

Oracle® Enterprise Manager

Cloud Control Getting Started Guide

12c Release 5 (12.1.0.5)

E39876-09

August 2015

Copyright © 2015, Oracle and/or its affiliates. All rights reserved.

Primary Author: Aravind Jayaraaman

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

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

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

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

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

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

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

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

Contents

1 Getting Started

2 Installing Browser Certificates

2.1	Screenshots for Importing Browser Certificates to Google Chrome 44+	2-3
2.1.1	Screenshot for Step 1: On the Privacy error page,	2-3
2.1.2	Screenshot for Step 2: In the address bar,	2-4
2.1.3	Screenshot for Step 5: Select the root node in the	2-5
2.1.4	Screenshot for Step 13: From the browser's menu,	2-6
2.1.5	Screenshot for Step 14: On the Settings page,	2-7

- 3 Verifying and Backing Up the Encryption Key**
- 4 Logging In to Enterprise Manager Cloud Control Console**
- 5 Exploring the Interface**
- 6 Setting Your Home Page**
- 7 Creating Roles and Administrators**
- 8 Configuring Auditing Framework**
- 9 Configuring My Oracle Support**
- 10 Configuring Software Library**
- 11 Configuring Self Update**
- 12 Downloading Oracle Management Agent Software**
- 13 Deploying Plug-Ins**
- 14 Discovering Targets**
- 15 Monitoring Targets**
- 16 Creating Monitoring Templates**
- 17 Setting Up Administration Group Hierarchy**
- 18 Setting Up Notifications**
- 19 Setting Up Incident Rule Sets and Subscribing to Receive E-Mail Notifications**
- 20 Setting Up Reporting Framework**

Preface

Oracle Enterprise Manager Cloud Control Getting Started Guide enables you to set up and get started with Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5).

This preface covers the following topics:

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

Audience

Oracle Enterprise Manager Cloud Control Getting Started Guide is meant for first-time users and other administrators who want to set up Enterprise Manager quickly and start using it for basic operations such as discovery and monitoring.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following books in the Enterprise Manager Cloud Control documentation library:

- *Oracle Enterprise Manager Cloud Control Basic Installation Guide*
- *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*
- *Oracle Enterprise Manager Cloud Control Upgrade Guide*
- *Oracle Enterprise Manager Cloud Control Administrator's Guide*

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

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

Enterprise Manager also provides extensive online Help. Click **Help** at the top-right corner of any Cloud Control 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.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in This Book Revision

In addition updating the books for an incremental software release or a patch set release, Oracle revises its books regularly to incorporate bug fixes and value-added feedback from customers, product managers, support teams, and other key stakeholders. Every time a book is revised, the revision number of the book is increased by one and then published on Oracle Technology Network (OTN).

This chapter lists the changes incorporated in the latest revision (E39876-09) and all the previous revisions of *Oracle Enterprise Manager Cloud Control Getting Started Guide* (this book). Note that the latest revision (E39876-09) is the current revision published on OTN, and the latest revision always contains all the changes incorporated in its previous revisions.

Changes Incorporated in the Latest Revision (Published)

The following are the changes incorporated in the latest revision (E39876-09) that is published on OTN.

Part, Chapter, or Section	Change Description
Chapter 2	Corrected the steps for importing browser certificates to Google Chrome.

Changes Incorporated in the Previous Revisions (Archived)

The following sections describe the changes incorporated in the previous revisions. These revisions have been archived, and therefore are not currently available on OTN.

Changes Incorporated in E39876-08

Part, Chapter, or Section	Change Description
Chapter 12	Explained the circumstances under which the Download button will be enabled.

Changes Incorporated in E39876-07

Part, Chapter, or Section	Change Description
All chapters	Improved the formatting of the tables.

Changes Incorporated in E39876-06

Part, Chapter, or Section	Change Description
Chapter 2	Corrected some invalid steps.

Getting Started



Super Administrator Operations

As a super administrator or designer, perform the following steps to get started with the product.

Step 1

Install Browser Certificates

Install trusted certificates to avoid any browser certification issues.

Step 2

Verify and Backup Encryption Key

Verify if emkey is configured properly, and back it up to a safe location.

Step 3

Log In to Enterprise Manager Console

Log in to the console using your super administrator credentials.

Step 4

Explore the User Interface

Take a tour of the user interface, and understand the menus and options.

Step 5

Set Up Your Home Page

Select any Enterprise Manager page, and set it up as your home page.

Step 6

Create Roles and Administrators

Create different roles and user accounts based on those roles.

Step 7

Configure Audit Framework

Configure the audit framework to track logins and other critical operations.

Step 8

Configure My Oracle Support

Configure My Oracle Support for online patching and other operations.

Step 9

Configure Software Library

Configure Software Library for storing entities, profiles, and so on.



Administrator Operations

As a normal administrator or operator, perform the following steps to get started with the product.

Step 1

Install Browser Certificates

Install trusted certificates to avoid any browser certification issues.

Step 2

Log In to Enterprise Manager Console

Log in to the console using your super administrator credentials.

Step 3

Explore the User Interface

Take a tour of the user interface, and understand the menus and options.

Step 5

Set Up Your Home Page

Select any Enterprise Manager page, and set it up as your home page.

Step 6

Discover Targets

Scan your network and discover hosts and targets running on those hosts.

Step 7

Monitor Targets

Promote and monitor the discovered targets.

Step 10 Configure Self Update Configure Self Update for automatically downloading software, software updates, plug-ins, and so on from My Oracle Support.	Step 11 Download Agent Software Download the Management Agent software for platforms other than the one on which OMS is running.	Step 12 Deploy Plug-Ins Download plug-ins and deploy them on the OMS so that you can discover and monitor targets in your network.
Step 13 Discover Targets Scan your network and discover hosts and targets running on those hosts.	Step 14 Monitor Targets Promote and monitor the discovered targets.	Step 15 Create Monitoring Templates Specify monitoring settings once and apply them to all monitored targets.
Step 16 Set Up Administration Group Hierarchy Create an administration group hierarchy so that the monitored targets can be logically grouped, and the monitoring templates can be applied globally	Step 17 Set Up Notifications Set up e-mail servers, e-mail addresses, and notification schedule for e-mail notifications.	Step 18 Set Up and Subscribe to Incident Rule Sets Set up incident rule sets and subscribe to them for e-mail notifications.
Step 19 Set Up Reporting Framework Set up Business Intelligence (BI) Publisher to create custom report based on the monitored targets.		

Installing Browser Certificates



When you connect to Enterprise Manager via HTTPS, the OMS presents your browser with a certificate to verify the identity of the OMS. 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 Framework Security is enabled, but you have not secured your Web tier properly. Oracle requires that you import these browser certificates to the browser's list of trusted root certificates to eliminate the certificate security alerts in future browser sessions.

Import to Microsoft Internet Explorer Version 11	Import to Mozilla Firefox Version 28.0	Importing to Google Chrome Version 44+
<ol style="list-style-type: none"> 1. On the error page, click the certificate error icon (a red-colored shield with a cross mark on it) that appears in the address bar. 2. In the pop-up, click View certificates. 3. In the Certificate dialog, click the Certification Path tab. 4. Select the first entry in the list of certification paths. 5. Click View Certificate. 6. In the second Certificate dialog, click the Details tab. 7. Click Copy to File. 8. In the Certificate Export Wizard, accept the default settings, enter a meaning certificate name to export it to your local system, and click Finish. Now the certificate is exported successfully. 9. In the Certificate Export Wizard success message, click OK. 10. In the second Certificate dialog, click OK. 11. In the first Certificate dialog, click OK. 12. From the browser's menu, select Settings, then select Internet Options. 13. In the Internet Options dialog, click the Content tab. 14. In the Certificates section, click Certificates. 15. In the Certificates dialog, click the Trusted Root Certification Authorities tab. 16. Click Import. 17. In the Certificate Import Wizard, accept the default settings, select the certificate you exported in Step (8), and click Finish. 18. In the Security Warning message, click Yes. 19. In the Certificate Import Wizard success message, click OK. 20. In the Certificates dialog, click Close. 21. In the Internet Options dialog, click OK. 22. Restart the browser. 	<ol style="list-style-type: none"> 1. On the Untrusted Connection page, click I Understand the Risks. 2. Click Add Exception. 3. In the Add Security Exception dialog, ensure that Permanently store this exception option is selected. 4. Click Confirm Security Exception. 	<ol style="list-style-type: none"> 1. On the Privacy error page, click Advanced. Then click Proceed to <host_name> (unsafe). Screenshot? 2. In the address bar of the Enterprise Manager Cloud Control Login page, click the red cross mark on the lock icon next to https. Screenshot? 3. In the pop-up, in the Connection tab, click Certificate Information. 4. In the Certificate dialog, click the Certification Path tab. 5. Select the root node in the list of certificate paths. Screenshot? 6. Click View Certificate. 7. In the second Certificate dialog, click the Details tab. 8. Click Copy to File. 9. In the Certificate Export Wizard, accept the default settings, enter a meaningful certificate name to export it to your local system, and click Finish. Now the certificate is exported successfully. 10. In the Certificate Export Wizard success message, click OK. 11. In the second Certificate dialog, click OK. 12. In the first Certificate dialog, click OK. 13. From the browser's menu, select Settings. Screenshot? 14. On the Settings page, in the top-right Search settings field, enter Certificates. Screenshot? 15. In the HTTPS/SSL section, click Manage certificates. 16. In the Certificate dialog, click the Trusted Root Certification Authorities tab. 17. Click Import... 18. In the Certificate Import Wizard, click Next, then select the certificate you exported in Step (9), accept the default settings, and then click Finish. 19. In the Security Warning dialog, click Yes. 20. In the Certificate Import Wizard success message, click OK. 21. In the Certificates dialog, click Close. 22. Restart the browser. 23. Now when you navigate to the Enterprise Manager Cloud Control Login page, you should see a green lock icon next to https in the address bar.

**Perform Additional Tasks**

How to Respond to Internet Explorer Security Alert Dialog Box?

**Perform Additional Tasks**

How to Respond to Mozilla Firefox New Site Certificate Dialog Box?

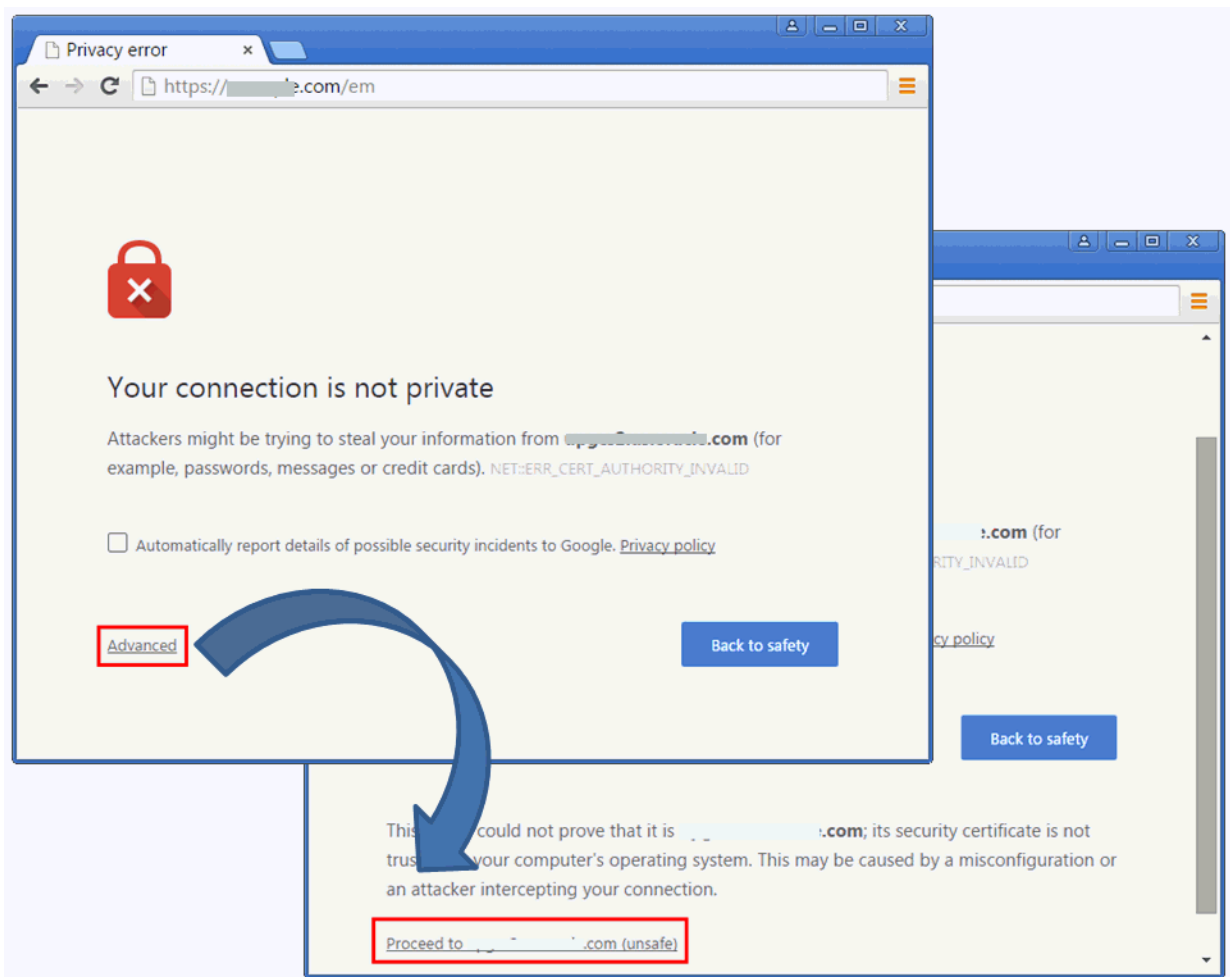
**Perform Additional Tasks**

How to Respond to Safari Security Dialog Box?

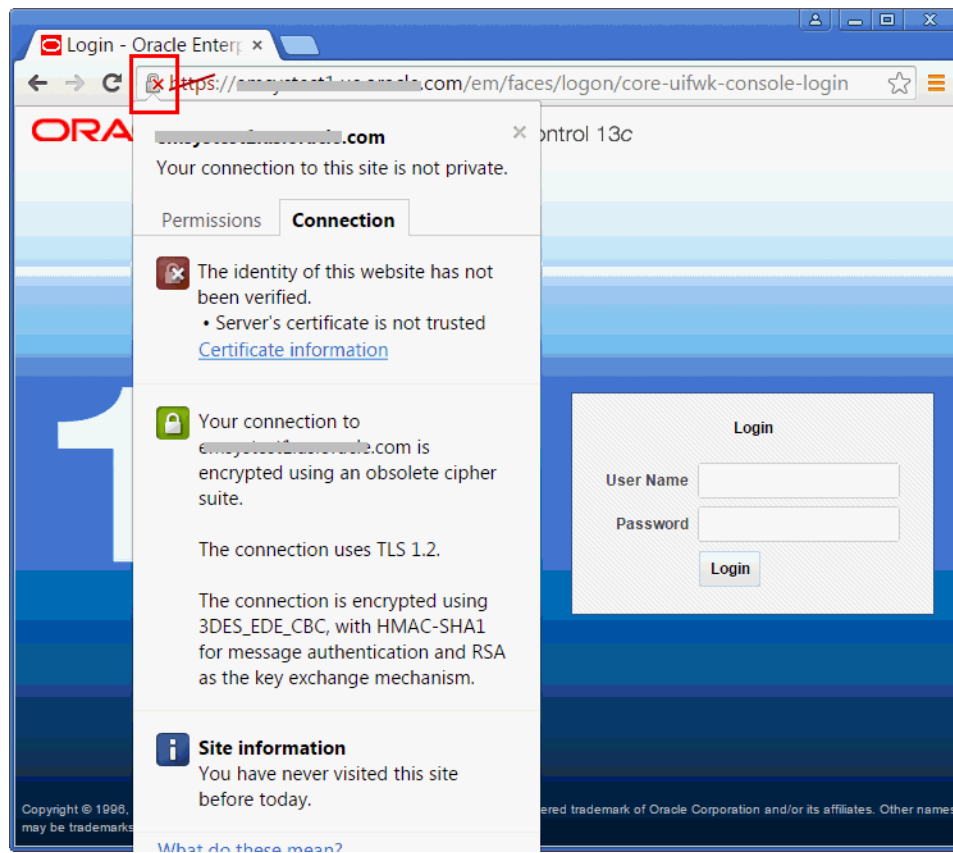
2.1 Screenshots for Importing Browser Certificates to Google Chrome 44+

The section provides the screenshots to support the steps listed for importing browser certificates to Google Chrome 44+. Note that the screenshots are provided only for complex steps or steps that are not very intuitive and that require a screenshot to help you understand better.

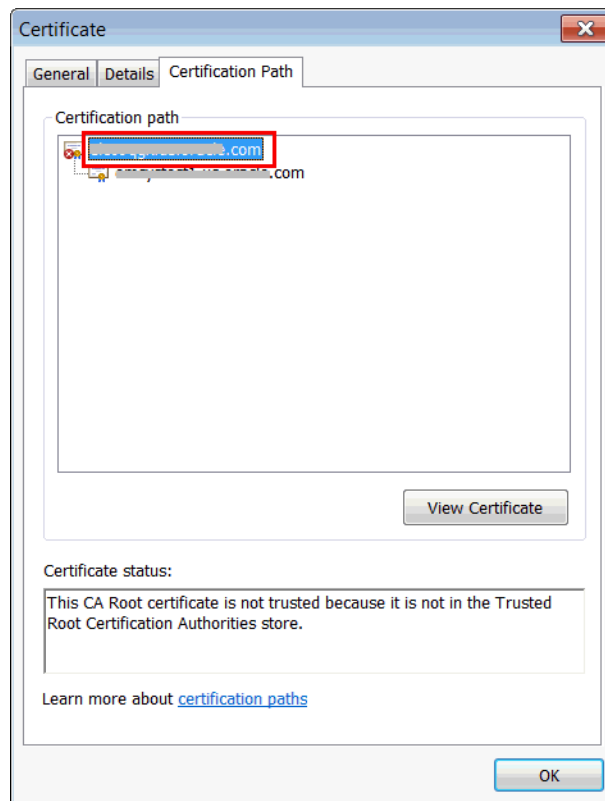
2.1.1 Screenshot for Step 1: On the Privacy error page, . . .



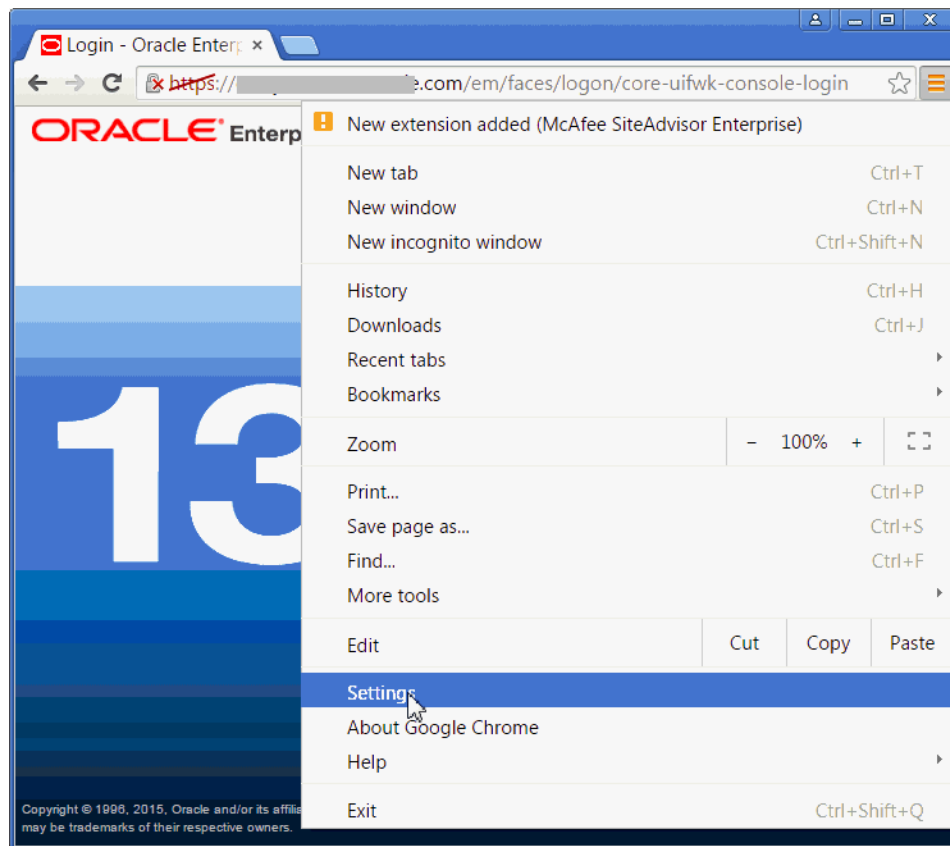
2.1.2 Screenshot for Step 2: In the address bar, . . .



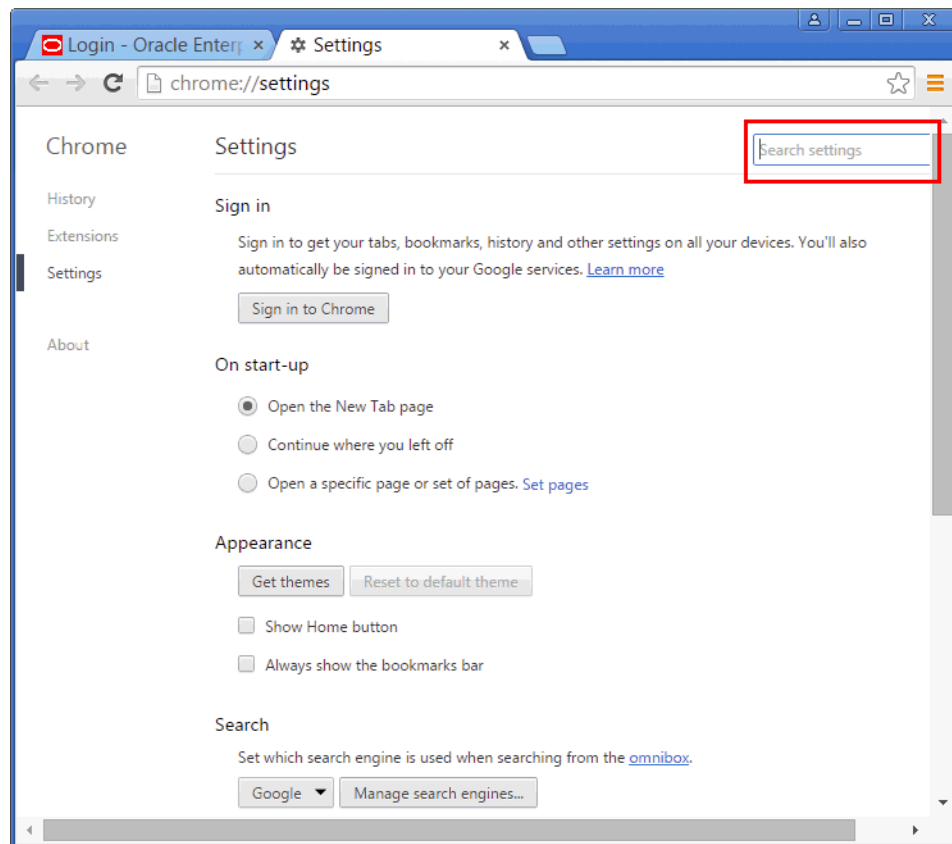
2.1.3 Screenshot for Step 5: Select the root node in the . . .



2.1.4 Screenshot for Step 13: From the browser's menu, . . .



2.1.5 Screenshot for Step 14: On the Settings page, . . .



Verifying and Backing Up the Encryption Key



Enterprise Manager uses an encryption key called *emkey* (or *emkey.ora* file) to encrypt and decrypt sensitive data, such as passwords and preferred credentials, which are stored in the Management Repository. The *emkey* is originally stored in the Management Repository, but is removed from there and copied to the Credential Store at the time of installation. Verify that the *emkey* is configured properly, and also back it up to a host different from the OMS host.

Step 1: Verify the emkey Configuration

Verify if the *emkey* is configured properly. To do so, run the following command:

```
$<OMS_HOME>/bin/emctl status emkey
```

- If it is configured properly, you will see the following message:

```
Oracle Enterprise Manager 12c Release 5 Cloud
Control
Copyright (c) 1996, 2015 Oracle Corporation.
All rights reserved.
The EMKey is configured properly.
```
- If it is configured properly, but not secure, then secure it. To do so, run the following command:

```
$<OMS_HOME>/bin/emctl config emkey -remove_from_
repos
```

Step 2: Back Up the emkey Configuration

1. Enterprise Manager automatically creates a backup of the *emkey* in the following location. Navigate to this location.

```
$<OMS_HOME>/sysman/config/emkey.ora
```
2. Copy the file to a host different from the OMS host.



Learn More

- What Are the Different Types of Security Threats?
- What Are the Basic Principles for Securing Your Environment?
- What Type of Security is Provided in Enterprise Manager?



Perform Additional Tasks

- How to Copy the *emkey* from the Repository to the Credential Store?
- How to Copy the *emkey* from the Credential Store to the Repository?
- How to Copy the *emkey* from the Credential Store to a Specified File?



Perform Additional Tasks

- How to Copy the *emkey* from the Repository to a Specified File?
- How to Copy the *emkey* from a Specified File to the Credential Store?
- How to Copy the *emkey* from a Specified File to the Repository?
- How to Remove the *emkey* from the Repository?

Logging In to Enterprise Manager Cloud Control Console



When you install Enterprise Manager Cloud Control, an administrator account with the user name *sysman* is created by default with the password you provided for it at the time of installation. Use this user name and password to log in to Enterprise Manager Cloud Control Console.

Step 1: Identify the Console Port

By default, the Enterprise Manager Cloud Control Console is secure. Therefore, the default console port that is assigned automatically by the installer at the time of installation is the first available free port from the range 7799 - 7809. However, you might have entered a custom port at the time of installation to overwrite the default port. You need this console port to access the Enterprise Manager Cloud Control Console.

To identify the console port assigned to the Enterprise Manager Cloud Control Console, run the following command:

```
$<OMS_HOME>/bin/emctl status oms -details
```

Step 2: Log In to Enterprise Manager Cloud Control Console

1. Open a browser, and access the Enterprise Manager Cloud Control Console using the following URL format:
`https://<oms_host_name>:<console_port>/em`
Ensure that the OMS host name is a fully qualified name, and the console port is the port you identified in the previous step.
 2. On the Login screen, enter the user name *sysman*, and the password you provided for this user account at the time of installation, and click **Login**.
 3. If you see an agreement page, click **I Accept**.
-

Exploring the Interface 5-1

Setting Your Home Page



Home page is the first, landing page you see when you log in to the Enterprise Manager Cloud Control Console. When you log in the first time after installing the product, by default, the Select Enterprise Manager Home Page page appears. You can select another page and set that as your Home page based on your on your job profile or role. This helps as it displays a page with information of your choice and interest immediately after you log in, thus saving your effort and time in navigating to that page from the menu.

Setting Your Home Page

To set a page as your Home page, decide on a page that suits your requirement based on your job profile or role, and click **Select As My Home**.

Once selected, your personal Home page appears immediately after logging in or by clicking the product logo on the top-left corner of any page within the Enterprise Manager Cloud Control Console.

If none of the pages listed on this Select Enterprise Manager Home Page page match your requirements, then navigate to the desired page, and then from the user name menu that appears in the top-right corner of the desired page, select **Set Current Page as My Home**.

Creating Roles and Administrators



An *administrator* is an authorized user who logs in and uses Enterprise Manager. A *role* is a collection of Enterprise Manager resource privileges, or target privileges, or both, which are granted to administrators or to other roles. 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. By default, when you install Enterprise Manager, the SYSMAN user account (super administrator) is created. Use this super administrator account to create roles and administrators for your organization.

Step 1: Create Roles

1. From the **Setup** menu, select **Security**, then select **Roles**.
2. On the Security page, click **Create**.
3. In the Create Role Wizard, on the Properties page, enter a unique name for the role, and click **Next**.
4. On the Roles page, from the Available Roles list, select the Oracle-defined roles you want to grant explicitly to the role you are creating, and click **Next**.
Explicitly granting roles to an already existing role will grant all privileges to grantee of current role.
5. On the Target Privileges page, select the privileges common to all targets and the privileges specific certain targets, you want to grant explicitly to the role you are creating, and click **Next**.
6. On the Administrators page, click **Next**.
7. On the Review page, click **Finish**.

Step 2: Create Administrators

1. From the **Setup** menu, select **Security**, then select **Administrators**.
2. On the Administrators page, click **Create**.
3. In the Create Administrator Wizard, on the Properties page, enter the user name and password, and an e-mail address for the administrator account, and click **Next**.
4. On the Roles page, from the Available Roles list, select the role you had created, and click **Next**.
5. On the Target Privileges page, click **Review**.
6. On the Review page, click **Finish**.



Learn More

- What Are the Different Classes of Users in Enterprise Manager?
- What Are Privileges and Roles?
- What Roles Can You Create for Different Job Responsibilities?



Learn More

- What Target Privileges Are Supported for All Types of Targets?
- What Target Privileges Are Supported for Specific Types of Targets?



Learn More

- What Privileges Are Supported for Resources?
- What Out-of-the-Box Roles Are Provided?

Configuring Auditing Framework



All operations performed by Enterprise Manager users such as creating users, granting privileges, starting a remote job, must be recorded and 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. Enable the auditing framework in Enterprise Manager so that all operations performed on credentials are recorded.

Step 1: Enable Auditing

Run the following command:

```
emcli enable_audit
```

For example,

```
emcli enable_audit
```

Step 2: Update Audit Settings

Run the following command:

```
emcli update_audit_settings
-audit_switch="ENABLE"
-operations_to_enable="ALL"
-externalization_switch="ENABLE"
-directory="<directory_to_archive_audit_data_files>"
-file_size="<file_size_in_bytes>"
-data_retention_period="data_retention_period_in_days"
```

For example,

```
emcli update_audit_settings
-audit_switch="ENABLE"
-operations_to_enable="ALL"
-externalization_switch="ENABLE"
-directory="u01/Oracle/auditdata"
-file_size="10000"
-data_retention_period="60"
```



Learn More

Why Enable Auditing?



Perform Additional Tasks

- How to Search the Audit Data?
- How to View a List of Supported Audit Operations?



Perform Additional Tasks

- How to Access the Audit Data Page?
- How to Configure the Audit Data Export Service?

Configuring My Oracle Support



My Oracle Support, which is a one-stop support solution for customers, is now integrated with Enterprise Manager, so you can access it from within the Enterprise Manager Cloud Control Console. Using the integrated view, you can now raise service requests; search the knowledge database for support notes; view certification details; download software, patches, and updates; and even collaborate in the My Oracle Support community, all from within the Enterprise Manager Cloud Control Console. Configure My Oracle Support to gain all the benefits of the integration.

Configure My Oracle Support

1. From the **Setup** menu, select **My Oracle Support**, then select **Set Credentials**.
 2. Enter the user name and password, click **Apply**.
-



Learn More

What Are the Benefits of Using My Oracle Support?



Perform Additional Tasks

How Do I Patch Software Deployments?



Perform Additional Tasks

How Do I Access the Enterprise Manager Certification Matrix from My Oracle Support?

Configuring Software Library



Oracle Software Library (Software Library) is a feature within Enterprise Manager Cloud Control that acts as a repository to store software entities such as software patches, virtual appliance images, reference gold images, application software, and their associated directive scripts. In addition to storing the software entities, Software Library also maintains their versions, maturity levels, and states. Configure Software Library so that you can use it for operations such as provisioning, patching, and so on.

Configure Software Library

1. From the **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.
2. From the **Storage Type** list, select **OMS Shared Filesystem**.
3. Enter a unique name, and the absolute path to a shared location on the OMS host.
4. Click **OK**.



Learn More

- What Is a Software Library and Why Do I Need It?
- Who Accesses the Software Library?
- What Privileges Are Required for Accessing the Software Library?
- What Storage Types Are Supported?
- What Are the Prerequisites for Setting Up the Software Library?
- What Are Entities?



Perform Additional Tasks

- How Do You Configure an OMS Shared File System Location?
- How Do You Configure an OMS Agent Filesystem Location?
- How Do You Configure a Referenced File Location?
- How Do You Organize, Create, Customize, and Manage Entities?






Perform Additional Tasks

- How Do You Maintain the Software Library?
- How Do You Remove (and Migrate) a Software Library Storage Location?
- How Do You Purge Deleted Entity Files?

Configuring Self Update



Self Update is a feature available via the Self Update Console, a common dashboard used to obtain information about new updates and a common workflow to review, download and apply the updates. The Self Update Console frees you from having to monitor multiple channels to get informed about new updates that are available from Oracle. The Self Update Console automatically informs you whenever new updates are made available by Oracle. Only those updates that are applicable to your site are shown, eliminating the need to wade through unrelated updates. For example, you can periodically check the availability of plug-ins and download them from the Enterprise Manager Store, via the Self Update Console. Configure Self Update so that you check the availability of new updates released by Oracle, and download and apply them as needed.

Step 1: Enable Online Mode	Step 2: Register My Oracle Support Credentials	Step 3: Configure Software Library
<ol style="list-style-type: none"> 1. From the Setup menu, select Extensibility, then select Self Update. 2. In the Status section, click the value set for Connection Mode. 3. Select Online. 	See Configuring My Oracle Support	See Configuring Software Library
 Learn More <ul style="list-style-type: none"> What Can Be Viewed, Downloaded, and Updated via the Self Update Console? What Privileges Are Required for Accessing the Self Update feature? 	 Perform Additional Tasks <ul style="list-style-type: none"> How Do I Assign Self Update Privileges to Administrators? How Do Apply the Updates Offline? 	 Perform Additional Tasks <ul style="list-style-type: none"> How Do I Access Informational Updates? How Do I Acquire or Update Management Agent Software via Self Update Console?

Downloading Oracle Management Agent Software



Oracle Management Agent (Management Agent) is one of the core components of Enterprise Manager Cloud Control that enables you to convert an unmanaged host to a managed host in the Enterprise Manager system. The Management Agent works in conjunction with the plug-ins to monitor the targets running on that managed host. By default, the OMS contains the Management Agent software for the operating system on which the OMS is running. However, for all other operating systems, you must manually download the Management Agent software via the Self Update Console.

Step 1: Configure Self Update	Step 2: Download Management Agent Software	Step 3: Stage Management Agent to Software Library
See Configuring Self Update	<ol style="list-style-type: none"> From the Setup menu, select Extensibility, then select Self Update. In the table, click the entity type Agent Software. On the Agent Software Updates page, select an update, and click Download. All entries other than the one which matches the platform of the OMS host should show their status as <i>Available</i>. The Download button is enabled only in the following cases: <ul style="list-style-type: none"> You must have the privilege to download and apply in Self Update Console. You must have selected at least one Management Agent software row in the table, and the Management Agent software must be in <i>Available</i> or <i>Download Failed</i> status. You must have configured the Software Library. You must have configured the Self Update staging area. You must have enabled the online mode for Self Update and set the My Oracle Support credentials. In the Schedule Download dialog, schedule the download activity, and click Select. 	<ol style="list-style-type: none"> From the Setup menu, select Extensibility, then select Self Update. In the table, click the entity type Agent Software. On the Agent Software Updates page, select the downloaded Management Agent software, and click Apply.

**Learn More**

Where Does Management Agent
Feature in the Enterprise
Manager Architecture?

**Perform Additional Tasks**

How Do I Download the
Management Agent Software in
Offline Mode?

**Perform Additional Tasks**




How Do I Manually Install a
Management Agent Using the
Add Host Targets Wizard?

Deploying Plug-Ins



Plug-Ins are modules that can be plugged to an existing Enterprise Manager system to provide target management or other vertical functionality. Plug-ins offer special solutions or new features, for example, connectivity to My Oracle Support, and extend monitoring and management capability to Enterprise Manager, which enable you to monitor a particular target on a host. Plug-ins work in conjunction with the OMS and the Management Agent to offer monitoring services, and therefore they are deployed to the OMS as well as the Management Agent.

Step 1: Configure Self Update	Step 2: Check the Availability of Plug-Ins	Step 3: Download Plug-Ins	Step 4: Deploy Plug-Ins to the OMS
See Configuring Self Update	<ol style="list-style-type: none"> From the Setup menu, select Extensibility, then select Plug-ins. On the Plug-ins page, in the Latest Available column of the table, check whether the plug-ins are available. If they are not available, then click Check Updates to refresh the list of available plug-ins. 	<ol style="list-style-type: none"> From the Setup menu, select Extensibility, then select Self Update. On the Self Update page, in the table, click the entity type Plug-in. In the Plug-in Updates table, select the plug-in available for download, and click Download. In the Schedule Download dialog, schedule the download activity, and click Select. 	<ol style="list-style-type: none"> From the Setup menu, select Extensibility, then select Plug-ins. On the Plug-ins page, select the plug-in you want to deploy. From the Deploy On menu, select Management Servers. In the Deploy Plug-in on Management Servers dialog, enter the Management Repository SYS password, and click Continue. <p>Proceed through the steps in the dialog box, and then click Deploy.</p>




Learn More	Perform Additional Tasks	Perform Additional Tasks
 <ul style="list-style-type: none"> What Is the Extensibility Paradigm? Are All Plug-Ins Deployed by Default? How Often Are Plug-Ins Released? What Is the Workflow of Plug-In Deployment? What is Plug-In Manager? 	 <ul style="list-style-type: none"> How to Access Plug-In Manager? How to Check the Availability of Plug-Ins? How to View Information about Plug-Ins? How to Identify the Targets and Operating Systems Certified for Deployed Plug-Ins? How to Download Plug-Ins in Online Mode? How to Download Plug-Ins in Offline Mode? 	 <ul style="list-style-type: none"> How to Deploy Plug-Ins to OMS? How to Upgrade Plug-Ins Deployed to OMS? How to Deploy Plug-Ins on Agents? How to Upgrade Plug-Ins Deployed to Agents? How to Undeploy Plug-Ins from Agents? How to Undeploy Plug-Ins from OMS? How to Troubleshoot Plug-In Deployment Issues?

Discovering Targets



Discovery refers to the process of *identifying* unmanaged hosts and targets in your environment. Once you discover these hosts and targets, you can *promote* them and add them to the Enterprise Manager system so that they can be monitored. Scan your network thoroughly, and identify the unmanaged targets you want to monitor.

Step 1: Scan Your Network	Step 2: Promote and Monitor Hosts	Step 3: Discover Targets
<ol style="list-style-type: none"> 1. From the Setup menu, select Add Target, then select Configure Auto Discovery. 2. In the Configure Auto Discovery section, in the Network Scan-based Auto Discovery table, in the Configure Network Scan Discovery column, click the Configure icon. 3. Click Create. 4. In the Network Scans section, click Add. Select a Management Agent that can scan the network. 5. Enter the IP ranges to scan. The range can contain absolute host names, IP addresses, a range of addresses, or/and Classless Inter-Domain Routing (CIDR) notations. 6. In the Schedule section, schedule the scan job to run immediately or on/at a particular date/time. 7. In the Credentials section, enter the credentials of the Management Agent that you have selected for scanning the network. 8. Click Save and Submit IP Scan. 	<ol style="list-style-type: none"> 1. From the Setup menu, select Add Target, then select Auto Discovery Results. 2. Click the Host Targets tab. 3. In the table, select a host, then click Promote. The Add Host Targets wizard appears. Use this wizard to install a Management Agent on the discovered host. 4. Repeat Step (3) for other hosts you want to monitor. 	<ol style="list-style-type: none"> 1. From the Setup menu, select Add Target, then select Configure Auto Discovery. 2. In the Configure Auto Discovery section, in the Auto Discovery table, against the All Discovery Modules row, in the Configure Auto Discovery column, click the Configure icon. 3. In the table, select the host whose targets you want to discover, and click Configure. 4. Set the frequency for the scan. 5. Select the discovery modules you want to discover on the host. 6. Click OK. 7. Repeat Step (3) to Step (6) for other hosts. 8. Click Run Discovery Now. The discovery job runs on the host immediately as well as at the set frequency.

	Learn More <ul style="list-style-type: none">■ What is Discovery?■ What is Promotion?■ What is Monitoring?■ Where Does Discovery Feature in the Lifecycle?■ What Is the High-Level Process of Workflow for Discovery and Monitoring?		Perform Additional Tasks <ul style="list-style-type: none">■ How Do I Discover and Promote All Target Types?■ How Do I Discover and Promote Oracle Homes?		Perform Additional Tasks <ul style="list-style-type: none">■ How Do I Discover, Promote, and Add Database Targets?■ How Do I Discover, Promote, and Add Middleware Targets?
---	---	---	---	--	---

Monitoring Targets



Monitoring refers to the process of gathering information and keeping track of activity, status, performance, and health of targets managed by Enterprise Manager Cloud Control on your host. A Management Agent deployed on the host in conjunction with plug-ins monitors every target in your environment. After discovering unmanaged hosts and targets in your network, promote them and add them to the Enterprise Manager system so that they can be monitored.

Step 1: Secure Management Agents

1. From the **Setup** menu, click **Agents**.
2. Click the Management Agent that is monitoring the host where the targets you want to promote are running.
3. On the Management Agent Home page, verify if it is secure. If it is not secure, from the **Agent** menu, click **Secure** to secure it.

Step 2: Promote and Monitor Targets

1. From the **Setup** menu, select **Add Target**, then select **Auto Discovery Results**.
2. Click the **Non-Host Targets** tab.
3. In the table, select one or more targets you want to promote, and click **Promote**.
4. Navigate to the target home pages and verify that they have been added to the console for monitoring.



Learn More

- What is Discovery?
- What is Promotion?
- What is Monitoring?



Perform Additional Tasks

- Where Does Monitoring Feature in the Lifecycle?
- What Is the High-Level Process of Workflow for Discovery and Monitoring?



Perform Additional Tasks

- How Do I Discover and Promote Oracle Home?
- How Do I Discover, Promote, and Add Database Targets?
- How Do I Discover, Promote, and Add Middleware Targets?

Creating Monitoring Templates



Monitoring templates let you standardize monitoring settings across your enterprise by enabling you to specify the monitoring settings once and apply them to your monitored targets. You can save, edit, and apply these templates across one or more targets or groups. A monitoring template is specified for a particular target type and can only be applied to targets of the same type. For example, you can define one monitoring template for test databases and another monitoring template for production databases. After discovering and monitoring targets, create monitoring templates so that the monitoring settings can be applied uniformly to each target type.

Create a Monitoring Template

1. From the **Enterprise** menu, select **Monitoring**, then **Monitoring Templates**.
2. On the Monitoring Templates page, click **Create**.
3. Select a target or a target type whose monitoring settings you want copy to the template.
4. Click **Continue**.
5. In the General tab, enter a for the monitoring template you are creating.
6. In the Metric Thresholds tab, select one or more metrics you want to add to the template.

If you want to add additional metrics, which are not listed on this page, click **Add Metrics to Template**. Then select a source from which you can copy metrics to the template.

7. Click **OK**.
-



Learn More

- What Is a Monitoring Template?
- What Does a Monitoring Template Define?



Perform Additional Tasks

- How to View a List of Monitoring Templates?
- How to Edit a Monitoring Template?
- How to Apply a Monitoring Template to a Target?
- How to Compare Monitoring Templates with Targets?



Perform Additional Tasks

- How to Compare Metric Settings Using Information Publisher?
 - How to Export and Import Monitoring Templates?
 - How to Change the Monitoring Template Apply History Retention Period?
-

Setting Up Administration Group Hierarchy



Administration groups are a special type of group used to fully automate application of monitoring and other management settings targets upon joining the group. When a target is added to the group, Enterprise Manager applies these settings using a template collection consisting of monitoring templates, compliance standards, and cloud policies. This completely eliminates the need for administrator intervention. After discovering and monitoring targets, and after creating monitoring templates, create an administration group hierarchy so that the monitored targets can be logically grouped, and the monitoring templates can be applied globally.

Step 1: Set Target Properties to Monitored Targets	Step 2: Define a Hierarchy	Step 3: Defining Template Collections	Step 4: Associate Template Collections and Set a Synchronization Schedule
<ol style="list-style-type: none"> 1. Access the Home page of the monitored target. 2. From the target menu, select Target Setup, then select Properties. 3. On the Target Properties page, click Edit. 4. Set or specify values for the properties of interest. 5. Click OK. <p>Note: For large numbers of targets, it is best to use the EM CLI verb <code>set_target_property_value</code> to perform a mass update. For more information, see <i>Oracle Enterprise Manager Command Line Interface Guide</i>.</p>	<ol style="list-style-type: none"> 1. From the Setup menu, select Add Target, then select Administration Groups. 2. On the Administration Groups and Template Collections page, click the Hierarchy tab. 3. In the Hierarchy Levels table, click Add. Select one of the available target properties. Repeat this step until you have added all target properties of interest. 4. In the Hierarchy Levels table, click on one of the newly added property. 5. In the Hierarchy Nodes table, if the property values to do appear by default, click Add. 6. Click OK. 7. Repeat Step (4) to Step (6) until all the newly added properties have been provided with a value. 8. Click on the group name, and set the time zone for the group. 9. Click Create. 	<ol style="list-style-type: none"> 1. From the Setup menu, select Add Target, then select Administration Groups. 2. On the Administration Groups and Template Collections page, click the Template Collections tab. 3. Click Create. 4. On the Create Template Collection page, provide a template collection name. 5. In the Monitoring Template subtab, click Add and select a monitoring template you want to apply. 6. (Optional) In the Compliance Standard subtab, click Add and select a compliance standard you want to apply. 7. (Optional) In the Cloud Policies subtab, click Add and select the cloud policy you want to apply. 8. Click Save. 9. Repeat Step (2) to Step (8) if you want to create additional template collections. 	<ol style="list-style-type: none"> 1. From the Setup menu, select Add Target, then select Administration Groups. 2. On the Administration Groups and Template Collections page, click the Associations tab. 3. Select the administration group at the highest level in the hierarchy, and click Associate Template Collection. 4. Choose the desired template collection and click Select. All sub-nodes in the hierarchy will automatically inherit the selected template collection. 5. Click Synchronization Schedule. 6. In the Synchronization Schedule dialog, click Edit. 7. Set a suitable schedule for the administration group changes to be applied to targets. 8. Click Save.



Learn More

- What Is an Administration Group?
- What Privileges Are Required for Developing an Administration Group?



Perform Additional Tasks




- How to Plan for Creating Administration Groups?
 - How to Remove Administration Groups?
-

Setting Up Notifications



The notification system notifies you when specific incidents, events, or problems arise. All Enterprise Manager administrators can set up e-mail notifications for themselves. Super Administrators also have the ability to set up notifications for other Enterprise Manager administrators. Set up the mail server, define e-mail addresses to be used, and set up a notification schedule so that you can be notified.

Step 1: Set Up a Mail Server	Step 2: Define E-mail Addresses	Step 3: Set Up a Notification Schedule
<ol style="list-style-type: none"> From the Setup menu, select Notifications, then select Notification Methods. On the Notification Methods page, in the Mail Server section, enter one or more outgoing mail server names. Enter the mail server authentication credentials. Enter the name you want to see displayed as the sender of the notification messages. Enter the e-mail address you want to use to send your e-mail notifications. Click Test Mail Servers. Verify if an e-mail was sent to the e-mail account entered in the Sender's E-mail Address field. Click Apply. 	<ol style="list-style-type: none"> From the <i>username</i> menu, in the top-right corner of the console, select Enterprise Manager Password & E-mail. On the Enterprise Manager Password & Email page, in the E-Mail Addresses section, click Add Another Row. Enter an e-mail address associated with your Enterprise Can contain up to 128 characters Click Apply. Repeat the steps to add additional e-mail addresses where notifications must be sent. 	<ol style="list-style-type: none"> From the Setup menu, select Notifications, then select My Notification Schedule. On the Notification Schedule page, click Edit Schedule Definition. On the Time Period page, edit the rotation frequency, and click Continue. On the E-Mail Addresses page, modify the e-mail addresses where the notifications must be sent at the set frequency. Click Finish. (Optional) On the Notification Schedule page, click the search icon (magnifying glass) and select another administrator. Click Change. (Optional) Repeat Step (2) to Step (5). (Optional) Repeat Step (6) and Step (7) for all other administrators.




Perform Additional Tasks	Perform Additional Tasks	Perform Additional Tasks
 <ul style="list-style-type: none"> How Do I Set Up E-mail Notifications for Other Administrators? How Do I Customize E-Mail Formats? How Do I Set Up Repeat Notifications? 	 <ul style="list-style-type: none"> How Do I Send SNMP Traps to Third Party Systems? How Do I Send Notifications Using OS Commands and Scripts? How Do I Send Notifications Using PL/SQL Procedures? 	 <ul style="list-style-type: none"> How Do I Troubleshoot Notifications?

Setting Up Incident Rule Sets and Subscribing to Receive E-Mail Notifications



An *incident rule* instructs Enterprise Manager to take specific actions when incidents, events, or problems occur, such as performing notifications. An *incident rule set* is a collection of *rules* that apply to a common set of objects such as targets (hosts, databases, groups), jobs, metric extensions, or self updates, and take appropriate actions when there are events and incidents. An *event* is a significant occurrence of interest on a target that has been detected by Enterprise Manager. An *incident* is a set of significant events or combination of related events that pertain to the same issue. Create your incident rule sets and subscribe to them so that you are notified every time there is an event or incident.

Step 1: Create and Subscribe to Custom Incident Rules	Step 2: Subscribe to Out-of-Box Incident Rules
<ol style="list-style-type: none"> From the Setup menu, select Incidents, then select Incident Rules. From the Actions menu, select Create Rule Set. Enter a name and description for the rule set. In the Targets tab, select the targets to which the rules set should apply. In the Rules tab, click Create. Select Incoming events and updates to events, and click Continue. On the Select Events page, set the criteria for events based on which the rule should act. Click Next. On the Add Actions page, click Add and add actions to be taken by the rule. In the Notifications section, enter the e-mail addresses where the notifications must be send. Click Next. Multiple conditional actions can be specified and evaluated sequentially (top down) in the order you add them. On the Specify Name and Description page, enter a name and description for the rule. Click Next. On the review page, review the details, and click Continue. On the Create Rule Set page, click Save. 	<ol style="list-style-type: none"> From the Setup menu, select Incidents, then select Incident Rules. On the Incident Rules - All Rules page, in the table, select the rule set to which you want to subscribe. From the Actions menu, select E-Mail, then select Subscribe Me.

	Perform Additional Tasks <ul style="list-style-type: none">■ What Are Events?■ What Are Incidents?■ What Are Problems?■ What Are the Out-of-Box Rule Sets?■ What Are the Types of Rule Sets?■ What Is an Incident Manager?■ What Are the Guidelines for Creating Rule Sets?		Perform Additional Tasks <ul style="list-style-type: none">■ How to Create a Rule to Manage Escalation of Incidents?■ How to Create a Rule to Escalate a Problem?■ How to Receive E-mails for Private Rules?■ How to Search Incidents?■ How to Set Up Custom Views?		Perform Additional Tasks <ul style="list-style-type: none">■ How to Respond and Work on a Simple Incident?■ How to Respond to and Manage Multiple Incidents, Events and Problems in Bulk?■ How to Suppress Incidents and Problems?■ How to Review Events Periodically?
---	--	---	--	--	--

Setting Up Reporting Framework



Oracle Business Intelligence Publisher (BI Publisher) is Oracle's primary reporting tool for authoring, managing, and delivering all your highly formatted documents. Set up the reporting framework using BI Publisher so that you can generate high-quality reports and documents, with pagination and headers/footers, and in formats such as PDF, Excel, Powerpoint, Word, and HTML.

Step 1: Download BI Publisher 11.1.1.6.0

Download the software from the Oracle Enterprise Manager Downloads page.

(Search for the product title *Oracle Business Intelligence Publisher 11.1.1.6.0*)

Step 2: Back Up the OMS and the Domain

1. Back up the OMS as described in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
2. Back up the domain:


```
cd
<Instance-Home>/user_projects/domains
zip -r
GCDomain.zip
GCDomain
```

Step 3: Install BI Publisher

1. Run the BI Publisher installer:
2. (Optional) Select an e-Mail address for updates, and click **Next**.
3. Select **Software-only Install**, and click **Next**.
4. After passing the prerequisite checks, click **Next**.
5. Select the Middleware home of your Enterprise Manager installation.
6. Retain the default name `Oracle_BI1` as the BI Oracle home name, and click **Next**.
7. (Optional) Enter the My Oracle Support credentials to be notified of any security update, and click **Next**.




Step 4: Integrate with Enterprise Manager

1. Run the `configureBIP` script:


```
$<OMS_HOME>/bin/configureBIP
```
2. Enter the necessary credentials when prompted.
3. Enter the HTTP and HTTPS ports when prompted. The script identifies free ports and ask if you want to take them as a default. Once entered, `Extend Domain` then runs. The ports can be in the range 9701-49152.

Step 5: Verify the Integration

1. From the **Enterprise** menu, select **Reports**, then select **BI Publisher Enterprise Reports**.
2. On the BI Publisher Enterprise Reports page, click the refresh icon at the top-right corner.
3. Expand **EM Sample Reports**, then click **Targets of Specified Type**.
4. Log in to BI Publisher using your Enterprise Manager credentials.
5. Verify if you are able to see the sample report.

	Learn More <ul style="list-style-type: none">■ What Limitations Apply to the Use of Reports and Data Sources?■ Do I Require a Centralized Inventory File for BI Publisher?■ What Are the Hardware Requirements for Installing BI Publisher?		Perform Additional Tasks <ul style="list-style-type: none">■ How Do I Authenticate and Limit Access to BI Publisher Features?■ How Do I Grant BI Publisher OPSS Application Roles to Administrators?■ How Do I Grant Access to Administrators Using the LDAP Authentication Security Model?■ How Do I Map LDAP Groups to BI Publisher OPSS Application Roles?		Perform Additional Tasks <ul style="list-style-type: none">■ How Do I Grant Access to Folders and Catalog Objects?■ How Do I Manage Enterprise Manager - BI Publisher Connection Credentials?■ How Do I Manage the BI Publisher Server?■ How Do I Configure BI Publisher with a Load Balancer?■ How Do I Troubleshoot BI Publisher-Related Issues?
---	--	---	---	--	---
