Oracle® Enterprise Manager

Cloud Control Getting Started Guide

13*c* Release 2

E74868-02

September 2016

ORACLE®

Oracle Enterprise Manager Cloud Control Getting Started Guide, 13*c* Release 2

E74868-02

Primary Author: Oracle Corporation

Contents

Preface

Oracle Enterprise Manager Cloud Control Getting Started Guide enables you to set up and get started with Enterprise Manager Cloud Control 13*c* Release 2.

This preface covers the following topics:

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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

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	Step 11	Step 12
Configure Self Update Configure Self Update for automatically downloading software, software updates, plug-ins, and so on from My Oracle Support.	**Download Agent Software** Download the Management Agent software for platforms other than the one on which OMS is running.	**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	**Step 14**	**Step 15**
Discover Targets Scan your network and discover hosts and targets running on those hosts.	**Monitor Targets** Promote and monitor the discovered targets.	**Create Monitoring Templates** Specify monitoring settings once and apply them to all monitored targets.
Step 16	**Step 17**	**Step 18**
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	**Set Up Notifications** Set up e-mail servers, e-mail addresses, and notification schedule for e-mail notifications.	**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.		

2

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

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.

Import to Mozilla Firefox Version 28.0

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.**

Importing to Google Chrome Version 44+

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?

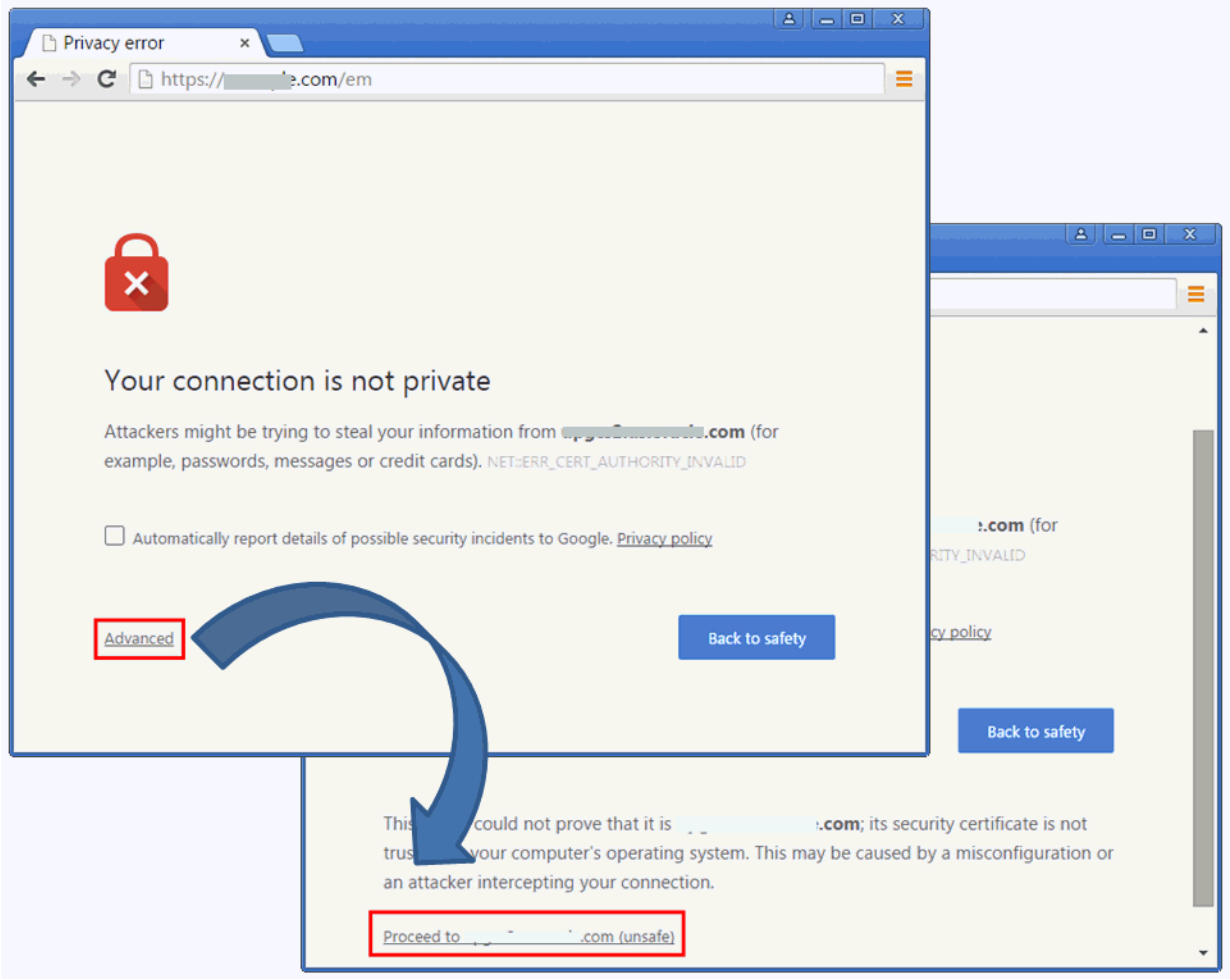
Perform Additional Tasks
How to Respond to Mozilla Firefox New Site Certificate Dialog Box?

Perform Additional Tasks
How to Respond to Safari Security Dialog Box?

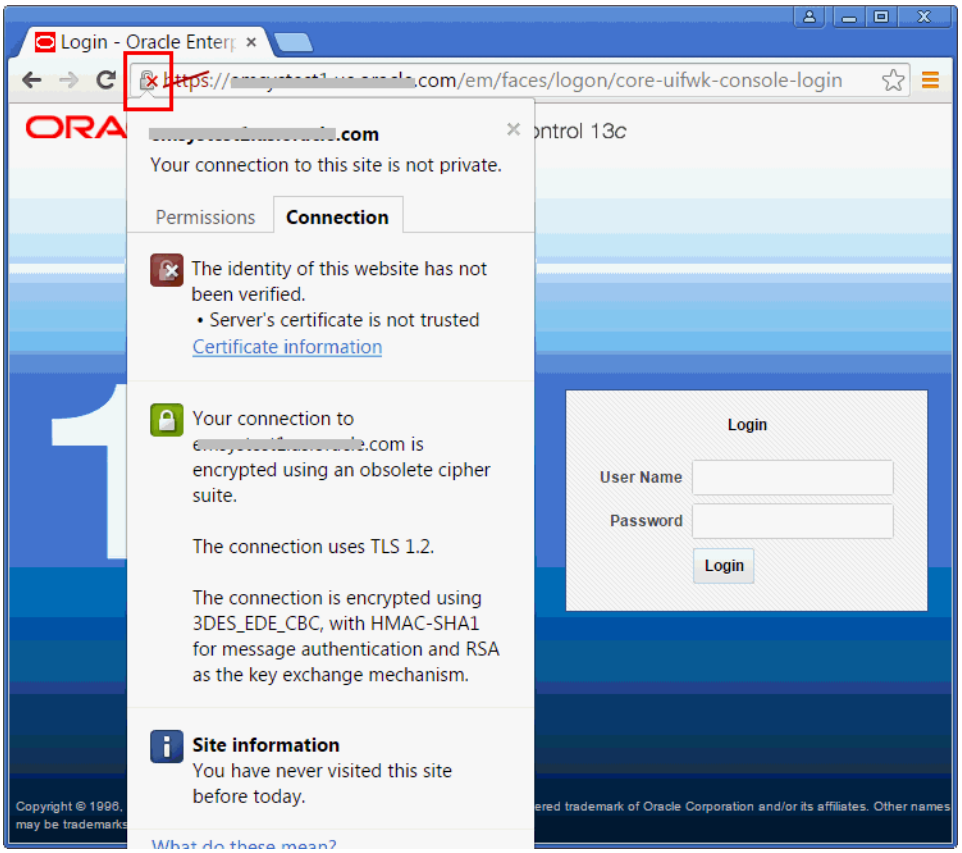
2.1 Screenshots for Importing Browser Certificates to Google Chrome 44+

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.

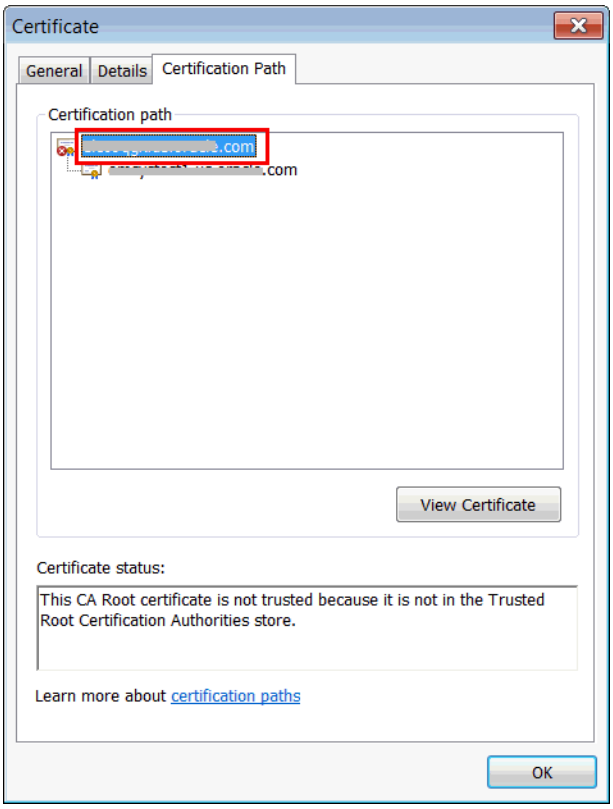
2.1.1 Screenshot for Step 1: On the Privacy error page, . . .



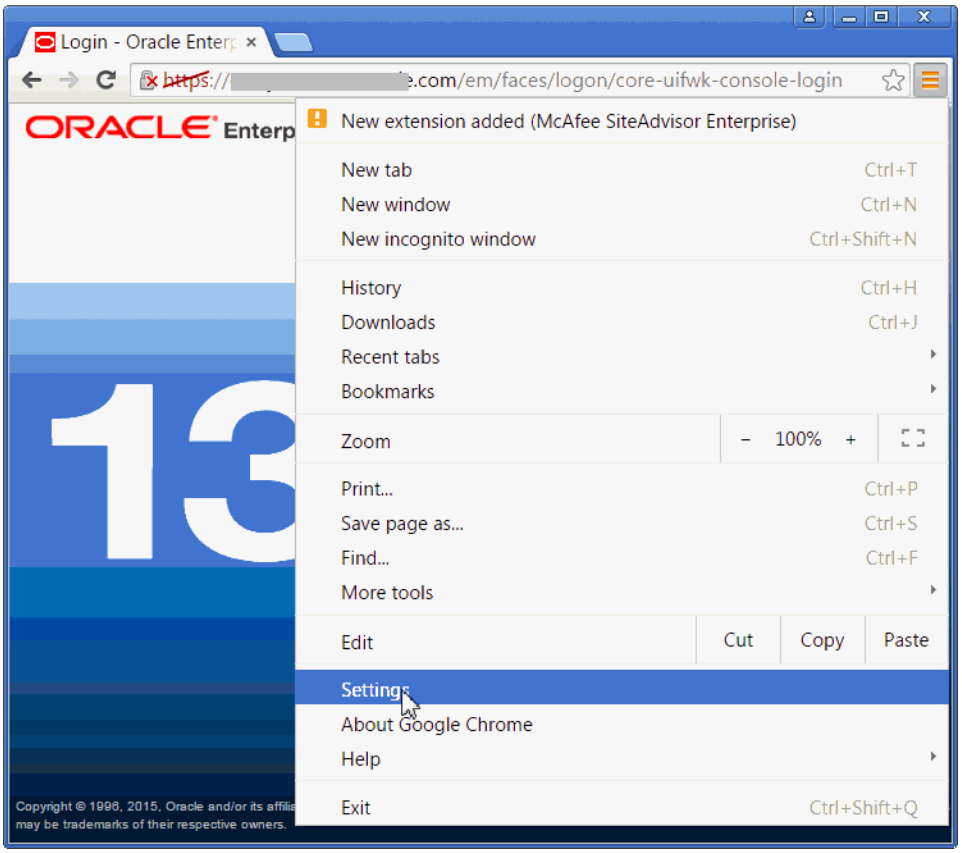
2.1.2 Screenshot for Step 2: In the address bar, . . .



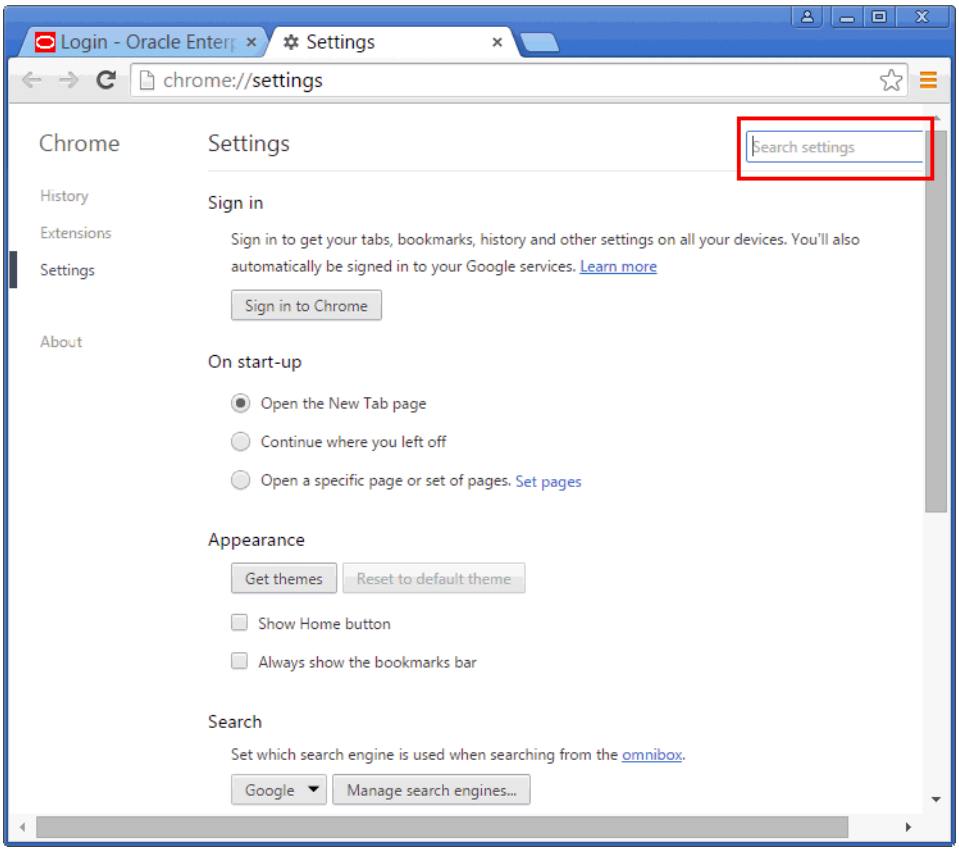
2.1.3 Screenshot for Step 5: Select the root node in the . . .



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



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



3

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?

4

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`

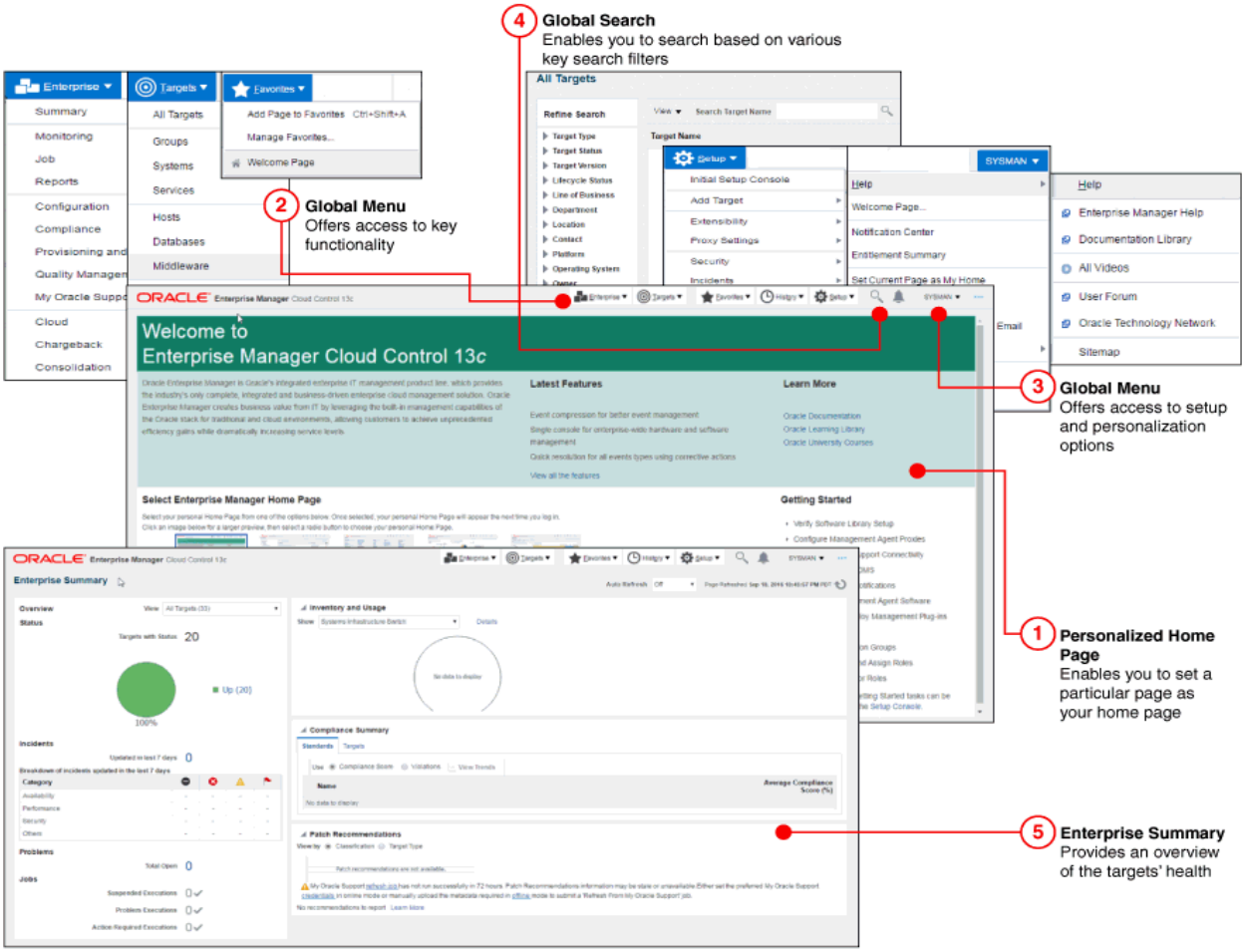
   Ensure that the OMS host name is a fully qualified name, and the console port is the port you identified in the previous step.

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.**

5

Exploring the Interface



6

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.**

7

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, click **Initial Setup Console.**
2. On the Initial Setup Console page, in the left panel, click **Create Roles.**
3. On the Create Roles page, collapse the **Top 5 Administrators with the Highest Number of Roles** section and the **Roles with the Highest Number of Nested Roles** section to see the following text below the section. Click **here.**

   Enterprise Manager Roles can be managed from here
4. On the Roles page, click **Create.**

   Enterprise Manager Cloud Control displays the Create Role Wizard.
5. In the Create Role Wizard, on the Properties page, enter a unique name for the role, and click **Next.**
6. 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 grants all privileges to grantee of current role.
7. On the Target Privileges page, select the privileges common to all targets and the privileges specific to certain targets, which you want to grant explicitly to the role you are creating, and click **Next.**
8. On the Resource Privileges page, select the resource privileges you want to grant explicitly to the role you are creating, and click **Next.**
9. On the Administrators page, select the administrator you want to grant this role to, click **Next.**
10. On the Review page, click **Finish.**

Step 2: Create Administrators

1. From the **Setup** menu, select **Initial Setup Console.**
2. On the Initial Setup Console page, click **Create Users.**
3. On the Create Users page, in the Enterprise Manager Super Administrators section, view a list of super administrators created so far in the Enterprise Manager system, and their last authenticated time.
4. Collapse the Enterprise Manager Super Administrators section to see the following text below the section. Click **here.**

   Enterprise Manager Administrators can be managed from here
5. On the Administrators page, click **Create.**

   Enterprise Manager Cloud Control displays the Create Administrator Wizard.
6. In the Create Administrator Wizard, on the Authentication page, select the authentication mechanism to be used for the user you are creating, and click **Next.**
7. On the Properties page, provide details of the user you are creating, and click **Next.**
8. On the Roles page, from the Available Roles list, select the roles you want to grant explicitly to the user you are creating, and click **Next.**
9. On the Target Privileges page, select the privileges you want to grant to the user you are creating, and click **Next.** These privileges give the user the right to perform particular management actions on a set of targets.
10. On the Resource Privileges page, select the resource privileges you want to grant explicitly to the user you are creating, and click **Next.**
11. 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?

8

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	Step 2: Update Audit Settings

Run the following command:
`emcli enable_audit`
 	
For example,
`emcli enable_audit`
	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?

9

Setting My Oracle Support Credentials

My Oracle Support connectivity enables you to view service request information, obtain patch recommendations, and download plug-ins and other entities to the Software Library, all from within the Enterprise Manager Cloud Control Console. To automatically sign in to My Oracle Support from within the Enterprise Manager Cloud Control Console, you must register the My Oracle Support credentials with Enterprise Manager Cloud Control. If you have already registered the My Oracle Support credentials, then this setup task appears as if it is complete.

Configure My Oracle Support

1. From the **Setup** menu, click **Initial Setup Console.**
2. On the Initial Setup Console page, in the left panel, click **Set MOS Credentials.**
3. On the Set MOS Credentials page, click **here.**
4. On the My Oracle Support page, enter the My Oracle Support credentials.
5. 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?

10

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 **Initial Setup Console.**
2. On the Initial Setup Console page, in the left panel, click **OMS Agent Proxy Setting.**
3. Follow Step (3) to Step (6) as outlined in *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

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?

11

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
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 Setting My Oracle Support Credentials	See Configuring Software Library

Learn More

- 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

- How Do I Assign Self Update Privileges to Administrators?
- How Do Apply the Updates Offline?

Perform Additional Tasks

- How Do I Access Informational Updates?
- How Do I Acquire or Update Management Agent Software via Self Update Console?

12

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	1. From the **Setup** menu, select **Extensibility,** then select **Self Update.** 2. In the table, click the entity type **Agent Software.** 3. 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 *Available.* The Download button is enabled only in the following cases: ▪ 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 Available or Download Failed 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. 4. In the Schedule Download dialog, schedule the download activity, and click **Select.**	1. From the **Setup** menu, select **Extensibility,** then select **Self Update.** 2. In the table, click the entity type **Agent Software.** 3. 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?

13

Setting Up Oracle Management Service Agent Proxy

You can secure the communication between Oracle Management Service (OMS) and Oracle Management Agents (Management Agents) by configuring a proxy. A proxy is an application external to Enterprise Manager Cloud Control that acts as an intermediary for managing HTTP as well as HTTPS requests across network boundaries or firewalls. By using a proxy, you can expose only certain ports for communication, and thereby have a more secure and reliable communication between the OMS and the Management Agents.

You can configure one proxy for all Management Agents, one proxy for a set of Management Agents and none for the rest, or different proxies for different sets of Management Agents.

In addition, you can configure two or more proxies as *redundant proxies* to support high availability of the proxies configured for OMS and Management Agent communication. Under such circumstances, by default, the proxy that is up and running is selected for communication, regardless of the status of the other proxies. Before starting to communicate if a proxy is found to be inactive or down, then an alternate proxy configured for that Management Agent is selected. However, note that after the communication begins through a particular proxy, if that proxy turns inactive or shuts down, then no fallback mechanism is currently available to select an alternate proxy that is up and running.

Note:

- NTLM-based Microsoft proxies are not supported. To enable access through such proxies, add all the available agent hosts to the *Unauthenticated Sites Properties* of the NTLM-based Microsoft proxy.
- Local addresses of each OMS automatically bypass the proxy.

Configure Proxy

1. From the **Setup** menu, select **Initial Setup Console.**
2. On the Initial Setup Console page, in the left panel, click **OMS Agent Proxy Setting.**
3. Follow Step (3) to Step (6) as outlined in *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*

14

Setting Up OMS My Oracle Support Proxy

Oracle Management Service (OMS) uses the Internet connectivity on its host to connect to My Oracle Support periodically to download patches, patch sets, patch recommendations, and Automated Release Updates (ARU) seed data. By default, Enterprise Manager Cloud Control assumes that there is no proxy configured between the OMS and My Oracle Support. However, to secure the communication, you can add a proxy between the two entities.

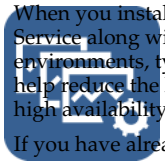
If you have already configured a proxy, then this setup task appears as if it is complete.

Set Up OMS My Oracle Support Proxy

1. From the **Setup** menu, select **Initial Setup Console.**
2. On the Initial Setup Console page, in the left panel, click **My Oracle Support.**
3. Follow Step (2) to Step (7) as outlined in *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*

15

Adding Additional Oracle Management Service



When you install Enterprise Manager Cloud Control, by default, the installer installs one Oracle Management Service along with one Oracle Management Agent. While this default configuration suits smaller environments, typically in larger production environments, you might require additional OMS instances to help reduce the load on a single Oracle Management Service, improve the efficiency of the data flow, and offer high availability of your Enterprise Manager system.

If you have already added an additional OMS, then this setup task appears as if it is complete.

Step 1: Review the Important Facts	Step 2: Meet the Prerequisites	Step 3: Add Oracle Management Service
Before you begin adding an additional Oracle Management Service, review the important facts as described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.	Meet the prerequisites for an additional Oracle Management Service as described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.	1. From the **Setup** menu, click **Initial Setup Console.** 2. On the Initial Setup Console page, in the left panel, click **Add Oracle Management Service.** 3. On the Add Management Service Getting Started page, complete the preinstallation tasks listed there. Once you are done, select each of the tasks you have complete, and then, click **Next.** 4. Follow Step (4) to Step (7) as outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. 5. After adding the additional Oracle Management Service, perform the postinstallation tasks as described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

16

Configuring Outgoing Mail Servers (SMTP Servers)

Notifications keep you informed when specific incidents, events, or problems arise, and thereby enable you to take corrective or preventive actions to circumvent the reported issue. Enterprise Manager uses different mechanisms for sending these notifications, including email, SNMP traps, or running custom scripts, or all three. Before Enterprise Manager Cloud Control can send e-mail notifications, you must set up the outgoing mail servers (SMTP servers).

If you have already configured the SMTP servers, then this setup task appears as if it is complete.

Configure Outgoing Mail Servers

1. From the **Setup** menu, click **Initial Setup Console.**
2. On the Initial Setup Console page, in the left panel, click **Configure Mail Servers.**
3. On the Configure Mail Servers page, in the Sender Identify section, click **Edit.**
4. In the Sender Identify dialog, enter the name of the administrator or system that should send the email notifications, and the email address from which the notifications should be sent. Click **OK.**
5. In the Outgoing Mail (SMTP) Servers section, click **Create.**
6. In the Outgoing Mail (SMTP) Servers dialog, enter the mail server host name, the mail server credentials, and the encryption method to be used. Click **OK.**

   If you configure multiple outgoing mail servers, automatic failover and load balancing is performed in round robin fashion.

17

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	1. From the **Setup** menu, select **Extensibility,** then select **Plug-ins.** 2. 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.	1. From the **Setup** menu, select **Extensibility,** then select **Self Update.** 2. On the Self Update page, in the table, click the entity type **Plug-in.** 3. In the Plug-in Updates table, select the plug-in available for download, and click **Download.** 4. In the Schedule Download dialog, schedule the download activity, and click **Select.**	1. From the **Setup** menu, select **Extensibility,** then select **Plug-ins.** 2. On the Plug-ins page, select the plug-in you want to deploy. 3. From the **Deploy On** menu, select **Management Servers.** 4. In the Deploy Plug-in on Management Servers dialog, enter the Management Repository SYS password, and click **Continue.** Proceed through the steps in the dialog box, and then click **Deploy.**

Learn More

- 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?

Perform Additional Tasks

- 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?

Perform Additional Tasks

- 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?

18

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. The steps to discover and add database, middleware, and system infrastructure targets might vary.

Step 1: Scan Your Network

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.**

Step 2: Promote and Monitor Hosts

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.

Step 3: Discover Targets

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

- 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

- How Do I Discover and Promote All Target Types?
- How Do I Discover and Promote Oracle Homes?

Perform Additional Tasks

- How Do I Discover and Add Host and Non-Host Targets?
- How Do I Discover and Add Database Targets?
- How Do I Discover and Add Middleware Targets?
- How Do I Discover and Add System Infrastructure Targets?

19

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?

20

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?

21

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

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.**

Note: For large numbers of targets, it is best to use the EM CLI verb `set_target_property_value` to perform a mass update. For more information, see *Oracle Enterprise Manager Command Line Interface Guide*.

Step 2: Define a Hierarchy

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.**

Step 3: Defining Template Collections

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.

Step 4: Associate Template Collections and Set a Synchronization Schedule

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?

22

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

1. From the **Setup** menu, select **Notifications,** then select **Notification Methods.**
2. On the Notification Methods page, in the Mail Server section, enter one or more outgoing mail server names.
3. Enter the mail server authentication credentials.
4. Enter the name you want to see displayed as the sender of the notification messages.
5. Enter the e-mail address you want to use to send your e-mail notifications.
6. 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.
7. Click **Apply.**

Step 2: Define E-mail Addresses

1. From the *username* menu, in the top-right corner of the console, select **Enterprise Manager Password & E-mail.**
2. On the Enterprise Manager Password & Email page, in the E-Mail Addresses section, click **Add Another Row.**
3. Enter an e-mail address associated with your Enterprise Can contain up to 128 characters
4. Click **Apply.**
5. Repeat the steps to add additional e-mail addresses where notifications must be sent.

Step 3: Set Up a Notification Schedule

1. From the **Setup** menu, select **Notifications,** then select **My Notification Schedule.**
2. On the Notification Schedule page, click **Edit Schedule Definition.**
3. On the Time Period page, edit the rotation frequency, and click **Continue.**
4. On the E-Mail Addresses page, modify the e-mail addresses where the notifications must be sent at the set frequency.
5. Click **Finish.**
6. (Optional) On the Notification Schedule page, click the search icon (magnifying glass) and select another administrator. Click **Change.**
7. (Optional) Repeat Step (2) to Step (5).
8. (Optional) Repeat Step (6) and Step (7) for all other administrators.

Perform Additional Tasks

- 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?

Perform Additional Tasks

- 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?

Perform Additional Tasks

How Do I Troubleshoot Notifications?

23

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

1. From the Setup menu, select **Incidents,** then select **Incident Rules.**
2. From the **Actions** menu, select **Create Rule Set.**
3. Enter a name and description for the rule set.
4. In the Targets tab, select the targets to which the rules set should apply.
5. In the Rules tab, click **Create.**
6. Select **Incoming events and updates to events,** and click **Continue.**
7. On the Select Events page, set the criteria for events based on which the rule should act. Click **Next.**
8. 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.
9. On the Specify Name and Description page, enter a name and description for the rule. Click **Next.**
10. On the review page, review the details, and click **Continue.**
11. On the Create Rule Set page, click **Save.**

Step 2: Subscribe to Out-of-Box Incident Rules

1. From the **Setup** menu, select **Incidents,** then select **Incident Rules.**
2. On the Incident Rules - All Rules page, in the table, select the rule set to which you want to subscribe.
3. From the **Actions** menu, select **E-Mail,** then select **Subscribe Me.**

Perform Additional Tasks

- 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

- 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

- 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?

24

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	Step 2: Back Up the OMS and the Domain	Step 3: Install BI Publisher	Step 4: Integrate with Enterprise Manager	Step 5: Verify the Integration

Download the software from the Oracle Enterprise Manager Downloads page.
(Search for the product title Oracle Business Intelligence Publisher 11.1.1.6.0)
	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`
		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.**
			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.
				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

- 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

- 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

- 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?