



# **Agile Product Lifecycle Management**

## **Customer Needs Management Security Guide**

Version 1.2

E26096-01

January 2012

# Oracle Copyright

Copyright © 1995, 2012, Oracle and/or its affiliates. All rights reserved.

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

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

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

## U.S. GOVERNMENT RIGHTS

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

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

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

This software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third party content, products and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third party content, products or services. The RMW product includes software developed by the Visigoth Software Society.

# CONTENTS

---

Oracle Copyright .....	ii
<b>Chapter 1.....</b>	<b>1</b>
<b>Overview .....</b>	<b>1</b>
Product Overview.....	1
General Security Principles.....	2
Keep Software Up To Date.....	2
Restrict Network Access to Critical Services.....	2
Follow the Principle of Least Privilege.....	3
Monitor System Activity.....	3
Keep Up To Date on Latest Security Information .....	3
<b>Chapter 2.....</b>	<b>5</b>
<b>Secure Installation and Configuration.....</b>	<b>5</b>
Installation Overview .....	5
Understand Your Environment.....	5
Recommended Deployment Topologies.....	6
Installing and Configuring a Secure CNM System .....	7
Installing Oracle Database Server Software.....	7
Installing Oracle WebLogic Server Application Software.....	7
Installing Agile CNM Database Schema.....	8
Installing Agile CNM .....	8
Installing Oracle Universal Content Management Server (Optional).....	8
Configuring LDAP Server (Optional) .....	8
Configuring Web Proxy Server (Optional) .....	8
Configuring AutoVue (Optional) .....	8
Post-Installation Configuration .....	9
<b>Chapter 3.....</b>	<b>11</b>
<b>Security Features.....</b>	<b>11</b>
The Security Model .....	11
Configuring and Using Authentication.....	11
Configuring and Using Access Control.....	12
Configuring and Using Security Audit.....	12

<b>Chapter 4.....</b>	<b>15</b>
<b>Security Considerations for Developers .....</b>	<b>15</b>
Extensibility Points .....	15
Web Services .....	15
<b>Appendix A.....</b>	<b>17</b>
<b>Secure Deployment Checklist.....</b>	<b>17</b>

# Preface

Oracle's Agile PLM documentation set includes Adobe® Acrobat PDF files. The [Oracle Technology Network \(OTN\) Web site](http://www.oracle.com/technetwork/documentation/agile-085940.html) <http://www.oracle.com/technetwork/documentation/agile-085940.html> contains the latest versions of the Agile PLM PDF files. You can view or download these manuals from the Web site, or you can ask your Agile administrator if there is an Agile PLM Documentation folder available on your network from which you can access the Agile PLM documentation (PDF) files.

---

**Note** To read the PDF files, you must use the free Adobe Acrobat Reader version 9.0 or later. This program can be downloaded from the [Adobe Web site](http://www.adobe.com) <http://www.adobe.com>.

---

The [Oracle Technology Network \(OTN\) Web site](http://www.oracle.com/technetwork/documentation/agile-085940.html) <http://www.oracle.com/technetwork/documentation/agile-085940.html> can be accessed through **Help > Manuals** in both Agile Web Client and Agile Java Client. If you need additional assistance or information, please contact My Oracle Support (<https://support.oracle.com>) for assistance.

---

**Note** Before calling Oracle Support about a problem with an Agile PLM manual, please have the full part number, which is located on the title page.

---

## TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

## Readme

Any last-minute information about Agile PLM can be found in the Readme file on the [Oracle Technology Network \(OTN\) Web site](http://www.oracle.com/technetwork/documentation/agile-085940.html) <http://www.oracle.com/technetwork/documentation/agile-085940.html>.

## Agile Training Aids

Go to the [Oracle University Web page](http://www.oracle.com/education/chooser/selectcountry_new.html) [http://www.oracle.com/education/chooser/selectcountry\\_new.html](http://www.oracle.com/education/chooser/selectcountry_new.html) for more information on Agile Training offerings.

## Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.



## Overview

**This chapter includes the following:**

---

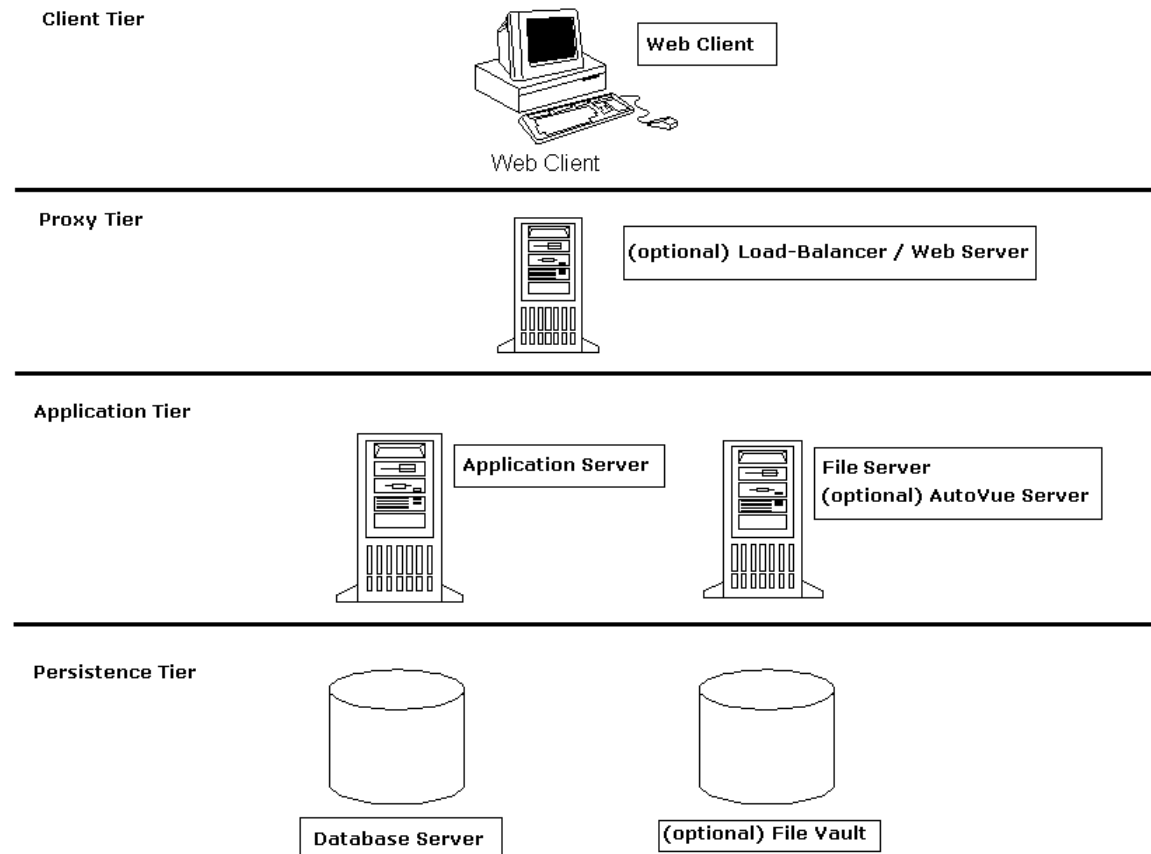
- Product Overview ..... 1
- General Security Principles ..... 2

This chapter gives an overview of Agile Customer Needs Management (CNM) and explains the general principles of application security.

### Product Overview

Agile Customer Needs Management (CNM) is a product that helps you transform market requirements into products. Those requirements can come in from a number of sources such as CRM, Quality or other enterprise applications or detailed documents received from customers, and so on. CNM offers a platform on which Product and Project owners can capture, filter, refine, collaborate on, prioritize and eventually incorporate those requirements into products.

The following diagram shows the CNM system's components and their general architecture.



## General Security Principles

The following principles are fundamental to using any application securely.

### Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. You should look at Oracle Critical Patch updates regularly to ensure that you have updated Agile CNM software to the latest version, as typically security vulnerabilities in the previous versions of the product are addressed in newer versions.

### Restrict Network Access to Critical Services

Keep both the application server and the database behind a firewall. The firewall provides assurance that access to these systems is restricted to a known network route, which can be



monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

## **Follow the Principle of Least Privilege**

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over-ambitious granting of responsibilities, roles, grants, etc., especially early on in an organization's life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

## **Monitor System Activity**

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

## **Keep Up To Date on Latest Security Information**

Oracle continually improves its software and documentation. Check this note yearly for revisions.



# Secure Installation and Configuration

**This chapter includes the following:**

---

- Installation Overview..... 5
- Installing and Configuring a Secure CNM System..... 7
- Post-Installation Configuration..... 9

This chapter describes recommended deployment topologies, and also provides recommendations for installing and configuring a secure setup for your CNM system.

## Installation Overview

This section outlines the planning process for a secure installation and describes the basic recommended topology for the CNM system.

## Understand Your Environment

To better understand your security needs, ask yourself the following questions:

*Which resources am I protecting?*

Many resources in the production environment can be protected, including information in databases accessed by the CNM server and the availability, performance, applications, and the integrity of the Web site. Consider the resources you want to protect when deciding the level of security you must provide.

*From whom am I protecting the resources?*

For most Web sites, resources must be protected from everyone on the Internet, but should the Web site be protected from the employees on the intranet in your enterprise? Consider setting up casual users with the Viewer role and power users with Participant role. Only system administrators should have the Administrator role. Should your employees have access to all data in the system? Consider assigning casual users as team members only to relevant non-confidential objects. You should assign only power users as team members to relevant confidential objects. A good approach is to use small sized groups while assigning team members to objects. You should avoid using very large groups such as ALL\_USERS. Should your system administrators have access to all the data in the system? You might consider giving access to highly confidential data or strategic resources to only a few system administrators. You may even decide that the best option is to not allow the system administrators access to any data. This can be achieved by not adding system administrators as team members to any objects. For general information about roles and user groups in CNM, see Appendix A in the *Customer Needs Management Guide*.

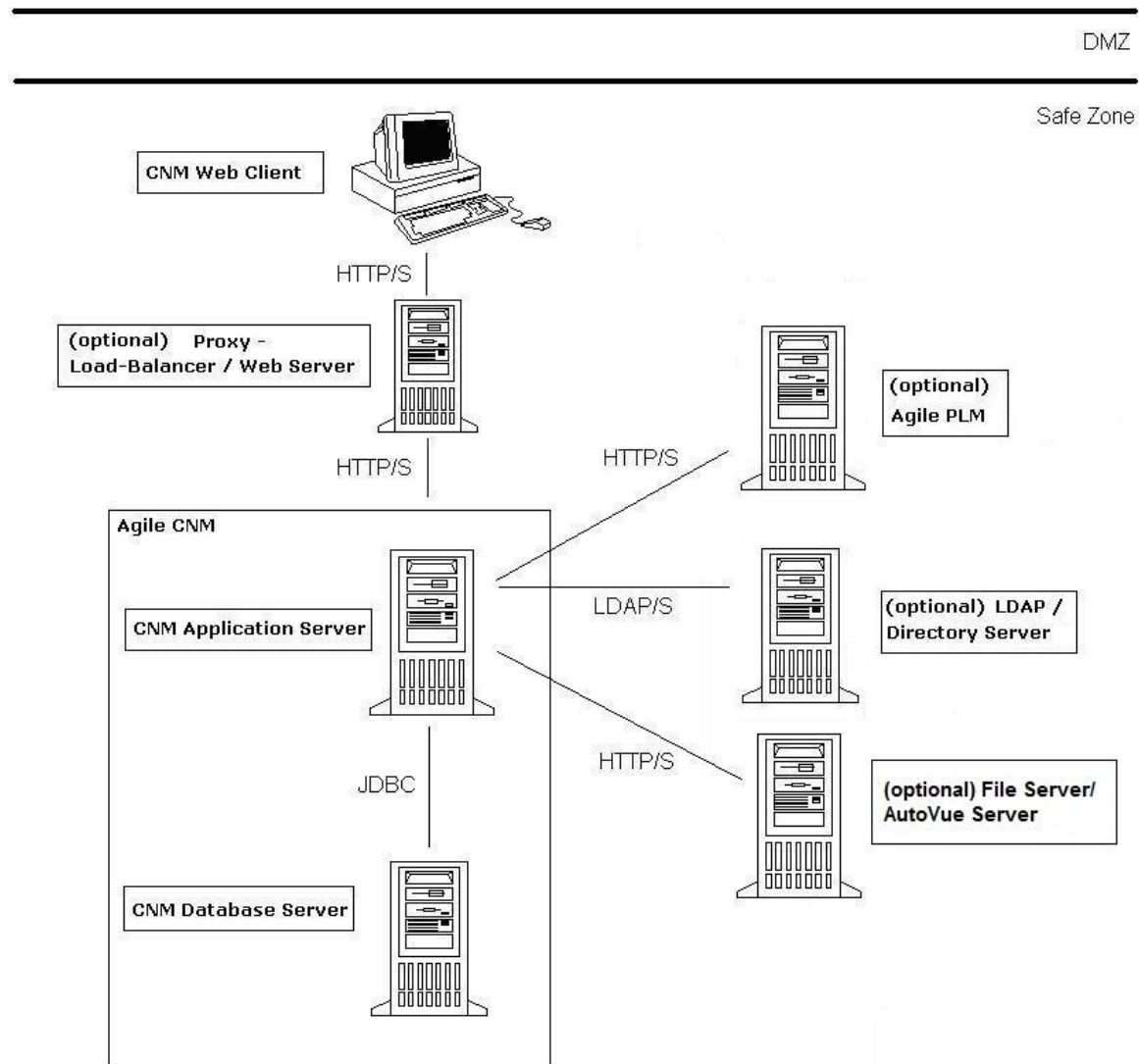
*What will happen if the protections on strategic resources fail?*

In some cases, a fault in your security scheme is easily detected and considered nothing more than an inconvenience. In other cases, a fault might cause great damage to companies or individual clients that use the Web site. Understanding the security ramifications of each resource will help

you protect it properly.

## Recommended Deployment Topologies

The following figure shows the general topology that is recommended for a secure CNM installation.



The components included in the topology diagram are defined below:

- **CNM Web Client** - The web browser used to access the Agile CNM application.
- **(optional) Proxy** - Load-balancer and/or Web Server Proxies requests from client to server(s). Recommend communication using HTTP over SSL (HTTPS) for the most secure deployment.
  - For standalone application server deployments, both the load-balancer and web server components are optional.

- For deployments where the application server is clustered/redundant, a load-balancer is required and the web server is optional.
- **CNM Application Server** - Provides the core Agile CNM application functionality. Recommend communication using HTTP over SSL (HTTPS) for the most secure deployment.
- **CNM Database Server** - Provides for storage of the Agile CNM application's data.
- **(optional) LDAP / Directory Server** - Provides centralized management of user accounts. Note that the AgilePLM file manager is not applicable when LDAP is selected as the authentication server. If using LDAP, we recommend communication using LDAPS for the most secure deployment. This component can be used by the Agile CNM application as an authentication source.
- **(optional) PLM Application Server** - Provides the core Agile PLM application functionality. Recommend communication using HTTP over SSL (HTTPS) for the most secure deployment. This component can be used by the Agile CNM application as an authentication source.
- **(optional) File Server/ AutoVue Server** - CNM requires a file server for storing files that are referenced by CNM objects. The Agile PLM File Manager component provides file upload/download functionality for the Agile CNM application. Recommend communication using HTTP over SSL (HTTPS) for the most secure deployment. The AutoVue Server component provides file viewing functionality for the Agile CNM application.

---

**Note** We recommend configuring the CNM system with the Agile PLM File Server, however, Oracle Universal Content Management server (UCM) can be configured as the file server if an Agile PLM system is not available for use with CNM.

---

## Installing and Configuring a Secure CNM System

### Installing Oracle Database Server Software

For the latest information on installing Oracle Database Server in a secure manner, refer to the *Oracle Database Security Guide* and make necessary configuration changes.

### Installing Oracle WebLogic Server Application Software

For the latest information on installing WebLogic Server in a secure manner and on a secure WebLogic server host, refer to the Oracle WebLogic Server documentation, especially *Securing a Production Environment for Oracle WebLogic Server*.

We especially recommend that you:

- Deploy WebLogic Server using SSL.
- After installation, change the WebLogic administrator username and password, as suggested in the *Customer Needs Management Implementation Guide*.
- Secure WebLogic Server by placing it behind a proxy server.

## Installing Agile CNM Database Schema

For the latest information on installing the Agile CNM database schema, refer to the *Agile Customer Needs Management Implementation Guide*.

## Installing Agile CNM

For the latest information on installing Agile CNM, refer to the *Agile Customer Needs Management Implementation Guide*.

For optimal security, we recommend that you:

- Use strong passwords.
- Deploy with SSL.
- Use the Agile PLM system for authentication. For more information, see *Configuring and Using Authentication*.

## Installing Oracle Universal Content Management Server (Optional)

For the latest information on installing Oracle Universal Content Management (OUCM) server in a secure manner, see the OUCM documentation. If you are using the Content Server as a file server, Agile CNM users can only be authenticated through your LDAP server. For improved security, you should deploy the Content Server and AutoVue VueLink with SSL connections.

We also recommend that you:

- Enable secure remote access to UCM by adding the IP address of the application server to the `SocketHostAddressSecurityFilter` parameter in the same `config.cfg` file. For example, `SocketHostAddressSecurityFilter = 10.xxx.xxx.xxx|xx.xxx.xxx.xxx|xxx.x.x.x`.  
  
This post-installation step is required because we do not use username/password to access UCM.
- Deploy UCM with SSL connections.

## Configuring LDAP Server (Optional)

For Oracle Directory Server, refer to the Oracle Directory Server documentation. For other LDAP systems, follow the security best practices recommended by the vendor.

## Configuring Web Proxy Server (Optional)

Refer to the documentation for your proxy server to determine the most secure configurations.

## Configuring AutoVue (Optional)

Refer to the *AutoVue Security Guide* for information about configuring AutoVue securely.

## Post-Installation Configuration

The following security configuration changes must be made after installation.

### **WebLogic Passwords**

We recommend that you change the WebLogic administrator user/password after installing CNM to enhance security. Refer to the *CNM Implementation Guide* for more information.

### **Setup proxy**

We recommend that you setup a proxy server after installing CNM to enhance security. Refer to the proxy server's installation documentation for more information.





# Security Features

**This chapter includes the following:**

---

▪ The Security Model.....	11
▪ Configuring and Using Authentication .....	11
▪ Configuring and Using Access Control .....	12
▪ Configuring and Using Security Audit .....	12

This chapter gives a high level overview of the threats that the system is designed to counter and how the individual security features combine to prevent the attacks.

## The Security Model

CNM includes some critical security features that provide data protection. These features include:

- Authentication – ensuring that only authorized individuals get access to the system and data.
- Authorization – access control to system privileges and data. This builds on authentication to ensure that individuals only get appropriate access.
- Audit – allows administrators to detect attempted breaches of the authentication mechanism and attempted or successful breaches of access control.

## Configuring and Using Authentication

CNM supports two kinds of authentication configurations. Customers can choose an appropriate type of authentication based on whether or not Agile PLM is already installed or not.

Your options are as follows:

- If you do not have Agile PLM installed, you have the option to use LDAP-based authentication. If you choose to use LDAP, the supported stacks/types of LDAP are Oracle Internet Directory, Oracle Sun Java System Directory Server, and Microsoft Active Directory.

---

**Note** There are no default accounts set up. CNM users have to be synchronized with LDAP users using database scripts. Please refer to the *CNM Implementation Guide*.

---

- (Recommended) Authentication is also supported through the Agile PLM system. CNM leverages Agile PLM system's authentication mechanism. We recommend authentication via the Agile PLM system. If this authentication is enabled, CNM is configured to seamlessly integrate with the Agile PLM system. The CNM login screen is shown first and then users are validated by the Agile PLM system. The SSO credentials are available in a cookie for subsequent access to the Agile PLM system.

---

**Note** There are no default accounts set up. CNM users have to be synchronized with Agile users using database scripts. Please refer to the *CNM Implementation Guide*.

---

## Password Security

The security of passwords is crucial to your CNM system's overall security. Refer to the *Account Policy* chapter in the *Agile PLM Administrator Guide* for details on how to configure a password policy, including password length, complexity, and expiry. We recommend that you configure passwords to be 8 characters or greater, including at least one non-alphabetic character. Passwords should be set to expire and require resetting at least every 6 months.

If using LDAP-based authentication, refer to the documentation for your specific LDAP server.

# Configuring and Using Access Control

Authorization, in general, includes primarily two processes:

- Permitting only certain users to access, process, or alter data.
- Applying varying limitations on user access or actions. The limitations placed on (or removed from) users can apply to objects, such as schemas, tables, or rows; or to resources, such as time (CPU, connect, or idle times).

In CNM, each user is granted one of three roles: administrator, viewer, or participant. The roles are defined as follows:

- viewer: role for novice users who need permission to read objects
- participant: role for power users who need permission to read and write objects
- admin: role for admin users who need permission to read & write objects, plus admin privileges

When a new user is created, you must determine what kind of permissions they need. We recommend that you give each user the least amount of privilege to perform their jobs.

Additionally, each CNM object, such as Idea, has object-level team membership that further restricts access to data. You must be a member of an object's team to access the object; non-members cannot access an object regardless of user role. An administrator, who must already be a team member, or the owner of each object, can add other users as team members of this CNM object. The Admin UI allows the administrator to set default team members for each type of object.

---

**Note** After initial installation, Idea objects have the default team set to ALL\_USERS, while Quote objects and Requirement objects do not have any entry for default team. The administrator should set default teams according to their business needs. In general, teams should consist of the least amount of users, as possible, to limit access and maximize security. For more information about managing teams, see the "Managing Object Team" section in the *Customer Needs Management Guide*.

---

# Configuring and Using Security Audit

CNM allows you to audit your system through object history tables, as well as through a system access table.

Each object in CNM has a history table, which includes all actions related to the object. The history table is viewable in the UI for each object on the object's History tab. You can audit this historical

data to find out when an object was modified, who performed the action, action detail, the previous value of a field, and more. See the *Customer Needs Management Guide* for more information about the History tab.

Additionally, CNM has a system access table named `system_access_history`, which provides the session ID for each session, the user who logged in, and the times of when the user logged in and logged out. This table is not exposed in the Admin UI. A database administrator can monitor successful logins by querying the system access table by using the following query:

```
select username, login_time, logout_time from system_access_history,  
users where system_access_history.user_id=users.id
```

We recommend that you set up logging capability at the WebLogic Server level. You can use WebLogic Server's logging capabilities to monitor system access. WebLogic's log files are located in the domain directory: `cnmDomain\servers\AdminServer\logs` (standalone) and `cnmDomain\servers\ManageServerName\logs` (cluster). Although CNM does not log failure access, you can configure WebLogic to log failed access attempts in the WebLogic auditor log file. See the "Configuring WebLogic Security Providers" section in the *Oracle Fusion Middleware Securing Oracle WebLogic Server* for more information. If Agile PLM is used for authentication, authentication attempt information is logged in the Agile PLM server log file, such as `serverXXXXXX.log` or `DefaultServer.logXXX`. For LDAP authentication, refer to LDAP Server's documentation to determine which log files contain authentication attempt information.



# Security Considerations for Developers

**This chapter includes the following:**

---

- Extensibility Points..... 15
- Web Services..... 15

This chapter discusses information useful to developers extending the application or producing applications using the product as a platform.

## Extensibility Points

The CNM application includes web services as one extensibility point - an area in the application suite used to extend functionality of the product suite. CNM web services can be leveraged to provide customized clients or integration modules. CNM web services authenticate using WS-Security. For optimal security protection, use SSL.

## Web Services

A set of 12 CNM web services provide the ability to create, retrieve, and update data. When calling web services related to any business objects, the user calling the web service is evaluated for security permissions and authentication similar to the CNM web application.

If the user does not have permission to read a given business object, then the business object is not returned in the web service result. The `GetObject` web service, for example, which returns the business object's name, status, and more, will not return an object if the calling user is not a member of the object's team. If the user only has a Viewer role, the business object can not be updated. The `UpdateObject` web service, for example, which updates the business object's name, status, and more, will not update an object if the calling user is not a member of the object's team or the calling user has only the Viewer role. If the user only has Viewer role, then it is still possible to add notes and comments as long as the calling user is a member of the object's team.

See the *Oracle Agile Customer Needs Management Web Service User Guide* for more details about the web services.



# Secure Deployment Checklist

Follow the secure deployment checklist provided for the Oracle Database Server, as defined in the *Oracle Database Security Guide*. Similarly, follow guidelines for deploying your Oracle WebLogic Server, as defined in the Oracle WebLogic Server documentation.

The following security checklist includes guidelines that help secure your CNM application:

1. Practice the principle of least privilege.
  1. Grant only the necessary role.
  2. Add only necessary users to object team.
  3. Add only necessary users to groups.
  4. Avoid using large groups such as ALL\_USERS.
2. Enforce access controls effectively and authenticate clients stringently.
3. Restrict network access.
  1. Use a firewall.
  2. Never poke a hole through a firewall.
  3. Monitor who accesses your systems.
  4. Check network IP addresses.
  5. Encrypt network traffic.
  6. Harden the operating system.
4. Apply all security patches and workarounds.
5. Use strong passwords.
6. Deploy WebLogic Server using SSL.
7. Change the WebLogic administrator's username and password.
8. Set up a proxy server.
9. Contact Oracle Security Products if you come across vulnerability in the CNM application.

