

Oracle® Enterprise Manager

Cloud Control Security Guide

12c Release 3 (12.1.0.3)

E36415-01

June 2013

E36415-01

Copyright © 2013, 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, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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 is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on 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. 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.

Contents

Preface	vii
Audience	vii
Documentation Accessibility	vii
Related Documents	vii
Conventions	viii
 1 Security Overview	
1.1 Security Threats	1-1
1.2 Security Principles	1-3
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)	1-4
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 Repository-Based Authentication	2-3
2.1.3 Oracle Access Manager Single Sign-On	2-4
2.1.3.1 Removing Oracle Access Manager Single Sign-On	2-5
2.1.3.2 Oracle Single Sign-On (SSO) Based Authentication	2-5
2.1.4 Enterprise User Security Based Authentication	2-11
2.1.4.1 Registering Enterprise Users (EUS Users) as Enterprise Manager Users	2-12
2.1.5 Oracle Internet Directory (OID)	2-12
2.1.6 Microsoft Active Directory Based Authentication	2-14
2.1.7 Restoring to Default Authentication Method	2-15
2.1.7.1 Bypassing the Single Sign-On Logon Page	2-15
2.1.7.2 Restoring the Default Authentication Method	2-15
2.1.8 External Authorization using External Roles	2-16
2.1.9 Mapping LDAP User Attributes to Enterprise Manager User Attributes	2-17
2.1.10 Changing User Display Names in Enterprise Manager	2-18
2.1.11 Configuring Other LDAP/SSO Providers	2-20
2.1.11.1 Configuring Single Sign-on based Authentication	2-21
2.1.12 Configuring Enterprise User Security based Authentication	2-27
2.1.12.1 Registering Enterprise Users as Enterprise Manager Users	2-28

2.1.13	Restoring to Default Authentication Method	2-29
2.1.13.1	Bypassing the Single Sign-On Logon Page	2-29
2.1.13.2	Restoring the Default Authentication Method.....	2-29
2.2	Configuring Privileges and Role Authorization	2-30
2.2.1	Understanding Users, Privileges and Roles	2-30
2.2.2	Classes of Users.....	2-32
2.2.3	Privileges and Roles	2-33
2.2.3.1	Granting Privileges.....	2-33
2.2.3.2	Creating Roles	2-44
2.2.3.3	Using Roles to Manage Privileges.....	2-46
2.2.4	Managing Privileges with Privilege Propagating Groups	2-46
2.2.4.1	Example1: Granting various teams different levels of access to target groups	2-47
2.2.4.2	Example2: Granting developers view access to target database instances.	2-52
2.2.4.3	Entitlement Summary	2-58
2.3	Configuring Secure Communication	2-59
2.3.1	About Secure Communication.....	2-59
2.3.2	Enabling Security for the Oracle Management Service.....	2-60
2.3.2.1	Configuring the OMS with Server Load Balancer	2-61
2.3.2.2	Enabling Security with Multiple Management Service Installations.....	2-62
2.3.2.3	Creating a New Certificate Authority	2-62
2.3.2.4	Viewing the Security Status and OMS Port Information	2-63
2.3.2.5	Configuring Transport Layer Security	2-64
2.3.3	Securing the Oracle Management Agent	2-65
2.3.4	Managing Agent Registration Passwords.....	2-66
2.3.4.1	Using the Cloud Control Console to Manage Agent Registration Passwords.	2-66
2.3.4.2	Using emctl to Add a New Agent Registration Password	2-67
2.3.5	Restricting HTTP Access to the Management Service	2-67
2.3.6	Enabling Security for the Management Repository Database	2-69
2.3.6.1	About Oracle Advanced Security and the sqlnet.ora Configuration File	2-69
2.3.6.2	Configuring the Management Service to Connect to a Secure Management Repository Database 2-70	
2.3.6.3	Enabling Oracle Advanced Security for the Management Repository.....	2-72
2.3.6.4	Enabling Security for a Management Agent Monitoring a Secure Management Repository or Database 2-72	
2.3.7	Custom Configurations.....	2-73
2.3.7.1	Configuring Custom Certificates for WebLogic Server	2-73
2.3.7.2	Configuring Custom Certificates for OMS Console Access.....	2-75
2.3.7.3	Configuring Custom Certificates for OMS Upload Access	2-75
2.3.7.4	Configuring Transport Layer Security	2-76
2.3.8	Secure Communication Setup Tools.....	2-77
2.3.8.1	emctl secure oms.....	2-77
2.3.8.2	emctl secure agent	2-79
2.3.8.3	emctl secure wls.....	2-79
2.3.8.4	emctl status oms -details.....	2-79
2.3.9	Configuring Third Party Certificates	2-79
2.3.9.1	Configuring a Third Party Certificate for HTTPS Console Users	2-79
2.3.9.2	Configuring Third Party Certificate for HTTPS Upload Virtual Host	2-80
2.4	Authentication Scheme	2-81

2.5	Configuring and Using Target Credentials	2-81
2.5.1	Credential Subsystem.....	2-81
2.5.1.1	Named Credential	2-82
2.5.1.2	Monitoring Credentials	2-85
2.5.1.3	Preferred Credentials	2-85
2.5.1.4	Managing Credentials Using EM CLI	2-86
2.5.1.5	Host Authentication Features	2-87
2.6	Configuring and Using Cryptographic Keys	2-96
2.6.1	Configuring the emkey	2-97
2.6.2	emctl Commands	2-97
2.6.2.1	emctl status emkey	2-98
2.6.2.2	emctl config emkey -copy_to_credstore.....	2-98
2.6.2.3	emctl config emkey -copy_to_repos	2-98
2.6.2.4	emctl config emkey -copy_to_file_from_credstore.....	2-99
2.6.2.5	emctl config emkey -copy_to_file_from_repos	2-99
2.6.2.6	emctl config emkey -copy_to_credstore_from_file.....	2-99
2.6.2.7	emctl config emkey -copy_to_repos_from_file	2-99
2.6.2.8	emctl config emkey -remove_from_repos	2-100
2.6.3	Install and Upgrade Scenarios	2-100
2.6.3.1	Installing the Management Repository	2-100
2.6.3.2	Installing the First Oracle Management Service	2-100
2.6.3.3	Upgrading from 10.2 or 11.1 to 12.1.....	2-100
2.6.3.4	Recreating the Management Repository	2-101
2.7	Configuring and Managing Audit	2-101
2.7.1	Configuring the Enterprise Manager Audit System.....	2-102
2.7.2	Configuring the Audit Data Export Service	2-102
2.7.3	Updating the Audit Settings	2-102
2.7.4	Searching the Audit Data	2-103
2.7.5	List of Operations Audited.....	2-103
2.7.6	Auditing the Infrastructure	2-104
2.8	Additional Security Considerations.....	2-105
2.8.1	Changing the SYSMAN and MGMT_VIEW Passwords.....	2-105
2.8.1.1	Changing the SYSMAN User Password	2-105
2.8.1.2	Changing the MGMT_VIEW User Password.....	2-106
2.8.2	Responding to Browser-Specific Security Certificate Alerts	2-106
2.8.2.1	Responding to the Internet Explorer Security Alert Dialog Box	2-107
2.8.2.2	Responding to the Mozilla Firefox New Site Certificate Dialog Box.....	2-110
2.8.2.3	Responding to the Google Chrome Security Alert Dialog Box	2-111
2.8.2.4	Responding to Safari Security Dialog Box	2-113

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
3.1.2	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	Enable ICMP.....	3-5
3.1.4.2	Configure Oracle Management Agent for Firewalls.....	3-6
3.1.4.3	Configure Oracle Management Service for Firewalls.....	3-6
3.2	Guidelines for SSL communication	3-6
3.2.1	Configure TLSv1 Protocol	3-7
3.2.2	Leave communication is Secure-Lock Mode	3-7
3.2.2.1	Secure and Lock the OMS and Agents	3-7
3.2.3	Disable Weak Ciphers	3-8
3.3	Guidelines for Authentication	3-10
3.3.1	Enable External Authentication	3-10
3.4	Guidelines for Authorization	3-11
3.4.1	Use Principle of Least Privileges for Defining Roles/Privileges	3-13
3.4.2	Use Privilege Propagation Groups	3-13
3.5	Guidelines for Auditing	3-13
3.6	Guidelines for Managing Target Credentials	3-15

4 Troubleshooting

4.1	Troubleshooting Authentication Issues in Enterprise Manager	4-1
-----	---	-----

5 References

Index

Preface

This guide describes how to set up Enterprise Manager Cloud Control 12c 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

<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.

Security Overview

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.

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

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

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

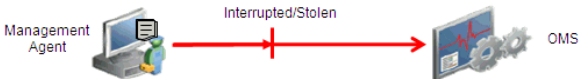

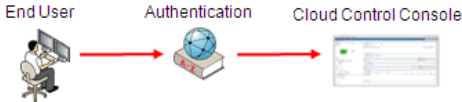
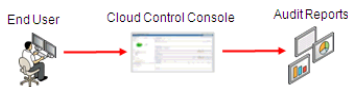
Threats	Security Consideration	Resolution/Best Practice
Man-in-the-middle attacks	Data confidentiality and integrity	<p>Data Confidentiality and Integrity</p> <ul style="list-style-type: none"> Not disclosed to any entities unless they are authorized to access Not changed, destroyed, or lost in unauthorized 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 Grid Control <p>Examples: guessing, dictionary and brute force attacks</p>  <pre> graph LR EndUser[End User] --> Authentication[Authentication] Authentication --> CloudControlConsole[Cloud Control Console] </pre> <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  <pre> graph LR EndUser[End User] --> CloudControlConsole[Cloud Control Console] CloudControlConsole --> AuditReports[Audit Reports] </pre> <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.

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 12c 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.

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 like password control via 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 [Section 2.1.2, "Repository-Based Authentication"](#).

- **Oracle Access Manager (OAM) SSO** - 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 would configure OAM for this. For more information about OAM, see *Oracle® Fusion Middleware Administrator's Guide for Oracle Access Manager 12c Release 1 (11.1.1)*.
- **Oracle SSO Based Authentication:** The single sign-on based authentication provides strengthened and centralized user identity management across the enterprise. After you have configured Enterprise Manager to use the Oracle Application Server Single Sign-On, you can register any single sign-on user as an Enterprise Manager administrator. You can then enter your single sign-on credentials to access the Oracle Enterprise Manager console.
- **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. Once the Enterprise Manager repository is configured with EUS, you can configure Enterprise Manager to use EUS as its authentication mechanism as described in [Section 2.1.4, "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. Thus, it is ideally suited for Oracle environments or enterprises with Oracle database expertise. When using an authentication scheme based on Oracle Internet Directory 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: For other authentication schemes not in the list, as long as a provider in the underlying WebLogic Server that the OMS uses.

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.

For more information on tuning the providers, see *Oracle® Fusion Middleware Securing Oracle WebLogic Server*

2.1.2 Repository-Based Authentication

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**.
2. Click the appropriate task button on the Administrators page. The following screen is displayed:

Figure 2–1 Create / Edit Administrator

The screenshot displays the 'Create Administrator: Properties' form in the Oracle Enterprise Manager interface. The form includes the following elements:

- Navigation:** 'Cancel', 'Step 1 of 5', 'Next', and 'Review' buttons at the top right.
- Fields:**
 - Name:** A text input field.
 - Password:** A text input field.
 - Confirm Password:** A text input field.
 - Password Profile:** A dropdown menu currently set to 'DEFAULT', with a 'View' link and a 'Manage Profiles' button.
 - Prevent password change:** An unchecked checkbox.
 - Expire password now:** An unchecked checkbox.
 - E-mail Address:** A text input field with a note: 'Specify one or more e-mail addresses separated by a comma or space. If you are entering these for the first time, they will be used to create a default 24x7 notification schedule for this Administrator.'
 - Description:** A large text area.
 - Super Administrator:** An unchecked checkbox.
- Footer:** 'Cancel', 'Step 1 of 5', 'Next', and 'Review' buttons at the bottom right.

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** checkbox is selected.

If you select the **Expire Password Now** checkbox, 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 following screen is displayed and he is prompted to change the password.

Figure 2–2 Password Expiry Page

ORACLE Enterprise Manager Cloud Control 12c Help

Change Password

Your current password has expired. Please change password first.
To change your password, specify and confirm a new password.

Administrator ADMIN2

Current Password

New Password

Confirm New Password

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

2.1.3 Oracle Access Manager Single Sign-On

When using an Oracle Access Manager Single Sign-On (OAM SSO) 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 (OAM) is installed on a separate host. Webgate needs to be installed on each OMS host where Apache server is running. For Webgate installation, refer to http://docs.oracle.com/cd/E21764_01/install.1111/e12002/webgate.htm

Enterprise Manager comes with an OAM template called *OAMRequest.xml.template*, which needs to be used when registering the Enterprise Manager application with the OAM SSO server. You can find the template at the following location:

```
$MW_HOME/oms/sysman/config
```

You need to replace the server, host identifier and Agent information before using for registration. For instructions on how to register, see the *Registering Partners (Agents and Applications) Remotely* chapter of the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*.

As part of the registration process, certain configuration files get generated, which need to be used while configuring Webgate on the OMS host. For more details, see the "Installing and Configuring Oracle HTTP Server 11g Webgate for OAM" chapter of the Oracle Fusion Middleware Installation Guide for Oracle Identity Management.

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

```
emctl config auth oam [-sysman_pwd <pwd>] -oid_host <host> -oid_port <port>
                    -oid_principal <principal> [-oid_credential <credential>] [-use_
anonymous_bind]
                    -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>] [-enable_auto_provisioning] [-auto_
provisioning_minimum_role <min_role>] [-minimum_privilege <min_priv>]
                    [-use_ssl] [-cert_file <cert>] [-trust_cacerts] [-keystore_pwd
<passwd>]
```

Command options are as follows:

- *[-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 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

Note: Pass 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
```

2.1.3.1 Removing Oracle Access Manager Single Sign-On

To remove SSO configuration, run `emctl config auth repos` command. This will remove the Weblogic providers that were configured with `emctl config auth oam` command and the OMS properties as well.

Note: The administrator has to manually un-install Webgate and edit `httpd.conf` to remove the Webgate related entries.

2.1.3.2 Oracle Single Sign-On (SSO) Based Authentication

If you are currently using Oracle Application Server Single Sign-On (Oracle SSO) to control access and authorization for your enterprise applications, 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 12c 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, make sure that the correct monitoring settings have been defined.
-

The following sections describe how to configure Enterprise Manager as an Oracle Application Server 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](#)
- [Bypassing the Single Sign-On Logon Page](#)

2.1.3.2.1 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.

6. Go back to the 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
```

7. Set the ORACLE_HOME environment variable to WebTier Oracle Home location.

```
setenv ORACLE_HOME /scratch/12c/MWHome/Oracle_WT
```

Then, run the following:

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

8. 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 12c Release 12.1.0.3.0
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
SSO Configuration done successfully. Please restart Admin & Managed Servers.
```

9. Run the following commands on each OMS:

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

2.1.3.2.2 Removing Single Sign-On Configuration

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

1. Run the following command on each OMS:

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

Sample command output:

```
Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.3.0
Copyright (c) 1996, 2013 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
```

2.1.3.2.3 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

2.1.3.2.4 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 Log on 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 an Enterprise Manager user, you can create them using the following procedure:

1. Log in to Enterprise Manager by connecting to Managed Server (MS) directly.
For example, *https://ms_host:ms_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.

2.1.3.2.5 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 via Oracle single sign-on.

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 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@oracle.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.

2.1.3.2.6 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.

2.1.3.2.7 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 12c Release 12.1.0.3.0
Copyright (c) 1996, 2013 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
```

2.1.4 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). 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: Enterprise User Security Configuration Tasks and Troubleshooting in the *Oracle Database Advanced 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 properties:

```
oracle.sysman.emSDK.sec.DirectoryAuthenticationType=EnterpriseUser
oracle.sysman.emSDK.sec.eus.Domain=<ClientDomainName> (For
example:mydomain.com)
oracle.sysman.emSDK.sec.eus.DASHostUrl=<das_url> (For example:
oracle.sysman.emSDK.sec.eus.DASHostUrl=http://my.dashost.com:7777 )
```

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 login 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. For more details, refer to [Registering Single Sign-On Users Using EM CLI](#).

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.

Prerequisites

Oracle Internet Directory LDAP server is set up and running.

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

```
emctl config auth oid -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" -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.

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`: 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.

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.

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 Restoring to Default Authentication Method

2.1.7.1 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.

2.1.7.2 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 12c Release 12.1.0.3.0
Copyright (c) 1996, 2013 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`.

2.1.8 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`.

Auto Provisioning

Typically the external LDAP users need to 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`.

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

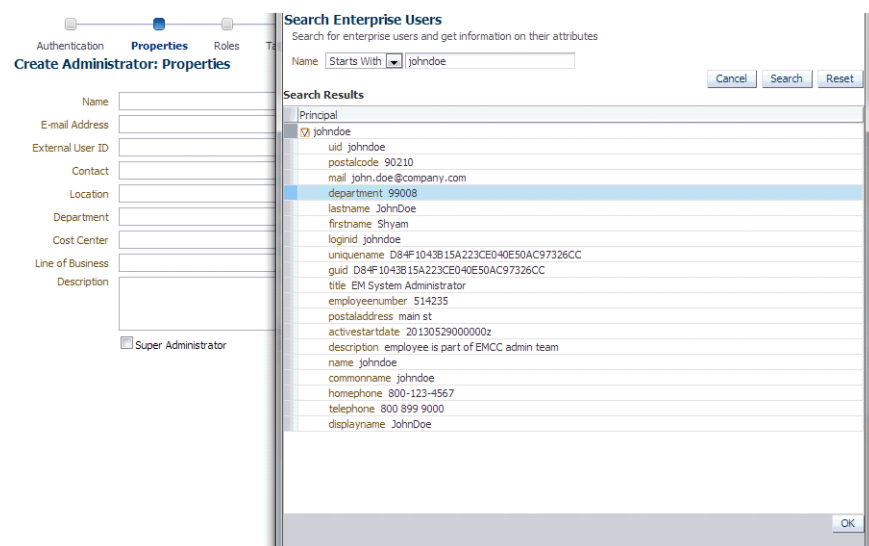
This allows the external users to login without being first created as an Enterprise Manager user in the Enterprise Manager repository. Their user account gets created automatically upon the first login. Once this property is set, all external LDAP users will be able to login to Enterprise Manager console. If you want to further restrict the auto provisioning feature to a subset of users, such as only to members of certain LDAP group, 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.

2.1.9 Mapping LDAP User Attributes to Enterprise Manager User Attributes

When external authentication is enabled, the 'Create User' flow of Enterprise Manager has a flash-light icon next to the name field. Clicking on the flash-light brings up a popup window, giving Enterprise Manager administrators the ability to search for enterprise users in the external LDAP server (for example AD/OID) that has 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, as shown in the following figure.

Figure 2–3 User Account Attributes



When external authentication has been configured, it is often desirable to automatically bring over user information such as email address, department, .that is defined for the user in LDAP into the corresponding Enterprise Manager user account. This can be done by setting the OMS property `oracle.sysman.core.security.auth.ldapuserattributes_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** -- is an the Enterprise Manager user property. Value values for user properties are USERNAME, EMAIL, CONTACT, LOCATION, DEPARTMENT, COSTCENTER, LINEOFBUSINESS ,DESCRIPTION. Other values specified for keys will be ignored.
- **attribute** - is the user attribute that need to be fetched from LDAP.and is used to set the properties of the user in Enterprise Manager.. The attribute should be specified in the 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 user will be "firstname lastname employee", e.g. "John Doe employee". Another example is CONTACT={telephone number %phone%}. If comma needs to be specified in the literal string value, it needs to be escaped with \ e.g. 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 back-slash (\) if specified in the literal string are ':' and '=', so it should look like \: 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. In the example above, the page appear as follows:

Figure 2–4 Create User Page: Administrator Properties

The screenshot shows the 'Create Administrator: Properties' page in the Oracle Enterprise Manager console. The page has a blue header with 'ORACLE Enterprise Manager Cloud Control 12c' and navigation tabs for Enterprise, Targets, Favorites, and History. Below the header, there are tabs for Authentication, Properties (selected), Roles, Target Privileges, Resource Privileges, and Review. The main content area contains a form with the following fields: Name (johndoe), Email Address (johndoe@company.com), Contact (2124540000), Location (90210), Department (EnterpriseAdmin), Cost Center, Line of Business, and Description (EM LDAP Admin). There is a checkbox for 'Super Administrator' at the bottom. The page also includes 'Cancel', 'Back', and 'Next' buttons.

2.1.10 Changing User Display Names in Enterprise Manager

Enterprise Manager has the ability to show user- friendly username in Enterprise Manager when user logs in using a numeric ID. In some LDAP environments, users may have numeric login IDs. 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 a 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 through Enterprise Manager console as well. These are dynamic properties and don't need a bounce.

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 will thus look like this (note the extra field 'External User ID').

The screenshot shows the 'Create Administrator: Properties' page. At the top, there is a navigation bar with tabs: Authentication, Properties (selected), Roles, Target Privileges, Resource Privileges, and Review. Below the tabs, the form fields are as follows:

- Name:
- E-mail Address:
- External User ID:
- Contact:
- Location:
- Department:
- Cost Center:
- Line of Business:
- Description:

At the bottom, there is a checkbox labeled 'Super Administrator'.

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:

This screenshot shows the same 'Create Administrator: Properties' page, but with example data entered into the fields:

- Name: johndoe
- E-mail Address:
- External User ID: 123456
- Contact:
- Location: US
- Department: IT
- Cost Center:
- Line of Business:
- Description:

The 'Super Administrator' checkbox remains at the bottom.

User 123456 will still login 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 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. Going by example above, if we set it to

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

When we select that user from popup and hit ok, the page will appear as follows:

Create Administrator: Properties

Name: JohnDoe

E-mail Address: johndoe@company.com

External User ID: 123456

Contact: 2124540000

Location: 90210

Department: EnterpriseAdmin

Cost Center:

Line of Business:

Description: EM LDAP Admin

☐ Super Administrator

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

2.1.11 Configuring Other LDAP/SSO Providers

To configure Enterprise Manager with any other supported WebLogic authentication schemes, the configuration of authentication providers has to be done manually using Weblogic Administrator Console. See the chapter "Configuring Authentication Providers" of the Oracle Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 documentation.

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

Providers

Authentication Providers

Name	Description
DefaultAuthenticator	WebLogic Authentication Provider
DefaultIdentityAsserter	WebLogic Identity Assertion provider
iplanetauth	Provider that performs LDAP authentication
EM_Repos_Authenticator	EM Repos Authentication Provider

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` to 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`

2.1.11.1 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](#)

2.1.11.1.1 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: Pass `-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
```

2.1.11.1.2 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 12c 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, make sure that the correct monitoring settings have been defined.
-
-

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](#)

2.1.11.1.3 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.

6. 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
```

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

```
setenv ORACLE_HOME /scratch/12c/MWHome/Oracle_WT
```

Then, run the following:

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

8. 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 12c Release 12.1.0.3.0
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
```

SSO Configuration done successfully. Please restart Admin & Managed Servers.

9. Run the following commands on each OMS:

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

2.1.11.1.4 Removing Single Sign-On Configuration To remove the single sign-on configuration, perform the following:

1. Run the following command on each OMS:

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

Sample command output:

```
Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.3.0  
Copyright (c) 1996, 2013 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
```

2.1.11.1.5 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

2.1.11.1.6 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 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. Log in to Enterprise Manager by connecting to Managed Server (MS) directly. For example, `https://ms_host:ms_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.

2.1.11.1.7 Registering Single Sign-On Users Using EM CLI s

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 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.

Argument	Description
-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@oracle.com;joe.shmoe@shmoeeshop.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.

2.1.11.1.8 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.

2.1.11.1.9 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 12c Release 12.1.0.3.0
Copyright (c) 1996, 2013 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
```

2.1.12 Configuring 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. 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: Enterprise User Security Configuration Tasks and Troubleshooting in the *Oracle Database Advanced Security Administrator's Guide*

If you currently use Enterprise User Security for all your Oracle databases, you can extend this feature to Enterprise Manager. 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 properties:

```
oracle.sysman.emSDK.sec.DirectoryAuthenticationType=EnterpriseUser
oracle.sysman.emSDK.sec.eus.Domain=<ClientDomainName> (For
example:mydomain.com)
oracle.sysman.emSDK.sec.eus.DASHostUrl=<das_url> (For example:
oracle.sysman.emSDK.sec.eus.DASHostUrl=http://my.dashost.com:7777 )
```

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.
4. Start the Management Service.

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.

2.1.12.1 Registering Enterprise Users as Enterprise Manager Users

After you have configured Enterprise Manager to use Enterprise Users, 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 Graphic User Interface
- Enterprise Manager Command Line Interface

2.1.12.1.1 Registering Enterprise Users Using the Graphical User Interface

You can use the graphical user interface 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.

2.1.12.1.2 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. For more details, refer to [Registering Single Sign-On Users Using EM CLI](#).

2.1.13 Restoring to Default Authentication Method

2.1.13.1 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.

2.1.13.2 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 12c Release 12.1.0.3.0
Copyright (c) 1996, 2013 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, 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, 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 user classes, roles, and privileges assigned to each user class.

2.2.1 Understanding Users, Privileges and Roles

When an Enterprise Manager administrator adds a user to the system, the first thought must be "what does this person need to do?" Once the job this new user must perform is understood, the Enterprise Manager administrator must then assign the appropriate privileges to and grant access only to those 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.

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.

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.

2.2.2 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.

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 12c 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..

2.2.3 Privileges and Roles

User 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 then creates 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 provides the minimum level of privileges required to allow administrators to perform their tasks within Enterprise Manager. For example, he 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.

2.2.3.1 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 privilege hierarchy the 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 2-3, "Target Privileges Applicable to Specific Targets"](#) for more information.
- VIEW: Lowest level permitting only view access to targets.

There are 2 types of target privileges:

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

The Target Privileges page shows a list of targets for which privileges can be granted.

Table 2–2 Target Privileges Applicable to All Targets

Display Name	Description	Internal Name	Included Privileges	Applicable Target types
Full any Target	Ability to do all operations on all the targets, including delete the target	FULL_ANY_TARGET	Operator any Target	
Execute Command as any Agent	Execute any OS Command as the Agent User at any Agent	PERFORM_OPERATION_AS_ANY_AGENT		Agent
Put File as any Agent	Put any File to any Agent's Filesystem as the Agent User	PUT_FILE_AS_ANY_AGENT		Agent
Execute Command Anywhere	Execute any OS Command at any Agent	PERFORM_OPERATION_ANYWHERE		Host
Operator any Target	Ability to perform administrative operations on all managed targets	OPERATOR_ANY_TARGET	View 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	VIEW_ANY_TARGET	Monitor Enterprise Manager	
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	CREATE_PROPAGATING_GROUP	Add any Target	
Add any Target	Add any target in Enterprise Manager	CREATE_TARGET		

Table 2–3 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 and manage target	CONNECT_TARGET	Connect Target Read-only	
Connect Target Readonly	Ability to connect to 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		
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	

Table 2–3 (Cont.) Target Privileges Applicable to Specific Targets

Display Name	Description	Internal Name	Included Privileges	Applicable Target types
Manage Target Metrics	Ability to edit threshold for metric and policy setting, apply monitoring templates, and manage User Defined Metrics	MANAGE_TARGET_METRICS		
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		

Resource: These privileges allow a user to perform operations against specific types of resources. The following table lists all available resource privileges.

Table 2–4 Resource Privileges

Resource Type	Privilege Name	Description	Privileges Required to Grant
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
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

Table 2–4 (Cont.) Resource Privileges

Resource Type	Privilege Name	Description	Privileges Required to Grant
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
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

Table 2–4 (Cont.) Resource Privileges

Resource Type	Privilege Name	Description	Privileges Required to Grant
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_DASH
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

Table 2–4 (Cont.) Resource Privileges

Resource Type	Privilege Name	Description	Privileges Required to Grant
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
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

Table 2–4 (Cont.) Resource Privileges

Resource Type	Privilege Name	Description	Privileges Required to Grant
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
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

Table 2–4 (Cont.) Resource Privileges

Resource Type	Privilege Name	Description	Privileges Required to Grant
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
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

Table 2–4 (Cont.) Resource Privileges

Resource Type	Privilege Name	Description	Privileges Required to Grant
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 Server (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
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

Table 2–4 (Cont.) Resource Privileges

Resource Type	Privilege Name	Description	Privileges Required to Grant
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
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_V_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

Table 2–4 (Cont.) Resource Privileges

Resource Type	Privilege Name	Description	Privileges Required to Grant
System	Super User	Provides all the privileges to any target in the system	SUPER_USER
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_DISC_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

2.2.3.2 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 task, 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"](#) on page 2-16.

Out-of-Box Roles: Enterprise Manager Cloud Control 12c 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.

Table 2–5 Out-of-the-Box Roles

Roles	Description
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, etc
EM_ALL_OPERATOR	Role has privileges to design Enterprise Manager operational entities such as Monitoring Templates, etc
EM_ALL_VIEWER	Role has privileges to view Enterprise Manager operations

Table 2–5 (Cont.) Out-of-the-Box Roles

Roles	Description
EM_BASIC_SUPPORT_REP	Role has privileges to provide basic support for Enterprise Manager
EM_CAP_ADMINISTRATOR	Change Activity Plan Role provides the ability to create, create-like, edit, delete and activate Change Activity Plans.
EM_CAP_USER	Change Activity Plan User Role provides the ability to view and manage Change Activity Plans.
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_DBREPLAY_OPERATOR	Role has privileges to administer Database Replay
EM_DBREPLAY_VIEWER	Role has privilege to view any reports in Database Replay.
EM_DB_SERVICE_SUPPORT_REP	Role has privileges to manage Database Service as support representative.
EM_FMW_SUPPORT_REP	Role has privileges to manage Java Services as support representative.
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 plugin lifecycle, managing self update, etc
EM_LINUX_PATCHING_ADMIN	Role has administration privileges in the Linux Patching area.
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
EM_PROXY_ADMINISTRATOR	Role has privileges to manage Proxy Settings for My Oracle Support and Agents.
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 Role: 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.

2.2.3.3 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.

2.2.4 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.

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 (Dev-Group) containing the relevant host targets. Then create a role (Dev-Role) and in this role include Operator privileges on Dev-Group. Finally grant the Dev-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 Dev-Group. As new host targets are added, you can simply add these new targets to Dev-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.

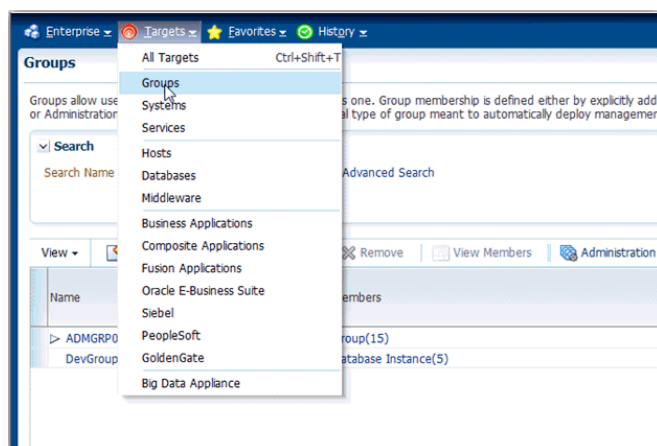
2.2.4.1 Example1: Granting various teams different levels of access to target groups

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.

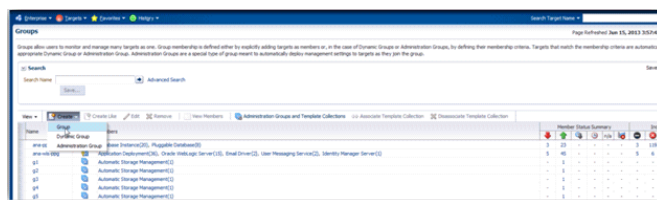
To manage privileges across the two teams, first create two privilege propagating groups containing the targets of the respective teams. For example, you can create a target group called DBAGroup containing the database Instances and another target group called WLSGroup containing the Oracle WebLogic 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.



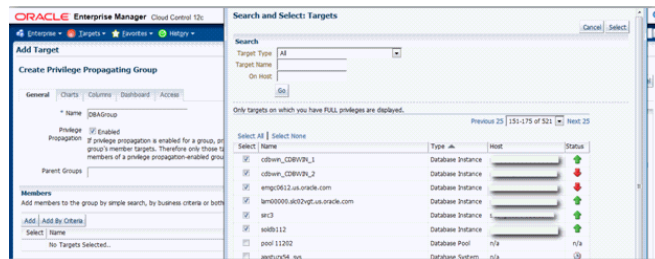
2. Click "Create" from the menu and select "Group" from the drop down menu.



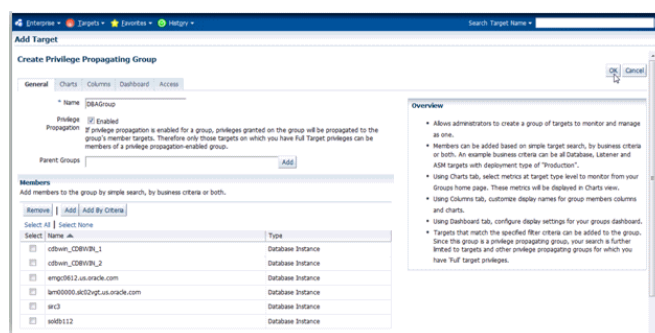
3. Enter the name DBAGroup.

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.

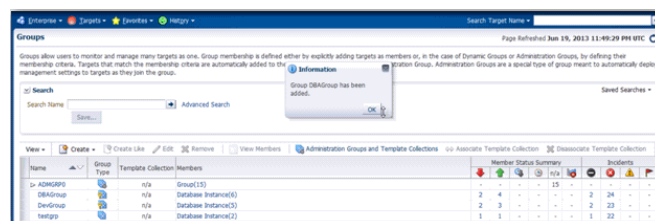
4. Add the database targets you want to add to the new database group, DBAGroup. This is done by hitting the "Add" button, selecting the Database Instance targets from the list. Hit the "Select" button.



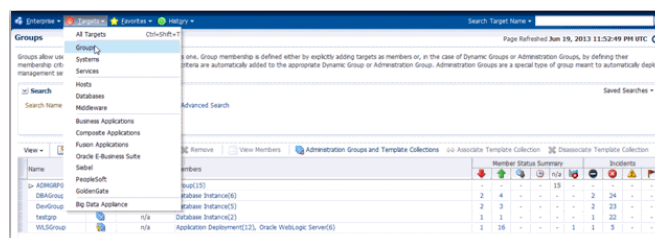
5. Select "OK".



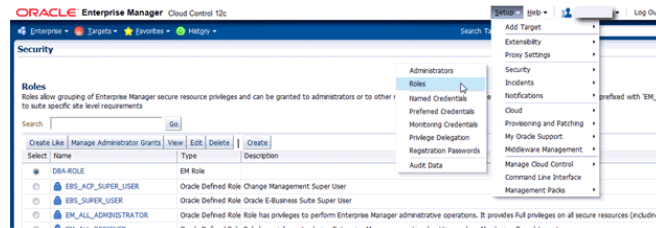
6. Your new group, DBAGroup, should be displayed in the list of available groups.



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.



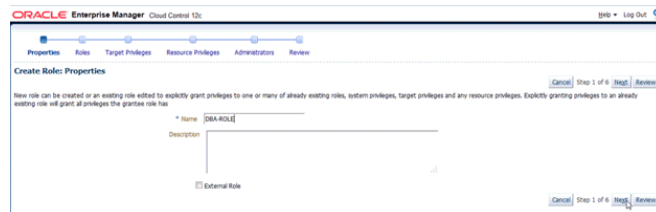
9. Next, create the Roles. A role contains privileges that can be granted to an administrator. Proceed to the Roles page. Go to the Setup->Security->Roles page. As in the snapshot below.



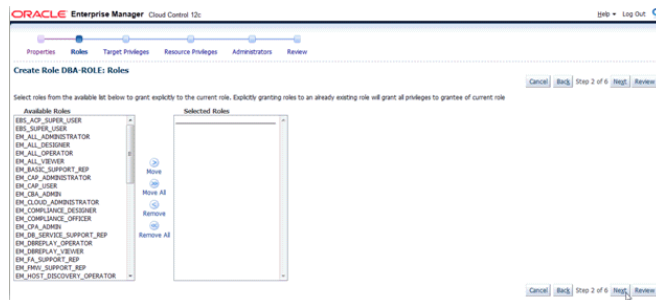
10. Click "Create" button.



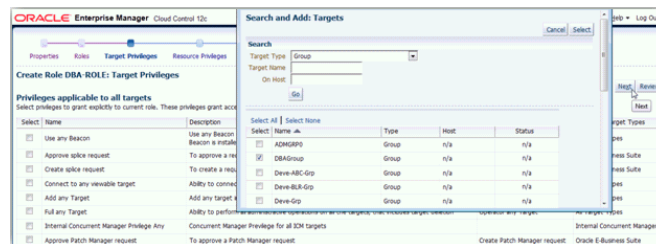
11. On the Properties page, type the name of your role. In this example we have named it DBA-ROLE. This Role will contain privileges for the DBA team. It will contain Full privilege on all database Instances in the DBAGroup and view privilege on all Web Logic Server Instances in the WLSGroup. Hit the "Next" button.



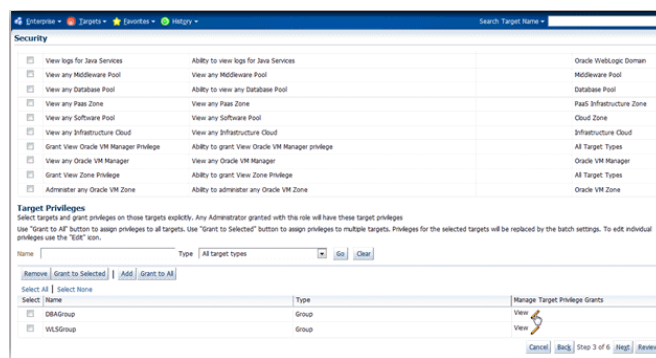
12. Click "Next" on the "Roles" page.



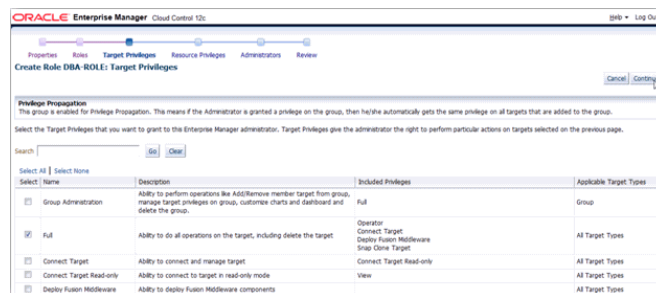
13. On the "Target Privileges" page, scroll down to the "Target Privileges" section, at the bottom of the page. Click the "Add" button. The list of available targets is displayed. Select the "Group" Target Type, to improve the search. Select the two groups we just created, DBAGroup and WLSGroup.



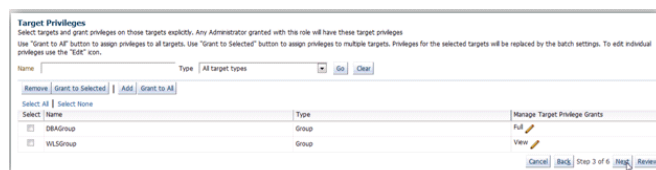
- Our two groups will be displayed. For this role, DBA-ROLE, we want to grant "Full" on all databases in the DBAGroup and grant "View" on all WebLogic server targets in the WLSGroup. As the default privilege is "View" we need only modify the DBAGroup privilege for this Role, leaving the WLSGroup, with the default "View" privilege. This is done by selecting the pencil icon, to the right of "View" in the "Manage Target Privilege Grants" column. Hit the "Continue" button.



- Click the privilege "Full", select the "Continue" button.



- The new privilege will be displayed. Select the "Next" button.



- Select the "Next" button on the Resource Privilege page.

Resource Type	Description	Privilege Grants Applicable to all Resources	Number of Resources with Privilege Grants	Manage Privilege Grants
Access	Defines the access to different application in Enterprise Manager Cloud Control	-	NA	
Application Performance Management	Application Performance Management allows users to manage business application service targets	-	NA	
Application Replay Entries	Application Replay Entries include captures, replay tasks, and history	-	NA	
Backup Configurations	Security Class for System Backup/Recovery Manager.	-	-	
Backup Status Report	Security Class for System Backup/Recovery status report	-	-	

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.

The screenshot shows the 'Create Role WLS-ROLE: Review' page in the Oracle Enterprise Manager Security console. The page is divided into several sections:

- Properties:** Name: WLS-ROLE. No description is defined for this role. External Role: NO.
- Roles:** A table with columns 'Name' and 'Description'. It shows 'No roles are granted.'
- Target Privileges:** A section for 'Privileges applicable to all targets' with a table showing 'No target resource type privileges are granted.'
- Target Privileges:** A table with columns 'Name', 'Type', and 'Manage Target Privilege Grants'. It lists 'DBAGroup' (Group) with 'View' and 'WLSGroup' (Group) with 'Full'.
- Resource Privileges:** A table with columns 'Resource Type', 'Description', 'Privilege Grants Applicable to all Resources', 'Number of Resources with Privilege Grants', and 'View Privilege Grants'. It shows 'No Privileges are granted explicitly.'
- Administrators:** A table with columns 'Name' and 'Description'. It lists 'ADMIN'.

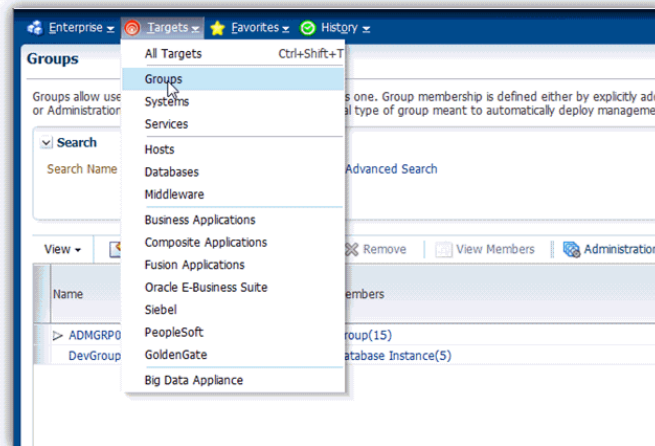
2.2.4.2 Example2: Granting developers view access to target database instances.

Datacenters would often like to provide application developers read-only access to database performance pages in Enterprise Manager in order for them to get firsthand information on the impact of their applications on the underlying database. The DBAs responsible for these databases want to grant these developers read-only access to these database performance pages and restrict them from doing 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.

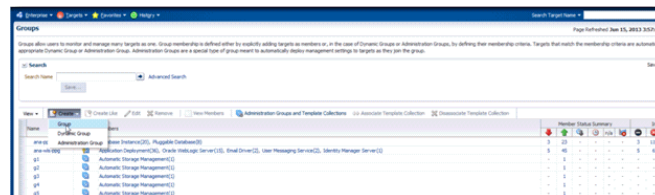
You can use the 'Connect Target Read-Only' privilege to enable read-only access to a target. To manage the granting of this privilege across many databases to a team of developers, you can create a privilege propagating group, and add the Database Instances to this target group, calling it, for example 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:

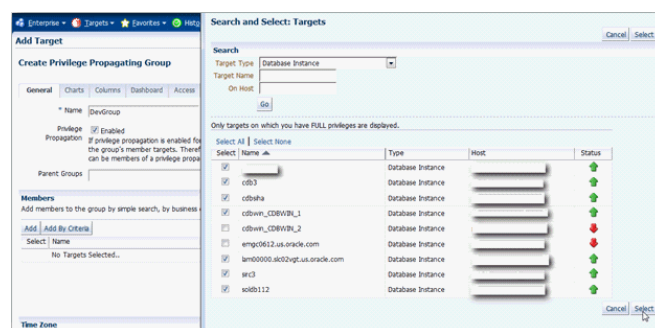
1. Create a group of targets. On the console go to Targets->Groups from the drop down menu.



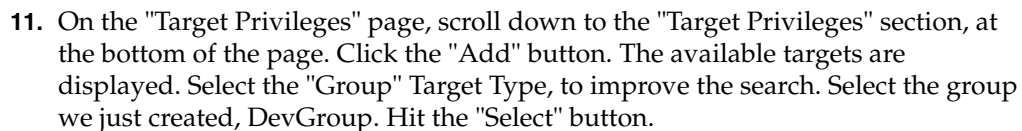
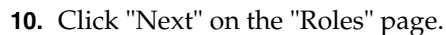
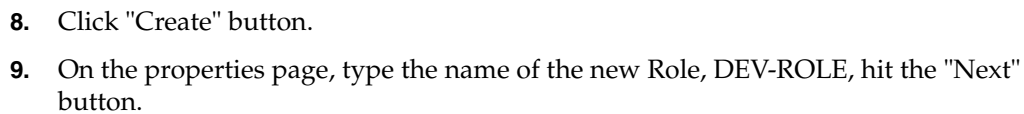
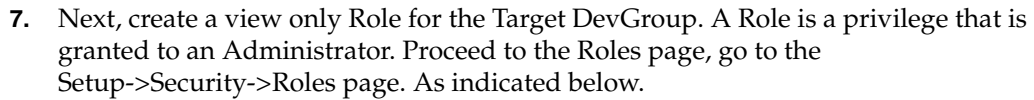
- Click "Create" and select "Group" from the drop down menu.

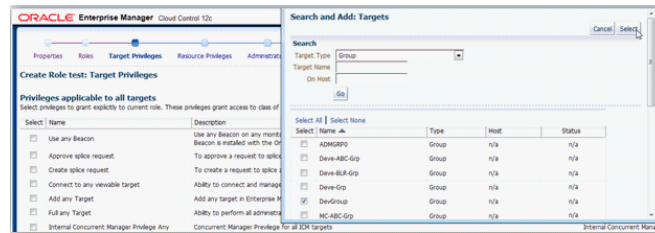


- Enter the name of your new target group, for this User Case we shall call it DevGroup.
- Enable "Privilege Propagation" group, by checking the box. This allows Administrators to do a one-time grant privileges on a group to a user and have that privilege be automatically propagated (or applied) to each 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.



- Select "OK".
- The new target group, DevGroup, is displayed in the list of available groups.





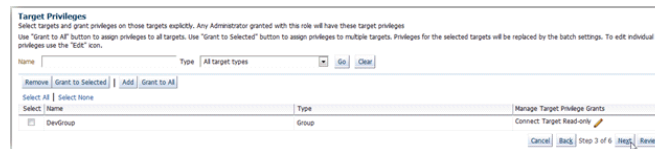
12. The target group is displayed. For this role, DEV-ROLE, we want to grant "Connect Target Read-Only" on all databases in the DevGroup. This is done by selecting the pencil icon, to the right of "View" in the "Manage Target Privilege Grants" column.



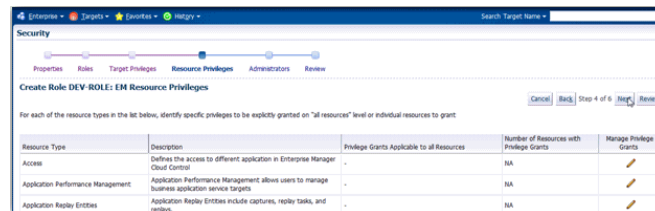
13. Click the privilege "Connect Target Read-Only", scroll to the bottom of the page. Select the "Continue" button.



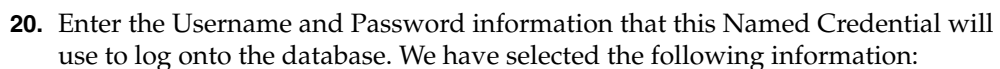
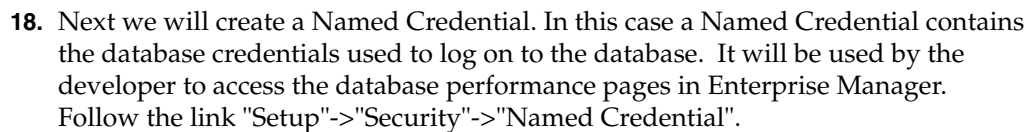
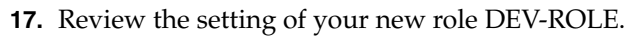
14. The new privilege is displayed. Select the "Next" button



15. Select the "Next" button on the Resource Privilege page.

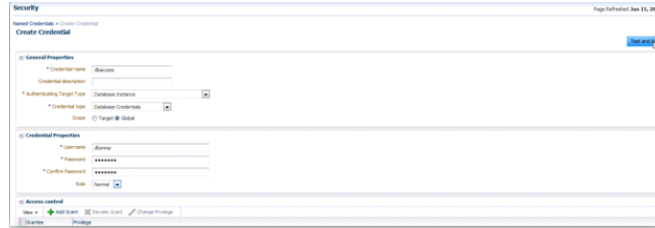


16. Select the Administrators you want to grant this role, DEV-ROLE too. Select the "Next" button.

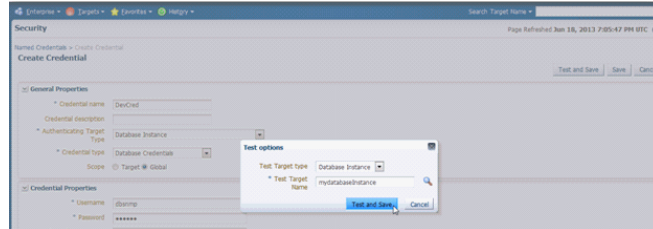


Authenticating Target Type: Database Instance -For this Use Case, we are interested in granting access to the development engineers the database Instances in the DevGroup.

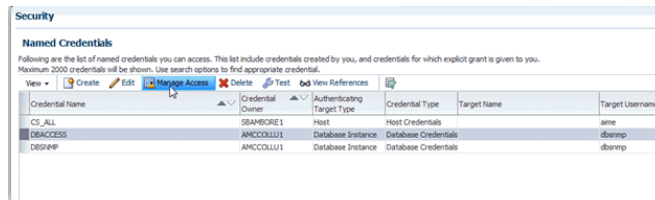
Scope: Global - For this User Case, this username and password will apply to every Database. Hit the "Test and Save" button.



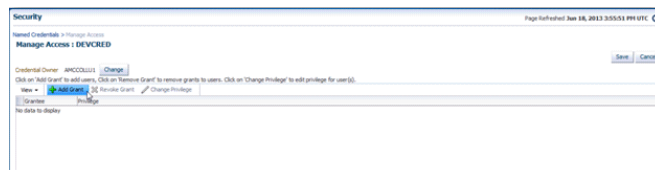
21. Enter a valid "Test Target Name", and hit the "Test and Save" button.



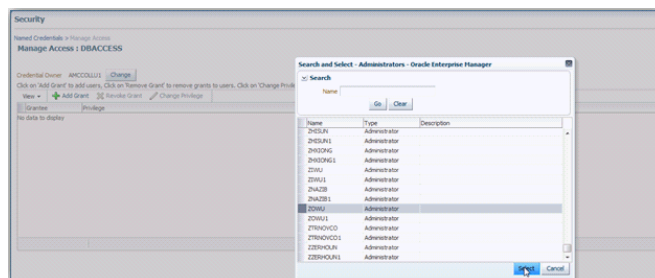
22. Our new Named Credential will be displayed. To Grant this Named Credential to one of the development Engineers, hit the "Manage Access" button.



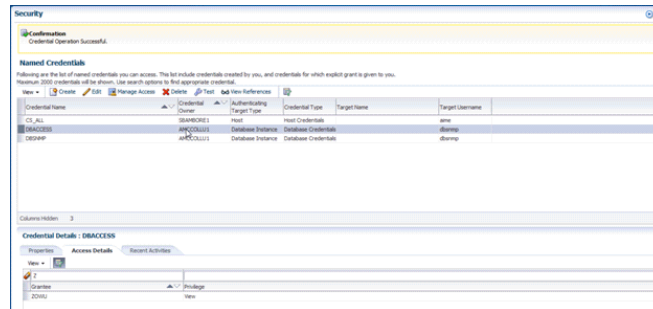
23. Hit the "Add Grant" button.



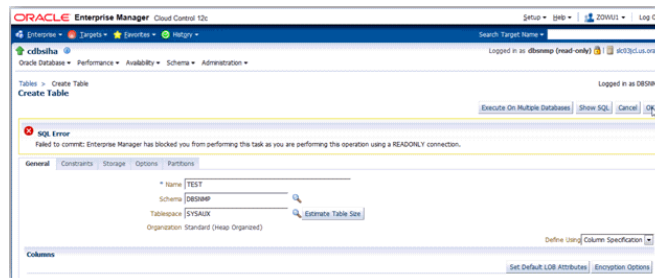
24. Select the Development Engineers you wish to use this Named Credential. Hit the "Select" button.



25. The User information will be 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 will be displayed in Enterprise Manager.



2.2.4.3 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.

Figure 2–5 Entitlement Summary Page

Entitlement Summary Page Refreshed May 15, 2013 9:06:07 PM UTC

This page summarizes administrator access to targets and other secure resources such as Jobs and Named Credentials. This access is provided by privileges and/or roles granted to the administrator. All secure objects owned by the administrator are also listed.

Administrator

User Name:

External User ID:

Email Address:

Contact:

Location:

Department:

Cost Center:

Line of Business:

Description: Super Administrator Yes

Targets

Target Privileges give the Administrator the right to perform particular actions on targets. The table below shows the list of targets owned, privileges granted across all targets or by target type, and privileges granted to specific targets.

Owned Targets

Target Name:

Name	Type
ADMGRP0	Group
MC-Aust-Grp	Group
Prod-Aust-Grp	Group
Test-Grp	Group
Prod-Grp	Group
Stag-Grp	Group
MC-Grp	Group
Prod-RC-Grp	Group
Stag-RC-Grp	Group
Test-RC-Grp	Group
MC-RC-Grp	Group

Row count: 16

Resource Summary

The table below shows all secure resources to which the Administrator has access.

Name	Description	Owned Resources	Resource Type Privileges	Resource Privileges
Named Credential	Credentials to perform Enterprise Manager Administrative Operations	0	0	1
Template	Template is collective settings of thresholds and collection schedule of metrics for a target type that can be applied to multiple targets	1	0	0
Template Collection	Template Collections are sets of Monitoring Template, Compliance Standard and/or Cloud Policies that are applied to targets.	2	0	0

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: *Oracle® Database 2 Day + Security Guide* for an overview of Public Key Infrastructure features, such as digital certificates and public keys

- 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 12c Release 3
Copyright (c) 1996, 2013 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 2–1 Sample Output of the emctl secure oms Command

```
$ emctl secure oms
Oracle Enterprise Manager Cloud Control 12c Release 3
Copyright (c) 1996, 2013 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://slbhost: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://slbost:slb_upload_port/em
```

2.3.2.2 Enabling Security with Multiple Management Service Installations

As you have already established at least one Agent Registration Password and a Root Key in your Management Repository, they must be used for your new Management Service. Your secure Management Agents can then operate against either Management Service.

All the registration passwords assigned to the current Management Repository are listed on the Registration Passwords page in the Oracle Enterprise Manager 12c Cloud Control console.

If you install a new Management Service that uses a new Management Repository, the new Management Service is considered to be a distinct enterprise. There is no way for the new Management Service to partake in the same security trust relationship as another Management Service that uses a different Management Repository. Secure Management Agents of one Management Service will not be able to operate against the other Management Service.

2.3.2.3 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 2-2 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 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
```

Creating CA... Started.
Successfully created CA with ID 2

Example 2-3 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
```

2.3.2.3.1 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>]
```

2.3.2.4 Viewing the Security Status and OMS Port Information

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

Example 2-4 emctl status oms -details

```
Oracle Enterprise Manager Cloud Control 12c Release 3
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
Console Server Host : mymachine.oracle.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.oracle.com:5416/em
Upload URL: https://mymachine.oracle.com:4473/empbs/upload

WLS Domain Information
Domain Name : EMGC_DOMAIN
Admin Server Host : mymachine.oracle.com
Admin Server HTTPS Port: 7022
```

Admin Server is RUNNING

Managed Server Information

Managed Server Instance Name: EMGC_OMS1

Managed Server Instance Host: mymachine.oracle.com

WebTier is Up

Oracle Management Server is Up

2.3.2.5 Configuring Transport Layer Security

The Oracle Management Service can be configured in the following modes:

- **TLsv1-only mode:** To configure the OMS to use only TLsv1 connections, do the following:
 1. Stop the OMS by entering the following command:

```
<OMS_ORACLE_HOME>/bin/emctl stop oms
```
 2. Enter the following command:

```
emctl secure oms -protocol TLsv1
```
 3. Append `-Dweblogic.security.SSL.protocolVersion=TLsv1` to `JAVA_OPTIONS` in `<Domain_Home>/bin/startEMServer.sh`/`<sh/cmd>`. If this property already exists, update the value to TLsv1. Use `startEMServer.sh` or `startEMServer.cmd` depending on your platform.
 4. Restart the OMS with the following command:

```
<OMS_ORACLE_HOME>/bin/emctl start oms
```
- **SSLv3 Only Mode:** To configure the OMS to accept SSLv3 connections only, do the following:
 1. Stop the OMS by entering the following command:

```
<OMS_ORACLE_HOME>/bin/emctl stop oms
```
 2. Enter the following command:

```
emctl secure oms -protocol SSLv3
```
 3. Append `-Dweblogic.security.SSL.protocolVersion=SSL3` to `JAVA_OPTIONS` in `Domain_Home/bin/startEMServer.sh` or `startEMServer.cmd` on Windows. If this property already exists, update the value to SSL3.
 4. Restart the OMS with the following command:

```
<OMS_ORACLE_HOME>/bin/emctl start oms
```
- **Mixed Mode:** To configure the OMS to use both SSLv3 and TLsv1 connections, do the following:
 1. Stop the OMS by entering the following command:

```
<OMS_ORACLE_HOME>/bin/emctl stop oms
```
 2. Enter the following command:

```
emctl secure oms
```

3. Append `-Dweblogic.security.SSL.protocolVersion=ALL` to `JAVA_OPTIONS` in `Domain_Home/bin/startEMServer.sh`. If this property already exists, update the value to `ALL`.
4. Restart the OMS with the following command:


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

Note: By default, the OMS is configured to use the Mixed Mode. To configure the Management Agent in TLSv1 only mode, set `allowTLSOnly=true` in the `emd.properties` file and restart the Agent.

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 2-5](#) 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 2-5 Sample Output of the `emctl secure agent` Utility

```
emctl secure agent
Oracle Enterprise Manager 12c Release 3 Cloud Control.
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
Securing agent... Started
Securing agent... Successful.
```

Example 2-6 Sample Output of the `emctl status agent secure` Command

```
$ emctl status agent -secure
Oracle Enterprise Manager Cloud Control 12c Release 3
Copyright (c) 1996, 2013 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.oracle.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.'

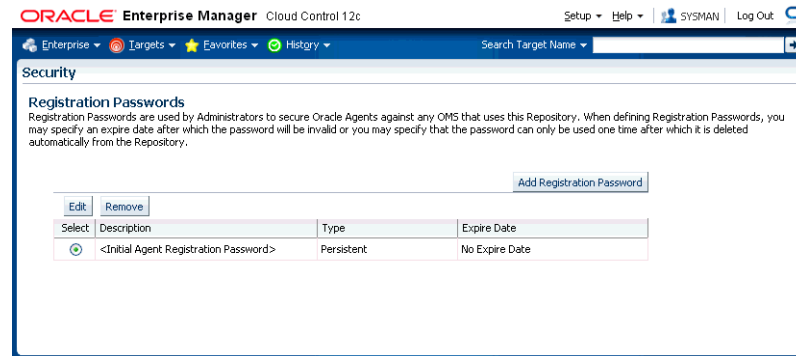
2.3.4.1 Using the Cloud Control Console to Manage Agent Registration Passwords

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 ([Figure 2-6](#)). 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.

Figure 2–6 Managing Registration Passwords in the Cloud Control Console



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. Change directory to the following location in the Management Service home:

```
<OMS_ORACLE_HOME>/bin
```

3. 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]
```

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

```
cd <OMS_ORACLE_HOME>/bin
```

```
emctl start oms
```

5. 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"

6. 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!
```

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
```

Example 2-7 Sample Output of the emctl secure lock Command

```
emctl secure lock
Oracle Enterprise Manager 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 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 2-8 Sample Output of the emctl secure unlock Command

```
emctl secure unlock
Oracle Enterprise Manager 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 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
```

Note: The Oracle Management Service is locked (both console & upload) by default beginning with Enterprise Manager 12c.

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 2–6 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 Management Service and Management Repository.</p> <p>Possible values are TRUE and FALSE. The default value is TRUE.</p> <p>For example:</p> <pre>emctl set property -name 'oracle.sysman.emrep.dbConn.enab leEncryption' -value 'true'</pre>
oracle.net.encryption_client	<p>Defines the Management Service encryption requirement.</p> <p>Possible values are REJECTED, ACCEPTED, REQUESTED, and REQUIRED.</p> <p>The default value is REQUESTED. In other words, 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.</p> <p>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>
oracle.net.crypto_checksum_types_client	<p>This property defines the different types of checksums algorithms the client supports.</p> <p>Possible values should be listed within parentheses. The default value is (MD5).</p> <p>For example:</p> <pre>oracle.net. crypto_checksum_types_client= (MD5)</pre>

3. 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:

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

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

2. 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*.

3. 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/ca1cert.cer, /scratch/ca2cert.cer, /scratch/ca3cert.cer

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 wallet>
```

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..

2.3.7.4 Configuring Transport Layer Security

The Oracle Management Service can be configured in the following modes:

- **TLSv1-only mode:** To configure the OMS to use only TLSv1 connections, do the following:

1. Stop the OMS by entering the following command:

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

2. Enter the following command:

```
emctl secure oms -protocol TLSv1
```

3. Append `-Dweblogic.security.SSL.protocolVersion=TLS1` to `JAVA_OPTIONS` in `Domain_Home/bin/startEMServer.sh/cmd`. If this property already exists, update the value to TLS1.
4. Restart the OMS with the following command:

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

- **SSLv3 Only Mode:** To configure the OMS to use SSLv3 connections only, do the following:

1. Stop the OMS by entering the following command:

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

2. Enter the following command:

```
emctl secure oms -protocol SSLv3
```

3. Append `-Dweblogic.security.SSL.protocolVersion=SSL3` to `JAVA_OPTIONS` in `Domain_Home/bin/startEMServer.sh` or `startEMServer.cmd` on Windows. If this property already exists, update the value to `SSL3`.

4. Restart the OMS with the following command:

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

- **Mixed Mode:** To configure the OMS to use both SSLv3 and TLSv1 connections, do the following:

1. Stop the OMS by entering the following command:

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

2. Enter the following command:

```
emctl secure oms
```

3. Append `-Dweblogic.security.SSL.protocolVersion=ALL` to `JAVA_OPTIONS` in `Domain_Home/bin/startEMServer.sh`. If this property already exists, update the value to `ALL`.

4. Restart the OMS with the following command:

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

Note: By default, the OMS is configured to use the Mixed Mode. To configure the Management Agent in TLSv1 only mode, set `allowTLSOnly=true` in the `emd.properties` file and restart the Agent.

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 <SLB 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>.
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.
cert_validity	The number of days for which the self-signed certificate is valid. The valid range is between 1 to 3650.

Parameter	Description
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 Apache's SSLProtocol directive. Note: The key_strength and cert_validity parameters are applicable only when the -wallet 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

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 wallet>
```

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 1

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 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.

2.5 Configuring and Using Target Credentials

The following topics are discussed in this section:

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

2.5.1 Credential Subsystem

Credentials like user names and passwords are typically required to access targets such as databases, application servers, and hosts.

Figure 2–7 Named Credentials Page

Credentials are encrypted and stored in Enterprise Manager. Beginning with Enterprise Manager 12c, 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 Manger 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 Credential](#)
- [Monitoring Credentials](#)
- [Preferred Credentials](#)

2.5.1.1 Named Credential

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. Named credentials permit the following:

- Named credentials can be used across the product.
- Define references
- Because they use a centralized store, password management is simplified.

Named credentials can be a username/password, or a public key-private key pair. An Enterprise Manager administrator can then use the named credential for performing operations like 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.

Typical Scenarios for using Named Credentials

- In datacenters 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 datacenters 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 12c: 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

There are two categories of named credentials:

- **Global Named Credential**

A global named credential is an entity, which is not associated with any Enterprise Manager object. Global named credentials consist of the authentication scheme along with any authentication parameters. Because these are independent entities,

an Enterprise Manager administrator can associate these credentials with objects at a later time.

- **Target Named Credentials**

Target named credential is an entity which are associated with individual targets at the time of creation. This entity will also contain authentication scheme along with authentication parameters for a specific target.

Access Control

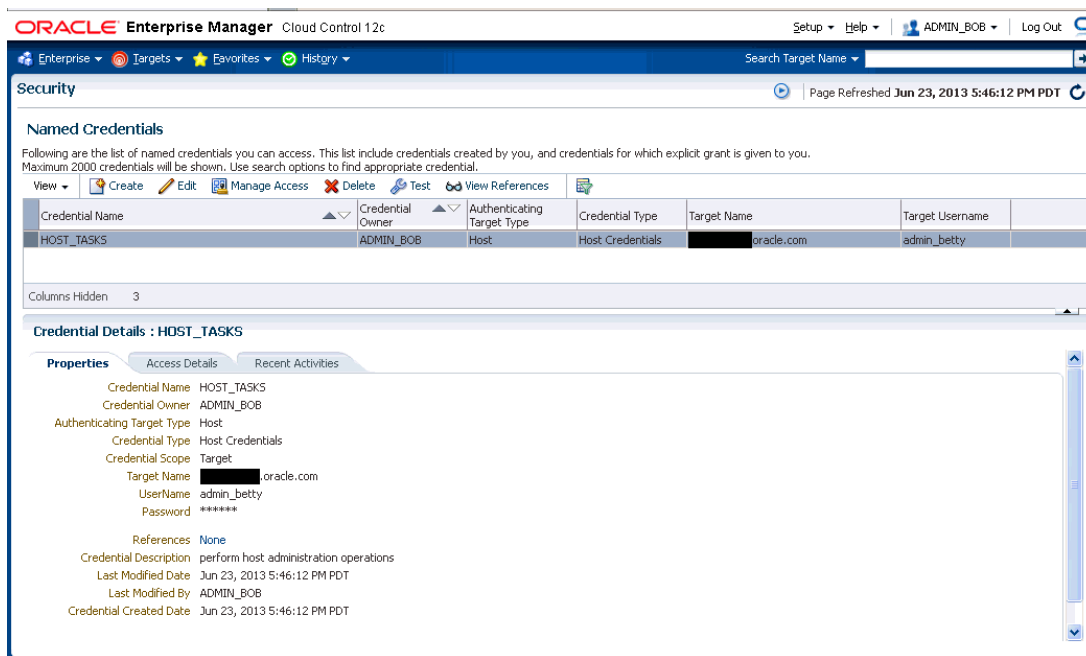
The owner of the named credential can share access to the credentials by granting them the appropriate level of privileges. The following privilege levels are available for all credentials:

- **VIEW:** Administrators with VIEW privilege on a credential will also be able to use the credentials for running jobs, patching and other system management operations within Enterprise Manager. An administrator with VIEW privileges on other administrator's credentials will be able to view the structure and username of the credential. Sensitive information of the credential such as the password will never be shown.
- **EDIT:** Allows an Enterprise Manager administrator to change a sensitive information such as the password, or the public/private key pair of the credential. The administrator can change both the Authentication Scheme of the credential as well as the username for the credential. The authenticating target type cannot be changed.
- **FULL:** Allows an Enterprise Manager administrator to change the credential username, sensitive information such as the password or the public/private key pair, and authentication scheme. An administrator with FULL privilege on a named credential will be able to delete the named credential.

Creating Named Credentials

To create or edit a named credential, from the **Setup** menu, choose **Security** and then **Named Credential**. Note: You need *Named Credential* resource privilege to create named credentials.

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. The Named Credential page displays as shown in the following figure.

Figure 2–8 Named Credentials Page

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.

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 credentials adhere to the following rules:

- Only credential owners can grant privileges on named credentials they have created to other users.
- Enterprise Manager Super Administrators cannot obtain any privileges on a newly created credential until he is explicitly granted privileges on the credential object.
- Enterprise Manager administrators, regardless of privilege level, cannot see the sensitive fields such as passwords and private keys from the console UI.
- Credentials 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 administrator cannot view other administrators' credentials unless an explicit grant is provided. Even Enterprise Manager Super Administrators cannot view other users' credentials.

- Any Enterprise Manager administrator can create his own credentials and have FULL privileges on the credentials owned.

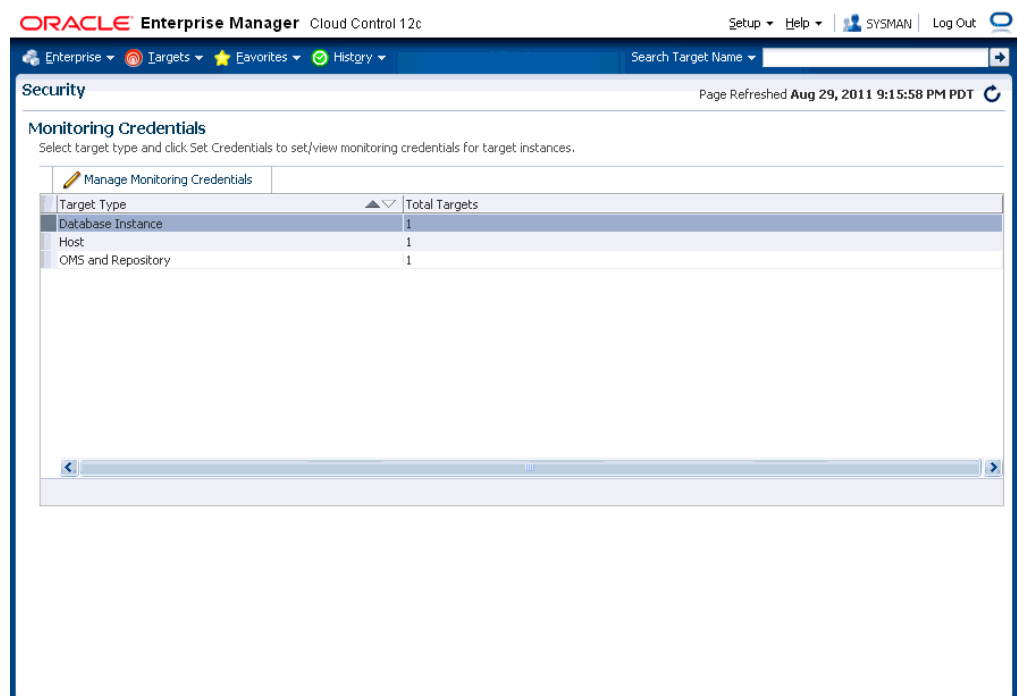
All the credentials owned by an Enterprise Manager administrator will be deleted if that administrator is deleted from Enterprise Manager. Since access to shared credentials is not automatically granted to Super Administrators, re-assigning named credentials belonging to a regular Enterprise Manager administrator by a Super Administrator is not allowed.

2.5.1.2 Monitoring Credentials

These credentials are used by the Management Agent to monitor certain types of targets. For example, most database monitoring involves connecting to the database, which requires a username, password, and optionally, a role. Monitoring credentials, if stored in the repository, can also be potentially used by management applications to connect directly to the target from the OMS.

To create or edit a monitoring credentials, from the **Setup** menu, choose **Security** and then **Monitoring Credentials**. The Monitoring Credentials page displays as shown in the following figure.

Figure 2–9 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.

2.5.1.3 Preferred Credentials

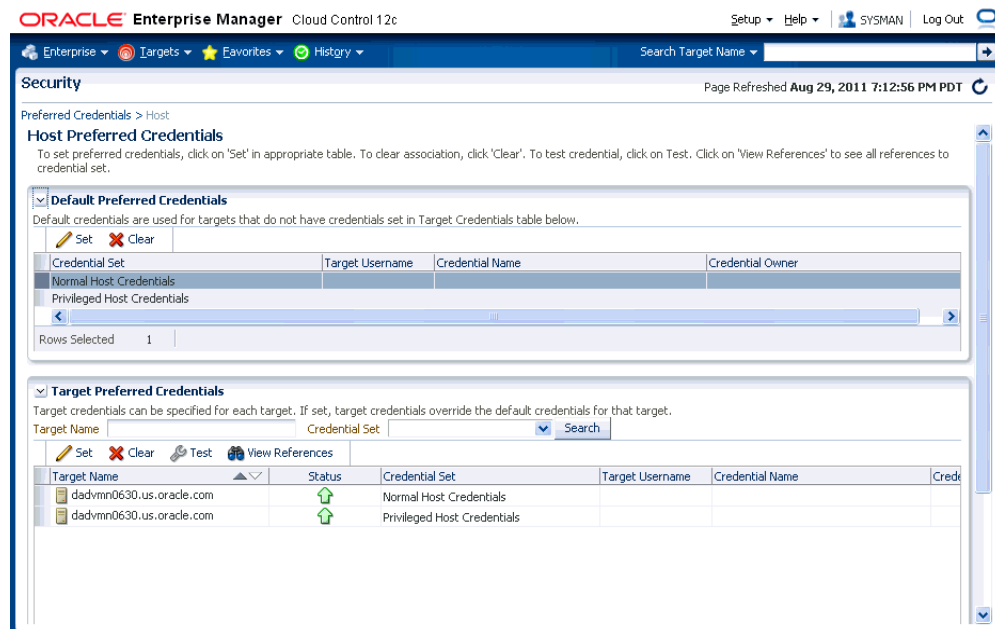
Preferred credentials are used to simplify access to managed targets by storing target login credentials in the Management Repository. With preferred credentials set, users

can access an Enterprise Manager target that recognizes those credentials without being prompted to log in to the target. Preferred credentials can also be used to carry out administrative operations using the job system. Preferred credentials are set on a per user basis, thus ensuring the security of the managed enterprise environment.

- **Default Credentials:** Default credentials can be set for a particular target type and will be available for all the targets of the target type. It will be overridden by target preferred credentials.
- **Target Credentials:** Target credentials are preferred credentials set for a particular target. They could be used by applications such as the job system, notifications, or patching. For example, if the user chooses to use preferred credentials while submitting a job, then the preferred credentials set for the target (target credentials) will be used. If the target credentials are not present, the default credentials (for the target type) will be used. If the default credentials are not present, the job will fail. If not specified, by default, 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.

Figure 2–10 Host Preferred Credentials



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

2.5.1.4 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"] "
```

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

2.5.1.5 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](#)
- [Authenticating host credentials](#)
- [Configuring the PAM "emagent" Service](#)
- [Sudo and PowerBroker Support](#)
- [Creating a Privilege Delegation Setting](#)
- [Sudo and Powerbroker Configuration](#)
- [Updating the PDP Configuration File](#)

2.5.1.5.1 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 via the SSH client on the host to perform the requested operations.

2.5.1.5.2 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.

Example 2–9 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
```

\$

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.

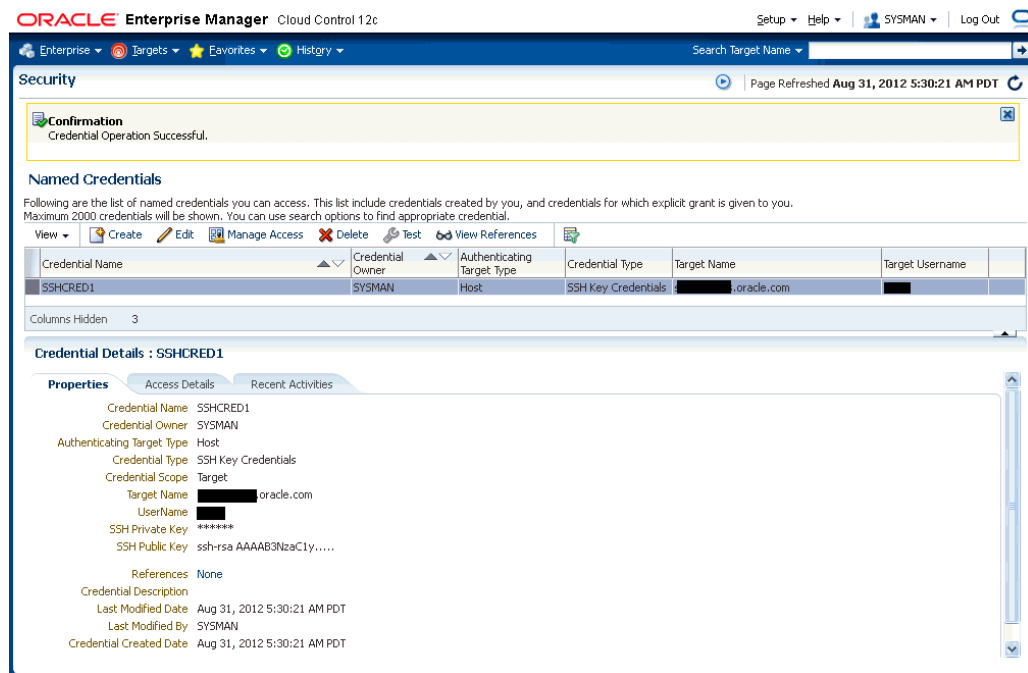
Note: The SSHCRED1 credential set will be used in [Section 2.5.1.5.3, "Setting Up Host Preferred Credentials Using SSH Key Credentials"](#)

4. Select **Host** from the **Authenticating Target Type** drop-down menu.
5. Select **SSH Key Credentials** from the **Credential Type** drop-down menu as shown in the following figure.

6. Ensure that the SSH private key/public key files have been copied to the host on which the browser is running.
7. From the **Credential Properties** region, click **Browse** for **Public Key** and **Private Key** to upload the generated public key/private key files.
8. Click **Test and Save** to verify the credentials and save them. The new named credential will appear as shown in the following figure.

Note: To view an instructional video Oracle Enterprise Manager 12c: 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

Figure 2–11 Named Credential Using SSH Keys

2.5.1.5.3 Setting Up Host Preferred Credentials Using SSH Key Credentials 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
-suggested_cred_types=HostSSHCreds
```

Credential set "HostSSHCredSet" created successfully.

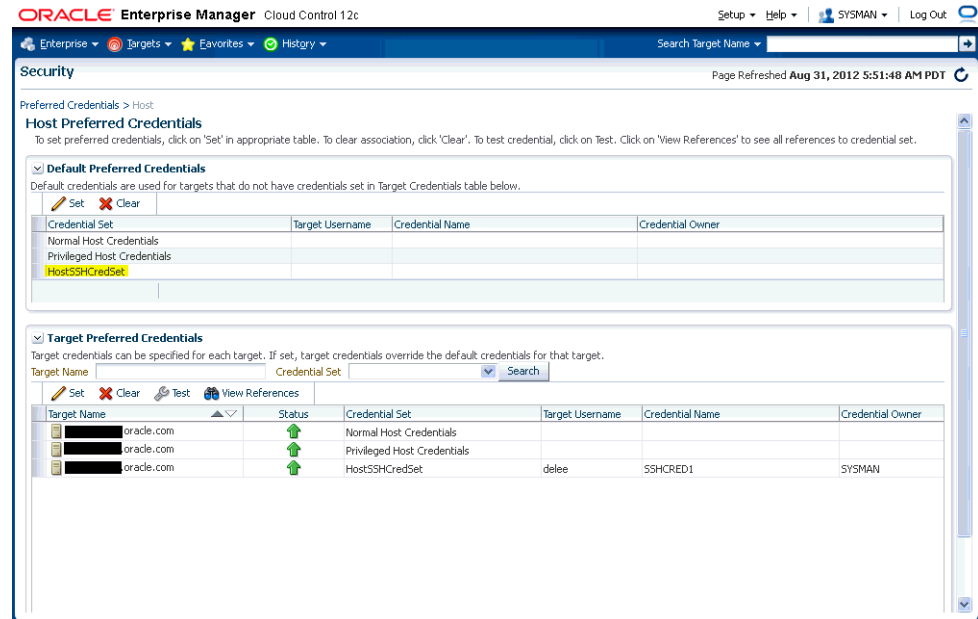
Once the credential set is created, Enterprise Manager administrators can set up preferred credentials for this newly created credential set using either EM CLI or the Enterprise Manager console.

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

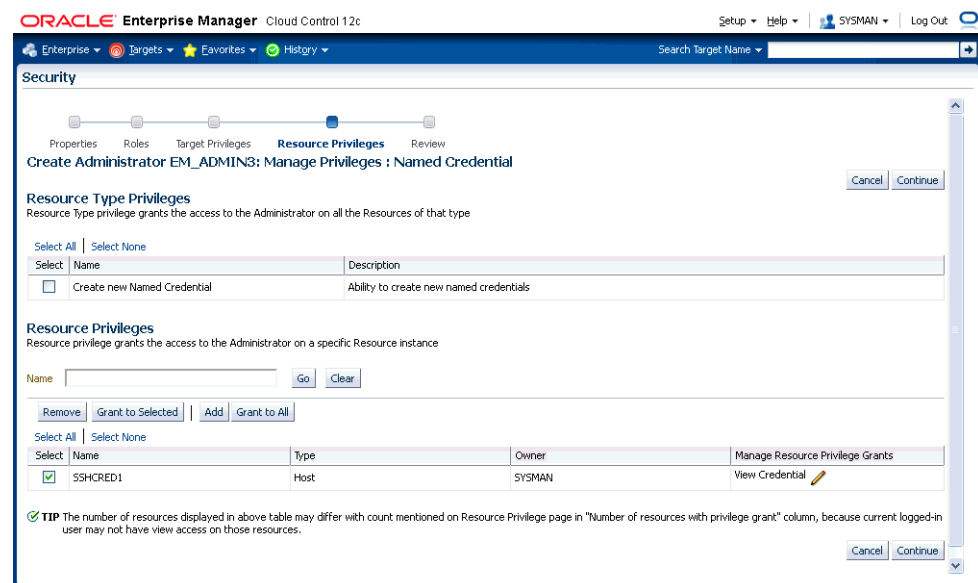
```
$ emcli set_preferred_credential -target_type=host -target_
name=myhost.oracle.com -set_name=HostSSHCredSet -credential_name=SSHCRED1
```

Successfully set preferred credentials for target myhost.oracle.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.



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. The following graphic shows the *manage privilege grants* UI for named credentials.



2.5.1.5.4 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/netsvc.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.

2.5.1.5.5 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 that 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 emagent 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.

2.5.1.5.6 Sudo and PowerBroker Support

Privilege delegation allows a logged-in user to perform an activity with the privileges of another user. Sudo and PowerBroker are privilege delegation tools that allow a logged-in user to be assigned these privileges. Typically, the privileges that are granted to a specific user are administered centrally. For example, the sudo command can be used to run a script that requires root access:

```
sudo -u root root.sh
```

In the invocation of sudo in the example above, an administrator can use the sudo command to run a script as root provided he has been granted the appropriate privileges by the system administrator. Enterprise Manager preferred credentials allow you to use two types of privilege delegation tools: Sudo and PowerBroker. You can use EM CLI or the Manage Privilege Delegation Settings page to set/edit privilege delegation settings for a host. See the *Enterprise Manager Command Line Interface* guide for more information on using the command line.

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 file /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.

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.

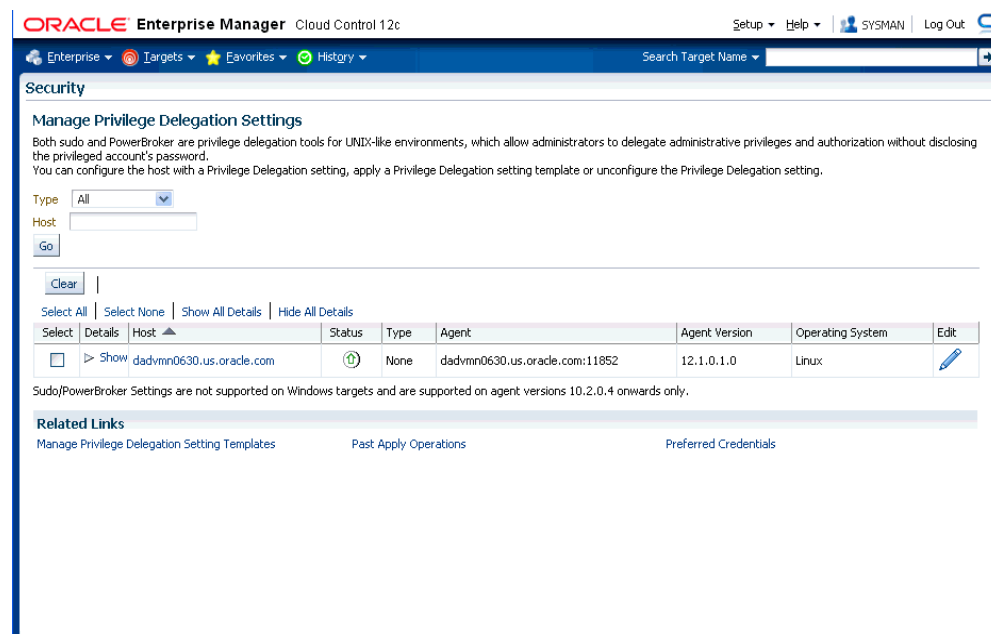
2.5.1.5.7 Creating a Privilege Delegation Setting Enterprise Manager allows you to create privilege delegation settings either by creating the setting directly on a host target, or by creating a Privilege Delegation Setting Template that you can apply to multiple hosts.

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 following screen is displayed:

Figure 2–12 Manage Privilege Delegation Settings



2. For any host target appearing in the table, click **Edit**. Enterprise Manager takes you to the Host Privilege Delegation Setting page.
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 **Update** to apply the settings to the host. The following figure shows the Host Privilege Delegation Setting window that you can use to create a PowerBroker setting.

Figure 2–13 Host Privilege Delegation Setting - PowerBroker

The screenshot shows the Oracle Enterprise Manager Cloud Control 12c interface. The breadcrumb trail is: Enterprise > Targets > Favorites > History > dadvmn0630.us.oracle.com > Manage Privilege Delegation Settings. The page title is "Host Privilege Delegation Setting : dadvmn0630.us.oracle.com". Below the title, there is a message: "You can configure the host with a Privilege Delegation setting or unconfigure the Privilege Delegation setting for this host." There are three radio buttons: "None", "Sudo", and "PowerBroker". The "PowerBroker" radio button is selected. Below the radio buttons, there is a "Settings" section with a "PowerBroker Password Prompt" label and a text input field. Below the text input field, there is a label "* PowerBroker command." and a text input field. Below the text input field, there is a note: "For eg. /usr/bin/pbrun -l -u %RUNAS% %COMMAND%". To the right of the "Settings" section, there is a "Parameters" section with a table. The table has two columns: "Name" and "Description". The table contains the following rows:

Name	Description
%COMMAND%	PowerBroker command.
%PROFILE%	Use this profile to run the command.
%RUNAS%	Run the command as this user.
%USERNAME%	Name of the user running the command.

At the bottom right of the "Parameters" section, there are "Cancel" and "Update" buttons.

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**.

2.5.1.5.8 Sudo and Powerbroker Configuration Enterprise Manager uses a trust-based model that permits specification of responsibilities with a high degree of granularity. Administrators can set up sudo or pbrun configuration entries to assign specific Enterprise Manager functional privileges to their OS users. The Management Agent executable nmosudo allows administrators to configure sudo/pbrun such that a less privileged user can 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, as shown in the examples below, 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 above, 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.

Sample entries for the sudo configuration file (/etc/sudoers) are shown below:

```
# Sample sudoersfile should have following entry

# If you do not have access to oracle and root accounts,
# then add the following entries into the file:

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

```
# 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, johndoe refers to the user who has been given the  
# SUDO access to Oracle and Root accounts for running  
# the nmosudo command.
```

A sample PowerBroker configuration file (/etc/pb.conf) would be:

```
if(user=="johndoe") if(command=="/u01/oracle/agent/sbin/nmosudo" )  
// /u01/oracle/agent/ is the Agent Home  
{  
  switch (requestuser  
  {  
    case "root":  
      runuser="root";  
      break;  
    case "oracle":  
      runuser="oracle";  
      break;  
    default:  
      reject;  
    }  
  }  
  accept;  
}
```

Refer to sudo/PowerBroker documentation for detailed configuration information.

2.5.1.5.9 Updating the PDP Configuration File The Management Agent uses nmosudo to run *Trusted Jobs* in Enterprise Manager. For PDP configuration settings, you should enter the location of nmosudo in your configuration file.

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 above, 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) and above, you must modify the PDP configuration files to update the new location of nmosudo.

For example, if you use SUDO as your PDP, the configuration file for sudo is typically /etc/sudoers. In this file, update the following entry with the new location to nmosudo.

```
sudouser ALL : oracle /eminstall/basedir/sbin/nmosudo *
```

2.6 Configuring and Using Cryptographic Keys

To protect the integrity of sensitive data in Enterprise Manager, a signing on 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.

2.6.1 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 2-10 emctl start oms Command

```
Oracle Enterprise Manager 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 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.
```

2.6.2 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 -copy_to_repos [-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_conn_desc <conn desc>) -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd <pwd>] -emkey_file <emkey file>`

2.6.2.1 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.

Example 2–11 emctl status emkey - Example 1

```
Oracle Enterprise Manager 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 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"
```

- When the emkey has been correctly configured in the Credential Store and has been removed from the Management Repository, the following message is displayed.

Example 2–12 emctl status emkey - Example 2

```
Oracle Enterprise Manager 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
The EMKey is configured properly.
```

- 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 3

```
Oracle Enterprise Manager 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 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"
```

2.6.2.2 emctl config emkey -copy_to_credstore

This command copies the emkey from the Management Repository to the Credential Store.

Example 2–14 Sample Output of the emctl config emkey -copy_to_credstore Command

```
emctl config emkey -copy_to_credstore [-sysman_pwd <pwd>]
Oracle Enterprise Manager 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
The EMKey has been copied to the Credential Store.
```

2.6.2.3 emctl config emkey -copy_to_repos

This command copies the emkey from the Credential Store to Management Repository.

Example 2–15 Sample Output of the `emctl config emkey -copy_to_repos` Command

```
emctl config emkey -copy_to_repos [-sysman_pwd <pwd>]
Oracle Enterprise Manager 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 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".
```

2.6.2.4 `emctl config emkey -copy_to_file_from_credstore`

This command copies the emkey from the Credential Store to a specified file.

Example 2–16 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 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
The EMKey has been copied to file.
```

2.6.2.5 `emctl config emkey -copy_to_file_from_repos`

This command copies the emkey from the Management Repository to a specified file.

Example 2–17 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 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 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.

2.6.2.6 `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 2–18 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 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
The EMKey has been copied to the Credential Store.
```

2.6.2.7 `emctl config emkey -copy_to_repos_from_file`

This command copies the emkey from a specified file to the repository.

Example 2-19 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_conn_desc <conn_desc>) -repos_user <username> [-repos_pwd
<pwd>] [-admin_pwd <pwd>] -emkey_file <emkey_file>
Oracle Enterprise Manager 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 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".
```

2.6.2.8 emctl config emkey -remove_from_repos

This command removes the emkey from the repository.

Example 2-20 Sample Output of `emctl config emkey -remove_from_repos` Command

```
emctl config emkey -remove_from_repos [-sysman_pwd <pwd>]
Oracle Enterprise Manager 12c Release 3 Cloud Control
Copyright (c) 1996, 2013 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.

2.6.3 Install and Upgrade Scenarios

This section explains the install and upgrade scenarios for emkey.

2.6.3.1 Installing the Management Repository

A new emkey is generated as a strong random number when the Management Repository is created.

2.6.3.2 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).

2.6.3.3 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: emkey needs to be copied to the Management Repository before starting the upgrade. After all 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
```

2.6.3.4 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.

2.7 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.

For Enterprise Manager 12c, 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 Manager 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

2.7.1 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.

2.7.2 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.

2.7.3 Updating the Audit Settings

The `update_audit_settings` command updates the current audit settings in the repository and restarts the Management Service.

Example 2-21 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)"
```

- `-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.

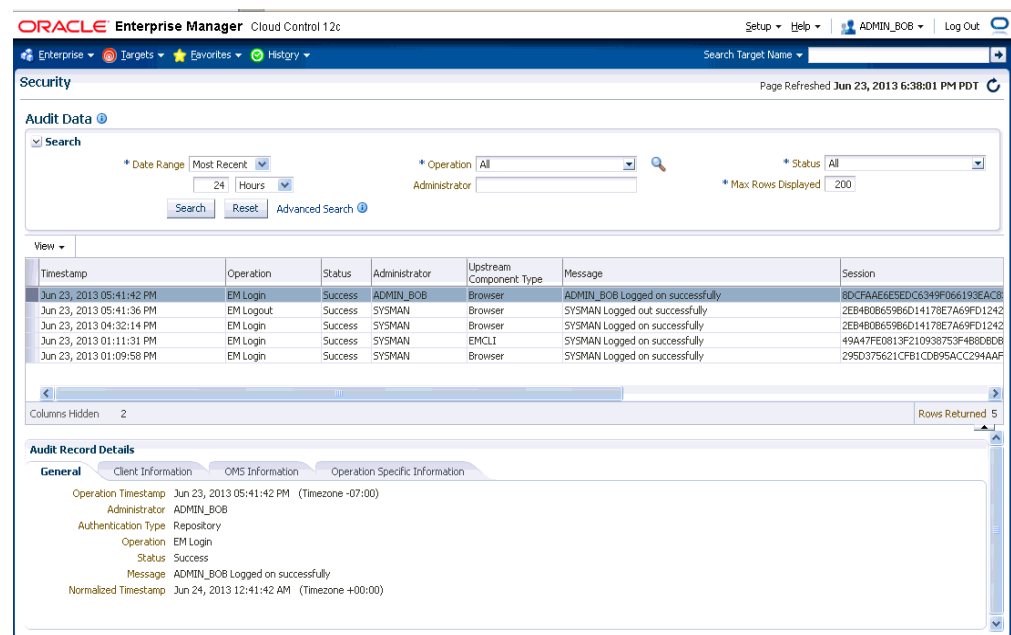
2.7.4 Searching the Audit Data

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.

Figure 2–14 Audit Data Search Page



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**.

2.7.5 List of Operations Audited

For a complete list of audit operations supported by Enterprise Manager, use the EM CLI `show_operation_list` verb.

Example 2-22 EM CLI show_operation_list

```
> emcli show_operation_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

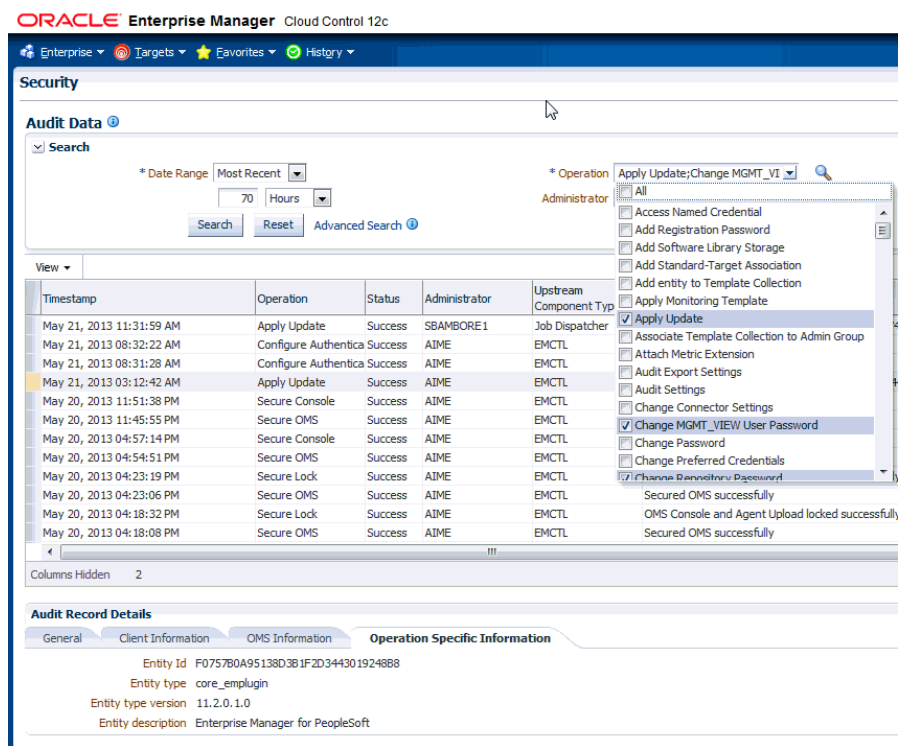
2.7.6 Auditing the Infrastructure

From Oracle Enterprise Manager Cloud Control Release 3, Basic and Infrastructure auditing is enabled by default for Enterprise Manager. In Enterprise Manager, there are over 150 options for auditing.

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.

Figure 2–15 Audit Page



2.8 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](#)

2.8.1 Changing the SYSMAN and MGMT_VIEW Passwords

This section describes the commands used to change the SYSMAN and MGMT_VIEW passwords.

2.8.1.1 Changing the SYSMAN User Password

To change the password of the SYSMAN user, you use the following command:

```
emctl config oms -change_repos_pwd [-old_pwd <old_pwd>] [-new_pwd <new_pwd>]  
[-use_sys_pwd [-sys_pwd <sys_pwd>]]
```

Parameter	Description
-change_repos_pwd	Used to change the SYSMAN password.

Parameter	Description
-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

1. Stop all OMS instances.

```
emctl stop oms
```

2. For each OMS, run the following command:

```
emctl config oms -change_repos_pwd'
```

3. Restart the Administration Server and all OMS instances.

```
emctl stop oms -all
```

```
emctl start oms
```

2.8.1.2 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_repos_pwd -change_in_db [-old_pwd <old_pwd>] [ -new_pwd <new_pwd>]
```

3. Restart the AdminServer and all the OMSs.

```
emctl stop oms -all
```

```
emctl start oms
```

2.8.2 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.

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.

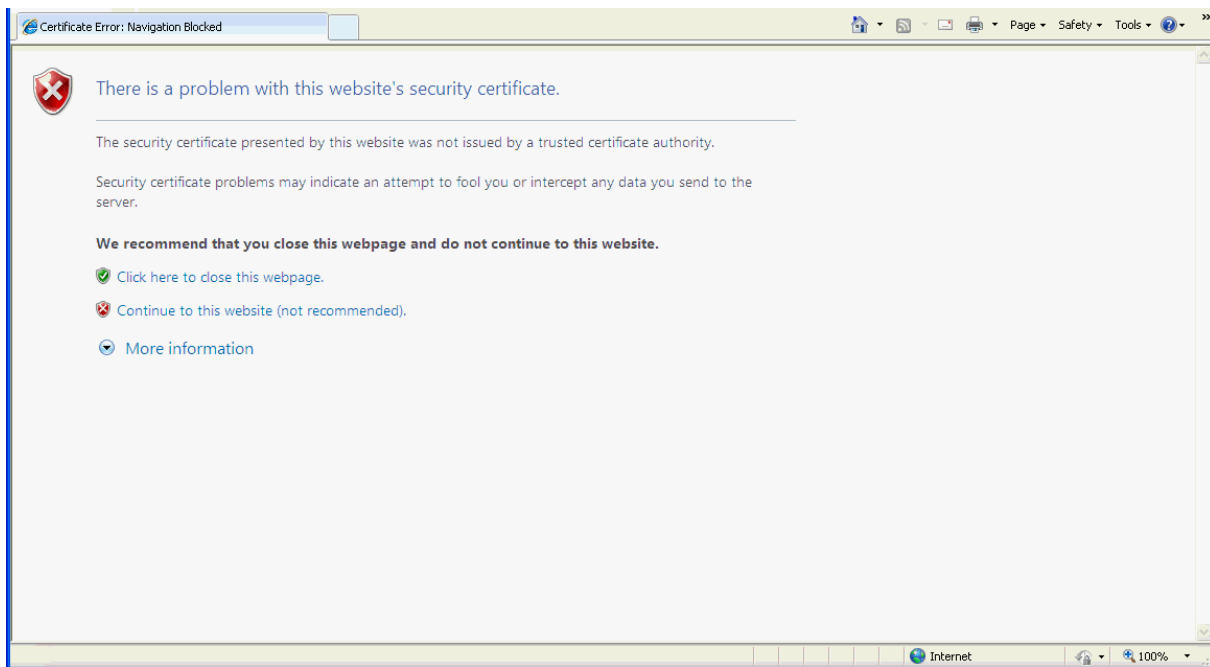
Step 2: Configure the custom wallets to each OMS. For instructions, see [Section 2.3.9.1, "Configuring a Third Party Certificate for HTTPS Console Users"](#)

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](#)

2.8.2.1 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.

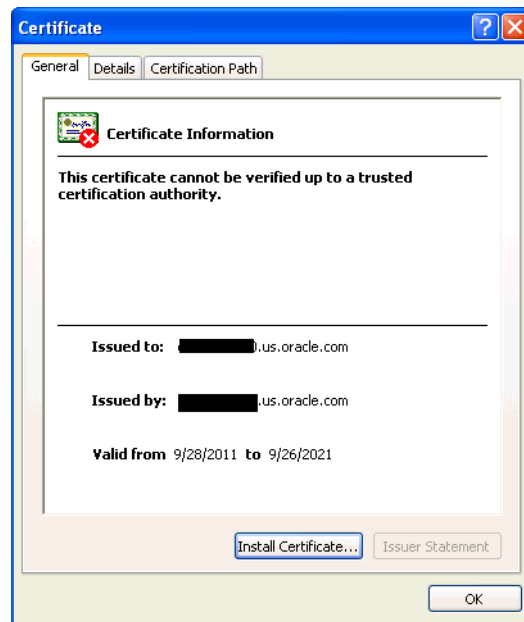
Figure 2–16 Internet Explorer Security Alert

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:

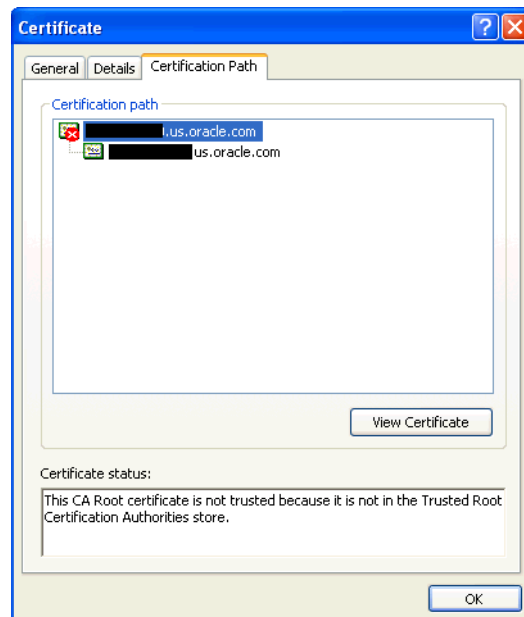
1. From the certificate warning page, click **Continue to this Web site (not recommended)**.
Internet Explorer displays a Security Warning dialog.
2. Click **Yes**. Internet Explorer may display a **Security Alert** dialog if you have not selected **In the future, do not show this warning.** in a previous 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.

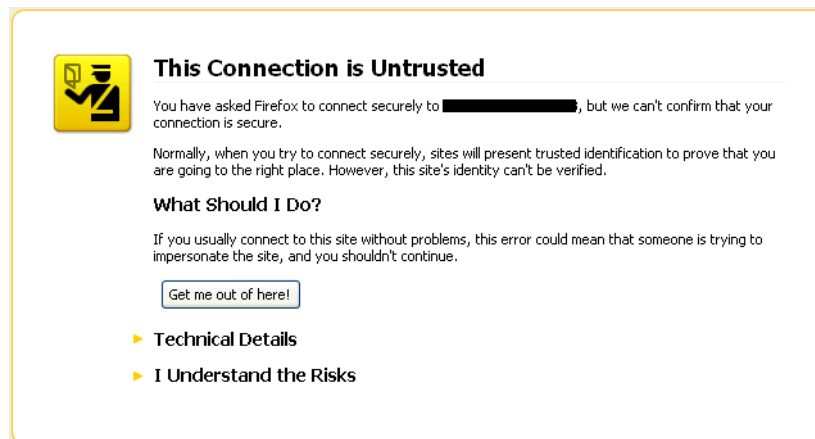


7. Click **View Certificate** to display a second Certificate dialog box.
8. Click **Install Certificate** to display the Certificate Import wizard.
9. Accept the default settings in the wizard, click **Finish** when you are done.
Internet Explorer displays a Security Warning asking if you want to install 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.

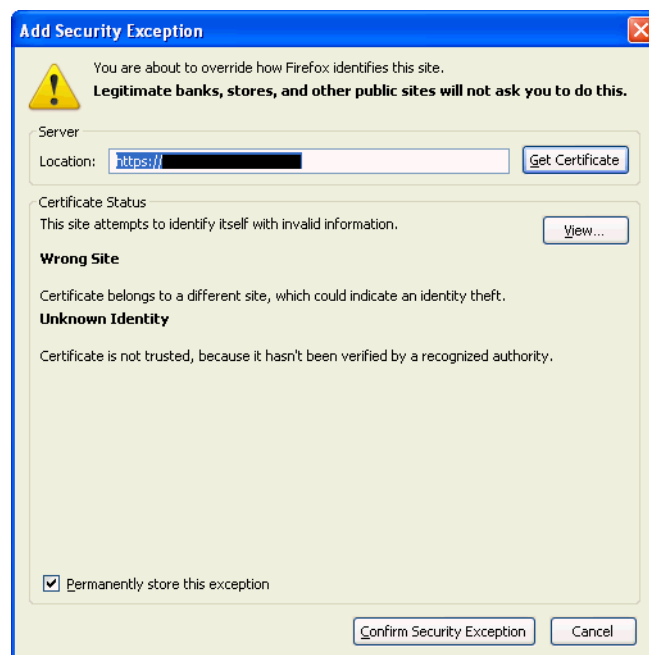
2.8.2.2 Responding to the Mozilla Firefox New Site Certificate Dialog Box

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.



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.

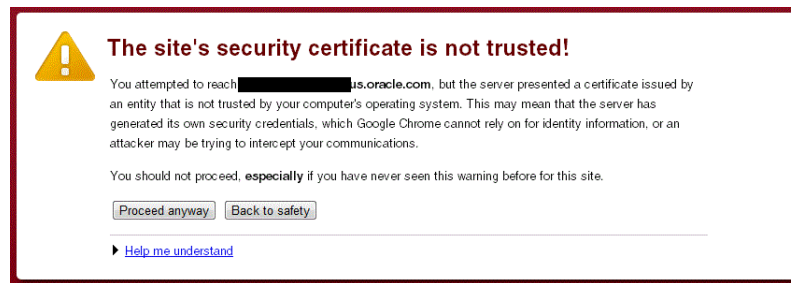
You should no longer receive the New Site Certificate dialog box when using the current browser.

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

2.8.2.3 Responding to the Google Chrome Security Alert Dialog Box

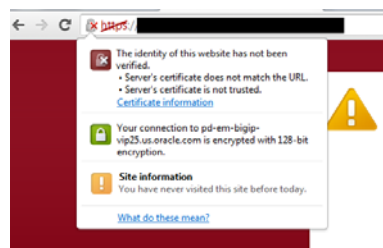
Google Chrome issues a warning if the security certificate of the Website is not trusted. When you first attempt to display the Cloud Control console using the HTTPS URL in Google Chrome, you will receive a warning because the connection is mistrusted.



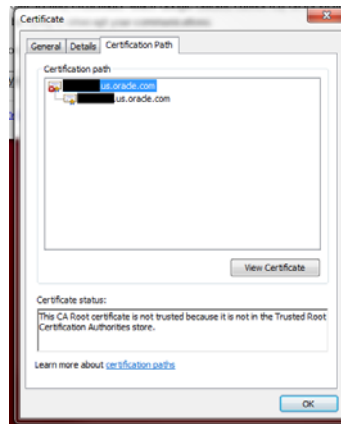
When Google Chrome displays the Untrusted Connection page, use the following instructions to install the certificate and avoid viewing this page again in future Enterprise Manager sessions:

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.

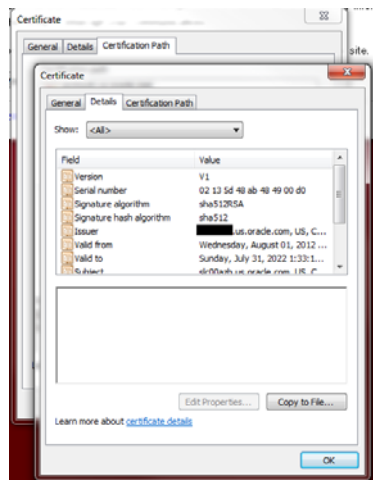
1. Click on the crossed out lock pad icon on the left hand side of the URL address bar.



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.

2.8.2.4 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.

Keeping Enterprise Manager Secure

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.

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
```

While the encryption key is required to be in the Repository for some operations such as Enterprise Manager patches and upgrades, if the operation does not automatically copy the emkey back to Repository (or remove it from the Repository afterwards), please copy it back to the Repository and after the operation remove it from the Repository by following the procedure below:

```
$ emctl config emkey -copy_to_repos You will be prompted for  
SYSMAN password
```

Remove the key from the Repository once the operation is done.

```
$ emctl config emkey -remove_from_repos
```

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.

Best Practices for Securing the Oracle Management Agent

- Utilize Enterprise Manager Agent Deployment method for agent installations.
- Use one-time registration passwords with expiry dates
- Install agent as a separate user from OMS or Targets

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 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.

3.1.4.2 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>
```

3.1.4.3 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 JVMD, 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.

3.2 Guidelines for SSL communication

3.2.1 Configure TLSv1 Protocol

It is recommended to configure OMS and Agents to support only TLS v1 protocol, which is the successor of SSL v3, for the communication. By default the OMS is configured in mixed-mode, accepting both SSLv3 and TLSv1 protocols.

To configure OMS for TLS v1 protocol only:

```
$ emctl stop oms
```

```
$ emctl secure oms -protocol TLSv1
```

Append the following to the JAVA_OPTIONS in Domain_Home/bin/startEMServer.sh. If this property already exists, update the value to TLS1

```
-Dweblogic.security.SSL.protocolVersion=TLS1
```

```
$ emctl start oms
```

To configure an Agent to support only TLS v1 protocol while the Agent listens as a server, edit the Agent properties in the Enterprise Manager Console or use emctl setproperty at the command line. To edit multiple Agents at a time, go to Setup -> Agents, select the Agents you want to modify, click Properties. This will create a job and you can specify the Agent property changes on the Parameters page that will get applied to all selected Agents. To use the command line, issue the following:

```
$ emctl setproperty agent -name allowTLSOnly -value true
```

3.2.2 Leave communication is 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 safe-guard 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 12c 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 12c 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 12c 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 12c 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 Disable Weak Ciphers

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 `RSA_WITH_RC4_128_MD5` uses RSA for key exchange, RC4 with a 128-bit key for bulk encryption, and MD5 for message digest. Enterprise Manager allows strong cipher suites for the communication between OMS and agent. By default, the following cipher suites will be allowed for the communication on the agent:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA

To see the current Cipher Suites enabled view the Agent properties in the Enterprise Manager Console or run:

```
$ emctl getproperty agent -name SSLCipherSuites
Oracle Enterprise Manager 12c Release 1 12.1.0.1.0
Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
SSLCipherSuites is unset; default value is SSL_RSA_WITH_RC4_128_MD5:SSL_RSA_WITH_
RC4_128_SHA:SSL_RSA_WITH_3DES_EDE_CBC_SHA:SSL_RSA_WITH_DES_CBC_SHA:SSL_RSA_EXPORT_
WITH_RC4_40_MD5:SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
```

To configure the strong cipher suites to be used for agent SSL/TLS communication edit the Agent properties in the Enterprise Manager Console or use the setproperty command:

```
$ emctl setproperty agent -name SSLCipherSuites -value <values>
```

The following are supported strong cipher suites:

- SSL_RSA_WITH_AES_128_CBC_SHA
- SSL_DH_anon_WITH_3DEC_EDE_CBC_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

To restrict the strong cipher suites used by OMS, please edit SSLCipherSuite parameter in \$INSTANCE_HOME/WebTierIH1/config/OHS/ohs1/httpd_em.conf and ssl.conf files with the appropriate values. Here are the default values:

- „h SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

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. Please refer to the section Configuring Secure Communications in Oracle Enterprise Manager Cloud Control Security Guide for detailed information.

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 Oracle Fusion Middleware Administrator's Guide.

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

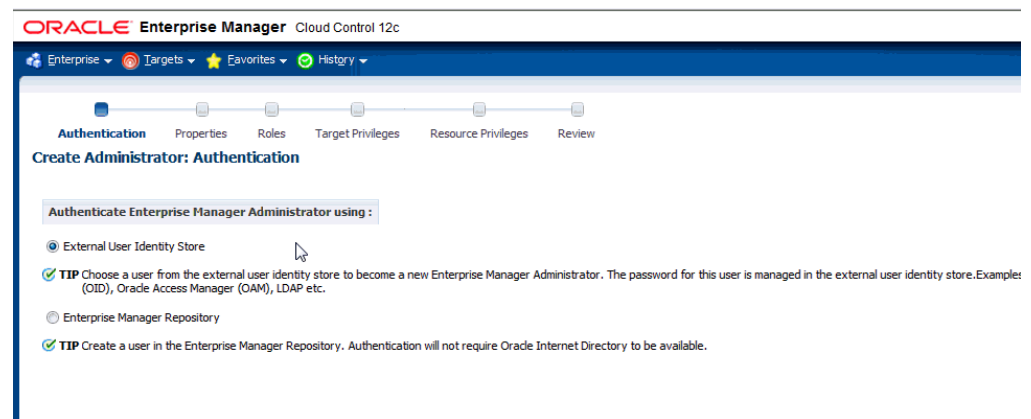
3.3.1 Enable External Authentication

Enterprise Manager Cloud Control 12c 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"](#) on page 2-1 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. The following figure shows the default window which appears during user creation.

Figure 3–1 Create Administrator Wizard: Authentication Page

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 12c, 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.

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 12c 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. 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 12c 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](#)" on page 2-30. 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'
```

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

3.4.1 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.

3.4.2 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 12c 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.

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 12c.

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](#)" on page 2-101 for the list of operations that are audited by Enterprise Manager.

In Enterprise Manager 12c, 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
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.

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.

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.

4.1 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, enable the WebLogic debug log level by going to the WebLogic Administrative Console. Under Environment->Servers->EMGC_OMS1, choose the logging tab. In that tab, set the log rotation file size to 64000.

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


Settings for EMGC_OMS1

Configuration Protocols **Logging** Debug Monitoring Control Deployments Services Security Notes


General HTTP Data Source

Save

Use this page to define the general logging settings for this server.

 **Log file name:** The name of on the name SERVER_NAH

Rotation

 **Rotation type:** Criteria for m


Rotation file size: The size (1 - file. The defa next time the SERVER_NAH that you spe


Begin rotation times: Determines tl [Info...](#)

Rotation interval: The interval (Requires the

☒ **Limit number of retained files** Indicates whi old messages [Info...](#)

Files to retain: The maximum number does that you ena

 **Log file rotation directory:** The directory stored in the

☒  **Rotate log file on startup** Specifies whi production m


[Advanced](#)

Message destination(s)

Log file :

Severity level: The minimum go to the log

Filter: The filter con

 **Log File Buffer:** Gets the und

Standard out :

Severity level: The minimum severity than

Filter: The filter con

Domain log broadcaster :

Severity level: The minimum broadcaster, to the domain

Filter: The filter con

Buffer Size: Broadcasts lo

Memory buffer :

Home > ipianetauth > Summary of Deployments > Summary of Servers > EMGC_OHS1

Settings for EMGC_OHS1

Configuration Protocols Logging **Debug** Monitoring Control Deployments Services Security Notes

Use this page to define debug settings for this server.

Debug settings for this Server

Enable Disable Clear

☐ **Debug Scopes and Attributes**

- ☐ default
- ☐ weblogic
 - ☐ application
 - ☐ classloader
 - ☐ cluster
 - ☐ connector
 - ☐ core
 - ☐ debug
 - ☐ default
 - ☐ deploy
 - ☐ descriptor
 - ☐ idmnetline
- ☐ protocol
- ☐ sca
- ☐ security
 - ☐ adjudicator
 - ☐ atn
 - ☒ DebugSecurityAtn
 - ☐ DebugSecuritySAML2Atn
 - ☐ DebugSecuritySAMLAtn
 - ☐ atz
 - ☐ auditor
 - ☐ certpath
 - ☐ certrevocchecking
 - ☐ credmap

5. Click Save/Activate changes.

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"`

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.

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.

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

An Appendix Title

Table A-1 Out-of-the-Box Roles

Roles	Description
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

Table A-1 (Cont.) Out-of-the-Box Roles

Roles	Description
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
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.

Index

A

Access Control, 2-83
Administration Groups, privilege propagating, 2-30
Administrator, 2-32
Agent Registration Password, 2-60
 changing, 2-66
Agent, Securing, 3-5
AGENT_HOME/network/admin, 2-72
attack, Man-in-the-middle, 1-2
attack, Denial-of-service, 1-2
attack, Password crack, 1-3
Audit Data, 2-103
Audit Data Export Service, 2-102
Audit Settings, 2-102
Audit SYS actions, 3-3
Audit, managing, 2-101
audited operations, 2-103
Auditing, Guidelines, 3-13
auditing, Infrastructure, 2-104
Authentication, 2-1
Authentication Schemes, 2-1
authentication, Repository-Based, 2-3
Authentication, Enterprise User Security Based, 2-11
Authorization, Guidelines, 3-11
authorization, Privileges and Role, 2-30
Auto Provisioning, 2-16

B

BASIC auditing, 2-101

C

Certificate Authority, 2-62
Certificate dialog box
 Internet Explorer, 2-108
Ciphers, 3-8
Credential Subsystem, 2-81
Cryptographic Keys, 2-96
Custom, 2-74
Custom CA Certificates, importing, 2-74
Custom Certificates for WebLogic Server, 2-73

D

Default Authentication, 2-15

Default Authentication Method, restoring, 2-29
Denial-of-service, attack, 1-2
Advanced Security Option, 3-2

E

emctl
 secure agent utility, 2-65
 secure agent utility, sample output, 2-66
 secure oms utility, 2-60
 secure oms utility, sample output, 2-61
 security commands, 2-60
emctl commands
 secure setpwd, 2-67
 secure unlock, 2-68
 start oms, sample output, 2-97
emkey, 2-97
emoms.properties
 oracle.net.crypto_checksum_client, 2-71
 oracle.net.crypto_checksum_types_client, 2-71
 oracle.net.encryption_client, 2-71
 oracle.net.encryption_types_client, 2-71
 oracle.sysman.emRep.dbConn.enableEncryption,
 2-71
Encryption, 1-4
Encryption Key, back up, 3-4
Enterprise Manager Framework Security
 enabling for Management Repository, 2-69
 enabling for multiple Management Services, 2-62
 restricting HTTP access, 2-67
 types of secure connections, 2-60
Enterprise Manager User Attributes, 2-17
Enterprise Manager, securing, 1-1
Enterprise User Security Based Authentication, 2-2
Enterprise User Security, configuring, 2-27
Enterprise Users (EUS Users), registering, 2-12
Entitlement, 2-58
External Authentication, 3-10
External Authorization, 2-16
External Roles, 2-16

F

FULL, 2-33

G

Global Named Credential, 2-82

H

Host Preferred Credentials, 2-90
HTTP access, restricting, 2-67
HTTPS, 2-60

I

ICMP, 3-5
Internet Explorer
 Certificate dialog box, 2-108
 security alert dialog box, 2-107
Invalid credentials, 4-3

L

LDAP Authentication, 2-2
LDAP Server, timeout, 4-4
LDAP User Attributes, 2-17
ldap_trace.logATN, 4-4
LDAP/SSO Providers, 2-20

M

Management Repository, recreating, 2-101
Managing Credentials
 EM CLI, 2-86
Man-in-the-middle, attacks, 1-2
Microsoft Active Directory, 2-14
Microsoft Active Directory, testing, 2-15
Monitoring Credentials, 2-85

N

Named Credential, 2-82
Named Credentials, creating, 2-83
Network Access, restricted, 3-2
network/admin, 2-70, 2-72
Non-repudiation, 1-5

O

OAM SSO, removing, 2-5
OID, 2-12
OID Configuration, testing, 2-14
OMS security, 2-60
OPERATOR, 2-33
ORA-12645 (security)
 Parameter does not exist, 2-70
Oracle Access Manager, 2-4
Oracle Access Manager (OAM) SSO, 2-2
Oracle Advanced Security, 2-60, 2-69
 enabling for Management Repository, 2-72
 enabling for the Management Agent, 2-72
Oracle AS SSO 10g, 2-22
Oracle Internet Directory, 2-12
Oracle Management Agent

 enabling security for, 2-65, 2-72
Oracle Management Repository
 enabling Oracle Advanced Security, 2-72
 enabling security for, 2-69
Oracle Management Service
 enabling security for, 2-60
 enabling security for multiple Management Services, 2-62
Oracle Single Sign-On, 2-5
ORACLE_HOME/network/admin, 2-70, 2-72
oracle.net.crypto_checksum_client
 property in emoms.properties, 2-71
oracle.net.crypto_checksum_types_client
 property in emoms.properties, 2-71
oracle.net.encryption_client
 property in emoms.properties, 2-71
oracle.net.encryption_types_client
 property in emoms.properties, 2-71
oracle.sysman.emRep.dbConn.enableEncryption
 entry in emoms.properties, 2-71

P

PAM Authentication
 authentication, PAM, 2-92
PAM, configuring, 2-92
PDP Configuration File, 2-96
PowerBroker, 2-93
Preferred Credentials, 2-85
Principle of Least Privilege, 1-4
Privilege Delegation, 2-94
Privilege Propagating Groups, 2-46
Privilege Propagation Groups, 3-13
Privileges and Roles, 2-33
Privileges, granting, 2-33
Public Key Infrastructure (PKI), 2-60

R

Repository Owner, 2-32
Repository-Based Authentication, 2-1
Roles to Manage Privileges, 2-46
root password
 See also SYSMAN
 when enabling security for the Management Service, 2-60

S

Secure Communication, 2-59
Secure Infrastructure, 3-1
Secure-Lock Mode, 3-7
Securing the Infrastructure, 3-2
security
 alert dialog box
 Internet Explorer, 2-107
 certificate alerts
 responding to, 2-106
security considerations, 1-1
Security Principles, 1-3
Security Threats, 1-1

- Separation of Duties, 1-4
- Server Load Balancer, 2-61
- Single Sign-On, bypassing, 2-10
- SQLNET.CRYPTO_SEED
 - entry in sqlnet.ora, 2-72
- SQLNET.ENCRYPTION_SERVER
 - entry in sqlnet.ora, 2-72
- sqlnet.ora, 2-69
 - SQLNET.CRYPTO_SEED, 2-72
 - SQLNET.ENCRYPTION_SERVER, 2-72
- SSL communication, 3-6
- SSLv3, 2-64
- SSO-Based Authentication, 2-2
- Sudo, 2-93
- Super Administrator, 2-32
- Suspicious activity, 1-4
- SYSMAN
 - entering SYSMAN password when enabling security, 2-60

T

- Target Credentials, 2-81
- Target Named Credentials, 2-83
- Target Privileges, 2-33
- Third Party Certificates, 2-79
- TLSv1 Protocol, 3-7
- Transport Layer Security, 2-64, 2-76
- Troubleshooting Authentication, 4-1

U

- User Accounts, securing, 3-3
- User Display Names, 2-18
- Users, Classes of, 2-32
- Users, Privileges and Roles, 2-30

V

- VIEW, 2-33
- view access, granting, 2-52

