Oracle® Enterprise Manager Ops Center

Security Guide

11*g* Release 1 Update 3 (11.1.3.0.0)

E20615-04

November 2011

Oracle Enterprise Manager Ops Center Security Guide 11*g* Release 1 Update 3 (11.1.3.0.0)

E20615-04

Primary Author: Barbara Higgins

Contributor: Jeff Hanson

Contents

3 Security Features

Preface

The *Oracle Enterprise Manager Ops Center Security Guide* describes good practices for managing security of Oracle Enterprise Manager Ops Center deployments.

Audience

This document is intended for system administrators who are responsible for planning the configuration of the Enterprise Manager Ops Center software.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the documents in the Oracle Enterprise Manager Ops Center 11g Release 1.0 documentation set:

- *Oracle Enterprise Manager Ops Center Concepts Guide*
- *Oracle Enterprise Manager Ops Center User's Guide*
- *Oracle Enterprise Manager Ops Center Advanced User's Guide*
- *Oracle Enterprise Manager Ops Center Provision and Update Guide*
- *Oracle Enterprise Manager Ops Center Administration Guide*
- *Oracle Enterprise Manager Ops Center Reference Guide*
- *Oracle Enterprise Manager Ops Center Installation Guide for Oracle Solaris Operating System*
- *Oracle Enterprise Manager Ops Center Installation Guide for Linux Operating Systems*
- *Oracle Enterprise Manager Ops Center Site Preparation Guide*

- *Oracle Enterprise Manager System Monitoring Plug-In for Oracle Enterprise Manager Ops Center Guide*
- *Oracle Enterprise Manager Ops Center Release Notes*
- *Oracle Enterprise Manager Ops Center Readme*

Conventions

The following text conventions are used in this document:

Convention	Meaning
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands, file names, and directories within a paragraph, and code in examples.

1 Overview

Oracle Enterprise Manager Ops Center is a data center management solution for managing both hardware and software from one console. This document presents good practices for managing the security of Oracle Enterprise Manager Ops Center deployments.

Product Architecture

The Oracle Enterprise Manager Ops Center software has a distributed architecture with a single master controller (Enterprise Controller) and multiple slave controllers (Proxy Controllers). The Proxy Controllers are used for fan-out operations, to gain the benefits of scaling, and to support complex network topologies. Each Proxy Controller connects either to multiple Agent Controllers hosted on an Operating System instance or to managed systems or to both. Using the Internet, the Enterprise Controller can also connect to an Oracle Knowledge Base to download software for installation and to get access to dependent knowledge for installation software.

Knowledge Base (KB)

The Knowledge Base is the repository for metadata about Oracle Solaris and Linux OS components, which resides on Oracle's website. Enterprise Manager Ops Center can connect to the Knowledge Base through the Internet to obtain software updates.

Enterprise Controller

The Enterprise Controller is the central server for Enterprise Manager Ops Center and there is only one Enterprise Controller in each installation. The Enterprise Controller stores firmware and OS images, plans, profiles, and policies. It also stores the asset data and site customizations in a PostgreSQL database and hosts the web container for the user interface components. The Enterprise Controller handles all user authentication and authorization. All operations are initiated from the Enterprise Controller.

Proxy Controller

A Proxy Controller links the managed assets to the Enterprise Controller and acts for the Enterprise Controller in operations that must be located close to managed assets, such as OS provisioning. The Proxy Controller provides fan-out capabilities to minimize network load. It also contains the logic for agent-less monitoring and management of hardware.

Agent

An Agent is lightweight Java software that identifies each OS asset or OS instance and responds to requests from a Proxy Controller. Hardware management does not require an agent. The Agent receives the command, performs the required action, and reports results to the Proxy Controller. An agent never communicates directly with the Enterprise Controller.

General Principles of Security

This section describes the principles fundamental to using the software securely.

Keep Software Up To Date

Good security is maintained when all software versions and patches are up to date. This document discusses Enterprise Manager Ops Center version 11.1.1.0.0. As new versions or updates of Enterprise Manager Ops Center become available, install the new software as soon as possible.

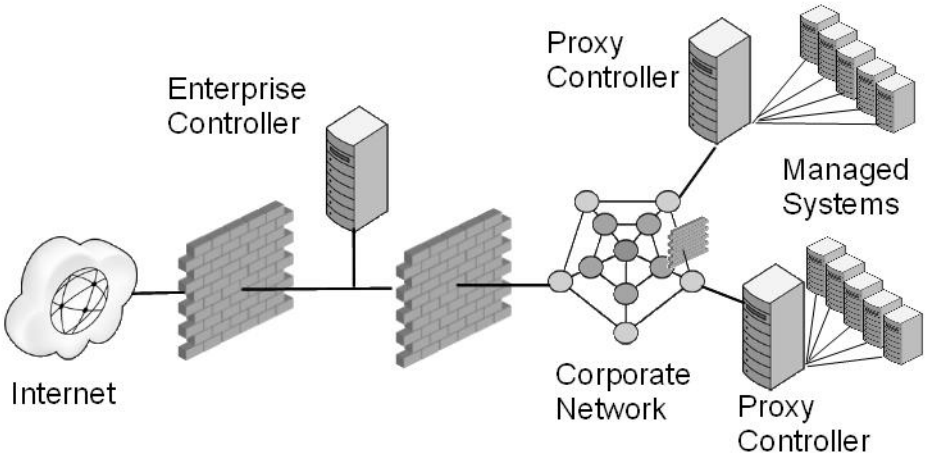
Restrict Network Access

Firewalls restrict access to systems to a specific network route, which can be monitored and controlled. When firewalls are used in combination, they create a DMZ, a term for a subnetwork that controls access from an untrusted network to the trusted network. Using firewalls to create a DMZ provide two essential functions:

- Blocks traffic types that are known to be illegal.
- Contains any intrusion that attempts to take over processes or processors.

In your deployment, design an environment that locates the Enterprise Controller's system in a DMZ, that is, with a firewall between the system and the Internet and a firewall between the system and the corporate intranet.

Figure 1–1 Firewalls Restrict Access to Enterprise Controller



If your data center includes remote Proxy Controllers, use firewalls between the Enterprise Controller's system and the Proxy Controllers' systems.

To use Enterprise Manager Ops Center in Connected mode to get access to Oracle and third-party sites, use the information in Table 1–1 to configure the firewall between the Enterprise Controller and the Internet.

Table 1–1 IP Address and Ports for Third-Party Sites

Site	IP Address	Port
updates.oracle.com	[1]	Port 443
aru-akam.oracle.com	[1]	Port 80
aru-llnw.oracle.com	[1]	Port 80
aru-llnw-dl.oracle.com	[1]	Port 80
a248.e.akamai.net	[1]	Port 443
inv-cs.sun.com	192.18.110.18	Port 443
inventory.sun.com	192.18.110.16	Port 443
getupdates.oracle.com	[1]	Port 443
inv-cs.oracle.com	192.18.110.10	Port 443
support.oracle.com	141.146.54.16	Port 443
hs-ws1.oracle.com	192.18.110.11	Port 443
www.oracle.com	96.17.111.33 and 96.17.111.49	Port 80

[1] This site provides local IP addresses to optimize download speed. You must resolve the IP addresses locally, use that local address in your firewall rules, and ensure that the host always uses the local address to match your firewall rules. To accomplish these tasks, use `nslookup` to resolve the IP address, add the address to the `/etc/hosts` file, and open the firewall for the address.

To configure the firewall between the Enterprise Controller and a Proxy Controller or a corporate network, allow the ports and protocols in Table 1–2.

Table 1–2 Required Ports and Protocols

Communication	Protocol and Port	Purpose
Browser to Enterprise Controller	HTTPS, TCP 9443	Web interface
Browser to Enterprise Controller	HTTP, TCP 80	Redirects to port 9443
Proxy Controller to Enterprise Controller	HTTPS, TCP 443	Proxy Controller pushes asset data to Enterprise Controller. Proxy Controller pulls data for jobs, updates, agents, and OS images.
Enterprise Controller to Proxy Controller	SSH: Port 22	During Proxy Controller installation or updates performed through the UI.
Java client to public APIs	Transport Layer Security (TLS): Port 11172	JMX access from clients
Proxy Controller to NFS server	Port 2049 (default) See operating system documentation for configuring NFS	Proxy Controller pulls provisioning images.
Enterprise Controller	Port 8005	Enterprise Controller in Disconnected mode

Follow the Principle of Least Privilege

The principle of least privilege states that users are given the least amount of privilege to perform their jobs. Granting roles or privileges in access of a user's responsibilities leaves a system open for non-compliance. Review privileges periodically to determine whether they remain appropriate for each user's current job responsibilities.

You can assign different Enterprise Manager Ops Center roles to users to restrict access to specific features or managed assets. The following roles have been defined in Enterprise Manager Ops Center:

- The Enterprise Controller Admin role grants root access. A user with the Enterprise Controller Admin role can perform asset discovery, perform administration actions on Oracle Enterprise Manager Ops Center, add new users, edit roles, and create new profiles, policies, and plans. When Oracle Enterprise Manager Ops Center is configured, the privileged user is given this role automatically. At least one user must have this role.
- The All Assets Admin role can perform any action, including provisioning, updating, and managing, on any asset or group. When Oracle Enterprise Manager Ops Center is configured, the privileged user is given this role automatically.

Managed assets can be assigned to one or more groups. Groups can also be used with roles to restrict access to specific assets. An Enterprise Controller Admin can grant one or more of these roles to any user for any group:

- Group Admin: A user with the Admin role for a group has unlimited access to assets within that group. They can take any action on the assets in the group, including installing agents, updating or provisioning operating systems, provisioning firmware, and managing and monitoring assets. However, they cannot edit or add assets to the group.
- Group Provision: A user with the Provision role for a group can provision operating systems and firmware onto assets in the group. The user can use existing profiles, policies, and plans to perform provisioning, but cannot edit them or create new ones. Deployment plans that include update components can be used by a user with this role.
- Group Update: A user with the Update role for a group can update operating systems in the group and run update reports. The user can use existing profiles, policies, and plans to perform the update, but cannot edit them or create new ones.
- Group Update Sim: A user with the Update Sim role for a group can perform simulated Update jobs on operating systems and run update reports.
- Group Manage: A user with the Manage role for a group can monitor assets, gain console access, and launch reports.

In addition, a user can be granted the Admin role for a specific deployment plan, operational plan, or profile. A user with the Admin role can edit, copy, and delete the plan or profile. A user can run the plan or profile on an asset without having the Admin role.

Caution: A user with Provision and Admin permissions is able to apply an operational profile to a managed system using root access. Take care when assigning Provision or Admin roles because the role also allows the user to use an operational profile to run scripts.

Monitor System Activity

Each Enterprise Manager Ops Center component has some auditing capability. Follow audit advice in this document and regularly monitor audit records.

Enterprise Manager Ops Center performs each action as a job. The details of a job show the order of operations in the job and the managed assets that were targets of the job. You can view the details of a job from either the browser or the command-line interface. Each job is stored until it is deleted explicitly.

In addition to the jobs record, log files can be a source of activity records. Logs are written during operations and can provide additional detail about system activity. Log files are protected by file permissions and therefore requires a privileged user to access them.

General Events

- Messages: `/var/adm/messages*`
- BUI: `/var/opt/sun/xvm/logs/emoc.log`
- Actions of the BUI and remote clients on the Enterprise Controller:
  - On Oracle Solaris: `/var/cacao/instances/oem-ec/audits/`
  - On Linux: `/var/opt/sun/cacao/instances/oem-ec/audits/`
- Events between controllers and agents:
  - On an Oracle Solaris Enterprise Controller: `/var/cacao/instances/oem-ec/logs`
  - On a Linux Enterprise Controller: `/var/opt/sun/cacao/instances/oem-ec/logs`
  - On each Oracle Solaris Proxy Controller: `/var/cacao/instances/scn-proxy/logs/cacao.`*n*
  - On each Linux Proxy Controller: `/var/opt/sun/cacao/instances/scn-proxy/logs/cacao.`*n*

Software Updates

The Software Update component has its own server with its own logs. The following logs provide information on the activity for this server:

- Audit Log
  - On Oracle Solaris: `/var/opt/SUNWuce/server/logs/audit.log`
  - On Linux: `/usr/local/uce/server/logs/audit.log`
- Errors
  - On Oracle Solaris: `/var/opt/SUNWuce/server/logs/error.log`
  - On Linux: `/usr/local/uce/server/logs/error.log`
  - Log of errors in download jobs: `/opt/SUNWuce/server/logs/SERVICE_CHANNEL/error.log`
- Job Log
  - On Oracle Solaris: `/var/opt/SUNWuce/server/logs/job.log`
  - On Linux: `/usr/local/uce/server/logs/job.log`

Component -Specific

- Agents: `/var/scn/update-agents/logs` directory.
- Libraries: `/var/opt/sun/xvm/logs/virtimagelib.log`
- Asset Database
  - On the Enterprise Controller:
    - Log of interactions with the database of assets: `/var/opt/sun/xvm/logs/db/mgmt/logs/db.log`
    - Log of events in collecting data for reports: `/var/opt/sun/xvm/logs/db/reports/logs/db.log`
  - On the Proxy Controller: `/var/opt/sun/xvm/proxydb/*`
  - On each agent: `/var/opt/sun/xvm/agentdb/*`

2

Secure Installation and Configuration

This chapter described how to plan an installation and then how to configure the software so that you use the software securely.

Planning the Deployment

This section outlines the options for a secure installation and describes several recommended deployment topologies for the systems.

High Availability

The simplest deployment architecture is a single-system deployment in which the Enterprise Controller and a Proxy Controller are installed on the same system. Although the simplicity is appealing, this type of deployment creates a single point of failure and cannot provide high availability because all components are stored on the same computer. The High Availability feature in Enterprise Manager Ops Center configures an active/passive architecture in which two systems have access to the same shared storage. High availability is a manual process and applies only to the Enterprise Controller and its co-located Proxy Controller.

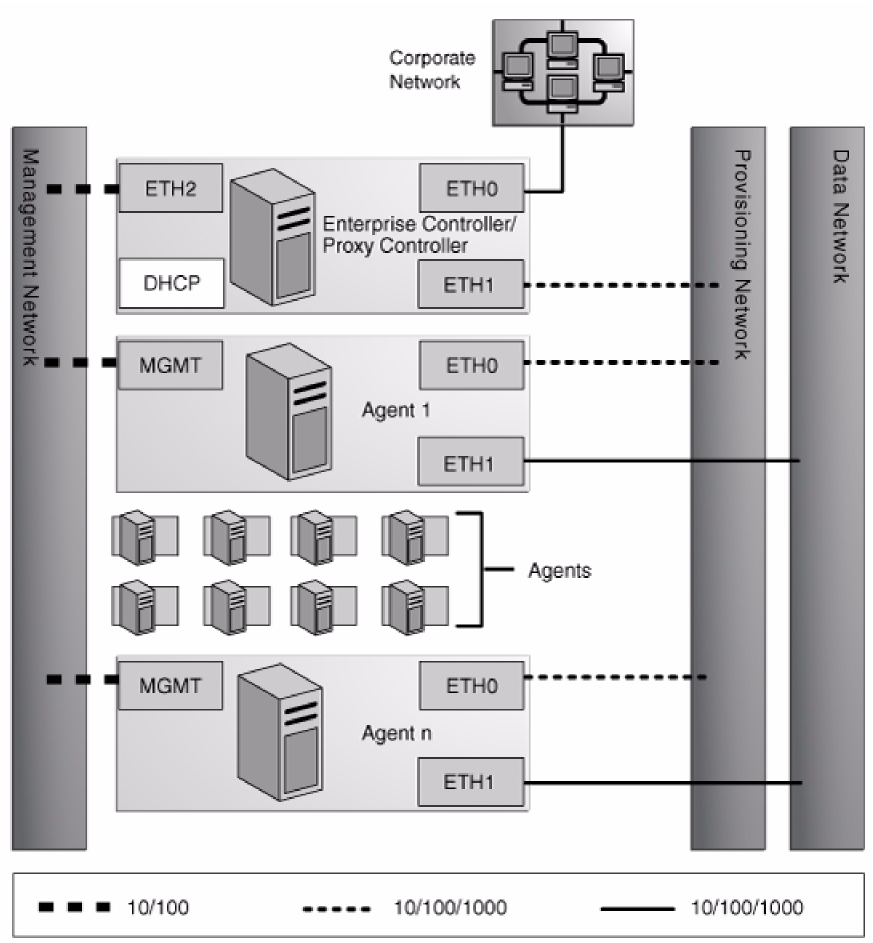
To avoid a single point of failure in your deployment, the Enterprise Controller must store the database files on shared storage and then provide a way to transfer the product directory structure manually from the primary Enterprise Controller to a secondary Enterprise Controller. The secondary Enterprise Controller duplicates the primary Enterprise Controller's configuration and takes over much of the primary Enterprise Controller's identity, including its host name, its IP addresses, its `ssh` keys, and its role. The secondary Enterprise controller must also have access to the shared storage where the database resides. Only one Enterprise Controller, either primary or secondary, can be operational at any time.

- User accounts and data that are not associated with Oracle Enterprise Manager Ops Center are not part of the failover process. Only Oracle Enterprise Manager Ops Center data is moved between the primary and secondary Enterprise Controllers.
- UI sessions are lost on failover.
- The HA configuration applies only to the Enterprise Controller and its co-located Proxy Controller and not to other standalone Proxy Controllers.

Network Configuration

Network connections are needed for data operations, for management operations, and for provisioning operations. The minimum configuration, but least secure, is to combine all operations on one network. Separate networks, as shown in Figure 2–1, provide the highest security and the lowest number of points of failure. However, additional network interface cards (NIC) are needed to support this configuration.

Figure 2–1 Separate Management, Provisioning, Data Networks



Infrastructure and Operating Systems

Enterprise Manager Ops Center manages and monitors assets in multiple locations and on multiple platforms. The responsibility for securing the network, hardware, and operating system of the server that runs the Enterprise Controller is that server's system administrator. The responsibility for securing the hardware, network, and operating system of Proxy Controllers and all assets falls on various sites' system administrators.

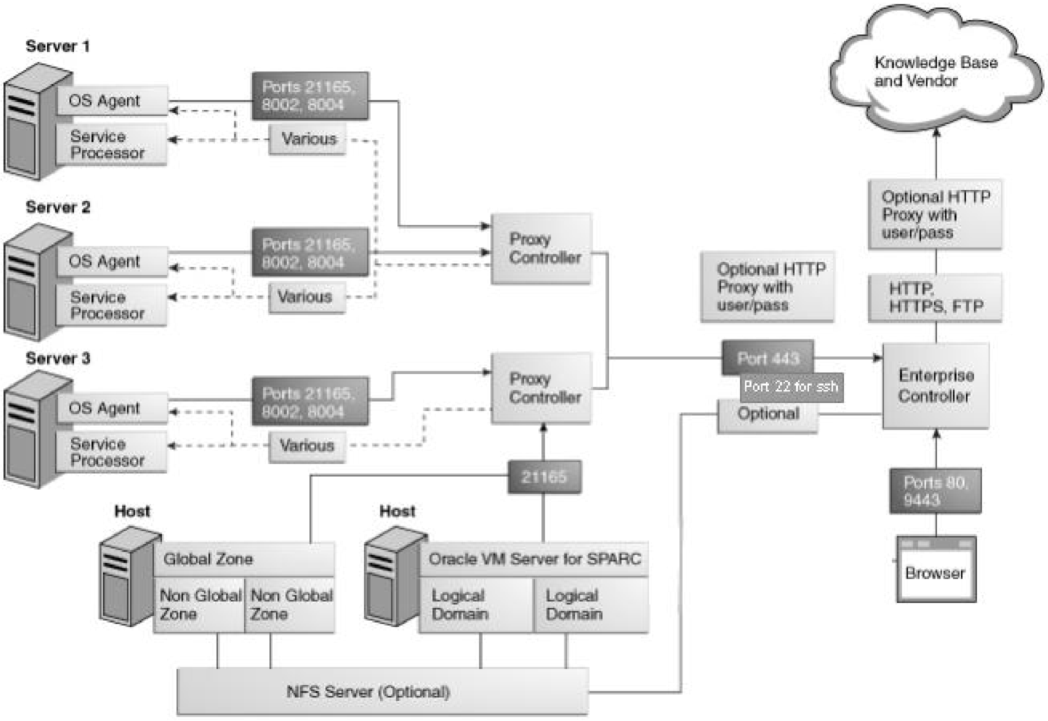
Storage Configuration

Enterprise Manager Ops Center stores its data and metadata in Software and Storage Libraries. These libraries can reside in local file systems but for a high-availability deployment, the libraries can reside on the shares of an NFS server. Because the Enterprise Controller does not mount the NFS share, install the NFS server on a system that is close to the systems where the NFS share will be used, that is, the systems that host global zones and Oracle VM Servers for SPARC.

Typical Deployment

The following diagram shows a deployment running the product software in Connected mode and with two Proxy Controllers.

Figure 2–2 Deployment Example



Installing Enterprise Manager Ops Center

Install the Enterprise Controller component only on a system where root access is controlled tightly because a root-privileged user must modify or create system services as part of the installation. To install the product on Linux systems, disable the SELINUX setting.

When installing a Proxy Controller that is not co-located with the Enterprise Controller, do not use the Proxy Controller Deploy action from the browser interface. Instead, copy the proxy controller bundle to the target system and then log in as root to install the software. This method removes the need to provide root credentials to the proxy controller's system and eliminates the need to use `ssh` from the Enterprise Controller system to the proxy controller system.

The installation logs are found in the following locations:

- Log of a failed installation: `/var/tmp/installer.log.`*`xxxx`*
- Log of a successful installation: `/var/tmp/installer.log.latest`

- Log of an agent installation: `/var/scn/install/log`

The log of upgrade actions for the Enterprise Controller and its co-located proxy controller is in the file: `/var/scn/update-saved-state/update_satellite_bundle_11.1.`*`n.xxxx`*`/updatelog.txt`

The log of upgrade actions for a proxy controller that is not co-located is in the file: `/var/scn/update-saved-state/update_proxy_bundle_11.1.`*`n.xxxx`*`/updatelog.txt`

The product installs a diagnostic program, OCDoctor, that gathers logged data, analyzes an installation for common errors, and responds to inquiries. OCDoctor can be removed at any time by removing its files and directories.

Configuring Enterprise Manager Ops Center

A privileged user must be enabled for the Enterprise Manager Ops Center software. Log in as the privileged user to configure the software.

Set the Connection Mode

Connection modes provide a way to keep the product software and all of the asset software current. However, Connected mode requires Internet access and if this access cannot be made secure or if a site's policy does not allow Internet access, the alternative is to run Enterprise Manager Ops Center in Disconnected mode. Although Disconnected mode might seem to provide the most secure environment, its use relies on manual procedures that can are error-prone without rigorous compliance to procedures and policies. The following operations are affected by the connection mode:

Table 2–1 Comparison of Functions in Different Connection Modes

	Connected Mode	**Disconnected Mode**
Obtaining a new version of the product software	Use the Oracle Ops Center Downloads action to create a job that obtains the latest version.	Log onto another system that is connected to the Internet and use the `harvestor` script to download the software. Then move the software to the proper Enterprise Controller directories.
Upgrading the product software	Use the Upgrade Enterprise Controller action. For each Proxy Controller, use the Update to Latest Available Version action.	For the Enterprise Controller and each Proxy Controller, log in to the system as root and create a temporary directory. Move the upgrade software to the new directory and uncompress the file. Run the install script.

Table 2–1 (Cont.) Comparison of Functions in Different Connection Modes

	Connected Mode	Disconnected Mode
Provisioning OS or firmware and updating existing OS or firmware. This operation requires access to the latest image.	Use the Upload ISO Images action, the Upload Firmware action, and the Import Images actions to update the contents of the Enterprise Controller's software library.	Obtain the image. For Oracle Solaris OS, use the `harvestor` script to download the OS image to an Internet-connected system and then move the software to a directory on the Enterprise Controller system. For other OS images and for firmware images, use a CD or DVD to load the software. Then use the Upload ISO Images action, the Upload Firmware action, and the Import Images actions to update the contents of the Enterprise Controller's software library.
Creating Services Requests	After you register the assets in the My Oracle Support database and register a user account as the My Oracle Support user, you have the option to create a service request whenever a problem is reported or, for a specific asset, by selecting the Open Service Request action.	The Open Service Request action is disabled. You must contact My Oracle Support to request service.
Verifying warranties	After you register the assets in the My Oracle Support database and register a user account as the My Oracle Support user, view the warranty of a specific asset or all assets.	You must contact My Oracle Support coordinate warranty records with your own records.

Change the password for the database accounts.

The Enterprise Manager Ops Center software includes an embedded PostgreSQL database, which it manages completely. The postgreSQL database processes runs in the `scndb` account. The account is locked.

The PostgreSQL database accounts are private to Enterprise Manager Ops Center. The passwords for these accounts are generated randomly at installation and can be changed manually. Use the utility appropriate to the type of database to change the passwords. Each utility performs the following operations:

- Generates a new random password.
- Gets access to the appropriate database using the current password.
- Changes the password to the new password.
- Updates the `xvm-db.properties` file with the new password.

To Change the Password for the Operational Database

1. Log in to the Enterprise Controller as the `root` user.
2. Execute the following utility:
   - Oracle Solaris: `$ /opt/SUNWscs/sbin/db_tool.pl genpw`
   - Linux: `$ /opt/sun/scs/sbin/db_tool.pl genpw`

To Change the Password for the Report Database

1. Log in to the Enterprise Controller as the `root` user.

2. Execute the following utility:
   - Oracle Solaris: `$$ /opt/SUNWscs/sbin/report_db_tool.pl genpw`
   - Linux: `$$ /opt/sun/scs/sbin/report_db_tool.pl genpw`

Disable the Data Model Navigator

Enterprise Manager Ops Center provides a Data Model Navigator to allow Oracle support personnel to gather detailed information about the state of the system from a model view of the system. This diagnostic interface is enabled by default and requires user authentication for access. Because it represents an internal view of the system, disable the interface and enable it only when in communication with Oracle support personnel.

Disable the interface using the following procedure:

1. Log in to the Enterprise Controller as the `root` user.
2. For an Oracle Solaris system, copy `/etc/cacao/instances/oem-ec/modules/restfuladaptor.xml` to `/etc/cacao/instances/oem-ec/modules/restfuladaptor.xml.orig`

   For a Linux system, copy `/etc/opt/sun/cacao/instances/oem-ec/modules/restfuladaptor.xml` to `/etc/opt/sun/cacao/instances/oem-ec/modules/restfuladaptor.xml.orig`
3. Edit the new file and locate the line: `ignored-at-startup="No"`
4. Change the value so that the line is: `ignored-at-startup="Yes"`
5. Save the file.
6. Repeat the procedure on each Proxy Controller:

   a. For an Oracle Solaris system, copy the file `/etc/cacao/instances/scn-proxy/modules/com.sun.hss.proxy.restfuladaptor.xml`

      For a Linux system, copy the file `/etc/opt/sun/cacao/instances/scn-proxy/modules/com.sun.hss.proxy.restfuladaptor.xml`

   b. Edit the file to change the value and save it.

   c. Stop and restart the Proxy Controller:

      ```
      /opt/SUNWxvmoc/bin/proxadm stop
      /opt/SUNWxvmoc/bin/proxadm start
      ```
7. Stop and restart the Enterprise Controller:

   ```
   /opt/SUNWxvmoc/bin/satadm stop
   /opt/SUNWxvmoc/bin/satadm start
   ```

Secure the Web Browsers

To implement transactions securely, Enterprise Manager Ops Center supports specific communications and security standards and methods such as HTTP, SSL, x.509 certificates, and Java. Most browsers support several of these features but users must configure their browsers properly to take advantage of security capabilities.

Information sent to and from a browser is transmitted in the clear so any intermediate site can read the data and potentially alter it in transit. Enterprise Manager Ops

Center's browsers and servers address this problem in part by using the Secure Sockets Layer to encrypt HTTP transmissions (referred to as HTTP/SSL or HTTPS). This ensures the security of data transmitted from the client to the server. However, because browsers do not ship with client certificates, most HTTP/SSL transmissions are authenticated in only one direction, from server to client. The client does not authenticate itself to the server.

The browser interface uses JavaScript extensively. Take care to protect against JavaScript-based attacks.

Substitute Certificates

Enterprise Manager Ops Center has self-signed certificates that it uses for authentication between its web container and a browser client. Self-signed Certificates are site-generated Certificates that have not been registered with any well-known Certificate Authority (CA), and are therefore not guaranteed. These certificates issue a warning when connecting with a browser and require users to accept the certificate.

To ensure that the data being transmitted and received is private and not vulnerable to eavesdropping, a self-signed certificate is sufficient. However, to ensure that connections are authentic, replace the self-signed certificates with Class A or B certificates from an third-party Certificate Authority such as Verisign.

Java's standard keystore format is JKS, the format created by the `keytool` command-line utility. This tool is included in the JDK and creates the self-signed certificates. The Enterprise Manager Ops Center keystore for the browser certificates is located in:

```
/var/opt/sun/xvm/bui/conf/truststore
```

To replace the self-signed certificate with certificates from a Certificate Authority, use the following general procedure:

1. Identify the Certificate Authority you want to use.
2. Submit a request for a certificate to the Certificate Authority, according to their instructions. The Certificate Authority returns a certificate to you.
3. Download a Chain Certificate from the Certificate Authority, according to their instructions.
4. Verify the certificates' fingerprints. When you add a certificate to the keystore, any transactions using that certificate become trusted. You must be certain that the certificates you received are authentic before you import them. Use the keytool's print command to see the fingerprints and then communicate with the Certificate Authority to compare the fingerprints. To see a certificate's fingerprint, use the following command:

   ```
   keytool -printcert -file <path/filename>
   ```

5. Import the Chain Certificate in the Enterprise Manager Ops Center keystore:

   ```
   keytool -import -alias root -keystore /var/opt/sun/xvm/bui/conf/truststore
   -trustcacerts -file <chain_certificate>
   ```

   You are prompted for the password to the keystore and you are asked to verify the certificate's authenticity.

6. Import the certificate that the CA sent to you into the keystore:

   ```
   keytool -import -alias <hostname>-ca -keystore
   /var/opt/sun/xvm/bui/conf/truststore \trustcacerts -file <your_certificate>
   ```

where *<hostname>* is the name of the system on which the Enterprise Controller is running and *<your_certificate>* is the name of the file containing the certificate sent from the Certificate Authority.

You are prompted for the password to the keystore and you are asked to verify the certificate's authenticity.

Protect Session Data

Enterprise Manager Ops Center uses cookies to store session data for individual users. The cookies are encrypted using JSESSIONID with the "http-only" flag. The cookies are transmitted using the HTTPS protocol.

The browser controls a session's inactivity timer with a default time of 30 minutes. Consider changing the expiration time to a shorter duration, using the following procedure:

1. Navigate to the `webapps` directory:

   ```
   cd /var/opt/sun/xvm/bui/webapps
   ```

2. Create a directory:

   ```
   mkdir emoc
   ```

3. Change to the new directory:

   ```
   cd emoc
   ```

4. Extract the `emoc.war` file.

   ```
   jar xf ../emoc.war
   ```

5. Copy the `emoc.war` file to save its original contents:

   ```
   mv ../emoc.war ../emoc.war.orig
   ```

6. Open the `WEB-INF/web.xml` file in an editor.
7. Search for the following content:

   ```
    <filter>
           <filter-name>AuthenticationFilter</filter-name>
           <filter-class>com.sun.xvm.ui.@PACKAGE@.auth.AuthenticationFilter</filte
   r-class>
       <!-- normal and config flow session idle timeouts, in minutes -->
           <init-param>
               <param-name>session-timeout</param-name>
               <param-value>30</param-value>
           </init-param>
   ```

8. In this filter, change the value of 30 to a smaller value to reduce the number of minutes of inactivity that are allowed.
9. Save and close the file.
10. Stop and restart the Enterprise Controller so that the change can take effect:

    ```
    /opt/SUNWxvmoc/bin/satadm stop
    /opt/SUNWxvmoc/bin/satadm start
    ```

3 Security Features

Enterprise Manager Ops Center provides security services for user authentication, custom user authorization, and protection for data in repositories and during network transmissions. Enterprise Manager Ops Center also provides network authentication between its infrastructure components using standard certificates.

Enterprise Manager Ops Center uses standard protocols and third-party solutions to secure data and operations, using SSL and X.509v3 certificates, and secure HTTP and PAM (Pluggable Authentication Modules) protocols to provide the following services:

- Authentication
- Authorization
- Access Control
- Data Protection

Configuring and Using Authentication

Authentication allows a system to verify the identity of users and other systems that request access to services or data. In a multitier application, the entity or caller can be a human user, a business application, a host, or one entity acting on behalf of another entity.

Identity Management

Users log in to the browser interface to use the product. The credentials must be valid user IDs for the underlying operating system and must have been added to Enterprise Manager Ops Center.

The operating system stores all user accounts and manages them. Enterprise Manager Ops Center uses Pluggable Authentication Modules (PAM) to validate credentials for user accounts of users who log into the browser interface. The default PAM service allows Enterprise Manager Ops Center users to log into the system in the standard way.

The PAM service is set by the `pam-service-name` configuration parameter for the `oem-ec` instance of the `cacao` daemon.

- Oracle Solaris: The default value is `pam-service-name=other`
- Linux: The default value is `pam-service-name=passwd`

If you require control of the PAM configuration used by Enterprise Manager Ops Center, you can create a PAM service with a different service name, which uses different PAM modules.

To see the current value of the pam-service-name parameter, use the following cacaoadm command:

```
./cacaoadm get-param -i oem-ec pam-service-name
```

To change the authentication service from the operating system's default to a different service name, use the following procedure:

1. On a Linux system, create a configuration file or edit the existing configuration file for the service to use. The configuration file has the same name as the service.

   ```
   /etc/pam.d/filename
   ```

   On an Oracle Solaris 10 system, edit the following file:

   ```
   /etc/pam.conf
   ```

2. Change the contents of the configuration file. For example:

   ```
   auth       required     pam_warn.so debug
   auth       required     pam_safeword.so.1 debug
   account    include      system-auth
   password   include      system-auth
   ```

3. To initialize the PAM service with the new configuration, stop the Enterprise Controller:

   ```
   /opt/sun/xvmoc/bin/satadm stop
   ```

4. Change the value of the pam-service-name parameter

   ```
   ./cacaoadm set-param -i oem-ec pam-service-name=opscenter
   ```

5. Verify the change:

   ```
   ./cacaoadm get-param -i oem-ec pam-service-name
   ```

6. Restart the Enterprise Controller:

   ```
   /opt/sun/xvmoc/bin/satadm start
   ```

Note: If you use the SafeNet SafeWord® Agent for PAM software (pam_safeword.so), you can use the SafeWord static password mode or single-use dynamic password mode, but you cannot use the dynamic challenge password mode. To use single-use dynamic passwords, you must modify the pam_safeword.cfg file to ensure that the User ID source is set to SYSTEM and not USER. The SYSTEM setting causes the authentication process to get the User ID from the /etc/passwd file.

Credential Management

Enterprise Manager Ops Center uses credentials to discover and manage assets and to establish trust between internal components. Passwords are protected by encryption if stored or transmitted over the network. Enterprise Manager Ops Center manages the following credentials:

- SSH credentials for managed Operating System instances and hardware service processors.

- IPMI credentials for hardware service processors

Enterprise Manager Ops Center requires administrative privileges for a system to discover and manage the system. To discover a system, Enterprise Manager Ops Center also requires remote network access to the system. This can be done either by using a privileged account or by combining the credentials of a non-privileged user account with the credentials for the administrative account. In this case, Enterprise Manager Ops Center uses the non-privileged user account to connect to the system and then uses the administrative account to inquire about the characteristics of the system.

To discover an ILOM system, the account must have administrator privileges on the system, and both IPMI and `ssh` credentials must be provided.

> **Note:** IPMI communications from the Proxy Controller to the ILOM system are not encrypted. Protect the transmissions by isolating the ILOM system and the Proxy Controller it uses within your private administrative network.

Enterprise Manager Ops Center does not provide certificates signed by a Certificate Authority such as Verisign because an authority's certificates require the domain where the certificate will be used to be specified. The Web server of the Enterprise Controller runs in the domain where the customer installs the software.

Enterprise Manager Ops Center has self-signed certificates that it uses for authentication between the web container and the browser client. Because the domain name is specific to your installation, the Enterprise Manager Ops Center software cannot be delivered with a generated signed certificate from a certificate authority. See Substitute Certificates for instructions in replacing the self-signed certificate with a certificate from a Certificate Authority.

In Connected mode, the Enterprise Manager Ops Center software requires the user to provide one or more sets of My Oracle Support credentials. These credentials are used to authenticate and authorize downloading product updates, creating Service Requests, and retrieving warranty information, in addition to the initial authentication between the Enterprise Controller's system and My Oracle Support.

Configuring and Using Authorization

Authorization allows a system to determine the privileges which users and other systems have for accessing resources on that system.

Roles grant users the ability to use the different functions of Oracle Enterprise Manager Ops Center. By giving a role to a user, an administrator can control what functions are available to that user and for which groups of assets.

An Enterprise Controller Admin can grant users different roles for the Enterprise Controller, the All Assets group, and any user-defined groups. A user who is assigned a role for a group receives the same role for all subgroups. See Follow the Principle of Least Privilege for a list of the available roles and their functions.

> **Caution:** A user with Provision and Admin permissions is able to apply an operational profile to a managed system using root access. Take care when assigning Provision or Admin roles because the role also allows the user to use an operational profile to run scripts.

Configuring and Using Access Control

Access control allows a system to grant access to resources only in ways that are consistent with security policies defined for those resources.

The Enterprise Controller connects to the Internet to download OS updates, Oracle Solaris images, and updates for the Enterprise Manager Ops Center software itself. When an update is requested, the Enterprise Controller retrieves the software from the KB or vendor site. This mode of operation is called Connected mode. If a site security policy does not allow Internet connections, Enterprise Manager Ops Center can operate in Disconnected mode.

In Disconnected mode, you must manually load the Knowledge Base data and updates to the Enterprise Controller so that provisioning tasks can be fulfilled. For the Oracle Solaris operating system, Enterprise Manager Ops Center provides a script to run on a system that is connected to the Internet to obtain the baselines and updates. You then transfer the baselines and updates to the Enterprise Controller. In effect, you create a static KB on the Enterprise Controller that you must maintain. For all other supported operating systems and firmware, obtain the software in a media format, such as a CD or DVD, and upload the information to Local Content library in Enterprise Manager Ops Center.

Configuring and Using Data Protection

NFS protocol requires agreement on the Domain Name System (DNS) that the NFS server and NFS clients use. The server and a client must agree on the identity of the authorized users accessing the share.

The Enterprise Manager Ops Center software prepares an NFS client to mount the share. Use the following procedure to prepare the NFS server:

To Set Up a Share on the NFS Server

1. Create the directory to share, and set its ownership and permission modes. For example:

   ```
   # mkdir -p /export/lib/libX
   # chmod 777 /export/lib/libX
   ```

2. Open the `/etc/dfs/dfstab` file on the NFS server.
3. Add an entry to share the directory. For example, to share the directory named `/export/lib/libX`, create the following entry:

   ```
   share -F nfs -o rw,"Share 0" /export/lib/libX
   ```

   If you want the NFS share to be accessible from other network domains, use the `rw` option to specify a list of allowed domains:

   ```
   share -F nfs -o rw=IPaddress1,IPaddress2 "Share 0" export/lib/libX
   ```

4. Share the directory and then verify that the directory is shared. For example:

   ```
   # shareall
   # share
   export/lib/libX   rw, "Share 0"
   ```

   The share now allows a root user on the NFS clients to have write privileges.