit`: Enables auditing for all user operations.
- `disable_audit`: Disables auditing for all user operations.
- `show_operations_list`: Shows a list of the user operations being audited.

- `show_audit_settings`: Shows the audit status, operation list, externalization service details, and purge period details.
- `update_audit_settings`: Updates the current audit settings in the repository.

## 2.6.4 Configuring the Audit Data Export Service

Audit data needs to be protected and maintained for several years. The volume of audit data may become very large and impact the performance of the system. To limit the amount of data stored in the repository, the audit data must be externalized or archived at regular intervals. The archived audit data is stored in an XML file complying with the ODL format. To externalize the audit data, the `EM_AUDIT_EXTERNALIZATION` API is used. Records of the format `<file-prefix>.NNNNN.xml`, where `NNNN` is a number, are generated. The numbers start with `00001` and continue to `99999`.

You can set up the audit externalization service for exporting audit data into the file system by using the `update_audit_setting -externalization_switch` command.

The externalization of audit system data is performed by the *EM Audit Externalization Service* job. By default, this job is scheduled to run once daily. You can view current status of this job from the Repository Scheduler Jobs Status area in the Enterprise Manager console, as shown in the following graphic.

To access this page, from the **Setup** menu, select **Manage Cloud Control**, and then **Repository**.

## 2.6.5 Updating the Audit Settings

The `update_audit_settings` command updates the current audit settings in the repository and restarts the Management Service.

- `-audit_switch`: Enables auditing across Enterprise Manager. The possible values are `ENABLE/DISABLE`. Default value is `DISABLE`.
- `-operations_to_enable`: Enables auditing for specified operations. Enter **All** to enable all operations.
- `-operations_to_disable`: Disables auditing for specified operations. Enter **All** to disable all operations.
- `-externalization_switch`: Enables the audit data export service. The possible values are `ENABLE/DISABLE`. Default value is `DISABLE`.
- `-directory`: The database directory that is mapped to the OS directory where the export service archives the audit data files.
- `-file_prefix`: The file prefix to be used by the export service to create the file in which audit data is to be stored.
- `-file_size`: The size of the file on which the audit data is to be stored. The default value is `5000000` bytes.
- `data_retention_period`: The period for which the audit data is to be retained inside the repository. The default value is `365` days.

### Example 2-22 Usage of the `update_audit_setting` command

```
emcli update_audit_settings
 -audit_switch="ENABLE/DISABLE"
```

```
-operations_to_enable="name of the operations to enable, for all oprtations
use ALL"
-operations_to_disable="name of the operations to disable, for all
oprations use ALL"
-externalization_switch="ENABLE/DISABLE"
-directory_name="directory_name (DB Directory)"
-file_prefix="file_prefix"
-file_size="file_size (Bytes)"
-data_retention_period="data_retention_period (Days)"
```

## 2.6.6 Searching the Audit Data

You can search for audit data that has been generated over a specified period. You can also search for the following:

- Audit details of a specific user operation or all user operations.
- Audit details of operations with a Success or Failure status or All operations.

From the **Setup** menu, select **Security** and then **Audit Data**. The Audit Data page is displayed. Specify the search criteria in the fields and click **Go**. The results are displayed in the Summary table.

To view the details of each record that meets the search criteria, select Detailed in the View drop-down list. To drill down to the full record details, click on the **Timestamp**.

## 2.6.7 List of Operations Audited

For a complete list of audit operations supported by Enterprise Manager, use the EM CLI `show_operations_list verb`.

### Example 2-23 EM CLI `show_operations_list`

```
> emcli show_operations_list
```

| Operation ID                    | Operation Name                  | Infrastructure Operation |
|---------------------------------|---------------------------------|--------------------------|
| ADD_AGENT_REGISTRATION_PASSWORD | Add Registration Password       |                          |
| NO                              |                                 |                          |
| ADD_CS_TARGET_ASSOC             | Add Standard-Target Association |                          |
| NO                              |                                 |                          |
| SECURITY_AUTH_CONFIG            | Configure                       |                          |
| Authentication                  | YES                             |                          |
| .                               |                                 |                          |
| .                               |                                 |                          |
| .                               |                                 |                          |
| UPDATE_PASSWORD                 | Update Password                 |                          |
| NO                              |                                 |                          |

## 2.6.8 Auditing the Infrastructure

Beginning with Oracle Enterprise Manger Cloud Control 12c, basic and Infrastructure auditing is enabled by default for Enterprise Manager. In Enterprise Manager, there are over 150 options for auditing. Audit infrastructure operations are always enabled and cannot be turned off. An enhanced Auditing page makes it easy to quickly view the privilege grants on a regular basis and also keep track of which users exercised



what privileges, this improves user accountability. Infrastructure activities are audited out of the box, these include updates, downloads, OMS password changes and emkey copy and removes from the Repository.

Also, the search capability of all Audit actions have been enhanced to improved, via the Cloud Control console, you can search for a subset of Audited operations and filter to see operations from specific client hosts and client types(browser or CLI). This provides more efficient ways for audit officers to locate specific operations of interest.

The following table lists all auditable events. Those auditable events shown as enabled are Infrastructure audit events and are turned on out-of-box and cannot be disabled.

**Table 2-4 Auditable Events**

| <b>Event</b>                                  | <b>Enabled/Disabled (By Default)</b> |
|-----------------------------------------------|--------------------------------------|
| Apply Update                                  | Enabled                              |
| Change MGMT_VIEW User Password                | Enabled                              |
| Change Repository Password                    | Enabled                              |
| Configure Authentication                      | Enabled                              |
| Copy Enterprise Manager Key to Repository     | Enabled                              |
| Create Custom CA                              | Enabled                              |
| Enterprise Manager Login                      | Enabled                              |
| Enterprise Manager Logout                     | Enabled                              |
| Remove Enterprise Manager Key from Repository | Enabled                              |
| Remove Update                                 | Enabled                              |
| Secure Console                                | Enabled                              |
| Secure Lock                                   | Enabled                              |
| Secure OMS                                    | Enabled                              |
| Secure WebLogic Server                        | Enabled                              |
| Access Named Credential                       | Disabled                             |
| Add Registration Password                     | Disabled                             |
| Add Software Library Storage                  | Disabled                             |
| Add Standard-Target Association               | Disabled                             |
| Add entity to Template Collection             | Disabled                             |
| Apply Monitoring Template                     | Disabled                             |
| Associate Template Collection to Admin Group  | Disabled                             |
| Attach Metric Extension                       | Disabled                             |
| Audit Export Settings                         | Disabled                             |
| Audit Settings                                | Disabled                             |
| Change Connector Settings                     | Disabled                             |
| Change Password                               | Disabled                             |
| Change Preferred Credentials                  | Disabled                             |
| Clear Manual Rule Violation                   | Disabled                             |
| Configure Connector                           | Disabled                             |

**Table 2-4 (Cont.) Auditable Events**

| <b>Event</b>                                     | <b>Enabled/Disabled (By Default)</b> |
|--------------------------------------------------|--------------------------------------|
| Create Administration Groups                     | Disabled                             |
| Create Change Management Setting                 | Disabled                             |
| Create Connector                                 | Disabled                             |
| Create Credential Set                            | Disabled                             |
| Create Custom Configuration Specification        | Disabled                             |
| Create Custom Configuration Specification Parser | Disabled                             |
| Create Custom Target Type                        | Disabled                             |
| Create Facet                                     | Disabled                             |
| Create Facet Parameter                           | Disabled                             |
| Create Facet Pattern                             | Disabled                             |
| Create Framework                                 | Disabled                             |
| Create Metric Extension                          | Disabled                             |
| Create Monitoring Template                       | Disabled                             |
| Create Named Credential                          | Disabled                             |
| Create Real-time Monitoring Rule                 | Disabled                             |
| Create Resolution state                          | Disabled                             |
| Create Role                                      | Disabled                             |
| Create Rule                                      | Disabled                             |
| Create Rule Set                                  | Disabled                             |
| Create Standard                                  | Disabled                             |
| Create Template Collection                       | Disabled                             |
| Create User                                      | Disabled                             |
| Database Login                                   | Disabled                             |
| Database Logout                                  | Disabled                             |
| Database Restart                                 | Disabled                             |
| Database Shutdown                                | Disabled                             |
| Database Startup                                 | Disabled                             |
| Delete Administration Groups                     | Disabled                             |
| Delete Credential Set                            | Disabled                             |
| Delete Custom Configuration Specification        | Disabled                             |
| Delete Custom Configuration Specification Parser | Disabled                             |
| Delete Facet                                     | Disabled                             |
| Delete Facet Parameter                           | Disabled                             |
| Delete Facet Pattern                             | Disabled                             |
| Delete Framework                                 | Disabled                             |
| Delete Job                                       | Disabled                             |
| Delete Management Connector                      | Disabled                             |
| Delete Metric Extension                          | Disabled                             |

**Table 2-4 (Cont.) Auditable Events**

| <b>Event</b>                                      | <b>Enabled/Disabled (By Default)</b> |
|---------------------------------------------------|--------------------------------------|
| Delete Monitoring Template                        | Disabled                             |
| Delete Named Credential                           | Disabled                             |
| Delete Real-time Monitoring Rule                  | Disabled                             |
| Delete Registration Password                      | Disabled                             |
| Delete Resolution state                           | Disabled                             |
| Delete Role                                       | Disabled                             |
| Delete Rule                                       | Disabled                             |
| Delete Rule Set                                   | Disabled                             |
| Delete Software Library Entity                    | Disabled                             |
| Delete Software Library Folder                    | Disabled                             |
| Delete Standard                                   | Disabled                             |
| Delete Target                                     | Disabled                             |
| Delete Template Collection                        | Disabled                             |
| Delete Update                                     | Disabled                             |
| Delete User                                       | Disabled                             |
| Deploy Custom Configuration Specification         | Disabled                             |
| Detach Metric Extension                           | Disabled                             |
| Disable Rule                                      | Disabled                             |
| Disable Rule Set                                  | Disabled                             |
| Disable Standard-Target Association               | Disabled                             |
| Disassociate Template Collection from Admin Group | Disabled                             |
| Download Update                                   | Disabled                             |
| Edit Framework                                    | Disabled                             |
| Edit Job                                          | Disabled                             |
| Edit Monitoring Template                          | Disabled                             |
| Edit Registration Password                        | Disabled                             |
| Edit Rule                                         | Disabled                             |
| Edit Rule Set                                     | Disabled                             |
| Edit Standard                                     | Disabled                             |
| Edit Standard-Target Association                  | Disabled                             |
| Edit Template Collection                          | Disabled                             |
| Enable Rule                                       | Disabled                             |
| Enable Rule Set                                   | Disabled                             |
| Enable Standard-Target Association                | Disabled                             |
| Execute Command As Agent                          | Disabled                             |
| File Transfer Job                                 | Disabled                             |
| Get File Job                                      | Disabled                             |

**Table 2-4 (Cont.) Auditable Events**

| <b>Event</b>                              | <b>Enabled/Disabled (By Default)</b> |
|-------------------------------------------|--------------------------------------|
| Grant Privilege                           | Disabled                             |
| Grant Role                                | Disabled                             |
| Import Facet                              | Disabled                             |
| Import Framework                          | Disabled                             |
| Import Real-time Monitoring Rule          | Disabled                             |
| Import Rule                               | Disabled                             |
| Import Standard                           | Disabled                             |
| Include Action To Monitor                 | Disabled                             |
| Include Filter Facet                      | Disabled                             |
| Include Monitoring Facet                  | Disabled                             |
| Job Execution                             | Disabled                             |
| Mark informational update as read         | Disabled                             |
| Modify Administration Groups              | Disabled                             |
| Modify Change Management Setting          | Disabled                             |
| Modify Custom Configuration Specification | Disabled                             |
| Modify Facet                              | Disabled                             |
| Modify Facet Content                      | Disabled                             |
| Modify Facet Parameter                    | Disabled                             |
| Modify Facet Pattern                      | Disabled                             |
| Modify Metric Settings                    | Disabled                             |
| Modify Named Credential                   | Disabled                             |
| Modify Real-time Monitoring Rule          | Disabled                             |
| Modify Resolution state                   | Disabled                             |
| Modify Role                               | Disabled                             |
| Modify User                               | Disabled                             |
| Move Software Library Entity              | Disabled                             |
| Publish Metric Extension                  | Disabled                             |
| Purge Software Library Storage            | Disabled                             |
| Put File As Agent                         | Disabled                             |
| Put File Job                              | Disabled                             |
| Refresh from Enterprise Manager Store     | Disabled                             |
| Registration Password Usage               | Disabled                             |
| Remote Operation Job                      | Disabled                             |
| Remove Action From Monitor                | Disabled                             |
| Remove Change Management Setting          | Disabled                             |
| Remove Filter Facet                       | Disabled                             |
| Remove Monitoring Facet                   | Disabled                             |
| Remove Privilege Delegation Setting       | Disabled                             |

**Table 2-4 (Cont.) Auditable Events**

| <b>Event</b>                                | <b>Enabled/Disabled (By Default)</b> |
|---------------------------------------------|--------------------------------------|
| Remove Software Library Storage             | Disabled                             |
| Remove Standard-Target Association          | Disabled                             |
| Remove entity from Template Collection      | Disabled                             |
| Rename Template Collection                  | Disabled                             |
| Reorder Rule                                | Disabled                             |
| Reorder Rule Set                            | Disabled                             |
| Resume Job                                  | Disabled                             |
| Resync Agent                                | Disabled                             |
| Resync Repository                           | Disabled                             |
| Retry Job                                   | Disabled                             |
| Revoke Privilege                            | Disabled                             |
| Revoke Role                                 | Disabled                             |
| Save Monitoring Settings                    | Disabled                             |
| Set Privilege Delegation Setting            | Disabled                             |
| Stop Job                                    | Disabled                             |
| Submit Job                                  | Disabled                             |
| Subscribe Update Type                       | Disabled                             |
| Suppress Violation                          | Disabled                             |
| Suspend Job                                 | Disabled                             |
| Target Login                                | Disabled                             |
| Target Logout                               | Disabled                             |
| Undeploy Custom Configuration Specification | Disabled                             |
| Unsubscribe Update Type                     | Disabled                             |
| Unsuppress Violation                        | Disabled                             |
| Update Database Password                    | Disabled                             |
| Update Metric Extension                     | Disabled                             |
| Update Password                             | Disabled                             |
| Update is available                         | Disabled                             |

### 2.6.8.1 WebLogic Server Auditable Events

The following WebLogic Server events can be audited:

- Domain update
- Domain login
- Domain logout

To audit these events, enter the following EM CLI command:

```
emcli update_audit_settings
 -operations_to_enable="WEBLOGIC_DOMAIN_UPDATE_INVOKE;WEBLOGIC_DOMAIN
 _LOGIN;WEB_LOGIC_DOMAIN_LOGOUT"
```

 **Note:**

only super administrators have permission to view the audited WebLogic Server data.

## 2.7 Additional Security Considerations

After you enable security for the Enterprise Manager components and framework, there are additional security considerations. This section provides the following topics:

- [Changing the SYSMAN and MGMT\\_VIEW Passwords](#)
- [Responding to Browser-Specific Security Certificate Alerts](#)

### 2.7.1 Changing the SYSMAN and MGMT\_VIEW Passwords

This section describes the commands used to change the SYSMAN and MGMT\_VIEW passwords.

#### 2.7.1.1 Changing the SYSMAN User Password

The SYSMAN user account is used by the Oracle Management Server to login into the Oracle Management Repository to store and query all activity. The password is stored encrypted. If the SYSMAN password changes at the OMR it must also be changed at the OMS, to ensure proper functioning of Enterprise Manager Cloud Control for all operations.

 **Note:**

From 12c onwards, directly modifying the password for SYSMAN or any other repository user at the Repository Database is not recommended. Hence, ensure that the passwords are changed only using one of the methods listed below.

##### 2.7.1.1.1 If the current SYSMAN password is known

1. Stop all OMS instances running `emctl stop oms`.

```
OMS_Home/bin/emctl stop oms
```

If BIP is configured: Stop BIP on each machine by running

```
OMS_Home/bin/emctl stop oms -bip_only
```

If JVMD and/or ADP is configured, stop the JVMD/ADP engines:

```
emctl extended oms jvmd stop -all
```

```
emctl extended oms adp stop -all
```

Execute the same command on all the OMS machines including the primary OMS machine. Do not include '-all' as the Admin Server needs to be up during this operation.

## 2. Modify the SYSMAN password:

```
cd <OMS_HOME>/bin
```

```
emctl config oms -change_repos_pwd [-old_pwd <old_pwd>] [-new_pwd <new_pwd>]
[-use_sys_pwd [-sys_pwd <sys_pwd>]]
```

```
emctl config oms -change_repos_pwd'
```

### Command Parameters

| Parameter         | Description                                                                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| -change_repos_pwd | Used to change the SYSMAN password.                                                                                                                    |
| -old_pwd          | This is the current SYSMAN password.                                                                                                                   |
| -new_pwd          | This is the new password.                                                                                                                              |
| -use_sys_pwd      | This parameter is optional and is used to connect to the database as a SYS user. Use this option if SYSMAN account on the database has expired/locked. |
| -sys_pwd          | This is the password for the SYS user. Required only if -use_sys_pwd is specified                                                                      |

### Command Behavior:

#### Note:

The above command will prompt you for the current password of the SYSMAN user and the new password.

The password will be modified at the Repository Database and the monitoring credentials for the 'OMS and Repository' target.

Along with the SYSMAN password, this command will modify the password for the EM users (SYSMAN\_MDS, BIP, SYSMAN\_OPSS, SYSMAN\_APM, SYSMAN\_RO) created in the Repository Database.

### Sample Command Output

```
emctl config oms -change_repos_pwd
Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.1.0
Copyright (c) 1996, 2011 Oracle Corporation. All rights reserved.
Enter Repository User's Current Password :
Enter Repository User's New Password :

Changing passwords in backend ...
Passwords changed in backend successfully.
Updating repository password in Credential Store...
Successfully updated Repository password in Credential Store.
Restart all the OMSs using 'emctl stop oms -all' and 'emctl start oms'.
Successfully changed repository password.
```

3. Stop the Admin server on the primary OMS machine and re-start all the OMS:

```
cd <OMS_HOME>/bin
emctl stop oms -all
```

4. Restart all the Management Services:

```
cd <OMS_HOME>/bin
emctl start oms
```

### 2.7.1.1.2 If the current SYSMAN password is unknown

1. Stop all the OMS:

```
cd <OMS_HOME>/bin
emctl stop oms
```

Execute the same command on the primary OMS machine as well. Do not include '-all' as the Admin Server needs to be up during this operation.

2. Modify the SYSMAN password:

```
cd <OMS_HOME>/bin
emctl config oms -change_repos_pwd -use_sys_pwd -sys_pwd <sys user password> -
new_pwd <new sysman password>
```

#### Note:

The '-use\_sys\_pwd' is used to connect to the database as a SYS user and modify the SYSMAN password in the Repository database.

The current SYSMAN password is not prompted for and only the new password needs to be entered. This will allow the reset of the old password to the new password entered.

The password will be modified at the Repository Database and the monitoring credentials for the 'OMS and Repository' target.

Along with the SYSMAN password, this command will modify the password for the EM users (SYSMAN\_MDS, BIP, SYSMAN\_OPSS, SYSMAN\_APM, SYSMAN\_RO) created in the Repository Database.

3. Stop the Admin server on the primary OMS machine and re-start all the OMS:

```
cd <OMS_HOME>/bin
emctl stop oms -all
emctl start oms
```

### 2.7.1.2 Changing the MGMT\_VIEW User Password

To change the password of the MGMT\_VIEW user, you use the following command:

```
emctl config oms -change_view_user_pwd [-sysman_pwd <sysman_pwd>] [-user_pwd
<user_pwd>] [-auto_generate]
```



| Parameter             | Description                                                  |
|-----------------------|--------------------------------------------------------------|
| -change_view_user_pwd | Used to change MGMT_VIEW user's password.                    |
| -sysman_pwd           | The password for the SYSMAN user.                            |
| -user_pwd             | The new password for theMGMT_VIEW user.                      |
| -auto_generate        | If this option is specified, the password is auto-generated. |

1. Stop all OMSs.

```
<OMS_HOME>/bin/emctl stop oms
```

2. On one of the OMSs, run the following command:

```
<OMS_HOME>/bin/emctl config oms -change_view_user_pwd [-old_pwd <old_pwd>] [-new_pwd <new_pwd>]
```

3. Restart the AdminServer and all the OMSs.

```
emctl stop oms -all
```

```
emctl start oms
```

## 2.7.2 Responding to Browser-Specific Security Certificate Alerts

When you connect to Enterprise Manager via HTTPS, the Management Service presents your browser with a certificate to verify the identity of the Management Service. This certificate has been verified by a third party that your computer trusts. When a Web browser encounters an untrusted certificate, it generates security alert messages. The security alert dialog boxes appear because Enterprise Manager's certificate is issued by a Certificate Authority which the browser does not trust.

You can choose to ignore the warnings and continue with your Enterprise Manager session, or you can import the CA certificates into the browser's list of trusted "root" certificates to eliminate the certificate security alerts in future browser sessions.

### 2.7.2.1 Third Party Certificate Workflow

The following high-level steps are involved in setting up Enterprise Manager to use third party certificates.

**Step 1:** Generate a wallet and have it certified by a third party authority such as Entrust, Verisign, Thwate, or DigiCert.

**Step 2:** Configure the custom wallets to each OMS. For instructions, see [Configuring a Third Party Certificate for HTTPS Console Users](#)

**Step 3:** Add the certificate to the browser's list of trusted root certificates to eliminate further browser certificate warnings. The following sections describe how to respond to browser-specific security alert dialog boxes when you are using Enterprise Manager in a secure environment. Note: Step 3 is not required for well-known certificate authorities such as Verisign or Entrus.

- [Responding to the Internet Explorer Security Alert Dialog Box](#)
- [Responding to the Internet Explorer Security Alert Dialog Box](#)
- [Responding to the Mozilla Firefox New Site Certificate Dialog Box](#)

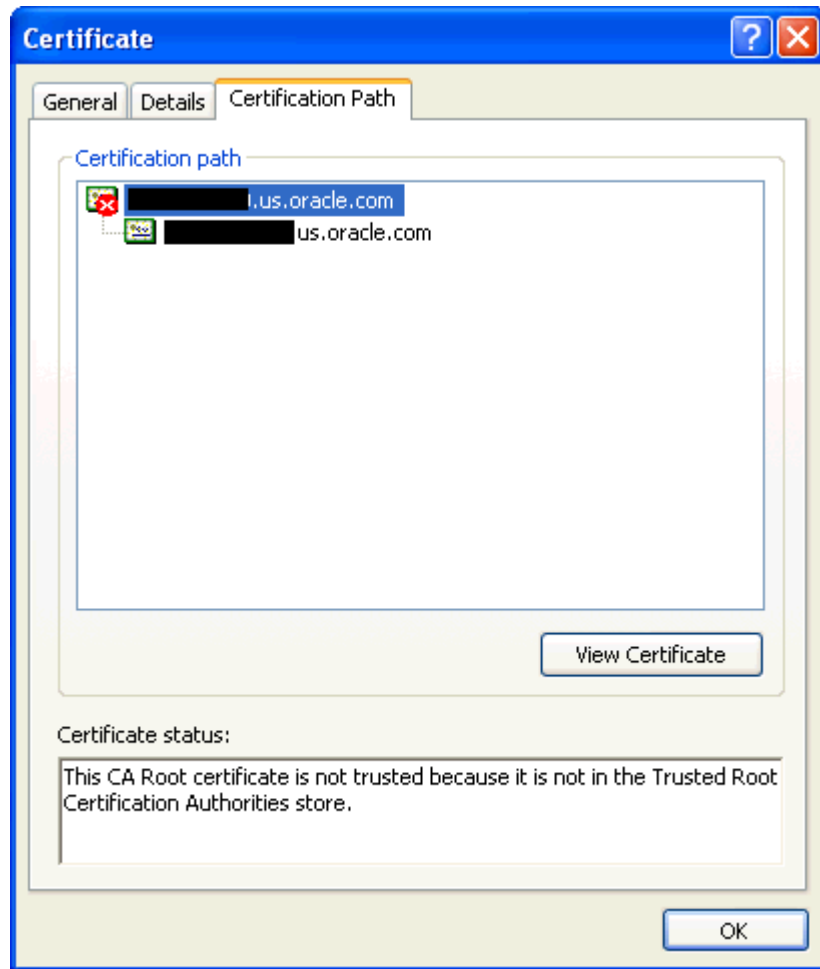
- [Responding to the Google Chrome Security Alert Dialog Box](#)
- [Responding to Safari Security Dialog Box](#)

### 2.7.2.2 Responding to the Internet Explorer Security Alert Dialog Box

Security is enabled by default for the Management Service. However, if you have not enabled the more extensive security features of your web tier, you will likely receive the following warning: "There is a problem with this Web site's security certificate." This occurs because Enterprise Manager's certificate is issued by a Certificate Authority which the browser does not trust.

When Internet Explorer displays the certificate warning page, use the following instructions to install the certificate and avoid viewing this page again in future Enterprise Manager sessions:


1. From the certificate warning page, click **Continue to this Web site (not recommended)**.  
Internet Explorer displays a Security Warning dialog.
2. Click **Yes**. Internet Explorer may display a **Security Alert** dialog if you have not selected **In the future, do not show this warning**. in a previous Internet Explorer session. Click **OK** to dismiss the dialog.
3. The Enterprise Manager console logon page displays.
4. At the top of the browser, click **Certificate Error** to display the **Certificate** pop-up.
5. Click **View Certificates**. The Certificates dialog appears.
6. Click the **Certificate Path** tab and select the first entry in the list of certificates as shown in the following graphic.



7. Click **View Certificate** to display a second Certificate dialog box.
8. Click **Install Certificate** to display the Certificate Import wizard.
9. Accept the default settings in the wizard, click **Finish** when you are done.  
Internet Explorer displays a Security Warning asking if you want to install the certificate. Click **Yes**. Internet Explorer will display a message stating that the certificate was imported successfully.
10. Click **OK** to close each of the security dialog boxes and click **Yes** on the Security Alert dialog box to continue with your browser session.  
You should no longer receive the **Security Alert** dialog box in any future connections to Enterprise Manager when you use this browser.

### 2.7.2.3 Responding to the Mozilla Firefox New Site Certificate Dialog Box

Firefox will also issue a connection warning when Enterprise Manager's certificate is issued by a Certificate Authority which the browser does not trust. When you first attempt to display the Cloud Control console using the HTTPS URL in Mozilla Firefox, you will receive a warning because the connection is untrusted.



### This Connection is Untrusted

You have asked Firefox to connect securely to ██████████, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

#### What Should I Do?

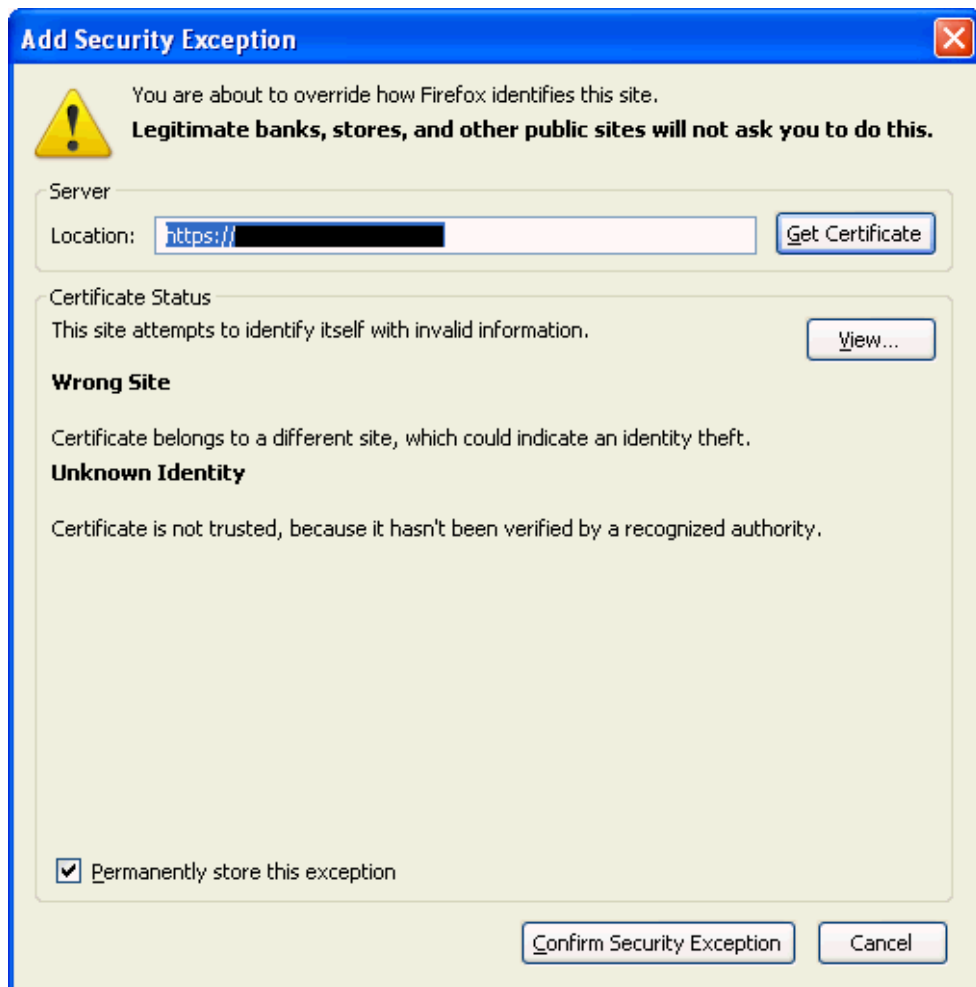
If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

When Firefox displays the Untrusted Connection page, use the following instructions to install the certificate and avoid viewing this page again in future Enterprise Manager sessions:

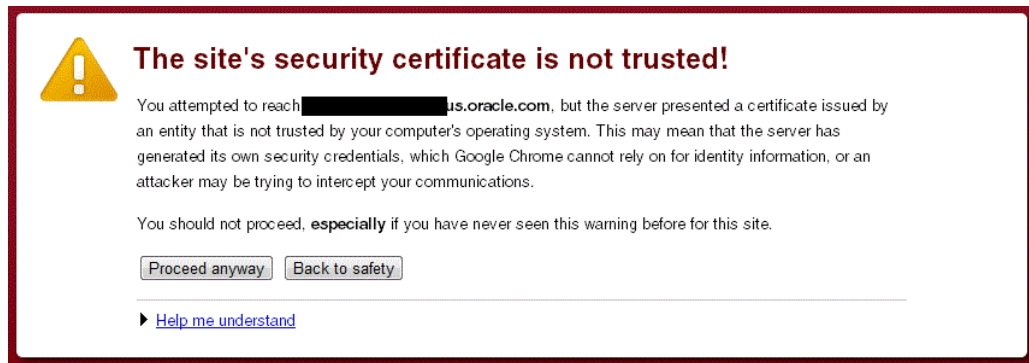
1. Review the instructions and information. Click **I Understand the Risks**. Firefox displays additional information and the opportunity to add the certificate.
2. Click **Add Exception...** . Firefox displays the **Add Security Exception** dialog.




3. Ensure that the **Permanently store this exception** option is selected.  
You should no longer receive the New Site Certificate dialog box when using the current browser.
4. Click **Confirm Security Exception**. The Enterprise Manager console displays.  
You will no longer receive the untrusted connection warning in any future connections to Enterprise Manager when you use this browser

### 2.7.2.4 Responding to the Google Chrome Security Alert Dialog Box

Google Chrome issues a warning if the security certificate of the Website is not trusted. When you first attempt to display the Cloud Control console using the HTTPS URL in Google Chrome, you will receive a warning because the connection is mistrusted.

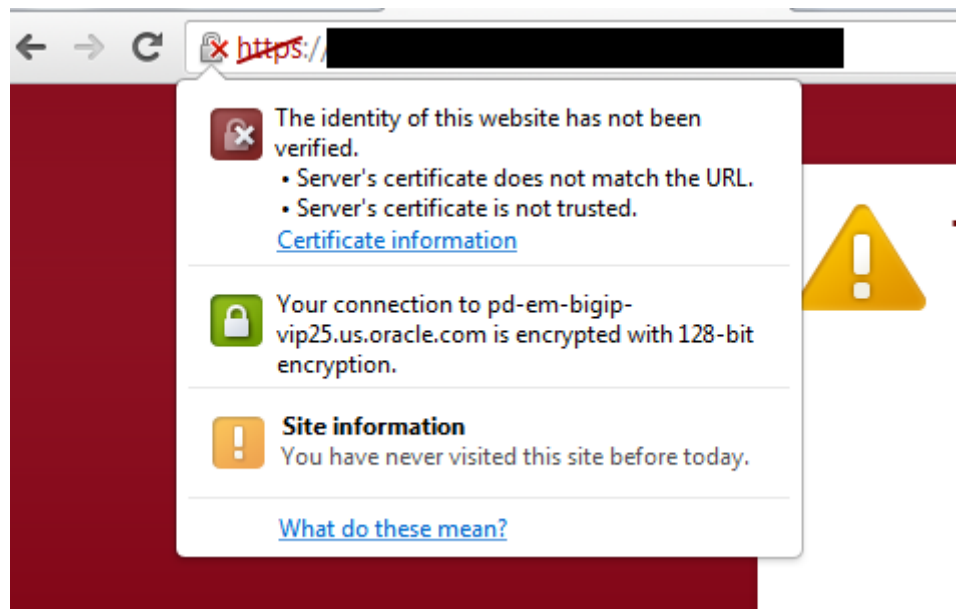


When Google Chrome displays the Untrusted Connection page, use the following instructions to install the certificate and avoid viewing this page again in future Enterprise Manager sessions:

 **Note:**

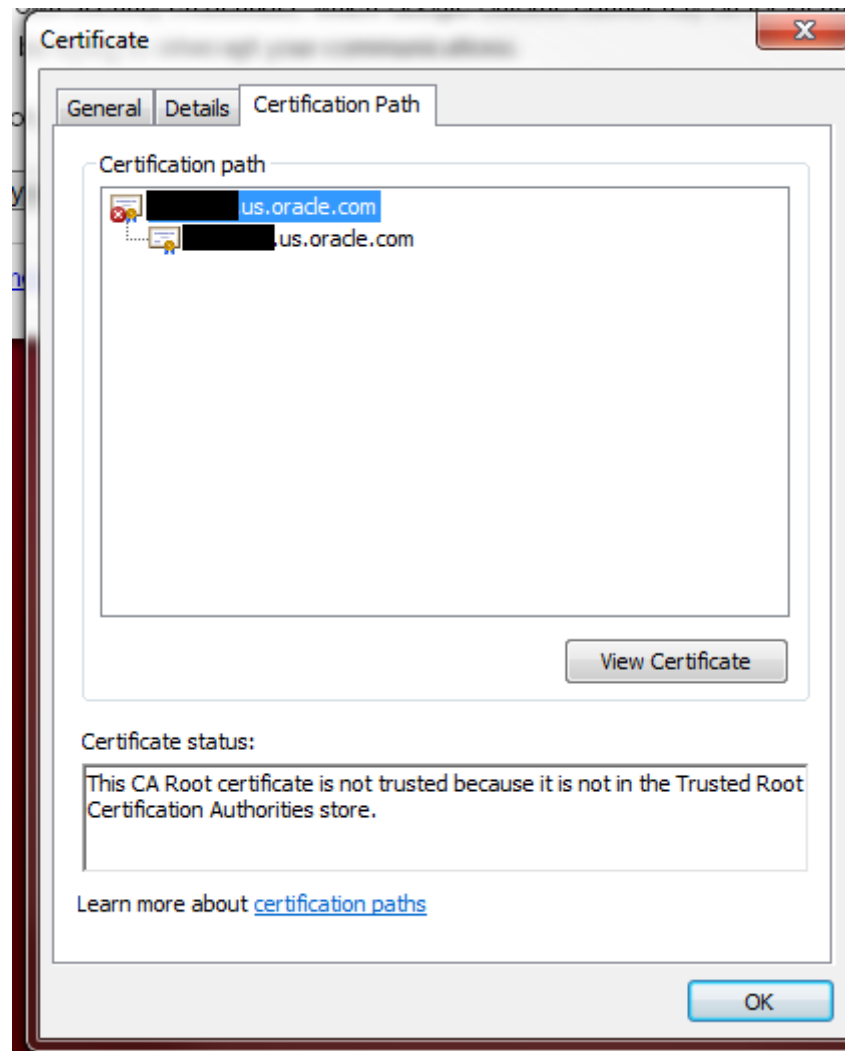
Installing a certificate using this method on Google Chrome may still lead to performance degradation. To solve this issue, the best option is to obtain a trusted certificate from a vendor of your choice.

1. Click on the crossed out lock pad icon on the left hand side of the URL address bar.

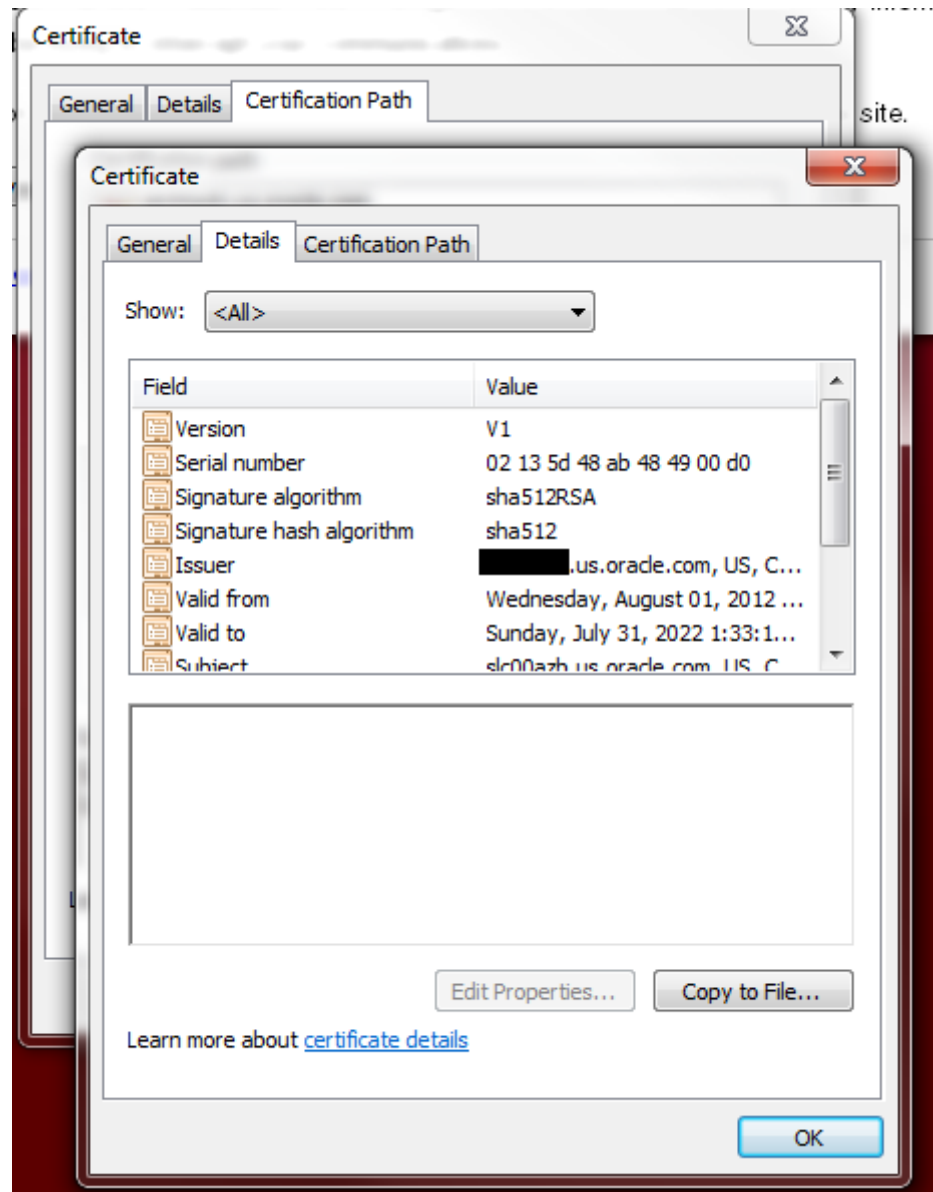


2. Click **Certificate Information** in the menu.
3. Select the **Certification Path** tab.
4. Select the OMS host name (a red cross icon).

5. Click **View Certificate**.



6. Select the **Details** tab.
7. Click **Copy to File...**



A wizard guides you through the process. Follow the wizard and select all the default options.

8. Save the certificate on your Desktop. For example, you can save it as:  
adc1110000.cer
9. From the Google Chrome menu, go to **Tools**, click **Settings**, and then select **Show Advanced Settings**.
10. Click **Manage Certificates**.
11. Select the **Trusted Root Certification Authority** tab.
12. Click **Import**.

A wizard guides you through the process of importing the saved certificate.



A warning window displays a message that the certificate you are importing cannot be verified and asks if you want to continue. Click **Yes** to proceed.

13. Check if the saved certificate appears in the **Trusted Root Certification Authority** table.
14. Restart the Google Chrome browser and load the Enterprise Manager URL. If the **Certificate Error** icon is not visible in the address bar, then the certificate is valid and trusted.

### 2.7.2.5 Responding to Safari Security Dialog Box

Safari does not support the option to install a certificate individually. To solve this issue, you have to obtain a trusted certificate from a vendor of your choice.

# 3

## Keeping Enterprise Manager Secure

This chapter provides guidelines for keeping Enterprise Manager secure.  
This chapter provides instructional guidelines for keeping Enterprise Manager secure.

- [Guidelines for Secure Infrastructure and Installations](#)
- [Guidelines for SSL Communication](#)
- [Guidelines for Authentication](#)
- [Guidelines for Authorization](#)
- [Guidelines for Auditing](#)
- [Guidelines for Managing Target Credentials](#)

### 3.1 Guidelines for Secure Infrastructure and Installations

Securing your Oracle Enterprise Manager deployment involves securing all layers of the stack starting with the underlying operating system (OS) on which the OMS and Repository reside all the way up to the Enterprise Manager components themselves. These recommendations will increase overall security as well as prevent certain DoS attacks.

#### 3.1.1 Secure the Infrastructure and Operating System

Harden the machines themselves by removing all unsecure services such as rsh, rlogin, telnet, and rexec on Linux platform (for the list of unsecure services and how to remove them on different platforms, please refer to the CIS benchmarks). It is also recommended to stop non-essential services, this minimizes the 'attack footprint' of the host and reduces resource consumption by services that are not required, freeing up system resources to deliver the best performance from the OMS.

Restrict OS access by supporting only indirect or impersonation-based access to all Oracle Homes by using utilities such as sudo or PowerBroker. Protect the WebLogic Server Home directory, especially the domain directory which contains configuration files, security files, log files and other Java EE resources for the WebLogic domain. Grant only one OS user who runs WebLogic Server the access privilege to the directory.

Ensure that all the Oracle Homes are patched with the latest CPU (Critical Patch Update). This is a recommended best practice for securing the Oracle Management Service, Repository, Agents and managed targets. Setup your My Oracle Support credentials to detect new Security Alerts and CPUs from the Patch Advisor. With the default Security Recommendations for Oracle Products compliance standard, when a target is missing the latest Security patches, a compliance standard violation will be triggered. In addition, the Secure Configuration for Host should be associated to the hosts of the OMS and Repository. There are additional compliance standards for Database and WLS that can be applied depending on your level of security. Review the Oracle Enterprise Manager Cloud Control Administrator's Guide section on

Compliance for more information on available compliance standards and how to associate targets.

The OMS runs on top of the Oracle WebLogic Server. Most of the best practices for securing Oracle WebLogic Server are applicable for securing the OMS as well. Refer to the Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server section Securing Oracle WebLogic Server for additional information.

Ensure that the OMS, Repository and Agent are monitored for filesystem space. The OMS writes a lot of information to log and trace files, and proper space needs to be available for successful operation and troubleshooting. The Agent also relies on filesystem space for log and trace files as well as collecting target metrics.

### 3.1.1.1 Best Practices for Securing the Infrastructure and Operating System

- Remove unsecure services and stop non-essential services on all infrastructure components
- Restrict OS access and protect critical files and directories
- Apply latest OS security patches
- Adhere to security Compliance Standards and apply latest Oracle CPU patches to all components (OMS, Repository and Agent)
- Monitor filesystem space for OMS, Repository and Agent

### 3.1.2 Securing the Oracle Management Repository

In addition to the above recommendations, steps are necessary to secure the Oracle Management Repository. Since the Oracle Management Repository resides within an Oracle database, a number of the best practices for securing the Oracle database itself are applicable to securing the Repository as well. For best practices on Oracle database security, please refer to the Oracle Database Security Checklist.

The above document also covers certain Operating System level steps that need to be performed to secure the database. Following are additional recommendations to be implemented in the Enterprise Manager deployment.

#### 3.1.2.1 Enable Advanced Security Option

Enable Advanced Security Option (ASO) between the OMS and Repository to ensure that the data between the OMS and Repository is secure both from confidentiality and integrity standpoints. In addition to the ASO configuration required on the Repository database, you will need to configure the OMS and Agent to connect to a secure Repository database. The detailed instructions for implementing ASO for Enterprise Manager can be found in the Enterprise Manager Security section of the Oracle Enterprise Manager Cloud Control Administrator's Guide.

Please refer to the Oracle Database Advanced Security Administrator's Guide to obtain detailed information about ASO.

##### 3.1.2.1.1 Restrict Network Access

Restrict network access to the host on which the Repository resides by putting the repository database behind a firewall and checking network IP addresses. The

Listener should be configured to accept requests only from OMS nodes by adding the following parameters into TNS\_ADMIN/protocol.ora file:

- tcp.validnode\_checking =YES
- tcp.excluded\_nodes = (list of IP addresses)
- tcp.invited\_nodes = (list of IP addresses), list all OMS nodes here)

The first parameter turns on the feature whereas the latter parameters respectively deny and allow specific client IP addresses from making connections to the Oracle listener. Please refer to the Secure the Network Connection section of the Oracle Database Security Guide for more information.

### 3.1.2.1.2 Audit SYS actions

Audit all SYS (schema) operations at the database level by setting AUDIT\_SYS\_OPERATIONS = TRUE.

Use the operating system syslog audit trail to minimize the risk that a privileged user, such as a database administrator, can modify or delete audit records stored in an operation system trail if the database version of Repository is 10gR2 or after.

- For 10gR2 DB, refer to the Auditing documentation to obtain more information about syslog audit trail.
- For 11g DB, set AUDIT\_SYS\_LEVEL initialization parameter appropriately to use syslog audit trail. Refer to the 11g documentation for details.

### 3.1.2.1.3 Securing User Accounts

Users should log in to the Console with their own individual accounts, and not use the SYSMAN user. SYSMAN is the schema owner and is more privileged than Enterprise Manager Super Administrators. Multiple users should be granted Super Administrator to reduce the need for SYSMAN access. One strong reason for creating multiple Super Administrator accounts is to ensure one user maintains account access in case another user becomes locked out by a dictionary/brute force attack. The Super Administrator privilege should be limited to users who truly need all the permissions that Super Administrator gives them.

In some cases, you may wish to prevent SYSMAN from logging into the console by executing the following SQL statement on the Repository database as the SYSMAN user:

```
UPDATE MGMT_CREATED_USERS
SET SYSTEM_USER='-1'
WHERE user_name='SYSMAN'
```

After disabling SYSMAN from logging into console, you can enable it by executing:

```
UPDATE MGMT_CREATED_USERS
SET SYSTEM_USER='1'
WHERE user_name='SYSMAN'
```

Use password profiles to enforce the password control of Enterprise Manager Administrators while Repository-based authentication is used. There is an out-of-box password profile MGMT\_ADMIN\_USER\_PROFILE with the following parameter settings for Enterprise Manager Administrators:

- FAILED\_LOGIN\_ATTEMPTS=10

- `PASSWORD_LIFE_TIME=180`
- `PASSWORD_REUSE_TIME=UNLIMITED`
- `PASSWORD_REUSE_MAX=UNLIMITED`
- `PASSWORD_LOCK_TIME=1`
- `PASSWORD_GRACE_TIME=7`
- `PASSWORD_VERIFY_FUNCTION=MGMT_PASS_VERIFY`

The out-of-box password verification function `MGMT_PASS_VERIFY` will ensure that the password cannot be same as username, its minimum length is 8, and it must have at least one alphabet, digit and punctuation character. You can create customized password profiles with different values to meet your special requirements, for example, a new password verification function to meet a stricter password complexity requirement.

Change `SYSMAN` and `MGMT_VIEW` users' password on a regular basis using only the method documented in the Security section of the Oracle Enterprise Manager Cloud Control Administrator's Guide. The documented command (`update_db_password()`) helps you change the `SYSMAN` related passwords in the OMS and in the repository database. If you do not execute this command properly, the OMS may fail to start due to inconsistent passwords for one of the many accounts. You will be prompted for the old and new `SYSMAN` passwords.

When changing the `MGMT_VIEW` password, you can select `"-auto_generate"` to generate a random password that no one will know. The `MGMT_VIEW` password is used only by the Reporting system and should not be used for login, therefore the `auto_generate` flag can ensure the password is not known.

To avoid the service interruption due to the lockout of internal users, `SYSMAN` and `MGMT_VIEW` users are associated with `MGMT_INTERNAL_USER_PROFILE` upon install. The password parameters are all set to `UNLIMITED`. In addition, to avoid sessions hanging or taking a long time due to resource consumption limit, `MGMT_INTERNAL_USER_PROFILE`'s kernel parameters are set to default, which is unlimited as well.

#### 3.1.2.1.4 Secure and Backup the Encryption Key

The Encryption Key is the master key that is used to encrypt/decrypt sensitive data, such as passwords and preferred credentials, stored in the Repository. The key itself is originally stored in the Repository and removed automatically once the installation is done. It only needs to be in the Repository during an upgrade. By storing the key separately from the Enterprise Manager schema, we ensure that the sensitive data such as Preferred Credentials remain inaccessible to the schema owner and other `SYSDBA` users (privileged users who can perform maintenance tasks on the database). Keeping the key outside of the Enterprise Manager schema will ensure that sensitive data remain inaccessible while Repository backups are accessed. Further, the Enterprise Manager schema owner (`SYSMAN`) should not have access to the OMS Oracle Homes to prevent reading or overwriting the `emkey`. See the Oracle Enterprise Manager Cloud Control Administrator's Guide for more detailed information about Enterprise Manager's Cryptographic Support and the `emkey`. Follow the process outlined below to secure the encryption key.

Backup the encryption key to a file by running the following command and keep the encryption file on a separate machine securely, restrict access to only the OMS

software owner. If the encryption key is lost or corrupted, the encrypted data in the repository is unusable.

```
$ emctl config emkey -copy_to_file_from_credstore -emkey_file emkey.ora
```

The encryption key is required to be in the Repository for some operations such as Enterprise Manager patches and upgrades.

Remove the key from the Repository once the operation is done.

```
$ emctl config emkey -remove_from_repos
```

#### 3.1.2.1.4.1 Best Practices for Securing the Oracle Management Repository

- Enable Advanced Security Option on the Repository database and configure OMS and Agent
- Restrict network access to known targets
- Grant Super Administrator privilege to select administrators and do not log in with SYSMAN account
- Enable strong password profiles and change application related account passwords regularly
- Secure and backup the encryption key

### 3.1.3 Securing the Oracle Management Agent

For better security during agent installation, agents should be deployed using Enterprise Manager Enterprise Manager's Agent Deploy which uses the secure SSH protocol. When manually deploying Agents, to protect against the possibility of users installing unauthorized agents, use one-time registration passwords that have a reasonable expiry date instead of persistent registration passwords. Registration passwords can be created in the Console or by using the `emctl secure setpwd` command.

Install the agent as a separate user from OMS installation and support only impersonation based access to this account such as `sudo` or `PowerBroker` post installation to prevent unauthorized changes.

### 3.1.4 Secure Communication

There are several ways to secure the communication between OMS and agent, including firewalls, the OMS secure-lock feature, enabling TLSv1, enabling strong cipher suites and certificates. The following section looks at these in more detail.

#### 3.1.4.1 Best Practices for Securing the Oracle Management Agent

- Utilize the Enterprise Manager Agent Deployment method for Agent installations.
- Use a one-time registration passwords with expiry dates
- Install the Agent as a separate user from OMS or Targets

 **Note:**

Agents on remote servers need to be installed as a separate OS user of the targets on that server, however, this does not apply to chained Agents. A chained Agent cannot be installed as a separate user because it gets installed along with the OMS.

### 3.1.4.2 Enable ICMP

Enterprise Manager uses the industry-standard Internet Control Message Protocol (ICMP) echo request to check status of target host machines if the agent has not uploaded or responded in a timely fashion or at expected intervals. If ICMP is disabled, the target will appear to be down. Firewall should be configured to allow ICMP to prevent false down target alerts.

A Beacon is a target that allows the Management Agent to remotely monitor services. A Beacon can monitor one or more services at any point in time. ICMP and User Datagram Protocol (UDP) are also used to transfer data between Beacon targets that allow an Agent to monitor services and the network components you are monitoring. If there is a firewall or ACL between the Web application components and the Beacons you use to monitor those components, you must configure it to allow ICMP, UDP, and HTTP traffic.

### 3.1.4.3 Configure Oracle Management Agent for Firewalls

When the host where the agent resides is protected by a firewall, you need to configure the agent to use a proxy, or configure the firewall to allow incoming communication from the OMS. To configure the firewall you must determine the port assigned to the agent and whether communication is HTTP or HTTPS. You can find this information by running `emctl status agent`.

To configure the proxy set the following properties using the Enterprise Manager Console to edit the Agent properties or `emctl setproperty agent` and restart the agent. The proxy realm, user and password may not be required in all environments.

```
$ emctl setproperty agent -name REPOSITORY_PROXYHOST -value proxy42.acme.com
$ emctl setproperty agent -name REPOSITORY_PROXYPORT -value 80
$ emctl setproperty agent -name REPOSITORY_PROXYREALM -value <value if needed>
$ emctl setproperty agent -name REPOSITORY_PROXYUSER -value <value if needed>
$ emctl setproperty agent -name REPOSITORY_PROXYPWD -value <value if needed>
```

### 3.1.4.4 Configure Oracle Management Service for Firewalls

In cases where the Oracle Management Service is behind a firewall, configurations will be needed to allow proxy communications to the agents or incoming communication through the firewall.

If the agents that are behind the firewall are in different domains, you can configure the proxy to allow communication for those agents and use the `dontProxyFor` parameter to identify the agents within the firewall. To configure the proxy on the Management Service set the following properties using `emctl set property`. The proxy realm, user and password may not be required in all environments.

```
$ emctl set property -name REPOSITORY_PROXYHOST -value proxy42.acme.com
$ emctl set property -name proxyPort -value 80
$ emctl set property -name dontProxyFor -value ".acme.com, .acme.us.com"
```

To configure the firewall to allow inbound communication from the agents for metric uploads, the firewall must be configured to accept HTTP/HTTPS traffic on the upload ports. The default ports are 4889 (HTTP) and 1159 (HTTPS). If your ports were customized you'll need to use those ports.

If there is a firewall between your browser and the Enterprise Manager Console, you must configure firewall to allow the console to receive HTTP/HTTPS traffic over port 7788/7799 (defaults). You can validate your port by looking at the URL you access the Console with.

```
https://mgmthost.acme.com:7799/em
```

Additional component installations such as JVM, APD and BI have additional port requirements. For example, if BI Publisher is installed additional ports may be needed for access to the reporting console. Default ports are 9702/9703 (http/https). For more information please see the documentation specific to the component.

To manage the database targets that are configured behind firewalls, you must allow Oracle Net traffic on the listener ports (typically 1521 but often customized). For more information regarding configuring Oracle Databases for firewalls see the Oracle Database 2 Day + Security Guide.

## 3.1.5 Security Console

The Security Console is available to Super Administrators only and provides all security related configuration information in one location, allowing you to view, analyze, and optimize security for your managed environment. To access the Security Console, from the **Setup** menu, select **Security**, and then **Security Console**.

When the Security Console first displays, it is divided into two main windows, the menu window on the left hand side and the information window on the right hand side.

The Security Console contains both static (text) and dynamic information. The text is to provide quick, high level context to the data, it is not intended as a replacement to your documentation.

The Security Console is categorized into the following security areas:

- [Overview](#)
- [Pluggable Authentication](#)
- [Fine-grained Access Control](#)
- [Secure Communication](#)
- [Credentials Management](#)
- [Comprehensive Auditing](#)
- [Active User Session Count](#)
- [Best Practices Analysis](#)



### 3.1.5.1 Overview

The overview section gives a high level description of each of the Security Console categories.

### 3.1.5.2 Pluggable Authentication

The Pluggable Authentication section is further divided into two tabs. An "Overview" tab and a "Configuration" tab.

#### 3.1.5.2.1 Pluggable Authentication Overview

The Overview section contains text from the documentation, however, it is not meant as a replacement for the documentation. Enterprise Manager Authentication is the process of determining the validity of the user attempting to access Enterprise Manager. The authentication feature is available across the different interfaces such as the Enterprise Manager console and the Enterprise Manager Command Line Interface (EM CLI). Oracle Enterprise Manager 13c relies on the WebLogic Server for external Authentication methods. For this reason, Enterprise Manager 13c can be authenticated using any authentication method supported by Oracle WebLogic Server.

This section also identifies the Authentication schemes supported by Enterprise Manager, for more information please see [Security Features](#) , [Configuring Authentication](#) .

#### 3.1.5.2.2 Pluggable Authentication Configuration

This section displays the current configuration information in your enterprise relating to Authentication.

##### **Authentication Configuration**

*Authentication Mode:* This parameter provides information on the various pluggable authentication schemes configured in your Enterprise Manager environment.

*External User Support Enabled:* Displays if you have external user authentication enabled. If using any authentication other than "repository" authentication, this will display "yes".

*Auto-provisioning supported:* The status of auto-provisioning is also displayed. Auto-provisioning allows for an externally authenticated user to log into Enterprise Manager without being preconfigured within Enterprise Manager and the information is transferred from the authentication application. It requires that the OMS property `oracle.sysman.core.security.auth.autoprovisioning` be set. For more information please see [Security Features](#) , [External Authorization using External Roles](#).

##### **Password Profile**

When creating an Administrator (Setup->Security->Administrators menu) you enter the type of password profile you want that user to use during login. This table gives a count of the number of users in Enterprise Manager which have been assigned the various password profiles. For more information on password profiles see [Securing User Accounts](#).

### 3.1.5.3 Fine-grained Access Control

Enterprise Manager implements granular privileges to control access to targets, and other resources, allowing administrators to better segregate their duties. For example, consider the provisioning designer and provisioning operator job responsibilities. The former has greater responsibilities (creates components in the Software Library) than the latter (submits deployments). Fine-grained access control explains the privileges and roles and how they serve to provide various levels of access control to different applications, groups, services and targets within Enterprise Manager. Information about the Administrators last login to the system, their number of privileges and roles granted and recommendations on best practices relating to appropriate usage of roles and privileges can be found in this section.

The Fine-grained Access Control area is divided into five tabs, An Overview, Administrators tab, Privileges tab, Roles tab and Privilege Propagation Aggregates tab.

#### 3.1.5.3.1 Overview

Giving the same level of access to all systems to all administrators is dangerous, but individually granting access to tens, hundreds, or even thousands of targets to every new member of the group is time consuming. With Enterprise Manager's administrator privileges and roles feature, this task can be performed within seconds, instead of hours. Authorization controls the access to the secure resources managed by Enterprise Manager via system, target, and object level privileges and roles.

This section describes Enterprise Manager's Authorization model including user classes, roles, and privileges assigned to each user class. The following topics are described:

- Classes of Users
- Privileges and Roles

#### 3.1.5.3.2 Classes of Users

Oracle Enterprise Manager supports different classes of Oracle users, depending upon the environment you are managing and the context in which you are using Oracle Enterprise Manager. There are three administrator access categories:

- Super Administrator: Powerful Enterprise Manager administrator with full access privileges to all targets and administrator accounts within the Enterprise Manager environment. The Super Administrator, SYSMAN is created by default when Enterprise Manager is installed. The super administrator account can manage all other administrator accounts and set up all administrator credentials. The super administrator can:
  - Create Enterprise Manager privileges and roles
  - Perform the initial setup of Enterprise Manager, for example, defining e-mail configurations and defining global notifications rules
  - Add targets to Enterprise Manager
  - Perform any action on any target in the system
- Administrator Regular Enterprise Manager administrator.

- Repository Owner Database administrator for the Management Repository. This account cannot be modified, duplicated, or deleted.

### Privileges and Roles

User privileges provide a basic level of security in Enterprise Manager. Privileges can be divided into two categories: **Target Privileges** and **Resource Privileges**

A role is a collection of Enterprise Manager resource privileges, or target privileges, or both, which you can grant to administrators or to other roles. These roles can be based upon geographic location (for example, a role for Canadian administrators to manage Canadian systems), line of business (for example, a role for administrators of the human resource systems or the sales systems), or any other model.

- Out-of-Box Roles
 

Enterprise Manager Cloud Control 13c comes with predefined roles to manage a wide variety of resource and target types.
- External Roles
 

Enterprise Manager Cloud Control 13c can be integrated with external authorization source like Active Directory by defining External roles.
- Private Role
  - Secure privileges like FULL\_CREDENTIAL,FULL\_JOB etc which are not granted to Super Administrators by default, can be granted to a private role.
  - Private roles can not be converted into System Roles. Creator of a private role handles the life cycle of it.
  - Private roles can be granted to administrators 'WITH\_ADMIN' option from Enterprise Manage command line interface (EMCLI) which will enable administrators to grantor revoke private roles to/from other administrators.

#### 3.1.5.3.3 Fine-grained Access Control Administrators

This lists all the Administrators current created in Enterprise Manager, and also lists the date and time in which they last logged in.

#### 3.1.5.3.4 Fine-grained Access Control Privileges

This lists the top five administrators with the number of privileges directly granted to them. Administrators with high numbers of privileges indicate an inefficient use of privileges and should be directed to use roles instead. It is recommended that an Administrator be granted the minimum number of privileges necessary to perform their task. For more information on privileges and roles, see section 2.2.3, "[Managing Privileges with Privilege Propagating Groups](#)".

This section also displays all the Target and Resource Privileges available in Enterprise Manager, whether the privilege can be applied to a single target, a specific target, a target type and if that privilege contains another privilege.

#### 3.1.5.3.5 Fine-grained Access Control Roles

This section allows us to view the top 5 Administrators with the Highest Number of Roles, if the number of role grants is high, it points to an inefficient role hierarchy, suggesting that roles could be combined for efficient manageability.

Roles with the Highest Number of Nested Roles can also be displayed here.

### 3.1.5.3.6 Fine-grained Access Control Privilege Propagation in Aggregates

An aggregate target is a target that consists of one or more member targets, such as groups and systems. Enterprise Manager support two type of aggregate targets based on privilege propagation mechanism:

- Normal aggregate target - If any privilege is granted on aggregate target, only view privilege will be propagated to its members
- Privilege Propagating aggregate target - If any privilege is granted on aggregate target then the same privilege will be propagated to its members

The following features are supported in case of target privileges on Aggregate Targets:

- Separation between the privilege grants on aggregate target and its members
- Along with the default existing behavior of propagating the same privilege on members, User can choose to have one privilege grant on aggregate target and another on its members. User can also choose to have no privilege on members.
- In case of non privilege propagating aggregate targets by default only view will be granted to the members where as in case of privilege propagating aggregate targets whatever privilege is specified by the administrator that will be granted appropriately.
- This feature is available from User and Role management pages as well as Target Access Page in the user interface. On these pages click on "Advanced Privilege Settings" button on top of Target Privileges table to see the advanced privileges in the table.
- EM CLI support is also available for this new feature. Please check EM CLI help for existing relevant verbs for more details on the usage.

Consider the following snapshot of the target privileges for a given administrator:

- Privileges listed under column "Manage Target Privilege Grants" are applicable to the Group as well as the members.
- Privileges listed under column "Manage Aggregate Only Privilege Grants" are applicable only on the Group.
- Privileges listed under column "Manage Member Only Privilege Grants" are applicable only on the members.
- In the following example PPG\_DB\_group1 is a privilege propagating group of database targets. PPG\_HOST\_group2 is a privilege propagating group of host targets. NORMAL\_group1 is a non-privilege propagating group.

**Table 3-1 Target Privileges and Privilege Propagation**

| Name            | Type  | Manage Target Privilege Grants | Manage Aggregate Only Privilege Grants | Manage Member Only Privilege Grants |
|-----------------|-------|--------------------------------|----------------------------------------|-------------------------------------|
| PPG_DB_group1   | Group | View                           | Configure Target                       | Blackout Target                     |
| PPG_HOST_group2 | Group | None                           | Configure Target                       | None                                |
| NORMAL_group1   | Group | None                           | Blackout Target                        | View                                |
| NORMAL_group1   | Host  | Host                           | Not Applicable                         | Not Applicable                      |

- Consider the first row in the above table. This configuration means that the given user has View privilege on group PPG\_group1 as well as the members. Along with that it has Configure Target privilege only on the group PPG\_group1 and Blackout Target privilege only on members. This means that the current user in the picture can create Blackout on the members of group PPG\_group1 but cannot do so on the group itself and it can configure PPG\_group1 but cannot configure the members. The user has View on group as well as the members.
- Consider the second row. PPG\_HOST\_group2 is a privilege propagating group. This configuration means that the given user has Configure Target privilege only on the group PPG\_group2 and it does not have even View on members.
- In the third row one can see a non privilege propagating group where the user is having Blackout Target privilege on the group and View privilege on the members.
- Note that the two new advanced privileges column values are not applicable in case of non aggregate target like host target.

Note that the above mentioned feature is applicable to all Aggregate Targets in general. The above example shows one of Aggregate Target type (Group).

### 3.1.5.4 Secure Communication

This section provides a high-level overview of Secure Communication terms and protocols used within Enterprise Manager. You can also view the current status of secured Enterprise Manager components, their certificate issuers, and details.

#### 3.1.5.4.1 Secure Communication Overview

Enterprise Manager Framework Security implements the following types of secure connections between the Enterprise Manager components:

- HTTPS and Public Key Infrastructure (PKI) components, including signed digital certificates, for communications between the Management Service and the Management Agents.
- Oracle Advanced Security for communications between the Management Service and the Management Repository.

##### 3.1.5.4.1.1 Enabling Security for the Oracle Management Service

To enable Enterprise Manager Framework Security for the Management Service, you use the `emctl secure oms` utility, performs the following actions:

- Generates a Root Key within your Management Repository. The Root Key is used during distribution of Oracle Wallets containing unique digital certificates for your Management Agents.
- Modifies your WebTier to enable HTTPS channel between your Management Service and Management Agent.
- Enables your Management Service to accept requests from Management Agents using Enterprise Manager Framework Security.

##### 3.1.5.4.1.2 Securing the Oracle Management Agent

When you install the Management Agent on a host, you must identify the Management Service that will be used by the Management Agent. To enable Enterprise Manager Framework Security for the Management Agent, use the `emctl secure agent` utility.

### 3.1.5.4.1.3 Restricting HTTP Access to the Management Service

It is important that only secure Management Agent installations that use the Management Service HTTPS channel are able to upload data to your Management Repository and Cloud Control console is accessible via HTTPS only.

### 3.1.5.4.1.4 Managing Agent Registration Passwords

Enterprise Manager uses the Agent Registration password to validate that installations of Oracle Management Agents are authorized to load their data into the Oracle Management Service.

The Agent Registration password is created during installation when security is enabled for the Oracle Management Service. You can add/edit/delete registration passwords directly from the Enterprise Manager console.

#### 3.1.5.4.1.4.1 Enabling Security for the Management Repository Database

You enable security for the Management Repository by using Oracle Advanced Security.

### 3.1.5.4.1.5 Secure Communication Current Configuration

*Agent Certificate Details:* Displays secured agents along with their certificate details, including the algorithm, its strength, when it was created, when it expires and when the agent was secured.

*Number of Unsecured Agents:* Indicates the number of Agents in your enterprise that are currently operating unsecured.

*Number of Expired Registration Passwords:* Indicates the number of Agents which have stopped running due to an expired certificate.

*Certificate Authority Details:* Lists the certificates being used in your Enterprise Manager installation.

*OMS Secure Configuration:* Details the Enterprise Manager configuration and communication with the Management Services and indicates the secure configuration details of each, including the console and upload certificate details along with the SLB details.

### 3.1.5.4.2 Database Encryption Configuration

Following are the configuration details about encryption between the OMS and Management Repository/Target Database. The list of encryption algorithms and the checksum algorithms that the client supports are mentioned below. For more details refer to the section "Enabling Security for the Management Repository Database" above.

- *Encryption Algorithms Supported:* Lists all the encryption algorithm details supported.
- *Encryption Algorithm In Use:* Lists the current Algorithm being used.
- *Checksum Algorithm Supported:* Lists the check-up Algorithm currently supported (MD5 and SHA1).
- *Checksum Algorithm in use:* Lists the Algorithm currently in use.

### 3.1.5.5 Credentials Management

Credentials like user names and passwords are typically required to access targets such as databases, application servers, and hosts. Credentials are encrypted and stored in Enterprise Manager. Beginning with Enterprise Manager 13c, the credential subsystem supports, in addition to basic username-password, strong authentication schemes such as PKI, SSH keys and Kerberos. SSH key based host authentication, used by jobs, deployment procedures and other Enterprise Manager subsystems, is now supported.

By using appropriate credentials, you can:

- Collect metrics in the background as well as real-time
- Perform jobs such as backup, patching, and cloning
- Perform real-time target administration such as start, and stop
- Connect to My Oracle Support

Based on their usage, credentials can be classified into the following categories:

- Named Credentials
- Monitoring Credentials
- Preferred Credentials

#### **Credentials Management Current Configuration**

*Encryption Key:* The Encryption Key is the master key that is used to encrypt/decrypt sensitive data, such as passwords and preferred credentials that are stored in the Repository. The key is originally stored in the Repository and is removed from the Repository and copied to the Fusion Middleware managed Credential Store during installation of the first OMS.

#### **Credentials Management Usage Statistics**

The Usage Statistics tab provides credential usage information.

### 3.1.5.6 Comprehensive Auditing

Comprehensive Auditing shows the current *auditable operations* and whether they have been configured for external backup to disk. Statistics on the top five most used operations are also displayed, as well as the most active Administrators.

All operations performed by Enterprise Manager administrators, such as creating users, granting privileges, starting a remote job like patching or cloning, need to be audited to ensure compliance with the contracted internal controls of a service organization.

Non-repudiation is the central tenet of auditing. Enterprise Manager Comprehensive auditing provides a tamper-free audit trail of all critical operations.

From the Usage tab, you can view:

- Current Auditing Configuration
- Specific Audit Operations



- Audit Usage Statistics (Top 5 Operations in the last 7 days and Top 5 Administrators in the last 7 days)

### 3.1.5.7 Active User Session Count

Active User Session Count shows information related to the session management, such as session timeout, max and active sessions per user count.

All authenticated open user sessions can be viewed from this area.

From the Active User Session Count area, you can view:

- Session Settings (Session Timeout, Maximum Number of Sessions Allowed Per User, Permitted Number of Active Sessions )
- Active Sessions

### 3.1.5.8 Best Practices Analysis

Based on observations of information in the above categories, best practices advice is indicated in this section and covers areas such as management of the repository encryption key and auditing operations management. You can quickly view Enterprise Manager security configuration adherence to recommended Oracle security protocols. In addition, suggested best practices are provided based on the specifics of your Enterprise Manager environment.

From the Best Practices Analysis area, you can view:

- Pluggable Authentication: Best practice advice tailored to the pluggable authentication scheme of your environment.
- Fine-grained Access Control: Best practice advice pertaining to role and privilege management.
- Secure Communication: Best practices regarding secure communication between the Management Service, Agent, and Enterprise Manager console.

## 3.2 Guidelines for SSL Communication

This section covers the following SSL Guidelines:

- [Ensure TLSv1.2 Protocol is Enabled](#)
- [Leave Communication in Secure-Lock Mode](#)
- [Modify Cipher Configuration if Required](#)
- [Best Practices for Securing Communication](#)

### 3.2.1 Ensure TLSv1.2 Protocol is Enabled

Transport Layer Security (TLS) is a cryptographic protocol used to increase security over computer networks by providing communication privacy and data integrity between applications. Although it is technically the successor of SSL, TLS is generically referred to as SSL. Beginning with Enterprise Manager 13c, TLSv1.2 is enabled by default.

In the case of Enterprise Manager, these *secure* communication channels are between various components of the Enterprise Manager framework. For Enterprise



Manager 13c, the TLSv1.2 protocol is supported on the infrastructure communication channels including:

- Oracle Management Services to 13c Agent
- 13c Agent to Agent
- EMCLI to Oracle Management Services
- Browser to Admin Server/Managed Server Console
- Oracle Management Services to Server Load Balancer
- 13c Agent to Always-On Monitoring Application
- Oracle Management Services to BI Publisher
- Oracle Management Services to My Oracle Support
- 13c Agent to Fusion Middleware Target
- Oracle Management Services to Fusion Middleware Target

### Enabling Oracle Management Service to Database Communication on TLS1.2

You can also configure TLSv1.2 communication channels between the OMS and target databases, which include the Enterprise Manager Management Repository.

- For specific instructions on enabling TLSv1.2 communication between the Oracle Management Service and the Management Repository, see [Configuring TLSv1.2 for Communication with the Enterprise Manager Repository](#).
- For information on configuring TLSv1.2 communication with target Oracle databases, see [Secured Communication \(TCPS\) Access to Databases](#).

### Enabling Always-On Monitoring Communication on TLS1.2

The Always-On Monitoring application provides the ability to monitor critical target status and metric alerts when the Oracle Management Service is unavailable. The service continuously monitors critical targets through the Enterprise Manager Agent and can be easily configured to send email notifications for these events to administrators. For information on configuring TLSv1.2 for communication between the Always-On Monitoring (AOM) application and AOM Repository, and between the AOM application and Enterprise Manager Repository, refer to *Configuring the Always-On Monitoring Application for Secure Communication Using the TLSv1.2 Protocol* in the *Enterprise Manager Administrator's Guide*.

### Locking Down the Oracle Management Service to Use the TLSv1.2 Protocol Only

In order to restrict Oracle Management Services communication to use the TLSv1.2 protocol only:

1. Stop the Oracle Management Services. From the command line, run the following:

```
<OMS_ORACLE_HOME>/bin/emctl stop oms
```

2. Set the OMS communication protocol: From the command line, run the following:

```
<OMS_ORACLE_HOME>/bin/emctl secure oms -protocol TLSv1.2
```

3. Enter the following command to restart the OMS:

```
$ emctl start oms
```

## Enabling TLS in Mixed Version Environments

If you are installing a Enterprise Manager Cloud Control 13c for the very first time, all of the aforementioned communication channels will use TLSv1.2 by default. If you have an existing Enterprise Manager deployment and you want to enable TLS, you need to be aware that older Agents do not support TLSv1.2..

If there are 12c Agents in the environment which are not yet upgraded to 13c, the communication between the Agent and Oracle Management Service will default to SSL. To configure a 12c Agent to support only TLS v1.0 protocol while the Agent listens as a server, edit the *Agent* properties in the Enterprise Manager console or run `emctl setproperty` at the command line. For example:

```
$ emctl setproperty agent -name allowTLSOnly -value true
```

To edit multiple Agents simultaneously, from the **Setup** menu, choose **Manage Cloud Control** and then **Agents**. From the list, select the Agents you want to modify and then click **Properties**. This will create a job definition where you specify the Agent property that needs to be changed. On the **Parameters** page, set the *minimumTLSVersion* property to *TLSv1.2*. The change will be applied to all selected Agents.

Once the changes have been made, you must bounce the Management Agent(s) in order for the changes to take effect.

## 3.2.2 Leave Communication in Secure-Lock Mode

### 3.2.2.1 Secure and Lock the OMS and Agents

The Oracle Management Service and Oracle Management Agents can run in non-secure (HTTP) or secure (HTTPS) modes. The recommendation is to always use secure mode, hence the default installation will automatically secure-lock the OMS. The secure-lock mode takes security one step further in requiring that agents communicate only through HTTPS port (HTTP port is locked). This ensures that the OMS-Agent communication is always encrypted and mutually authenticated. All requests from un-secure agents are rejected by the OMS. Similarly, any un-secure request from the OMS is rejected by the agent. This helps safeguard the management system from any malicious 'man-in-the-middle' attack happening from within the infrastructure.

If your installation was done before Oracle Enterprise Manager 10g Release 5, you may be required to secure-lock your OMS manually. In the case of upgrades, if the pre-upgrade environment is secured, the upgrade retains the secure mode but does not secure-lock the OMS. If the pre-upgrade environment is already secure-locked, the upgrade retains the secure-lock mode between OMS and Agent.

To check the secure status of the OMS and secure-lock the communication between OMS and agent run the command and restart the OMS:

```
$ emctl status oms -details
Oracle Enterprise Manager Cloud Control 13c Release 12.1.0.3.0
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
Enter Enterprise Manager Root (SYSMAN) Password :
Console Server Host : mgmthost.acme.com
HTTP Console Port : 7790
HTTPS Console Port : 7803
```

```

HTTP Upload Port : 4890
HTTPS Upload Port : 4904
OMS is not configured with SLB or virtual hostname
Agent Upload is locked.
OMS Console is locked.
Active CA ID: 1
Console URL: https://mgmthost.acme.com:7803/em
Upload URL: https://mgmthost.acme.com:4904/empbs/upload
...

```

```

$ emctl secure lock -upload
Oracle Enterprise Manager Cloud Control 13c Release 12.1.0.3.0
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
Enter Enterprise Manager Root (SYSMAN) Password :
Agent Upload is locked. Agents must be secure and upload over HTTPS port. Restart
OMS.

```

Note that once OMSs are running in secure-lock mode, unsecure agents will not be able to upload any data to the OMSs. To check the status and secure the agent issue the following, you will be prompted for the registration password:

```

$ emctl status agent -secure
Oracle Enterprise Manager 13c Cloud Control 12.1.0.1.0
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
Checking the security status of the Agent at location set in /scratch/cllamas/oracle/
em12/agent/agent_inst/sysman/config/emd.properties... Done.
Agent is secure at HTTPS Port 3872.
Checking the security status of the OMS at https://mgmthost.acme.com:4904/empbs/
upload/... Done.
OMS is secure on HTTPS Port 4904

```

```

$ emctl secure agent
Oracle Enterprise Manager 13c Cloud Control 12.1.0.1.0
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
Agent successfully stopped... Done.
Securing agent... Started.
Enter Agent Registration Password :
Agent successfully restarted... Done.
EMD gensudoprops completed successfully
Securing agent... Successful.

```

To ensure the console access from the client browser is secure over SSL/TSL, the console must be locked as well. From Oracle Enterprise Manager 10g Release 5 installations are secure-locked by default. In the case of upgrades, if the pre-upgrade environment is not secure-locked, after the upgrade you need to run the following command to secure-lock the console access:

```
$ emctl secure lock -console
```

### 3.2.3 Modify Cipher Configuration if Required

A cipher suite is a combination of cryptographic parameters that define the security algorithms and key sizes used for authentication, key agreement, encryption, and integrity protection. Cipher suites protect the integrity of a communication. For example, the cipher suite called `SSL_RSA_WITH_AES_128_CBC_SHA` uses RSA for key exchange, AES with a 128-bit key, CBC, and SHA for bulk encryption. A cipher suite is a combination of cryptographic parameters that define the security algorithms and key sizes used for authentication, key agreement, encryption, and integrity protection. Cipher suites protect the integrity of a communication. For example, the

cipher suite called `SSL_RSA_WITH_AES_128_CBC_SHA` uses RSA for key exchange, AES with a 128-bit key, CBC, and SHA for bulk encryption.

In Enterprise Manager, ciphers are configured for the following end points:

- Oracle Management Services (OMS) Console end point
- OMS Upload end point
- Agent end point
- WebLogic end point

### Ciphers Supported for OMS Console and Upload End Points

Ciphers supported for OMS Console and Upload end points depends on the ciphers supported and exposed by Oracle HTTP Server (OHS), the web server front-ending the OMS server. The ciphers supported by the OHS web server is listed in Table 1: Cipher Suites Supported in the OMS Console and Upload End Points,

A subset of the OHS-supported ciphers are set as default in the configuration files available within the `EMGC_DOMAIN` home and is used for OMS Console and Upload end points. The default set of OHS-supported ciphers used for the OMS Console and Upload end points are listed in the table [Table 3-2](#).

In order to modify the default cipher suites for OMS Console end points, edit the `SSLCipherSuite` property in the following `ssl.conf` file and add/modify from the list of OHS-supported ciphers list.

For a typical multi-OMS scenario:

1. Modify the following file on the primary OMS server:

```
<WEBTIER_INSTANCE_HOME>/user_projects/domains/EMGC_DOMAIN/config/fmwconfig/
components/OHS/ohs1/ssl.conf
```

2. Modify the following file on each of the additional OMS servers:

```
<WEBTIER_INSTANCE_HOME>/user_projects/domains/EMGC_DOMAIN/config/fmwconfig/
components/OHS/instance/ohs1/ssl.conf.emctl_secure
```

In order to modify the default cipher suites for the Upload end point, edit the `SSLCipherSuite` property in the following `httpd_em.conf` file and add/modify from the list of OHS supported ciphers.

For a typical multi-OMS scenario,

1. Modify the following file on primary OMS server:

```
<WEBTIER_INSTANCE_HOME>/user_projects/domains/EMGC_DOMAIN/config/fmwconfig/
components/OHS/ohs1/moduleconf/httpd_em.conf
```

2. Modify the following file on each additional OMS server:

```
<WEBTIER_INSTANCE_HOME>/user_projects/domains/EMGC_DOMAIN/config/fmwconfig/
components/OHS/instance/ohs1/moduleconf/httpd_em.conf.emctl_secure
```

Any modification of cipher suites for the OMS console and Upload end points requires a restart of the OMS, including the Admin server.

**Table 3-2 Cipher Suites Supported in the OMS Console and Upload End Points**

| OHS Supported Cipher Suites     | OMS Default: Console | OMS Default: Upload |
|---------------------------------|----------------------|---------------------|
| SSL_RSA_WITH_3DES_EDE_CBC_SHA   | Yes                  | No                  |
| SSL_RSA_WITH_AES_128_CBC_SHA    | No                   | Yes                 |
| RSA_WITH_AES_128_CBC_SHA256     | No                   | Yes                 |
| SSL_RSA_WITH_AES_256_CBC_SHA    | No                   | Yes                 |
| RSA_WITH_AES_256_CBC_SHA256     | No                   | Yes                 |
| ECDHE_RSA_WITH_3DES_EDE_CBC_SHA | No                   | Yes                 |
| ECDHE_RSA_WITH_AES_128_CBC_SHA  | No                   | Yes                 |
| ECDHE_RSA_WITH_AES_256_CBC_SHA  | No                   | Yes                 |
| RSA_WITH_AES_128_GCM_SHA256     | No                   | Yes                 |
| RSA_WITH_AES_256_GCM_SHA384     | No                   | Yes                 |

**Ciphers Supported for Agent End Points**

Ciphers supported for Agent EMD\_URL / end points ( if it is enabled in Agent’s JDK) are listed in Table 2. A subset of these supported ciphers are set as defaults on the agent end points. The table also shows which ciphers for the Agent EMD\_URL /end point are enabled by default.

In order to override the default cipher suites used by the agent , edit the *SSLCipherSuites* property in emd.properties to include the ciphers from the list of supported ones. Optionally, you can use the `setproperty` command as follows:

```
$ emctl setproperty agent -name SSLCipherSuites -value <values>
```

**Table 3-3 Cipher Suites Supported on the Agent End Point**

| Supported Cipher Suites           | Agent Default |
|-----------------------------------|---------------|
| RSA_WITH_3DES_EDE_CBC_SHA         | Yes           |
| RSA_WITH_AES_128_CBC_SHA          | Yes           |
| RSA_WITH_AES_128_CBC_SHA256       | Yes           |
| RSA_WITH_AES_256_CBC_SHA          | No            |
| RSA_WITH_AES_256_CBC_SHA256       | Yes           |
| ECDHE_RSA_WITH_3DES_EDE_CBC_SHA   | No            |
| ECDHE_RSA_WITH_AES_128_CBC_SHA    | No            |
| ECDHE_RSA_WITH_AES_128_CBC_SHA256 | Yes           |
| ECDHE_RSA_WITH_AES_256_CBC_SHA    | No            |
| ECDHE_RSA_WITH_AES_256_CBC_SHA384 | Yes           |
| DHE_RSA_WITH_3DES_EDE_CBC_SHA     | No            |
| DHE_RSA_WITH_AES_128_CBC_SHA      | No            |
| DHE_RSA_WITH_AES_128_CBC_SHA256   | Yes           |
| DHE_RSA_WITH_AES_256_CBC_SHA      | No            |

**Table 3-3 (Cont.) Cipher Suites Supported on the Agent End Point**

| Supported Cipher Suites         | Agent Default |
|---------------------------------|---------------|
| DHE_RSA_WITH_AES_256_CBC_SHA256 | Yes           |

Notes:

- AES\_256 ciphers will only work if the Agent JKS has unlimited strength policy file corresponding to the Agent Java version currently installed on the system. For instance, 13.2 agents using Java 7, download unlimited strength policy file from <http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>. Unzip and copy local\_policy.jar & US\_export\_policy.jar in to <agent\_base\_directory>/agent\_13.2.0.0.0/oracle\_common/jdk/jre/lib/security.
- All cipher suites using SHA256 & above will only work for TLS1.2. See [Ensure TLSv1.2 Protocol is Enabled](#) for information on making sure the end point is configured on TLS1.2.
- For SSL handshake to happen on a particular cipher suite, it should be enabled on both client and server. For example, if the communication from agent to OMS Server should happen on 'ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA' cipher suite, then this cipher suite should be configured on both agent (client) and OMS Upload end point(server).

### Ciphers Supported for WebLogic End Points

WebLogic end point uses the ciphers provided by the underlying JDK by default. In order to change the default ciphers, refer to the official guide on *Fusion Middleware Administering Security for Oracle WebLogic Server 12.1.3*.

## 3.2.3.1 Third Party Certificates

Use a certificate from well-known Certificate Authority (CA) to secure OMS-Agent communication and console access to take advantage of the well-known trusted certificates with different expiry and key size.

## 3.2.3.2 Oracle Wallets

Oracle has introduced the concept of a wallet, which is a password-protected container used to store authentication and signing credentials, including private keys, certificates, and trusted certificates needed by SSL.

To secure the console using a custom certificate authority, you need to create a wallet location and secure the console against that wallet location. For more information on creating a wallet, see the *Oracle Fusion Middleware Administrator's Guide*.

### 3.2.3.2.1 Creating an Oracle Wallet

The following example shows you how to create and add a certificate to an Oracle wallet.

1. Create the wallet container:

 **Note:**

Currently, only single sign-on (SSO) wallets are supported.

```
S /u01/app/oracle/middleware/oracle_common/bin/orapki wallet create -wallet /
home/oracle/labs/mywallet -auto_login_only
```

2. Add a certificate to the wallet: When creating the wallet you must specify the Common Name (CN) as the hostname of the machine where the OMS is installed or the SLB name, if the OMS is behind an SLB. In this example, the OMS is behind an SLB, test.example.com.

```
S /u01/app/oracle/middleware/oracle_common/bin/orapki wallet add -wallet /home/
oracle/labs/mywallet -dn 'CN=test.example.com, OU=Oracle, O=Oracle University,
L=Boise, ST=ID, C=US' -keysize 2048 -self_signed -validity 3650 -auto_login_only
```

3. Set the required environment variables for the existing Weblogic domain. They must be set before using orapkiles:

```
$. setDomainEnv.sh
```

4. View the certificates in the wallet:

```
S /u01/app/oracle/middleware/oracle_common/bin/orapki wallet display -wallet /
home/oracle/labs/mywallet
```

## 3.2.4 Best Practices for Securing Communication

Here is a summary of the best practices for securing communication:

- Enable ICMP for ping check validation
- Configure firewalls as appropriate in your environment
- Secure and lock the OMS and Agents
- Configure strong cipher suites for the OMS and Agent
- Secure upload and console virtual HTTPS hosts with third party certificates

## 3.3 Guidelines for Authentication

### 3.3.1 Enable External Authentication

Enterprise Manager Cloud Control 13c offers multiple methods of authentication. In addition to the predefined methods, a customized provider/module can be plugged in to Cloud Control authentication. The default system authentication method is the standard Repository based authentication. Additional predefined methods include:

- Oracle Single Sign-On (OSSO)
- Enterprise User Security (EUS)
- Integration with Oracle Access Manager Single Sign-On (OAM SSO)
- Direct LDAP integration (Oracle Internet Directory, Microsoft Active Directory)

Refer to "[Configuring Authentication](#)" for detailed information about how to configure Enterprise Manager to use the pre-defined providers.

Using one of the extended authentication modules enables you to take advantage of centralized identity management across the enterprise. Doing this allows you to rely on the external identity management system for password security compliance, password changes and resets. To create a user in Enterprise Manager with external authentication, you select the "external" flag upon creation. During creation of every new user in Enterprise Manager you are prompted for that users mode of Authentication, via an external Identity store such as Oracle Access Manager (OAM), LDAP or Oracle Internet Directory (OID), or internally via Enterprise Manager Repository.

When the account is deleted from the identity management system, it will no longer authenticate in Enterprise Manager but still needs to be manually removed. Ideally, a script or job could be run to remove the user from Enterprise Manager once removed from the identity management system.

When using external Authentication, Enterprise Manager allows the creation of external roles which map to the identity management systems groups by name (i.e. Enterprise Manager role "DBA" maps to LDAP group "DBA"). Thus allowing synchronized user access and privileges based on external group membership.

Target authentication provides access to the host, database or application targets managed through Enterprise Manager. Using strong target authentication methods, named credentials and configuring database password profiles are a few ways to ensure secure target authentication.

To ensure target authentication security, choose strong host and database authentication methods. Credentials for target access are encrypted and stored in Enterprise Manager. With Enterprise Manager Cloud Control 13c, strong authentication such as SSH-keys for host and Kerberos tickets for database are now supported. These credentials can be used by jobs, deployment procedures and other subsystems.

### 3.3.1.1 Best Practices for Authentication

- Integrate with corporate identity management system for enterprise wide authentication
- Use external roles to automatically assign privileges to users based on external group membership
- Automate user creation/deletion based on external group membership using EMCLI
- Utilize strong authentication methods (SSH for host, Kerberos for database)
- For local accounts set up password policies

## 3.4 Guidelines for Authorization

Authorization is the act of validating the privileges and permissions of an authenticated subject. To avoid exploiting authorization, you must implement a policy of segregation of duties. This means no one person should be given responsibility for more than one related function.



Enterprise Manager users may vary widely among a company, and they may have very different roles and purposes.

Enterprise Manager 13c comes with several out-of-the-box roles that provide role based authentication for various operational roles. Segregation of Operator, Designer and Administrator functions for Patching, Provisioning, Cloud, Compliance, and Plug-ins allow more granular authentication for users. Use the Create Like feature to further enhance or restrict as required for your operations.

**Note:**

Performing a Create Like operation on an existing role enables the newly created role to contain all of the privileges of the original role.

With using Role Based Access Control (RBAC), privilege management becomes easier; managing role grants is simpler than managing privilege grants. For a complete list of the out-of-the-box roles see the Privileges and Roles section of the Oracle Enterprise Manager Cloud Control Administrator's Guide.

With Enterprise Manager 13c we have the ability to specify target privileges and resource privileges. Target privileges allow an administrator to perform operations on a target. Some of the new target privileges include Connect to any Viewable Target, Execute Command Anywhere, Execute Command as any Agent and more. The target privileges can be assigned for all targets or for specific targets. Resource privileges grant access to a function, button or page within Enterprise Manager. Some of the new resource privileges include Backup Configurations, Cloud Policy, Compliance Framework, Enterprise Manager Plug-in, Job System, Patch Plan, Self Update and Template Collection. For a complete list, see "[Configuring Privileges and Role Authorization](#)". With these new privileges, it's much easier to implement the Principal of Least Privilege by creating specific roles with very fine grained privileges assigned that match the job duties.

An extended auditing system makes it easy to monitor the privilege grants on a regular basis and also keep track of which users exercised what privileges. Some of the key privilege related auditable actions are listed here:

- Grant job privilege
- Grant privilege
- Grant role
- Grant target privilege
- Grant system privilege
- Revoke job privilege
- Revoke privilege
- Revoke role
- Revoke target privilege
- Revoke system privilege

Super Administrators have FULL privileges on targets/reports/templates/jobs. These are the only users who can create other users and Super Administrators, and grant/

revoke privileges to/from other users. Super Administrator privilege should be granted with caution. Using the following query to get the list of Super Administrators:

```
SELECT grantee FROM MGMT_PRIV_GRANTS WHERE PRIV_NAME = 'SUPER_USER'
```

### 3.4.1 Best Practices for Privilege and Role Management

- Create meaningful roles and grant roles to users instead of granting privileges to users.
- Grant only the minimum set of privileges a user needs for carrying out his/her responsibilities by granting the fine-grained privileges/roles only when needed.
- Audit privilege and role actions for complete monitoring and accountability.
- Limit the number of Super Administrators

### 3.4.2 Use Principle of Least Privileges for Defining Roles/Privileges

The fine granularity of privileges provided in Enterprise Manager allows for the Principle of Least Privileges to be implemented, this recommends that an Administrator must only be able to access the information or resources that are necessary for legitimate purposes.

### 3.4.3 Use Privilege Propagation Groups

Using groups and systems to organize your targets helps reduce security administration overhead. There are two types of groups available in Enterprise Manager 13c that help simplify privilege management and authorization. By granting roles to groups, instead of users and using privilege propagating groups, you can reduce the direct grants and ensure users have access to the targets as needed.

Privilege Propagating Groups simplify the privilege assignment, revocation, and administration along with group management by propagating the assigned privileges to all members of the group. For example, a user can be granted access to a privilege propagating group Sales, and they in turn receive access to all targets within that group.

Administration Groups are privilege propagating groups that automate the application of monitoring settings to targets upon joining the group. Targets cannot be assigned directly to the group, rather they are automatically added based on membership criteria.

Systems are also privilege propagating and allow you to group all related targets of a particular application or function into a system.

#### 3.4.3.1 Best Practices for Groups and Systems

- Create meaningful roles and grant roles to users instead of granting privileges to users.
- Grant only the minimum set of privileges a user needs for carrying out his/her responsibilities by granting the fine-grained privileges/roles only when needed.
- Utilize privilege propagating groups and systems to reduce administration overhead

## 3.5 Guidelines for Auditing

Enterprise Manager has additional auditing that is available for purposes of tracking and validating infrastructure actions performed in Enterprise Manager, including jobs and credentials accessed. Basic and infrastructure auditing is enabled by default for Enterprise Manager 13c.

To enable audit for a subset of audited operations, please use the following EMCLI verb:

```
$ emcli update_audit_settings -audit_switch="ENABLE/DISABLE" -
operations_to_enable="name of the operations to enable,for all operations use ALL" -
operations_to_disable="name of the operations to disable, for all operations use ALL"
```

For example to audit only logon/logoff you would issue:

```
$ emcli update_audit_settings -audit_switch="ENABLE" -
operations_to_enable="LOGIN;LOGOUT"
```

Refer to the section "[Configuring and Managing Audit](#)" for the list of operations that are audited by Enterprise Manager.

In Enterprise Manager 13c, there are over 150 options for auditing. The following command will show you the list of operations that can be audited by Enterprise Manager:

```
$ emcli show_operations_list
```

The following example shows the output of this command.

```
$./emcli show_operations_list
Operation ID Operation Name Infrastructure
Operation
ADD_AGENT_REGISTRATION_PASSWORD Add Registration Password NO
ADD_CS_TARGET_ASSOC Add Standard-Target Association NO
AGENT_REGISTRATION_PASSWORD_USAGE Registration Password Usage NO
AGENT_RESYNC Resync Agent NO
AG_AUD_CREATE Create Administration Groups NO
AG_AUD_DELETE Delete Administration Groups NO
AG_AUD_MODIFY Modify Administration Groups NO
APPLY_TEMPLATE Apply Monitoring Template NO
APPLY_UPDATE Apply Update YES
ATTACH_MEXT Attach Metric Extension NO
```

Once audit is enabled, the audit records are kept in MGMT\$AUDIT\_LOG view in the Repository. Use Enterprise Manager Cloud Control Console to monitor the audit data as user with Super Administrator, click Setup -> Security -> Audit Data.

The externalization service via EMCLI verb `update_audit_settings` externalizes the audit data from the Repository to an external file system on a regular basis. Make sure there is enough space in the directory for the audit log files.

```
$ emcli update_audit_settings -file_prefix=<file_prefix> -
directory_name=<directory_name> -file_size = <file size> -
data_retention_period=<period in days>
```

The following example shows that the audit data will be retained in the Repository for 14 days and once exported the data will be stored in the OS directory that corresponds

to database directory AUDIT with filenames prefixed with gc12\_audit, and the file size will be 50M bytes each:

```
$ emcli update_audit_settings -externalization_switch=ENABLE -file_prefix=gc12_audit
-directory=AUDIT -file_size=50000000 -data_retention_period=14
```

Achieve separation of duties by restricting the access to the directory where the externalized audit data is stored. No Enterprise Manager users should have access to the externalized audit data.

### 3.5.1 Best Practices for Auditing

- Formalize the audit process by setting up an Audit Review schedule or integrating with an Audit tool such as Audit Vault for notifications and alerts.
- Externalize the audit service and secure the files created

## 3.6 Guidelines for Managing Target Credentials

Preferred Credentials simplify access to managed targets by storing target login credentials in the Management Repository. Users can access an Enterprise Manager target that recognizes those credentials without being prompted to log into the target. Preferred credentials are set on a per user basis, thus ensuring the security of the managed enterprise environment. Default credentials can be set for a particular target type as well as target credentials for a particular target. The target credentials override the default credentials.

Do not set preferred credentials for group/common accounts such as SYSMAN. If preferred credentials are set for common accounts, then the accountability of the use of these credentials is lost. The following SQL statements can be used to report the list of users who have the preferred credentials set:

```
SELECT t.target_name,tc.user_name,tc.credential_set_name FROM
MGMT_TARGET_CREDENTIALS tc, MGMT_TARGETS t WHERE tc.target_guid=t.target_guid
```

```
SELECT t.target_name,tc.user_name, tc.set_name FROM EM_TARGET_CREDS tc, MGMT_TARGETS
t WHERE tc.target_guid=t.target_guid and tc.user_name = 'SYSMAN'
```

Credentials can be stored as Named Credentials and then privileges granted to other users to use, update or own the credentials. These credentials can be used for jobs, patching or other administration tasks on specific targets or globally. Eligible credential types include username/password, SSH-key for host and Kerberos for database. This method allows administrators to configure Named Credentials for privileged access and grant to specific users. Auditing tracks Named Credential creation, modification and usage.

Named Credentials provide a secure mechanism in Enterprise Manager to allow for separation of privilege management from privilege delegation for targets. Using Named Credentials an organization can separate the management of the specific username/password/authentication details from the actual authority to use these credentials. This is an essential tool in modern, secure organizations where there needs to be certainty that a malicious user cannot conduct operations outside Enterprise Manager using a set of known credentials obtained from inside Cloud Control. Additionally, the management of a central set of Named Credentials removes a significant burden on the proliferation of credentials information across many Enterprise Manager administrators and also therefore reduces the likelihood of these

being used outside the Enterprise Manager environment or helps prevent against the accidental publication of credentials.

### 3.6.1 Best Practices for Credentials

- Use EMCLI to automate routine password changes on privileged named credentials, this allows one administrator to know and update the password for granted users.
- Utilize named credentials when setting preferred credentials to simplify credential management.
- Do not set preferred credentials for group/common accounts such as SYSMAN.

# 4

## Security Best Practices for Database Management in Enterprise Manager

This chapter provides information about the security best practices that can be implemented for database management using Enterprise Manager 13. It contains the following sections:

- [Flexible Database Access Control](#)
- [Secured Communication \(TCPS\) Access to Databases](#)
- [Account Management](#)

### 4.1 Flexible Database Access Control

Enterprise Manager 13.1 introduces flexible database access control for Enterprise Manager Database Plug-in. The new out of box roles align with database personas and provide tighter access control on managed target databases. Before the introduction of this feature an Enterprise Manager user granted access on the database had access to all of the database management features, such as performance management, high availability management, storage management, security management and so forth. Enterprises have different classes of users such as DBA, Application Developer, Application DBA, and Infrastructure DBA that need to access database management functions. There is a need for a flexible privilege model to accommodate these roles. For example, enterprises may want their application developers to access only performance management functions in a View Only mode.

Providing enterprise users access to unnecessary features and pages opens up the database to security vulnerabilities. Oracle recommends that you grant Enterprise Manager users the minimum number of privileges required to perform their job. Introducing these out of box database management roles grants users access to only the Enterprise Manager pages required to perform their job.

Fine grained privilege control for Enterprise Manager Database plug-in provides a privilege control model for database pages. This enables Enterprise Manager super administrators to grant the minimum access to Enterprise Manager administrators and users required to complete their more specific responsibilities.

High levels of security can be implemented using the new flexible DB access control features for database management. This section includes the following:

- [Database Management Roles and Responsibilities](#)
- [Application DBA Access](#)
- [Application Developer Access](#)
- [Database Monitoring User Access](#)
- [Database Administrator Access](#)
- [Privilege Groups](#)

## 4.1.1 Database Management Roles and Responsibilities

Oracle Enterprise Manager supports granting different levels of access to DBAs based on their roles and responsibilities in the organization. The following roles are recommended to implement security best practices for an organization.

- **Application DBA**  
An application DBA is a restricted database administrator who manages application schemas, application objects, and application performance in the database. An application DBA should be able to identify and fix application performance issues in the database. An application DBA is responsible for keeping the application up and running and in good performance.
- **Application Developer**  
An application developer is a person who develops an application. Application developers capture requirements from customers and develop the application according to customer requirements. Application developers use Oracle Enterprise Manager to tune SQL in their application modules for optimal performance in production environments. Application developers are responsible for the modules of the application in development, test, and production environments.
- **Monitoring User**  
The database monitoring user monitors the database for smooth functioning of the application in production environments. Monitoring users respond to alerts raised in the Enterprise Manager environment. Monitoring users can update the schedule of metrics and setup blackouts on the databases. Monitoring users are not allowed to make any changes to the production database. Monitoring users ensure that the application is up and running by responding to any issues reported and ensuring that the issues are assigned to the DBAs responsible for resolution.
- **Database Administrator**  
Database administrators performs full database lifecycle management including installation configuration, monitoring, backup, recovery, and performance tuning.

## 4.1.2 Application DBA Access

Application DBAs should have access to the Performance and Schema Management pages in Enterprise manager.

### 4.1.2.1 Creating an Application DBA Account

To create an application DBA account in Enterprise Manager:

1. Follow the instructions in "[Creating a New Administrator](#)" to create an Enterprise Manager administrator.
2. Grant the privilege Database Application DBA on the database target.
3. Grant the Full privilege on the database host target.
4. Using the Resource Privileges Page, grant the Create New Named Credentials privilege on the Named Credential Resource Type privilege page and Create Privilege on Job System Resource Type privilege.

### 4.1.2.2 Creating Named Credentials

To create named credentials, the database administrator can create their own named credential or it can be created by the super administrator (or a privileged Administrator with the system resource privilege) and then granted to the application DBA. The named Credential is granted the view privilege on the named credential so that the application DBA does not even know or see the contents of the named credential.

### 4.1.3 Application Developer Access

Application developers generally work on their development environments and have full access to their development databases. Application developers are not usually granted access to the production databases. However they might need access to a production database to see performance of application queries in a production environment. The access of the application developer to a production database must be READ ONLY access. Application developers should not be allowed to make any changes to the database. The application developer's access to a production database should be liberal enough to allow the developer to access performance management reports for a production database.

An Enterprise Manager administrator with the user management or grants management resource type privilege can grant application developer access on a database to an Enterprise administrator in Oracle Enterprise Manager 13c.

#### 4.1.3.1 Granting Application Developer Access on the Database

To grant application developer access on the database, follow the instructions in ["Creating a New Administrator"](#) to create an Enterprise Manager administrator then grant the privilege Database Application Developer on the database.

#### 4.1.3.2 Granting Application Developer Access to the Database Named Credentials

To access database management performance management pages the user must log in to the database using database named credentials. An application DBA should grant view credential access on a database named credential to the application developer in Enterprise Manager. The database named credential should have at least the SELECT\_CATALOG\_ROLE role on the database.

The application developer must not be given the user's password. The application developer should not be granted view access on the host, or any database host named credential.

The application developer account created in this way in Enterprise Manager will be able to view only the Performance Management and Schema Management pages in Enterprise Manager. The user will not be able to make any changes to the database.

### 4.1.4 Database Monitoring User Access

The database monitoring user has user access and views the database monitoring pages in Enterprise Manager.



#### 4.1.4.1 Granting View Database Performance Access on the Database

To grant view database performance access on the database, follow the instructions in ["Creating a New Administrator"](#) to create an Enterprise Manager administrator then grant the privilege View Database Performance on the database target.

#### 4.1.4.2 Sharing credentials with the Database Monitoring User

To share credentials with the database monitoring user:

1. Create the database account for the database monitoring user.
2. Grant the SELECT\_CATALOG\_ROLE role to the database account.
3. Create a named credential in Enterprise Manager using the database account username and password.
4. Grant the view credential access privilege on the named credential to the database monitoring user in Enterprise Manager.

The database monitoring user can now use the database account to log in to the database in Enterprise Manager.

Users that do not have at least the SELECT\_CATALOG\_ROLE role cannot log in to the database in Enterprise Manager. If the database login user does not have at least the SELECT\_CATALOG\_ROLE role, the following error message is displayed:

The application requires more database privileges than you have currently been granted. Click on Help to get more version specific information.

### 4.1.5 Database Administrator Access

The database administrator has full access on the database and can perform any operation on the database.

#### 4.1.5.1 Creating a Database Administrator Account

To create a database administrator account:

1. Follow the instructions in ["Creating a New Administrator"](#) to create an Enterprise Manager administrator
2. On the Create Administrator <Name>: Roles page add the EM\_PATCH\_ADMINISTRATOR and EM\_PROVISIONING\_OPERATOR roles.
3. On the Target Privileges page grant the Add Any Target privilege from the Privileges Applicable to all Targets section.

#### 4.1.5.2 Creating Named Credentials

To create named credentials the database administrator logs in to Enterprise Manager and creates a database named credential and a host named credential.

The database administrator provisions the database and adds the database to Enterprise Manager for management. Doing this makes the database administrator the owner of the database and listener targets in Enterprise Manager. The owner has FULL access on the targets in Enterprise Manager.

### 4.1.5.3 Granting Privileges Through Roles and Privilege Propagating Groups

A similar level of access on the database to multiple users can be granted by creating Enterprise Manager roles. Privileges can be granted to roles and the roles can be granted to the Enterprise Manager administrators. Access changes made to the roles are reflected to the Enterprise Manager administrators granted that role.

To manage a similar level of access across multiple databases to a user, privilege propagating groups should be created. Individual databases should be added to a privilege propagating group. Privileges can be granted on the privilege propagating group. Privileges granted at the group level are automatically propagated to the group members. The user automatically receives the privileges to any database that is later added to the privilege propagating group.

Enterprise Manager roles are explained in Section 2.2.1 of the Oracle Enterprise Manager Cloud Control Security Guide.

 **Note:**

For more information about Enterprise Manager roles, see "[Understanding Users, Privileges, and Roles](#)"

### 4.1.6 Privilege Groups

Flexible DB Access Control privileges are broadly categorized into 12 privilege groups for easy manageability. The following sections describe the 12 privilege groups available in Enterprise Manager:

 **Note:**

The privilege groups listed in this section apply to the following target types:

- Database Instance
  - Cluster Database
  - Pluggable Database
- 
- [Database Application DBA](#)
  - [Database Application Developer](#)
  - [Manage Database High Availability Privilege Group](#)
  - [View Database High Availability Privilege Group](#)
  - [Manage Database Performance Privilege Group](#)
  - [View Database Performance Privilege Group](#)
  - [Manage Database Schema Privilege Group](#)
  - [View Database Schema Privilege Group](#)

- [Manage Database Security Privilege Group](#)
- [View Database Security Privilege Group](#)
- [Manage Database Storage Privilege Group](#)
- [Manage Database Storage Privilege Group](#)

### 4.1.6.1 Database Application DBA

The Database Application DBA can manage the application schema, application objects, and application performance in the database. In addition, the Database Application DBA can view and update the database to fix performance and other issues on the database.

| Target Privileges                               | Menu Items                                  |
|-------------------------------------------------|---------------------------------------------|
| Manage the Database Performance Privilege group | Manage Database Performance Privilege Group |
| Manage the Database Schema Privilege group      | Manage Database Schema Privilege Group      |

### 4.1.6.2 Database Application Developer

The Database Application Developer can view the database performance in Enterprise Manager but cannot make any changes to the database.

| Target Privileges                             | Menu Items                                |
|-----------------------------------------------|-------------------------------------------|
| View the Database Performance Privilege group | View Database Performance Privilege Group |
| View the Database Schema Privilege group      | View Database Schema Privilege Group      |

### 4.1.6.3 Manage Database High Availability Privilege Group

The Manage Database High Availability Privilege group has the ability to manage database high availability pages in Enterprise Manager.

| Target Privileges                  | Menu Items                                                                                                                                                                                                                                                                                            |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View the database backup           | Availability>MAA AdvisorAdministration>Resource ManagerAvailability>Backup & Recovery>Backup ReportsAvailability>Backup & Recovery>Backup SettingsAvailability>Backup & Recovery>Recovery SettingsAvailability>Backup & Recovery>Recovery Catalog SettingsAvailability>Backup & Recovery>Transactions |
| View database advanced queues      |                                                                                                                                                                                                                                                                                                       |
| View database redo logs            |                                                                                                                                                                                                                                                                                                       |
| View recovery settings             |                                                                                                                                                                                                                                                                                                       |
| View the high availability console |                                                                                                                                                                                                                                                                                                       |
| View database resources            |                                                                                                                                                                                                                                                                                                       |

### 4.1.6.4 View Database High Availability Privilege Group

The Manage Database High Availability Privilege group has the ability to view database high availability pages in Enterprise Manager.

| Target Privileges                  | Menu Items                                                                                                                                                                                                                                                                                            |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View the database backup           | Availability>MAA AdvisorAdministration>Resource ManagerAvailability>Backup & Recovery>Backup ReportsAvailability>Backup & Recovery>Backup SettingsAvailability>Backup & Recovery>Recovery SettingsAvailability>Backup & Recovery>Recovery Catalog SettingsAvailability>Backup & Recovery>Transactions |
| View database advanced queues      |                                                                                                                                                                                                                                                                                                       |
| View database redo logs            |                                                                                                                                                                                                                                                                                                       |
| View recovery settings             |                                                                                                                                                                                                                                                                                                       |
| View the high availability console |                                                                                                                                                                                                                                                                                                       |
| View database resources            |                                                                                                                                                                                                                                                                                                       |

#### 4.1.6.5 Manage Database Performance Privilege Group

Members of this group have the ability to manage all database performance and advisory features including SQL Monitor, SQL Performance Analyzer, memory advisors, segment advisors, and so on.

| Target Privileges                             | Menu Items                                                                                                                                                             |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Use the database SQL Access Advisor           | Performance>Performance Home                                                                                                                                           |
| Manage the database SQL plan control          | Performance>SQL>SQL Performance Analyzer Home<br>Performance>SQL>Optimizer statistics                                                                                  |
| Use the database SQL Tuning Advisor           | Performance>Top Activity                                                                                                                                               |
| Manage the database SQL Tuning sets           | Performance>ASH Analytics                                                                                                                                              |
| Database SPA administration                   | Performance>SQL Monitor                                                                                                                                                |
| Manage database sessions                      | Performance>SQL>SQL Tuning Sets                                                                                                                                        |
| Database segment administration               | Performance>SQL>SQL Plan Control                                                                                                                                       |
| View database memory usage                    | Performance>SQL>Cloud Control SQL History                                                                                                                              |
| View the Database Performance Privilege Group | Performance>SQL>Search SQL                                                                                                                                             |
| Database optimizer statistics administration  | Performance>Search Sessions                                                                                                                                            |
| Connect target                                | Performance>Blocking Sessions                                                                                                                                          |
| Database ADDM administration                  | Performance>Advisors Home                                                                                                                                              |
| Database advisor tasks administration         | Performance>Real-Time ADDM                                                                                                                                             |
| Automated maintenance tasks administration    | Administration>Storage>Automatic Undo Management                                                                                                                       |
| Manage database ASH reports                   | Performance>AWR>AWR Report                                                                                                                                             |
| Manage database automatic undo management     | Performance>AWR>AWR Administration                                                                                                                                     |
| Manage database AWR settings                  | Performance>AWR>Compare Period ADDM                                                                                                                                    |
| Manage database health checkers               | Performance>AWR>Compare Period Reports                                                                                                                                 |
| Manage database memory usage                  | Performance>SQL>SQL Performance Analyzer Setup<br>Performance>SQL>SQL Tuning Advisor<br>Performance>SQL>SQL Access Advisor<br>Administration>Initialization Parameters |

#### 4.1.6.6 View Database Performance Privilege Group

Members of this group have the ability to view all database performance and advisory features including SQL Monitor, SQL Performance Analyzer, memory advisors, segment advisors, and so on.

| Target Privileges                          | Menu Items                                       |
|--------------------------------------------|--------------------------------------------------|
| Connect to a target (read-only)            | Performance>Performance Home                     |
| View database actions                      | Performance>SQL>SQL Performance Analyzer Home    |
| View database ADDM                         | Performance>SQL>Optimizer statistics             |
| View Database Advisor Home                 | Performance>Top Activity                         |
| View automated maintenance tasks           | Performance>ASH Analytics                        |
| View database ASH reports and analytics    | Performance>SQL Monitor                          |
| View database automatic undo management    | Performance>SQL>SQL Tuning Sets                  |
| View database AWR reports                  | Performance>SQL>SQL Plan Control                 |
| View database health checkers              | Performance>SQL>Cloud Control SQL History        |
| View database clients                      | Performance>SQL>Search SQL                       |
| View the database Data Recovery Advisor    | Performance>Search Sessions                      |
| View the database in-memory setting        | Performance>Blocking Sessions                    |
| Install database management packages       | Performance>Advisors Home                        |
| View database modules                      | Performance>Real-Time ADDM                       |
| View the Database Performance Home Page    | Administration>Storage>Automatic Undo Management |
| View Database Optimizer statistics         | Performance>AWR>AWR Report                       |
| View database segments                     | Performance>AWR>AWR Administration               |
| View database services                     | Performance>AWR>Compare Period ADDM              |
| View database sessions                     | Performance>AWR>Compare Period Reports           |
| View the database SQL Performance Analyzer |                                                  |
| View the Database SQL monitor              |                                                  |
| View the database SQL plan control         |                                                  |
| View the database SQL tuning sets          |                                                  |
| View database SQL scripts                  |                                                  |
| View database top activity                 |                                                  |

### 4.1.6.7 Manage Database Schema Privilege Group

Members of this group have the ability to manage database schema elements such as tables, views, indexes, packages, functions, and so on.

| Target Privileges                           | Menu Items                                                    |
|---------------------------------------------|---------------------------------------------------------------|
| Manage database directory objects           | Schema>Database Objects>Synonyms                              |
| Manage database export                      | Schema>Database Objects>Sequences                             |
| Manage database import                      | Schema>Database Objects>Database Links                        |
| Manage database indexes                     | Schema>Database Objects>Directory Objects                     |
| Manage database Java content                | Schema>Text Manager>Text Indexes                              |
| Manage database materialized views          | Schema>Workspaces                                             |
| Manage database tables                      | Schema>XML Database>Resources                                 |
| Manage database procedures and functions    | Schema>XML Database>XML Schemas                               |
| Reorganize database objects                 | Schema>XML Database>XMLType Views                             |
| Manage database sequences                   | Schema>XML Database>XML Indexes                               |
| Manage database synonyms                    | Schema>XML Database>XML Repository Events                     |
| Manage database workspaces                  | Schema>XML Database>XMLType Tables                            |
| Manage the XML database                     | Schema>Programs>Packages                                      |
| Manage database types                       | Schema>Programs>Package Bodies                                |
| Manage database triggers                    | Schema>Programs>Java Sources                                  |
| Manage database text indexes                | Schema>Programs>Java Classes                                  |
| View database table data                    | Schema>Materialized Views>Materialized Views                  |
| Manage database dimensions                  | Schema>Materialized Views>Materialized View Logs              |
| Manage database links                       | Schema>Materialized Views>Refresh Groups>Dimensions           |
| Manage database packages and package bodies | Schema>User Defined Types>Array Types                         |
|                                             | Schema>User Defined Types>Object Types                        |
|                                             | Schema>User Defined Types>Table Types                         |
|                                             | Schema>Database Objects>Reorganize Objects                    |
|                                             | Schema>Database Export/Import>Export to Export Files...       |
|                                             | Schema>Database Export/Import>Import from Export Files...     |
|                                             | Schema>Database Export/Import>Import from Database...         |
|                                             | Schema>Database Export/Import>Load Data from User Files...    |
|                                             | Schema>Text Manager>Query Statistics                          |
|                                             | Schema>XML Database>Configuration                             |
|                                             | Schema>Change Management>Data Comparisons Schema Change Plans |
|                                             | Schema>Change Management>Schema Baselines                     |
|                                             | Schema>Change Management>Schema Comparisons                   |
|                                             | Schema>Change Management>Schema Change Plans                  |
|                                             | Schema>Change Management>Schema Synchronizations              |

#### 4.1.6.8 View Database Schema Privilege Group

Members of this group have the ability to view database schema elements such as tables, views, indexes, packages, functions, and so on.

| Target Privileges                         | Menu Items                                       |
|-------------------------------------------|--------------------------------------------------|
| View the XML database                     | Schema>Database Objects>Tables                   |
| View database workspaces                  | Schema>Database Objects>Views                    |
| View database types                       | Schema>Database Objects>Indexes                  |
| View database triggers                    | Schema>Database Objects>Synonyms                 |
| View database text indexes                | Schema>Database Objects>Sequences                |
| View database tables                      | Schema>Database Objects>Database Links           |
| View database synonyms                    | Schema>Database Objects>Directory Objects        |
| View database sequences                   | Schema>Text Manager>Text Indexes                 |
| View database procedures and functions    | Schema>Workspaces                                |
| View database packages and package bodies | Schema>XML Database>Resources                    |
| View database materialized views          | Schema>XML Database>XML Schemas                  |
| View database Java content                | Schema>XML Database>XMLType Views                |
| View database indexes                     | Schema>XML Database>XML Indexes                  |
| View database directory objects           | Schema>XML Database>XML Repository Events        |
| View database dimensions                  | Schema>XML Database>XMLType Tables               |
| View database links                       | Schema>Programs>Packages                         |
|                                           | Schema>Programs>Package Bodies                   |
|                                           | Schema>Programs>Java Sources                     |
|                                           | Schema>Programs>Java Classes                     |
|                                           | Schema>Materialized Views>Materialized Views     |
|                                           | Schema>Materialized Views>Materialized View Logs |
|                                           | Schema>Materialized Views>Refresh                |
|                                           | Groups>Dimensions                                |
|                                           | Schema>User Defined Types>Array Types            |
|                                           | Schema>User Defined Types>Object Types           |
|                                           | Schema>User Defined Types>Table Types            |

#### 4.1.6.9 Manage Database Security Privilege Group

Members of this group have the ability to manage all database security features including users, roles, profiles, transparent data encryption, database vault, and so on.

---

| Target Privileges                                    | Menu Items                                    |
|------------------------------------------------------|-----------------------------------------------|
| Manage database roles                                | Security>Home                                 |
| Manage database audit settings                       | Security>Reports                              |
| Manage database audit trails                         | Security>Database Vault                       |
| Manage the database vault                            | Administration>Oracle Scheduler>Jobs          |
| Manage database virtual private database policies    | Administration>Oracle Scheduler>Job Classes   |
| Manage database users                                | Administration>Oracle Scheduler>Chains        |
| Manage database transparent data encryption settings | Administration>Oracle Scheduler>Schedules     |
| View the Database Security Privilege group           | Administration>Oracle Scheduler>Programs      |
| Manage the database scheduler                        | Administration>Oracle Scheduler>Windows       |
| Database redaction administration                    | Administration>Oracle Scheduler>Window Groups |
| Manage database profiles                             | Security>Roles                                |
| Manage privilege analysis                            | Security>Users                                |
| Manage database Oracle label security                | Security>Profiles                             |
|                                                      | Security>Audit Settings                       |
|                                                      | Security>Transparent Data Encryption          |
|                                                      | Security>Data Redaction                       |
|                                                      | Security>Label Security                       |
|                                                      | Security>Application Contexts                 |
|                                                      | Security>Enterprise User Security             |
|                                                      | Security>Virtual Private Database             |
|                                                      | Security>Application Contexts                 |
|                                                      | Security>Enterprise User Security             |
|                                                      | Security>Privilege Analysis                   |

---

#### 4.1.6.10 View Database Security Privilege Group

Members of this group have the ability to view all database security features including users, roles, profiles, data encryption, data vault, audit vault, and so on.



| Target Privileges                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Menu Items                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| View database audit settings<br>View the database audit trail<br>Monitor the database vault<br>View database feature usage<br>View database Oracle label security<br>View privilege analysis<br>View database profiles<br>View database redaction<br>View database roles<br>View the database scheduler<br>View the Database Security Home<br>View database security reports<br>View database transparent data encryption settings<br>View database users<br>View database virtual private database policies | Security>Home<br>Security>Reports<br>Security>Database Vault<br>Administration>Oracle Scheduler>Jobs<br>Administration>Oracle Scheduler>Job Classes<br>Administration>Oracle Scheduler>Chains<br>Administration>Oracle Scheduler>Schedules<br>Administration>Oracle Scheduler>Programs<br>Administration>Oracle Scheduler>Windows<br>Administration>Oracle Scheduler>Window Groups<br>Security>Roles<br>Security>Users<br>Security>Profiles<br>Security>Audit Settings<br>Security>Transparent Data Encryption<br>Security>Data Redaction<br>Security>Label Security<br>Security>Application Contexts<br>Security>Enterprise User Security<br>Security>Virtual Private Database<br>Security>Application Contexts<br>Security>Enterprise User Security<br>Security>Privilege Analysis |

#### 4.1.6.11 Manage Database Storage Privilege Group

The members of this group have the ability to manage database storage.

| Target Privileges                                                                                                                                               | Menu Items                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manage database control files<br>Manage database data files<br>Manage database redo logs<br>Manage database tablespaces<br>Manage database transport tablespace | Administration>Storage>Archive Logs<br>Administration>Storage>Datafiles<br>Administration>Storage>Control Files<br>Administration>Storage>Redo Log Groups<br>Administration>Storage>Tablespaces<br>Administration>Storage>Temporary Tablespace Groups<br>Administration>Storage>Database File Systems<br>Administration>Storage>Information Lifecycle Management |

## 4.2 Secured Communication (TCPS) Access to Databases

Out of the box support is provided for discovering, monitoring, and administration of TCPS enabled listeners. All databases created through the Admin provisioning flow or Cloud Self Service portal support SSL enabled connection strings by default. Target databases can be monitored securely by configuring the TCPS connection protocol.

By configuring secured access, data transport encryption is enabled between OMS and the database server target and between the Agent and the database server target.

As businesses look towards cloud solutions, secure user authentication is a key requirement of the product offering. Oracle's default authentication protocols O3LOGON and O5LOGON (introduced in Enterprise Manager 11g) have been revamped to enable user authentication using the TCPS protocol for Oracle Database Server instead of the not-so-secure TCP protocol.

 **Note:**

Using secure authentication has no impact on normal database performance.

## 4.2.1 Configuring TCPS

To configure TCPS:

1. Enable the Oracle Advanced Security TLS setting on the target database.  
For TLSv1.2 configuration,
  - 1) Ensure `SSL_VERSION` is set to **1.2** for configuring TLSv1.2 in the `sqlnet.ora` or the `listener.ora` file,
  - 2) Ensure the `SSL_CLIENT_AUTHENTICATION` parameter in the `sqlnet.ora` file is set to **TRUE**.
2. Configure secure wallets with third party CA certificates.
3. Configure third party CA certificate wallets for OMS and Agent communication.
4. Set the connection protocol to TCPS in the monitoring configuration properties of target database.

## 4.2.2 Configuring Third Party CA Certificates for Communication With Target Databases

You must set the following set of properties at the OMS server and Agent for secure target monitoring. Bounce the OMS and the agent to bring the changes into effect.

 **Note:**

For more information about `emctl`, see "Using `emctl` partool Utility" in the Oracle Enterprise Manager Lifecycle Management Administrator's Guide. .

### Properties to be Set at the OMS Server:

- `#Client authority`
  - `emctl set property -sysman_pwd sysman -name em.targetauth.db.pki.KeyStore -value <...wallet..>`

- emctl set property -sysman\_pwd sysman -name em.targetauth.db.pki.KeyStorePassword -value <...>
- emctl set property -sysman\_pwd sysman -name em.targetauth.db.pki.KeyStoreType -value <..>
- #Server authority
  - emctl set property -sysman\_pwd sysman -name em.targetauth.db.pki.TrustStorePassword -value <...>
  - emctl set property -sysman\_pwd sysman -name em.targetauth.db.pki.TrustStoreType -value <..>
  - emctl set property -sysman\_pwd sysman -name em.targetauth.db.pki.TrustStore -value <...wallet..>

**Properties to be set at the Agent residing on the target database host:**

- #Client authority
  - emctl setproperty agent -name connectionKeyStoreLocation -value <...wallet..>
  - emctl setproperty agent -name connectionKeyStoreType -value <..>
  - emctl setproperty agent -name connectionTrustStoreType -value <..>
- #Server authority
  - emctl setproperty agent -name connectionTrustStoreLocation -value <...wallet..>
  - emctl setproperty agent -name connectionTrustStorePassword -value <..>
  - emctl setproperty agent -name connectionTrustStoreType -value <..>

## 4.3 Account Management

The following new EM CLI verbs have either been added or modified for target database account management:

 **Note:**

For more information about these verbs, including examples, see the "Verb Reference" chapter in the *Oracle Enterprise Manager Command Line Interface*.

- get\_db\_profile
 

Displays the database profile details such as profile, resource name, resource type, and limits for a specific search criteria. The following example displays details about the profile with the name DEFAULT:

```
emcli get_db_profile
 -target_name=myDB
 -profile= DEFAULT
 -connect_as="DBNamedCreds:SYS_myDB"
```
- get\_db\_account

Displays database account details such as username, profile, account status, and authentication type for a specific search criteria. The following example displays the details of the user Admin1:

```
emcli get_db_account
 -target_name=myDB
 -user_name=Admin1
 -connect_as="DBNamedCreds:SYS_myDB"
```

- **update\_db\_account\_status**

Updates the database account status to LOCKED, OPEN, EXPIRED, or LOCKED & EXPIRED. The following example locks the account:

```
emcli update_db_account_status
 -target_name=myDB
 -user_name=Admin1
 -action=LOCK
 -connect_as="DBNamedCreds:SYS_myDB"
```

- **update\_db\_password**

Updates the target database password change in the Enterprise Manager Credential sub-system and can change the password on the target database as well. This verb also propagates the collection or monitoring credentials to Enterprise Manager Management Agents.

The EM CLI verb `update_db_password` can now change passwords for all users, including SYS/SYSDBA users. The verb can change passwords for the database target and all Enterprise Manager credentials. It syncs the password file across RAC and Dataguard instances. It accepts database named credentials to logon to database targets if it is used for changing other users' passwords. The following example updates the database password:

```
emcli update_db_password
 -target_name=myDB
 -user_name=Admin1
```

# 5

## Troubleshooting

This chapter contains information about troubleshooting security issue in Oracle Enterprise Manager.

### 5.1 Troubleshooting Authentication Issues in Enterprise Manager

Authentication can fail for a number of reasons. This section discusses ways to troubleshoot authentication failures. When Enterprise Manager is configured with external authentication, the LDAP/SSO WebLogic authentication providers authenticate the user. If authentication succeeds, the Enterprise Manager authentication layer checks if that user exists in Enterprise Manager repository. If authentication fails, the Enterprise Manager administrator should check `ldap_trace.logATN` located in the `../gc_inst/user_projects/domains/GCDomain'` directory. This file contains authentication entries from the LDAP authenticator. If that file does not exist, you need to enable the WebLogic debug flag (`DebugSecurityAtn`).

#### 5.1.1 Enabling the WebLogic Debug Flag

From the WebLogic Server Console, enable logging, set the WebLogic debug log level and then enable the debug flag.

1. Navigate to **Environment->Servers->EMGC\_OMS1** and choose the **Logging** tab.
2. Under **Rotation**, set the **file rotation size** to 64000.
3. Expand **Advanced**.
4. Under **Message destinations(s) (Log file: region)** set the **Severity level** to **Trace**.
5. Navigate to the **Environment->Servers->EMGC\_OMS1** and choose the **Debug** tab.
6. Check **WebLogic->security->atn->DebugSecurityAtn**.
7. Click **Save**.

#### 5.1.2 Debugging errors in `ldap_trace.logATN` file

1. In the **Advanced** section, set **Minimum severity to log** to **Debug**.
2. In **Message destinations**, set the **Log file Severity** level to **Debug**
3. Click **Save/Activate changes**.
4. Navigate to the **Debug** tab and enable debug for `weblogic->security->atn->DebugSecurityAtn`
5. Click **Save/Activate changes**.

## 5.1.3 Invalid Credentials

Now, let's say user johndoe tries to log in with bad credentials. You should see something like the following in the `ldap_trace.logATN`. The non-zero `resultCode` of 49 indicates a bad password.

```
12:39:36.529 ldc=3 Connected to ldaps://<ldaphost>:3060
12:39:36.529 ldc=3 op=215 BindRequest {version=3, name=cn=orcladmin,
authentication=*****}
12:39:36.566 ldc=3 op=215 BindResponse {resultCode=0}
12:39:36.568 ldc=3 op=216 BindRequest {version=3,
name=cn=johndoe,cn=Users,dc=us,dc=company,dc=com, authentication=*****}
12:39:36.608 ldc=3 op=216 BindResponse {resultCode=49}
```

If user johndoe authenticates successfully by the LDAP provider but does not exist in the Enterprise Manager repository, then there should be no errors in the `ldap_trace.logATN` (you will see `resultCode` of 0) but in the Enterprise Manager log file `emoms.log` (under `../gc_inst/em/sysman/log`) you should see something like the following:

```
2013-05-28 12:47:43,295 [[ACTIVE] ExecuteThread: '3' for queue:
'weblogic.kernel.Default (self-tuning)'] WARN auth.EMRepLoginFilter doFilter.457 -
InvalidEMUserException caught in EMRepLoginFilter: Failed to login using external
authentication for user: johndoe
oracle.sysman.emSDK.sec.auth.InvalidEMUserException: Failed to login using external
authentication for user: johndoe
 at
oracle.sysman.emSDK.sec.auth.EMLoginService._performLogin(EMLoginService.java:1269)
 at
oracle.sysman.emSDK.sec.auth.EMLoginService._doSSOLogin(EMLoginService.java:754)
 at
oracle.sysman.emSDK.sec.auth.EMLoginService.doSSOLogin(EMLoginService.java:727)
 at oracle.sysman.emSDK.sec.auth.EMLoginService.doLogin(EMLoginService.java:
228)
 at oracle.sysman.emSDK.sec.auth.EMLoginService.doLogin(EMLoginService.java:
256)
```

To obtain more detailed debug data in `emoms.trc`, you can enable the Enterprise Manager authentication logger via the following command:

```
emctl set property -name "log4j.category.oracle.sysman.core.security.auth" -value
"DEBUG, emtrcAppender
```

`emctl list properties` will display something similar to the following output.

```
log4j.category.oracle.sysman.core.security.auth=DEBUG, emtrcAppender
```

### Note:

Do not leave this debug logger enabled for performance reasons. Once the authentication issue has been diagnosed, turn this logger off using `'emctl delete property -name ".category.oracle.sysman.core.security.auth"`

## 5.1.4 Timeout in LDAP Server'

There could be other non-zero resultCodes in `ldap_trace.logATN` that would indicate some other type of failure in the LDAP authentication layer. If the provider times out while trying to fetch results from the LDAP server, you should see something similar to the following in the file.

```
09:36:44.168 ldc=2 op=214 AbandonRequest {msgid=213}
```

To fix this issue, you can increase the *Results time limit* configuration parameter in the LDAP provider.

## 5.1.5 Errors Outside `ldap_trace.logATN`'

Sometimes, `ldap_trace.logATN` may not give the complete picture. In that case, check the diagnostic log `EMGC_OMS1-diagnostic.log` for errors/warnings from the configured external authentication provider.

Occasionally, There might be intermittent network issues between the LDAP server and the OMS host or the search base given as input might be too broad. You can use the 'ldapsearch' command that comes with the OS on your OMS host to validate connection/result retrieval timing issues. This command may not be available on all operating systems. You may use other LDAP tools. For example,

```
ldapsearch -h hostname -p 3060 -D cn=orcladmin -x -w xxxxxxxx -b
"cn=users,dc=us,dc=oracle,dc=com" -s one -l 5 -z 15
```

Where:

- `lh` - hostname of the ldap server
- `p` - port of the ldap server
- `D` - bind dn
- `x` - use simple authentication rather than SASL
- `w` - password for the bind dn used above
- `l` - gives a time limit in seconds for a search to complete
- `b` - search base
- `s` - specify scope search
- `z` - specifies the limit of search result entries to be returned

You can give the user as well as the group base dn (that you specify in the `emctl` command) for the `-b` option and check if the appropriate results are returned and within the expected timeframe.

If you start seeing delays or timeouts, you should run this command from the same machine where Enterprise Manager is installed to ensure it is not LDAP server/network related.

# 6

## References

The following Oracle documentation provides in-depth information on the topics discussed in the book.

- Oracle Database Advanced Security Administrator's Guide
- Oracle Database Security Guide
- Oracle Database Security Checklist
- Oracle Database 2 Day + Security Guide
- Oracle Enterprise Manager Cloud Control Administrator's Guide
- Oracle Fusion Middleware Administrator's Guide
- Oracle Fusion Middleware Securing Oracle WebLogic Server
- Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server



# A.1 Out-of-Box Roles

The following table lists predefined roles that are available out-of-box with Enterprise Manager.

**Table 1 Out-of-Box Roles**

| <b>Roles</b>               | <b>Description</b>                                                                                                                                                                                                                                            |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EM_ALL_ADMINISTRATOR       | Role has privileges to perform Enterprise Manager administrative operations. It provides Full privileges on all secure resources (including targets)                                                                                                          |
| EM_ALL_DESIGNER            | Role has privileges to design Enterprise Manager operational entities such as Monitoring Templates.                                                                                                                                                           |
| EM_ALL_OPERATOR            | Role has privileges to manage Enterprise Manager operations.                                                                                                                                                                                                  |
| EM_ALL_VIEWER              | Role has privileges to view Enterprise Manager operations.                                                                                                                                                                                                    |
| EM_CBA_ADMIN               | Role has privileges to manage Chargeback Objects. It provides the ability to create and view chargeback plans, chargeback consumers, assign chargeback usage, and view any CaT targets.                                                                       |
| EM_CLOUD_ADMINISTRATOR     | Enterprise Manager user for setting up and managing the infrastructure cloud. This role could be responsible for deploying the cloud infrastructure (servers, pools, zones) and infrastructure cloud operations for performance and configuration management. |
| EM_COMPLIANCE_DESIGNER     | Role has privileges for create, modify and delete compliance entities.                                                                                                                                                                                        |
| EM_COMPLIANCE_OFFICER      | Role has privileges to view compliance framework definition and results.                                                                                                                                                                                      |
| EM_CPA_ADMIN               | Role to manage Consolidation Objects. It gives the capability to create and view consolidation plans, consolidation projects and view any CaT targets.                                                                                                        |
| EM_HOST_DISCOVERY_OPERATOR | Role has privileges to execute host discovery                                                                                                                                                                                                                 |
| EM_INFRASTRUCTURE_ADMIN    | Role has privileges to manage the Enterprise Manager infrastructure such as managing plug-in lifecycle or managing self update.                                                                                                                               |
| EM_PATCH_ADMINISTRATOR     | Role for creating, editing, deploying, deleting and granting privileges for any patch plan.                                                                                                                                                                   |
| EM_PATCH_DESIGNER          | Role for creating and viewing for any patch plan                                                                                                                                                                                                              |
| EM_PATCH_OPERATOR          | Role for deploying patch plans                                                                                                                                                                                                                                |
| EM_PLUGIN_AGENT_ADMIN      | Role to support plug-in lifecycle on Management Agent                                                                                                                                                                                                         |
| EM_PLUGIN_OMS_ADMIN        | Role to support plug-in lifecycle on Management Server                                                                                                                                                                                                        |
| EM_PLUGIN_USER             | Role to support view plug-in console                                                                                                                                                                                                                          |
| EM_PROVISIONING_DESIGNER   | Role has privileges for provisioning designer                                                                                                                                                                                                                 |
| EM_PROVISIONING_OPERATOR   | Role has privileges for provisioning operator                                                                                                                                                                                                                 |

---

**Table 1 (Cont.) Out-of-Box Roles**

| <b>Roles</b>                 | <b>Description</b>                                                                                                                                                             |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EM_SSA_ADMINISTRATOR         | Enterprise Manager user with privilege to set up the Self Service Portal. This role can define quotas and constraints for self service users and grant them access privileges. |
| EM_SSA_USER                  | This role grants Enterprise Manager user the privilege to access the Self Service Portal.                                                                                      |
| EM_TARGET_DISCOVERY_OPERATOR | Role has privileges to execute target discovery.                                                                                                                               |
| EM_TC_DESIGNER               | Role has privileges for creating Template Collections                                                                                                                          |
| EM_USER                      | Role has privilege to access Enterprise Manager Application.                                                                                                                   |
| PUBLIC                       | PUBLIC role is granted to all administrators. This role can be customized at site level to group privileges that need to be granted to all administrators.                     |

---

## A.2 User Access to Database Targets without SYSDBA Privileges

A user may need to perform operation on a database target such as:

- Monitor Performance Page
- Review and administer AWR
- Use SQL Access Advisor
- Use SQL Tuning

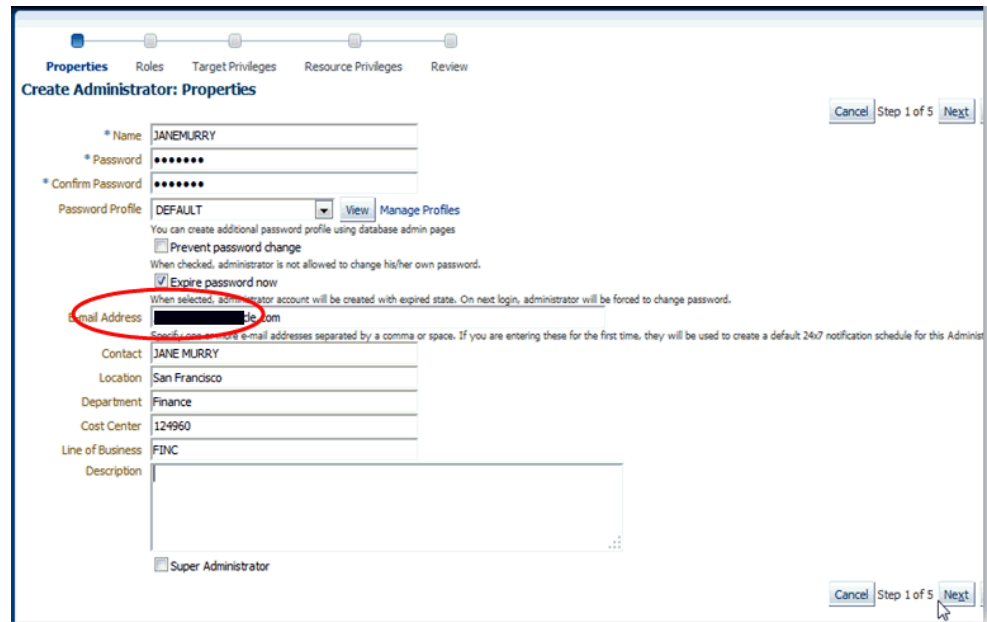
In circumstances where a user is required to access database monitoring/management functions in Enterprise Manager but has not been given full SYSDBA access to database targets, you can create an Enterprise Manager administrator and give him the EM\_USER and PUBLIC roles as well as, "Connect to any viewable target" privileges to the database targets that you want the administrator to access.

In the following steps we will grant "Connect to any viewable target" to all targets (instead of listing specific target instances). Depending on the type of authentication model being used, the administrator details will be stored in either the Cloud Control Repository or an external store, such as LDAP.

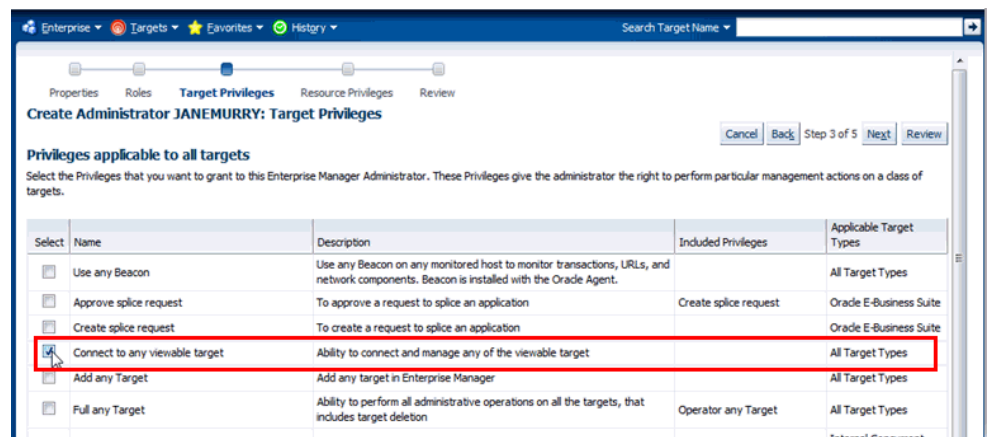
### A.2.1 Creating an Administrator

1. From the Setup menu, select Security and then Administrators.
2. Click Create.
3. From the Create Administrator: Properties page, enter all necessary information, including the password profile as enforced by your security team. In the graphic shown below, "Expire password now", has been selected so that when this user logs in with the temporary password, they will be forced to reset their password.

Once you have entered the requisite information, click **Next**.



4. From the Create Administrator: Roles Page, choose the default roles and click **Next**.
5. From the Create Administrator: Target Privilege page, Select the **Connect to any viewable** target privilege. This enables the administrator to connect to all targets viewable in his console.



- Click **Next**.
6. From the Resource page, click **Next**. This accepts the default settings.
  7. Review your settings on the Review page. Click **Finish**.
- Valid users must reside on the target instances.

## A.2.2 Users Requiring Access to the Database Performance Page

1. On the DB Target host, log in as sysdba and create a <dbmonitor\_admin> user and grant appropriate privileges:
 

```
SQL> create user <dbmonitor_admin> identified by <password>;
SQL> grant select any dictionary to <dbmonitor_admin>;
SQL> grant create session to <dbmonitor_admin>;
```
2. Log in to the Cloud Control console as <gc\_user> user, which is JANEMURRY in the example:
 

```
TARGETS > DATABASE > ORADB > PERFORMANCE
```

 Enter login and password for <dbmonitor\_admin> user.
 

The Performance page should now appear. The following user will now be able to access all pages under the section of Additional Monitoring Links.

## A.2.3 User Requiring Accessing AWR/ADDM

1. On a DB Target host log in as sysdba and create an <awr\_admin> user and grant appropriate privileges:
 

```
SQL> create user <awr_admin> identified by <password>;
SQL> grant select any dictionary to <awr_admin>;
SQL> grant create session to <awr_admin>;
SQL> grant execute on dbms_workload_repository to <awr_admin>;
```
2. Log in to the Cloud Control console as <gc\_user> user, which is JANEMURRY in our example:
 

```
TARGETS > DATABASE > ORADB > Related Links: Advisor Central
```

 Enter login and password for the <awr\_admin> user.
3. Then to generate the AWR/ADDM report:
 

```
ADDM > OK
```

## A.2.4 User Requiring Access to SQL Access Advisor

1. On the DB Target host log in as sysdba and create a <sqlaccess\_admin> user and grant the appropriate privileges:
 

```
SQL> create user <sqlaccess_admin> identified by <password>;
SQL> grant select any dictionary to <sqlaccess_admin>;
SQL> grant create session to <sqlaccess_admin>;
SQL> grant oem_advisor to <sqlaccess_admin>;
```
2. Log in to the Cloud Control console as <gc\_user> user, which is JANEMURRY in our example:
 

```
TARGETS > DATABASE > ORADB > Related Links: Advisor Central >SQL
Access Advisor
```

 Enter login and password for <sqlaccess\_admin> user.
3. To perform SQL Access tasks, complete steps in the wizard

## A.2.5 User Requiring Access to SQL Tuning Advisor

1. On the DB Target host, log in as sysdba and create a <sqltune\_admin> user and grant appropriate privileges:

```
SQL> create user <sqltune_admin> identified by <password>; SQL> grant select any dictionary to <sqltune_admin>; SQL> grant create session to <sqltune_admin>; SQL> grant oem_advisor to <sqltune_admin>;
```

2. Log in to the Cloud Control console as <gc\_user> user, which is JANEMURRY in our example:

TARGETS > DATABASE > ORADB > Related Links: Advisor Central > SQL Tuning Advisor  
Enter login and password for <sqltune\_admin> user.

3. You may now perform SQL Tuning tasks. For example, click on TOP ACTIVITY > Run ASH reports.

# B.1 Privileges

The following tables list available target privileges.

**Table 2 Target Privileges Applicable to All Targets**

| Display Name                   | Description                                                                                                                            | Included Privileges        | Applicable Target types | Internal Name                  |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-------------------------|--------------------------------|
| Full any Target                | Ability to do all operations on all the targets, including delete the target                                                           | Operator any Target        |                         | FULL_ANY_TARGET                |
| Execute Command as any Agent   | Execute any OS Command as the Agent User at any Agent                                                                                  |                            | Agent                   | PERFORM_OPERATION_AS_ANY_AGENT |
| Put File as any Agent          | Put any File to any Agent's Filesystem as the Agent User                                                                               |                            | Agent                   | PUT_FILE_AS_ANY_AGENT          |
| Execute Command Anywhere       | Execute any OS Command at any Agent                                                                                                    |                            | Host                    | PERFORM_OPERATION_ANYWHERE     |
| Operator any Target            | Ability to perform administrative operations on all managed targets                                                                    | View any Target            |                         | OPERATOR_ANY_TARGET            |
| Connect to any viewable target | Ability to connect and manage any of the viewable target                                                                               |                            |                         | CONNECT_ANY_VIEW_TARGET        |
| Use any beacon                 | Use any Beacon on any monitored host to monitor transactions, URLs, and network components. Beacon is installed with the Oracle Agent. |                            |                         | USE_ANY_BEACON                 |
| Monitor Enterprise Manager     | Monitor Enterprise Manager performance                                                                                                 |                            |                         | EM_MONITOR                     |
| View any Target                | Ability to view any target                                                                                                             | Monitor Enterprise Manager |                         | VIEW_ANY_TARGET                |

**Table 2 (Cont.) Target Privileges Applicable to All Targets**

| Display Name                       | Description                                                                                                                                                  | Included Privileges | Applicable Target types | Internal Name            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|-------------------------|--------------------------|
| Create Privilege Propagating Group | Ability to create privilege propagating groups.Privileges granted on a privilege propagating group will be automatically granted on the members of the group | Add any Target      |                         | CREATE_PROPAGATING_GROUP |
| Add any Target                     | Add any target in Enterprise Manager                                                                                                                         |                     |                         | CREATE_TARGET            |

**Table 3 Target Privileges Applicable to Specific Targets**

| Display Name             | Description                                                                                                               | Internal Name            | Included Privileges                                                                                                                                                                   | Applicable Target types |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Group Administration     | Ability to administer groups                                                                                              | GROUP_ADMINISTRATION     | Full Target on group members                                                                                                                                                          | Group                   |
| Full Target              | Ability to do all operations on the target, including delete the target                                                   | FULL_TARGET              | Connect Target, Operator Target                                                                                                                                                       |                         |
| Connect Target           | Ability to connect to the target.                                                                                         | CONNECT_TARGET           | Connect Target Read-only                                                                                                                                                              |                         |
| Connect Target Readonly  | Ability to connect to the target in readonly mode                                                                         | CONNECT_READONLY_TARGET  |                                                                                                                                                                                       |                         |
| Operator Target          | Ability to do normal administrative operations on the target, such as configure a blackout and edit the target properties | OPERATOR_TARGET          | Manage Template Collection Operations, Manage Target Patch, Manage Target Metrics, Manage Target Compliance, Manage Target Events, Configure Target, Blackout Target, Execute Command |                         |
| Manage Target Compliance | Ability to manage compliance of the target                                                                                | MANAGE_TARGET_COMPLIANCE |                                                                                                                                                                                       |                         |



**Table 3 (Cont.) Target Privileges Applicable to Specific Targets**

| Display Name             | Description                                                                                                                                                                                                               | Internal Name              | Included Privileges | Applicable Target types |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|---------------------|-------------------------|
| Execute Command as Agent | Execute any OS Command as the Agent User                                                                                                                                                                                  | PERFORM_OPERATION_AS_AGENT | Agent               |                         |
| Put File as Agent        | Put any File to the Agent's Filesystem as the Agent User                                                                                                                                                                  | PUT_FILE_AS_AGENT          | Agent               |                         |
| Execute Command          | Execute any OS Command                                                                                                                                                                                                    | PERFORM_OPERATION          | Host                |                         |
| Manage Target Events     | Ability to clear events, re-evaluate metric alert events, create incidents, add events to incidents, and define what actions the administrator can perform on individual incidents, such as acknowledgment or escalation. | MANAGE_TARGET_ALERTS       |                     |                         |
| Configure target         | Ability to edit target properties and modify monitoring configuration                                                                                                                                                     | CONFIGURE_TARGET           |                     |                         |
| Manage Target Patch      | Privilege to Analyze, Apply and Rollback patches on the target                                                                                                                                                            | MANAGE_TARGET_PATCH        | Blackout Target     |                         |
| Manage Target Metrics    | Ability to edit threshold for metric and policy setting, apply monitoring templates, and manage User Defined Metrics                                                                                                      | MANAGE_TARGET_METRICS      |                     |                         |

**Table 3 (Cont.) Target Privileges Applicable to Specific Targets**

| Display Name                                            | Description                                                                                                                     | Internal Name              | Included Privileges | Applicable Target types |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------|---------------------|-------------------------|
| Manage Template Collection Operations                   | Ability to associate a template collection to a administration group and Sync targets with the associated template collections. | MANAGE_TC_OPERATION        |                     |                         |
| Blackout Target                                         | Ability to create, edit, schedule and stop a blackout on the target                                                             | BLACKOUT_TARGET            |                     |                         |
| View Target                                             | Ability to view properties, inventory and monitor information about a target                                                    | VIEW_TARGET                |                     |                         |
| View FA Target                                          | Ability to view all Fusion Application Service targets                                                                          | FA_VIEW_FASVC_TARGET       |                     |                         |
| Manage Events for Any Fusion Application Service Target | Ability to manage events for all Fusion Applications service targets                                                            | MANAGE_EVENT_ANY_FASVC_TGT |                     |                         |
| View Logs for All Fusion Applications Service Targets   | Ability to view logs for all Fusion Applications service targets                                                                | VIEW_ANY_FASVC_TARGET_LOG  |                     |                         |

**Resource Privileges:** These privileges allow a user to perform operations against specific types of resources. The following table lists all available resource privileges.

**Table 4 Resource Privileges**

| Resource Type                      | Privilege Name                | Description                                                                                | Internal Name           |
|------------------------------------|-------------------------------|--------------------------------------------------------------------------------------------|-------------------------|
| Access                             | Access Enterprise Manager     | Ability to access Enterprise Manager interfaces                                            | ACCESS_EM               |
| Application Performance Management | Real User Session Diagnostics | Gives ability to access real user session diagnostic capabilities in Business Applications | ACCESS_APM_SESSION_DIAG |

**Table 4 (Cont.) Resource Privileges**

| Resource Type                      | Privilege Name                                 | Description                                                                                                             | Internal Name          |
|------------------------------------|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|------------------------|
| Application Performance Management | Associate APM Entities to Business Application | Gives ability to associate Application Performance Management managed entities to a Business Application service target | ASSOCIATE_APM_ENTITIES |
| Application Performance Management | View Payload Content                           | Gives ability to view page/object or transaction/message payload content in Business Applications                       | VIEW_APM_PAYLOAD       |
| Application Performance Management | Business Applications Menu Item                | Shows Business Applications menu item in the Targets menu                                                               | VIEW_BA_MENU_ITEM      |
| Application Replay Entities        | Application Replay Viewer                      | View any Application Replay entity.                                                                                     | ASREPLAY_VIEWER        |
| Application Replay Entities        | Application Replay Operator                    | View, create, and edit any Application Replay entity.                                                                   | ASREPLAY_OPERATOR      |
| Backup Configurations              | Create Backup Configuration                    | Ability to create a backup configuration.                                                                               | CREATE_BACKUP_CONFIG   |
| Backup Configurations              | Edit Backup Configuration                      | Ability to edit a backup configuration.                                                                                 | EDIT_BACKUP_CONFIG     |
| Backup Configurations              | Full Access                                    | Full access to a backup configuration.                                                                                  | FULL_BACKUP_CONFIG     |
| Backup Configurations              | Use Backup Configuration                       | Ability to use a backup configuration.                                                                                  | USE_BACKUP_CONFIG      |
| Backup Status Report               | Create Backup Status Report                    | Ability to create a backup status report.                                                                               | CREATE_BACKUP_REPORT   |
| Backup Status Report               | Full Access                                    | Full access to a backup report.                                                                                         | FULL_BACKUP_REPORT     |
| Backup Status Report               | View Backup Status Report                      | Ability to view a backup report.                                                                                        | VIEW_BACKUP_REPORT     |
| Change Activity Plan               | Basic Change Activity Plan Access              | Basic Access privilege provides the ability to view and manage Change Activity Plans.                                   | BASIC_CAP_ACCESS       |
| Change Activity Plan               | Create Change Activity Plan                    | Create privilege provides the ability to create, edit, delete and activate Change Activity Plans                        | CREATE_CAP_PLAN        |
| Change Plan                        | View change plan                               | View a Change Manager Change Plan                                                                                       | VIEW_CHANGE_PLAN       |
| Change Plan                        | Edit change plan                               | Edit a Change Manager Change Plan                                                                                       | EDIT_CHANGE_PLAN       |

**Table 4 (Cont.) Resource Privileges**

| Resource Type         | Privilege Name                                 | Description                                                                                | Internal Name              |
|-----------------------|------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------|
| Change Plan           | Manage change plans                            | Create and delete Change Manager Change Plans                                              | MANAGE_ANY_CHANGE_PLAN     |
| Cloud Policy          | Create any Policy                              | Ability to Create any Policy                                                               | CREATE_ANY_POLICY          |
| Cloud Policy          | View any Policy                                | Ability to View any Policy                                                                 | VIEW_ANY_POLICY            |
| Cloud Policy          | View Policy                                    | Ability to View a Policy                                                                   | VIEW_POLICY                |
| Cloud Policy          | Modify Policy                                  | Ability to Modify a Policy                                                                 | MODIFY_POLICY              |
| Cloud Policy          | Full Policy                                    | Privilege required to View, Modify, Delete a Policy                                        | FULL_POLICY                |
| Cloud Policy Group    | Create Policy Group                            | Ability to Create Policy Group                                                             | CREATE_POLICY_GROUP        |
| Cloud Policy Group    | View any Policy Group                          | Ability to View any Policy Group                                                           | VIEW_ANY_POLICY_GROUP      |
| Cloud Policy Group    | View Policy Group                              | Ability to View a Policy Group                                                             | VIEW_POLICY_GROUP          |
| Cloud Policy Group    | Modify Policy Group                            | Ability to Modify a Policy Group                                                           | MODIFY_POLICY_GROUP        |
| Cloud Policy Group    | Full Policy Group                              | Privilege required to View, Modify, Delete a Policy Group                                  | FULL_POLICY_GROUP          |
| Compliance Framework  | Create Compliance Entity                       | Ability to create compliance framework, standard, rules                                    | CREATE_COMPLIANCE_ENTITY   |
| Compliance Framework  | Full any Compliance Entity                     | Ability to edit/delete compliance framework, standard, rules                               | FULL_ANY_COMPLIANCE_ENTITY |
| Compliance Framework  | View any Compliance Framework                  | Ability to view compliance framework definition and results                                | VIEW_ANY_COMPLIANCE_FWK    |
| Custom Configurations | Manage custom configurations owned by any user | Ability to create new and edit/delete Custom Configuration specification owned by any user | FULL_ANY_CCS               |
| Custom Configurations | Manage custom configurations owned by the user | Ability to create new and edit/delete Custom Configuration specification owned by the user | FULL_OWNED_CCS             |
| Dashboards            | Create Services Dashboard                      |                                                                                            | SVCD_CREATE_DASHBOARD      |

**Table 4 (Cont.) Resource Privileges**

| Resource Type                        | Privilege Name                                      | Description                                                                                             | Internal Name              |
|--------------------------------------|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------|----------------------------|
| Dashboards                           | Edit Services Dashboard                             |                                                                                                         | SVCD_EDIT_DASH             |
| Database Replay Entities             | Database Replay Viewer                              | Ability to view any Database Replay entity.                                                             | VIEW_DBREPLAY_ENTITY       |
| Database Replay Entities             | Database Replay Operator                            | Ability to view, create, and edit any Database Replay entity.                                           | OPERATE_DBREPLAY_ENTITY    |
| Deployment Procedure                 | Create                                              | Ability to create deployment procedures.                                                                | CREATE_DP                  |
| Deployment Procedure                 | Launch                                              | Ability to perform launch and create like operations on a Deployment Procedure.                         | LAUNCH_DP                  |
| Deployment Procedure                 | Full                                                | Ability to perform launch, create like, edit structure and delete operations on a Deployment Procedure. | FULL_DP                    |
| Deployment Procedure                 | Import                                              | Ability to create deployment procedures and ability to import/export customized deployment procedures.  | IMPORT_DP                  |
| Deployment Procedure                 | Grant launch privilege                              | Ability to grant launch privilege on deployment procedures.                                             | GRANT_LAUNCH_DP            |
| Deployment Procedure                 | Grant full privilege                                | Ability to grant upto full privilege on deployment procedures.                                          | GRANT_FULL_DP              |
| Enterprise Manager High Availability | Enterprise Manager High Availability Administration | Gives access to manage Enterprise Manager High Availability                                             | EMHA_ADMINISTRATION        |
| Enterprise Manager Plug-in           | Plug-in Agent Administrator                         | Gives access to manage Enterprise Manager plug-in on Agent                                              | PLUGIN_AGENT_ADMINISTRATOR |
| Enterprise Manager Plug-in           | Plug-in OMS Administrator                           | Gives access to manage Enterprise Manager plug-in on Management Server                                  | PLUGIN_OMS_ADMINISTRATOR   |

**Table 4 (Cont.) Resource Privileges**

| Resource Type                         | Privilege Name                        | Description                                                                                                                                                | Internal Name         |
|---------------------------------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Enterprise Manager Plug-in            | Plug-in view privilege                | Gives access to manage Enterprise Manager plug-in life cycle console                                                                                       | PLUGIN_VIEW           |
| Fusion MiddleWare Offline Diagnostics | View object                           | Ability to view the offline diagnostics objects                                                                                                            | VIEW_OBJECT           |
| Fusion MiddleWare Offline Diagnostics | Create Object                         | Ability to manage the offline diagnostic object lifecycle                                                                                                  | CREATE_OBJECT         |
| JVM Diagnostics                       | JVM Diagnostics Administrator         | Gives capability to manage all JVM Diagnostic Administrative operations                                                                                    | AD4J_ADMINISTRATOR    |
| JVM Diagnostics                       | JVM Diagnostics User                  | Gives capability to view the JVM Diagnostic data                                                                                                           | AD4J_USER             |
| JVM Diagnostics                       | JVM Diagnostics View Locals Privilege | Gives capability to view the JVM Diagnostics frame locals data                                                                                             | JVMD_VIEW_LOCALS_PRIV |
| Job System                            | Create                                | Ability to submit jobs, create library jobs, create deployment procedure instance and create deployment procedure configuration.                           | CREATE_JOB            |
| Job System                            | View                                  | Ability to view, do create like on a job, launch deployment procedure configuration and view deployment procedure instance.                                | VIEW_JOB              |
| Job System                            | Grant view privilege                  | Ability to grant view privilege on jobs.                                                                                                                   | GRANT_VIEW_JOB        |
| Job System                            | Manage                                | Ability to perform various operations except edit and delete on job, library job, deployment procedure configuration and on deployment procedure instance. | MANAGE_JOB            |

**Table 4 (Cont.) Resource Privileges**

| Resource Type              | Privilege Name                             | Description                                                                                                                               | Internal Name           |
|----------------------------|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Job System                 | Full                                       | Ability to perform all the valid operations on job, library job, deployment procedure configuration and on deployment procedure instance. | FULL_JOB                |
| Linux Patching             | Setup Linux Patching                       | Ability to perform Linux Patching setup.                                                                                                  | LINUX_PATCHING_SETUP    |
| Metric Extensions          | Create New Metric Extension                | Create or import new metric extensions                                                                                                    | CREATE_MEXT             |
| Metric Extensions          | Edit MEXT                                  | Can edit or create the next version of a metric extension object, but cannot delete it                                                    | EDIT_MEXT               |
| Metric Extensions          | Full MEXT                                  | Gives complete access to edit, and delete metric extension object                                                                         | FULL_MEXT               |
| Named Credentials          | Edit Credential                            | User can update credential but cannot delete it.                                                                                          | EDIT_CREDENTIAL         |
| Named Credentials          | Full Credential                            | Full Credential                                                                                                                           | FULL_CREDENTIAL         |
| Named Credentials          | View Credential                            | View Credential                                                                                                                           | GET_CREDENTIAL          |
| Named Credentials          | Create new Named Credential                | Ability to create new named credentials                                                                                                   | CREATE_CREDENTIAL       |
| OMS Configuration Property | View any OMS configuration property        | Gives access to view any OMS configuration property                                                                                       | VIEW_ANY_OMS_PROPERTY   |
| OMS Configuration Property | View / Edit any OMS configuration property | Gives access to view / edit any OMS configuration property                                                                                | MANAGE_ANY_OMS_PROPERTY |
| Patch Plan                 | Create Patch Plan                          | Privilege for creating a Patching Plan object                                                                                             | CREATE_PATCH_PLAN       |
| Patch Plan                 | Create Patch Plan Template                 | Privilege for creating a Patching Plan Template object                                                                                    | CREATE_PLAN_TEMPLATE    |
| Patch Plan                 | View Patching Plan                         | Privilege to View a Patching Plan Object                                                                                                  | VIEW_PATCH_PLAN         |
| Patch Plan                 | Full Patch Plan                            | Privilege to view, modify, execute and delete a Patching plan object                                                                      | FULL_PATCH_PLAN         |
| Patch Plan                 | View any Patching Plan                     | Privilege to view any Patching plan object                                                                                                | VIEW_ANY_PATCH_PLAN     |

**Table 4 (Cont.) Resource Privileges**

| Resource Type      | Privilege Name                                  | Description                                                                                                                 | Internal Name              |
|--------------------|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Patch Plan         | View any Patching Plan Template                 | Privilege to view any Patching Plan Template object                                                                         | VIEW_ANY_PLAN_TEMPLATE     |
| Patch Plan         | Manage privileges on a Patching Plan            | Privilege to grant or revoke privileges on a Patching plan object                                                           | MANAGE_PRIV_PATCH_PLAN     |
| Patch Plan         | Full privileges on any Patching Plan            | Privilege to view, modify, execute and delete any Patching plan object                                                      | FULL_ANY_PATCH_PLAN        |
| Patch Plan         | Manage privileges on any Patching Plan          | Privilege to grant or revoke privileges on any Patching plan object                                                         | MANAGE_PRIV_ANY_PATCH_PLAN |
| Patch Plan         | Privileges for Patch Setup                      | Privilege to grant privileges any Patching plan object                                                                      | PATCH_SETUP                |
| Patching Setup     | Setup Offline Patching                          | Ability to perform Offline Patching setup.                                                                                  | SETUP_OFFLINE_PATCHING     |
| Proxy Settings     | Setup Proxy for connecting to Agents            | Ability to set up a proxy server which can be used by your Oracle Management Server (OMS) to connect to Agents.             | SETUP_PROXY_FOR_AGENTS     |
| Proxy Settings     | Setup Proxy for connecting to My Oracle Support | Ability to set up a proxy server which can be used by your Oracle Management Service (OMS) to connect to My Oracle Support. | SETUP_PROXY_FOR_MOS        |
| Reports            | Publish Report                                  | Ability to publish reports for public viewing                                                                               | PUBLISH_REPORT             |
| Reports            | View Report                                     | Ability to view report definition and stored reports, generate on demand reports and do a create like                       | VIEW_REPORT                |
| Request monitoring | Request Monitoring Administrator                | Gives capability to manage all Request Monitoring Administrative Operations                                                 | BTM_ADMINISTRATOR          |
| Request monitoring | Request Monitoring User                         | Gives capability to view the Request Monitoring Data                                                                        | BTM_USER                   |
| Ruleset            | Create Business Ruleset                         | Create Business Ruleset                                                                                                     | CREATE_BUSINESS_RULESET    |



**Table 4 (Cont.) Resource Privileges**

| Resource Type                   | Privilege Name                          | Description                                                                                                                                                                                                      | Internal Name               |
|---------------------------------|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| Ruleset                         | Edit Business Ruleset                   | Edit Business Ruleset                                                                                                                                                                                            | EDIT_BUSINESS_RULESET       |
| Self Update                     | View any Enterprise Manager Update      | Gives access to view any Enterprise Manager Update                                                                                                                                                               | VIEW_ANY_SELFUPDATE         |
| Self Update                     | Self Update Administrator               | Gives access to manage Enterprise Manager Update                                                                                                                                                                 | SELFUPDATE_ADMINISTRATOR    |
| Software Library Administration | Software Library Storage Administration | Ability to manage upload and reference file storage locations, import and export entities, and purge deleted entities                                                                                            | SWLIB_STORAGE_ADMIN         |
| Software Library Entity         | Create Any Software Library Entity      | Ability to create any Software Library entity                                                                                                                                                                    | SWLIB_CREATE_ANY_ENTITY     |
| Software Library Entity         | Edit Any Software Library Entity        | Ability to edit any Software Library entity                                                                                                                                                                      | SWLIB_EDIT_ANY_ENTITY       |
| Software Library Entity         | Edit an Software Library Entity         | Ability to edit a Software Library entity                                                                                                                                                                        | SWLIB_EDIT_ENTITY           |
| Software Library Entity         | Export Any Software Library Entity      | Ability to view and export any Software Library entity to a Provisioning Archive (PAR) file                                                                                                                      | SWLIB_EXPORT                |
| Software Library Entity         | Grant Any Entity Privilege              | Ability to grant view, edit and delete privilege on any Software Library entity. This privilege is required if the user granting the privilege on an entity is not a super administrator or owner of the entity. | SWLIB_GRANT_ANY_ENTITY_PRIV |
| Software Library Entity         | Import Any Software Library Entity      | Ability to import any Software Library entity from a Provisioning Archive (PAR) file                                                                                                                             | SWLIB_IMPORT                |
| Software Library Entity         | Manage Any Software Library Entity      | Ability to create, view, edit and delete any Software Library entity                                                                                                                                             | SWLIB_MANAGE_ANY_ENTITY     |
| Software Library Entity         | Manage Entity                           | Ability to view, edit and delete a Software Library entity                                                                                                                                                       | SWLIB_MANAGE_ENTITY         |
| Software Library Entity         | View Any Software Library Entity        | Ability to view any Software Library entity                                                                                                                                                                      | SWLIB_VIEW_ANY_ENTITY       |
| Software Library Entity         | View Software Library Entity            | Ability to view a Software Library entity                                                                                                                                                                        | SWLIB_VIEW_ENTITY           |

**Table 4 (Cont.) Resource Privileges**

| Resource Type              | Privilege Name                               | Description                                                                                   | Internal Name                       |
|----------------------------|----------------------------------------------|-----------------------------------------------------------------------------------------------|-------------------------------------|
| Software Library Entity    | View any Oracle Load Testing Scenario Entity | Ability to view any Oracle Load Testing Scenario Entity                                       | VIEW_ANY_SWLIB_OLT_SCE_ENTITY       |
| Software Library Entity    | View any User Defined Test Entity            | Ability to view any User Defined Test Entity                                                  | VIEW_ANY_SWLIB_USERTEST_ENTITY      |
| Software Library Entity    | View any Template Entity                     | Ability to view any Template Entity                                                           | VIEW_ANY_SWLIB_TEMPLATE_ENTITY      |
| Software Library Entity    | View any Virtual Disk Entity                 | Ability to view any Virtual Disk Entity                                                       | VIEW_ANY_SWLIB_VIRTUAL_DISK_ENTITY  |
| Software Library Entity    | View any Assembly Entity                     | Ability to view any Assembly Entity                                                           | VIEW_ANY_SWLIB_ASSEMBLY_ENTITY      |
| Software Library Entity    | View any ISO Entity                          | Ability to view any ISO Entity                                                                | VIEW_ANY_SWLIB_ISO_ENTITY           |
| System                     | Create Role and Manage System                | Provides all the privileges to any target in the system                                       | CREATE_ROLE<br>MANAGE_SYSTEM_ROLES  |
| Target Discovery Framework | Scan Network                                 | Ability to create, edit and delete host discovery configuration                               | CAN_SCAN_NETWORK_PRIVILEGE          |
| Target Discovery Framework | View Any Discovered Hosts                    | Ability to view any discovered hosts                                                          | VIEW_ANY_DISCOVERED_HOSTS           |
| Target Discovery Framework | View Any Discovered Targets On Host          | Ability to view any discovered targets on host                                                | VIEW_ANY_DISCOVERED_TARGETS_ON_HOST |
| Template                   | View Template                                | Ability to view a template and apply it to any target on which you have Manage Target Metrics | VIEW_TEMPLATE                       |

---

# C.1 Audit Operations

To view a list of current audit operations, do one of the following:

- From the Enterprise Manager Security Console:
  1. In Enterprise Manager, select **Security>Security Console** from the **Setup** menu.
  2. Under Enterprise Manager Security, click **Comprehensive Auditing**.
  3. Select the Audit Operations tab.

The list of audit operations appears.

- From the Enterprise Manager Command Line Interface (EM CLI), enter the following command:

```
$ emcli show_operations_list
```

The list of audit operations appears.

# D.1 Configuring TLSv1.2 for Communication with the Enterprise Manager Repository

By enabling the TLSv1.2 protocol for communication with the Enterprise Manager Repository, the Oracle Management Service communicates with the repository in a secured mode using TLS to encrypt communication traffic and allow the Enterprise Manager Repository to authenticate itself to the Oracle Management Service.

To enable TLSv1.2 protocol for communication with the Enterprise Manager Repository, follow these steps:

## Step 1: Configure TLSv1.2 for the Enterprise Manager Repository

Because the Enterprise Manager Repository resides within an Oracle database, the best practices for configuring SSL on an Oracle database also apply to the Enterprise Manager Repository. Refer to the *Oracle Database Security Guide* to obtain detailed information on configuring SSL.

- For a sample configuration on an Oracle 11.2 RAC, refer to MOS Note **ID 1448841.1**.
- In the *sqlnet.ora* or the *listener.ora* file, ensure that the `SSL_VERSION` parameter is set to 1.2 for configuring TLSv1.2.
- In the *sqlnet.ora* file, ensure that the `SSL_CLIENT_AUTHENTICATION` parameter is set to `FALSE`.
- Verify the configuration by making an SSL connection using the `SQLPLUS` and `TCPS` connect descriptors before proceeding to the next step.

To ensure that the connect descriptors are correct, you can test the connection by running the following command:

```
./sqlplus sysman/
<sysman_pwd>@" (DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)
(HOST=<REPOS_HOST/SCAN_HOST>)(PORT=<TCPS_PORT>)))(CONNECT_DATA= (SID=<SID/
SERVICE>))"
```

### Note:

It is important to keep both TCP and TCPS listeners up until the Oracle Management Service connect descriptor is changed to use TCPS, as show in Step 2.

## Step 2: Configuring the Oracle Management Service to connect to the TLSv1.2-enabled Enterprise Manager Repository

Perform the following sequence of steps in a rolling manner—start with the *Primary Oracle Management Service* first and then proceed with the remaining Oracle Management Services.

1. Import the database server CA certificate into the Oracle Management Service JDK TrustStore.

Execute the following after backing up the server CA certificates

```
$ORACLE_HOME/oracle_common/jdk/bin/keytool -importcert -file trustCert.pem -alias emreprootca -keystore $ORACLE_HOME/oracle_common/jdk/jre/lib/security/cacerts -storepass "changeit"
```

 **Note:**

The JDK TrustStore password is "changeit".

2. Disable Oracle DB client native encryption.

Edit the `<ORACLE_HOME>/gc_inst/em/EMGC_OMS<n>/emgc.properties` file and add the following line:

```
oracle.sysman.core.conn.enableEncryption=false
```

Execute the following on the Primary Oracle Management Service only:

```
emctl set property -name "oracle.sysman.core.conn.enableEncryption" -value "false" -sysman_pwd sysman
```

3. Change the connect descriptor to use only TCPS.

Obtain the existing connect descriptor using the command: `emctl config oms -list_repos_details`

Execute the following using the changed TCPS protocol and port.

```
emctl config oms -store_repos_details -repos_user sysman -repos_pwd <SYSMAN_PWD> -repos_conn_desc "(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)(HOST=<REPOS_HOST/SCAN_HOST>)(PORT=<TCPS_PORT>)))(CONNECT_DATA= (SID=<SID/SERVICE>)))"
```

Ensure Port and Protocol properties are modified in the following files. If not, modify **Port** and **Protocol** properties to use the TCPS setting.

```
<EM_INSTANCE>/user_projects/domains/GCDomain/config/fmwconfig/jps-config.xml
<EM_INSTANCE>/user_projects/domains/GCDomain/config/fmwconfig/jps-config-jse.xml
<EM_INSTANCE>/user_projects/domains/GCDomain/config/fmwconfig/embi-policystoremerge-jpscfcg.xml
```

4. Change the Connect Descriptor of Services to use only TCPS.

If there are other services created for subsystems such as Ping, Events, Jobs and Loader, modify its connect descriptor to use the new TCPS configuration details.

**Execute the following on the Primary Oracle Management Service first.**

For the Ping subsystem connect descriptor:

```
emctl set property -name "oracle.sysman.core.omsAgentComm.ping.connectionService.connectDescriptor" -value "\ (DESCRIPTION=\ (ADDRESS_LIST=\ (ADDRESS=\ (PROTOCOL=TCPS\)\ (HOST=<REPOS_HOST/SCAN_HOST>)\)\ (PORT=<TCPS_PORT>)\)\)\)\ (CONNECT_DATA= (SERVICE_NAME=ping\)\)\)" -sysman_pwd <SYSMAN_PWD>
```

For the Event subsystem connect descriptor:

```
emctl set property -name "oracle.sysman.core.events.connectDescriptor" -value "\ (DESCRIPTION=\ (ADDRESS_LIST=\ (ADDRESS=\ (PROTOCOL=TCPS\)\ (HOST=<REPOS_HOST/
```

```
SCAN_HOST>)\(PORT=<TCPS_PORT>)\)\)\(CONNECT_DATA=(SERVICE_NAME=event)\)\)" -
sysman_pwd <SYSMAN_PWD>
```

For the Jobs subsystem connect descriptor:

```
emctl set property -name "oracle.sysman.core.jobs.conn.service" -value "\
(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)\(HOST=<REPOS_HOST/
SCAN_HOST>)\(PORT=<TCPS_PORT>)\)\)\(CONNECT_DATA=(SERVICE_NAME=emjob)\)\)" -
sysman_pwd <SYSMAN_PWD>
```

For Loader subsystem connect descriptor:

```
emctl set property -name "oracle.sysman.core.pbs.gcloader.connectDescriptor" -
value "\(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)\(HOST=
T=<REPOS_HOST/SCAN_HOST>)\(PORT=<TCPS_PORT>)\)\)\(CONNECT_DATA=(
SERVICE_NAME=loader)\)\)" -sysman_pwd <SYSMAN_PWD>
```

**Once steps 2–1 through 2–4 have been run on the Primary Oracle Management Service, repeat them for all remaining Oracle Management Services .**

### Step 3: Configure blackouts for Enterprise Manager Repository-related targets

In order to suppress alerts until the target configurations are complete, place all targets related to the Enterprise Manager Repository (oracle\_database , oracle\_emrep, oracle\_oms ,and metadata\_repository target types) under blackout.

### Step 4: Bounce all Oracle Management Services

Execute the following on all Oracle Management Services starting with Primary Oracle Management Service:

```
emctl stop oms -all
```

Disable the TCP listener in the *listener.ora* file of Enterprise Manager Repository and bounce the listener again to enable only the TCPS connection.

Start the primary Oracle Management Service.

```
emctl start oms
```

#### Note:

If the Oracle Management Services do not start, you will need to do one of the following:

Add "SQLNET.RECV\_TIMEOUT=100000" to the database sqlnet.ora file.

**OR**

Apply database patch 20544797 (preferred method).

Once the Primary Oracle Management Service is up, start the remaining Oracle Management Services one at a time.

### Step 5: Reconfigure the Agents monitoring the Enterprise Manager Repository

Reconfigure the Primary Oracle Management Service central agent that is monitoring the Management Repository by locating the target "Management Services and

Repository" in its target.xml file. If RAC is configured for the repository, you will also need to locate the Enterprise Manager Repository host Agent(s).

Execute the following on each of the above two agents identified which monitors a target referring to Repository connection:

```
<AGENT_INSTANCE>/bin/emctl setproperty agent -name connectionTrustStoreLocation -value <...>/client/wallet/ewallet.p12
```

```
<AGENT_INSTANCE>/bin/emctl setproperty agent -name connectionTrustStorePassword -value <...>
```

```
<AGENT_INSTANCE>/bin/emctl setproperty agent -name connectionTrustStoreType -value PKCS12
```

Locate the sqlnet.ora configuration file in the following directory inside the home directory for the Primary Oracle Management Service central agent that is monitoring the Management Repository:

*AGENT\_HOME*/network/admin (UNIX)

*AGENT\_HOME*network\admin (Windows)

Ensure sqlnet.ora contains the following snippet:

```
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_VERSION = 1.2
WALLET_LOCATION = (SOURCE =
 (METHOD = FILE) (METHOD_DATA =
 (DIRECTORY = <...>/client/wallet))
)
```

Bounce the agents that have been modified in this step.

### Step 6: Reconfigure the targets referencing the Enterprise Manager Repository connection

Identify the targets referencing the repository connection in the target XML of the Primary Oracle Management Service central Agent monitoring the Enterprise Manager Repository. Also, identify the targets in target XML of the local physical host Agent if it is deployed on the Enterprise Manager Repository host.

Execute the following EMCLI command for each of the targets identified:

```
emcli modify_target -name="<Target Name>" -type="<target_type>" -properties="<Property>:<Property Value>;<Property>:<Property Value>" -on_agent
```



#### Note:

Make sure you use the target\_name, target\_type, property and property value format gathered from the Agent's targets.xml file.

#### Examples:

```
emcli modify_target -name="database1.mycompany.com" -type="oracle_database" -properties="Port:<TCPS_PORT>;Protocol:TCPS" -on_agent
```

```
emcli modify_target -name="Management Services and Repository" -type="oracle_emrep" -properties="ConnectDescriptor:(DESCRIPTION=(ADDRESS_LIST=(ADDRESS= (PROTOCOL=TCPS)
```

---

```
(HOST=<REPOS_HOST/SCAN_HOST>)(PORT=<TCPS_PORT>))(CONNECT_DATA=(SID=<SID>))" -
on_agent
```

```
emcli modify_target -name="primary_oms.mycompany.com:4889_Management_Service" -
type="oracle_oms" -properties="ConnectDescriptor:
(DESCRIPTION=(ADDRESS_LIST=(ADDRESS= (PROTOCOL=TCPS)(HOST=<REPOS_HOST/SCAN_HOST>
(PORT=<TCPS_PORT>)))(CONNECT_DATA=(SID=<SID>)))" -on_agent
```

```
emcli modify_target -name="/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER/mds-owsm" -
type="metadata_repository" -properties="JdbcUrl|
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADD RESS=(PROTOCOL=TCPS)
(HOST=<REPOS_HOST/SCAN_HOST>)(PORT=< TCPS_PORT>)))(CONNECT_DATA=(SID=<SID>)))" -
on_agent -subseparator=properties="|"
```

```
emcli modify_target -name="/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER/mds-sysman_mds" -
type="metadata_repository" -
properties="DatabaseName:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCPS)
(HOST=<REPOS_HOST/SCAN_HOST>)(PORT=<TCPS_P ORT>)))(CONNECT_DATA=(SID=<SID>)))" -
on_agent
```

### Step 7: End blackouts for Management Repository-related targets

Bring the Enterprise Manager Repository-related targets out of blackout and verify that the targets have *Target Up* status in Enterprise Manager Console.



# Index

## A

---

Access Control, [2-64](#)  
Administration Groups, privilege propagating, [2-33](#)  
Administrator, [2-26](#)  
Agent Registration Password, [2-41](#)  
    changing, [2-46](#)  
AGENT\_HOME/network/admin, [2-53](#)  
Agent, Securing, [3-5](#)  
Application DBA Access, [4-2](#)  
Application Developer Access, [4-3](#)  
attack, Man-in-the-middle, [1-1](#)  
attack, Denial-of-service, [1-1](#)  
attack, Password crack, [1-1](#)  
Audit Data, [2-97](#)  
Audit Data Export Service, [2-96](#)  
Audit Settings, [2-96](#)  
Audit SYS actions, [3-3](#)  
Audit, managing, [2-94](#)  
audited operations, [2-97](#)  
Auditing, Guidelines, [3-26](#)  
auditing, Infrastructure, [2-97](#)  
Authentication, [2-1](#)  
Authentication Schemes, [2-1](#)  
authentication, Creating a New Administrator, [2-3](#)  
Authentication, Enterprise User Security Based, [2-6](#)  
Authorization, Guidelines, [3-23](#)  
authorization, Privileges and Role, [2-24](#)  
Auto Provisioning, [2-11](#), [2-12](#)

## B

---

BASIC auditing, [2-94](#)

## C

---

Certificate Authority, [2-43](#)  
Certificate dialog box  
    Internet Explorer, [2-107](#)  
Ciphers, [3-18](#)  
Credential Preference, Hierarchy, [2-71](#)  
Credential Subsystem, [2-61](#)  
Cryptographic Keys, [2-89](#)

Custom CA Certificates, importing, [2-54](#)  
Custom Certificates for WebLogic Server, [2-53](#)

## D

---

Database Administrator Access, [4-4](#)  
Default Authentication, [2-4](#)  
Default Authentication Method, restoring, [2-24](#)  
deleting an administrator, [2-5](#)  
Denial-of-service, attack, [1-1](#)  
Advanced Security Option, [3-2](#)

## E

---

emctl  
    secure agent utility, sample output, [2-45](#)  
    secure oms utility, [2-40](#)  
    secure oms utility, sample output, [2-40](#)  
    security commands, [2-40](#)  
emctl commands  
    secure setpwd, [2-47](#)  
    secure unlock, [2-48](#)  
    start oms, sample output, [2-90](#)  
emkey, [2-90](#)  
emoms.properties  
    oracle.net.crypto\_checksum\_client, [2-51](#)  
    oracle.net.crypto\_checksum\_types\_client, [2-52](#)  
    oracle.net.encryption\_client, [2-51](#)  
    oracle.net.encryption\_types\_client, [2-51](#)  
    oracle.sysman.emRep.dbConn.enableEncryption, [2-51](#)  
Encryption, [1-4](#)  
Encryption Key, back up, [3-4](#)  
Enterprise Manager Framework Security  
    enabling for Management Repository, [2-49](#)  
    restricting HTTP access, [2-47](#)  
    types of secure connections, [2-40](#)  
Enterprise Manager User Attributes, [2-14](#)  
Enterprise Manager, securing, [1-1](#)  
Enterprise User Security Based Authentication, [2-1](#)  
Enterprise User Security, configuring, [2-24](#)  
Enterprise Users (EUS Users), registering, [2-7](#)  
Entitlement, [2-39](#)  
External Authentication, [3-22](#)

External Authorization, [2-11](#)  
 External Roles, [2-11](#)

## F

---

fine grained access control, [4-1](#)  
 Flexible Database Access Control, [4-1](#)  
 FULL, [2-29](#)

## G

---

get\_db\_account, [4-14](#)  
 get\_db\_profile, [4-14](#)  
 Global Named Credential, [2-63](#)  
 Global Preferred Credentials, [2-70](#)

## H

---

Host Preferred Credentials, [2-76](#), [2-77](#)  
 HTTP access, restricting, [2-47](#)  
 HTTPS, [2-40](#)

## I

---

ICMP, [3-6](#)  
 Internet Explorer  
     Certificate dialog box, [2-107](#)  
     security alert dialog box, [2-107](#)

## L

---

LDAP Authentication, [2-1](#)  
 LDAP Server, timeout, [5-3](#)  
 LDAP User Attributes, [2-14](#)  
 ldap\_trace.logATN, [5-3](#)  
 LDAP/SSO Providers, [2-17](#)

## M

---

Man-in-the-middle, attacks, [1-1](#)  
 Management Repository, recreating, [2-94](#)  
 Managing Credentials  
     EM CLI, [2-73](#)  
 Microsoft Active Directory, [2-10](#)  
 Monitoring Credentials, [2-69](#)

## N

---

Named Credential, [2-63](#)  
 Named Credentials, creating, [2-65](#)  
 Network Access, restricted, [3-2](#)  
 network/admin, [2-50](#), [2-52](#), [2-53](#)  
 Non-repudiation, [1-5](#)

## O

---

OID, [2-8](#)  
 OMS security, [2-40](#)  
 OPERATOR, [2-29](#)  
 ORA-12645 (security)  
     Parameter does not exist, [2-50](#)  
 Oracle Access Manager (OAM) SSO, [2-1](#)  
 Oracle Advanced Security, [2-40](#), [2-49](#)  
     enabling for Management Repository, [2-52](#)  
     enabling for the Management Agent, [2-53](#)  
 Oracle AS SSO 10g, [2-18](#)  
 Oracle Internet Directory, [2-8](#)  
 Oracle Management Agent  
     enabling security for, [2-45](#), [2-53](#)  
 Oracle Management Repository  
     enabling Oracle Advanced Security, [2-52](#)  
     enabling security for, [2-49](#)  
 Oracle Management Service  
     enabling security for, [2-40](#)  
 ORACLE\_HOME/network/admin, [2-50](#), [2-52](#)  
 oracle.net.crypto\_checksum\_client  
     property in emoms.properties, [2-51](#)  
 oracle.net.crypto\_checksum\_types\_client  
     property in emoms.properties, [2-52](#)  
 oracle.net.encryption\_client  
     property in emoms.properties, [2-51](#)  
 oracle.net.encryption\_types\_client  
     property in emoms.properties, [2-51](#)  
 oracle.sysman.emRep.dbConn.enableEncryption  
     entry in emoms.properties, [2-51](#)

## P

---

PAM Authentication  
     authentication, PAM, [2-78](#)  
 PAM, configuring, [2-79](#)  
 PowerBroker, [2-80](#)  
 Preferred Credentials, [2-69](#)  
 Principle of Least Privilege, [1-4](#)  
 Privilege Delegation, [2-89](#)  
 Privilege Groups, [4-5](#)  
 Privilege Propagating Groups, [2-33](#)  
 Privilege Propagation Groups, [3-25](#)  
 Privileges and Roles, [2-28](#)  
 Privileges, granting, [2-29](#)  
 Public Key Infrastructure (PKI), [2-40](#)

## R

---

Repository Owner, [2-26](#)  
 Repository-Based Authentication, [2-1](#)  
 Roles to Manage Privileges, [2-32](#)  
 root password  
     See also SYSMAN, [2-41](#)

root password (*continued*)  
when enabling security for the Management Service, [2-41](#)

## S

---

Secure Communication, [2-39](#)  
Secure Infrastructure, [3-1](#)  
Secure-Lock Mode, [3-17](#)  
security  
alert dialog box  
Internet Explorer, [2-107](#)  
certificate alerts  
responding to, [2-106](#)  
security considerations, [1-1](#)  
Security Principles, [1-4](#)  
Security Threats, [1-1](#)  
Separation of Duties, [1-4](#)  
Server Load Balancer, [2-42](#)  
SQLNET.CRYPTO\_SEED  
entry in sqlnet.ora, [2-52](#), [2-53](#)  
SQLNET.ENCRYPTION\_SERVER  
entry in sqlnet.ora, [2-52](#)  
sqlnet.ora, [2-49](#)  
SQLNET.CRYPTO\_SEED, [2-52](#), [2-53](#)  
SQLNET.ENCRYPTION\_SERVER, [2-52](#)  
SSL communication, [3-15](#)  
Sudo, [2-80](#)  
Super Administrator, [2-26](#)  
Suspicious activity, [1-5](#)

SYSMAN  
entering SYSMAN password when enabling security, [2-41](#)

## T

---

Target Credentials, [2-61](#)  
Target Named Credentials, [2-63](#)  
Target Privileges, [2-29](#)  
TCPS, [4-12](#)  
Third Party Certificates, [2-60](#)  
TLSv1.2 Protocol, [3-15](#)  
Transport Layer Security, [2-44](#)  
Troubleshooting Authentication, [5-1](#)

## U

---

update\_db\_account\_status, [4-15](#)  
update\_db\_password, [4-15](#)  
User Accounts, securing, [3-3](#)  
User Display Names, [2-16](#)  
Users, Classes of, [2-26](#)  
Users, Privileges and Roles, [2-25](#)

## V

---

VIEW, [2-30](#)  
view access, granting, [2-36](#)