Oracle® Agile Product Lifecycle Management for Process

Security Configuration Guide

Release 6.1.1

E29793-01

January 2013

ORACLE®

Oracle Agile Product Lifecycle Management for Process Security Configuration Guide, Release 6.1.1

E29793-01

Contents

Preface

The *Oracle Agile Product Lifecycle Management for Process Security Configuration Guide* contains guidelines for managing security configurations in Oracle Agile Product Lifecycle Management (PLM) for Process.

This preface contains these topics:

Audience

This guide is intended for end users who are responsible for creating and managing information in Oracle Agile Product Lifecycle Management for Process. Information about administering the system resides in the *Oracle Agile Product Lifecycle Management for Process Administrator User Guide*.

Variability of Installations

Descriptions and illustrations of the Oracle Agile PLM for Process user interface included in this manual may not match your installation. The user interface of Oracle Agile PLM for Process applications and the features included can vary greatly depending on such variables as:

- Which applications your organization has purchased and installed
- Configuration settings that may turn features off or on
- Customization specific to your organization
- Security settings as they apply to the system and your user account

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to

evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

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.

Accessibility of Links to External Web Sites in Documentation

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.

TTY Access to Oracle Support Services

To reach AT&T Customer Assistants, dial 711 or 1.800.855.2880. An AT&T Customer Assistant will relay information between the customer and Oracle Support Services at 1.800.223.1711. Complete instructions for using the AT&T relay services are available at http://www.consumer.att.com/relay/tty/standard2.html. After the AT&T Customer Assistant contacts Oracle Support Services, an Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process.

Related Documents

For more information, see the following documents in the Oracle Agile Product Lifecycle Management for Process Release 6.1.1 documentation set:

- *Oracle Agile Product Lifecycle Management for Process Administrator User Guide*
- *Oracle Agile Product Lifecycle Management for Process Configuration Guide*
- *Oracle Agile Product Lifecycle Management for Process Install/Upgrade Guide*
- Oracle Agile Product Lifecycle Management for Process Release Notes. Up-to-date Release Notes and other documentation are posted on Oracle Technology Network (OTN) at this location:

  http://www.oracle.com/technetwork/documentation/agile-085940.html#plmprocess

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

Security Overview

This chapter gives an overview of Oracle Agile Product Lifecycle Management (PLM) for Process and explains the general principles of application security:

Product Overview

The Oracle Agile PLM for Process solution is a fully integrated and comprehensive suite of software and services for collaborative product lifecycle management.

Customers are able to increase revenues, bring their products to market faster and lower risk by managing their new product introduction processes with flexible, collaborative tools. They can lower costs by managing their sourcing relationships and raw materials as well as optimizing their formulas. Using these tools that are designed for the process industry, customers will be able to improve labelling accuracy and avoid costly recalls.

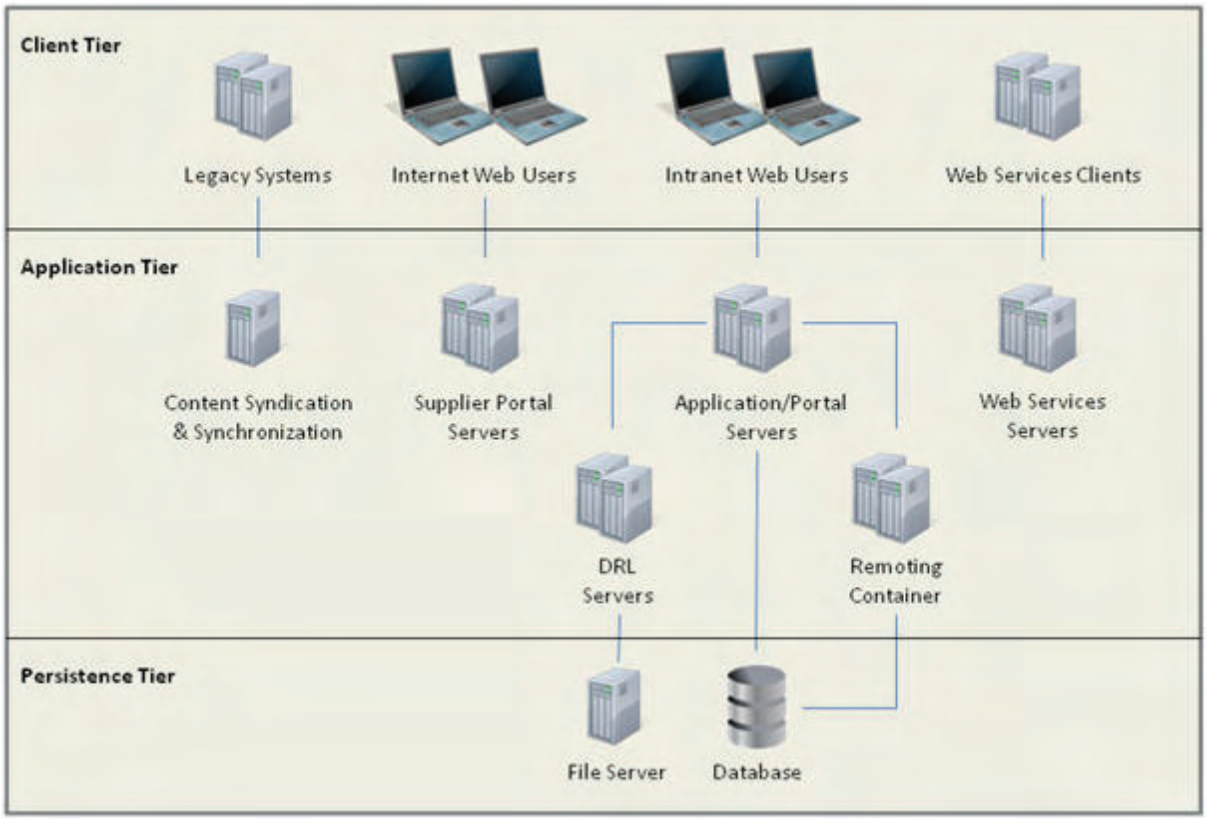
Security Overview

Agile PLM for Process offers several layers of security, as defined below:

- **Object Level Security (OLS)** — Users have access to securable objects within business objects.
- **GSM Business Unit Security** — Users can only access specifications and data about specifications if they are members of one of the business units that the specification is associated to.
- **SCRM Business Unit Security** — Users are assigned an SCRM business unit, which determines visibility and access to companies and facilities. All search screens in Agile PLM for Process that include SCRM companies and facilities respect this visibility.

Product Architecture

Figure 1–1 Product Architecture



Supported Software

For supported versions of the following software, see the *Oracle Agile PLM for Process Install/Upgrade Guide*.

Client Tier:

- Internet Explorer

Application Tier:

- Microsoft Windows
- Microsoft IIS
- Microsoft .NET Framework

Persistence Tier:

- Microsoft SQL Server
- Oracle Database Server

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. Throughout this document, we assume Oracle Agile PLM for Process is version 6.1 or later.

Restrict Network Access to Critical Services

Keep both the application servers and the database behind a firewall. In addition, place a firewall between the middle-tier and the database. The firewalls provide 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.

If firewalls cannot be used, be certain to configure the TNS Listener Valid Node Checking feature which restricts access based upon IP address. Restricting database access by IP address often causes client/server programs to fail for DHCP clients. To resolve this, consider using a static IP address, a software/hardware VPN or Windows Terminal Services or its equivalent.

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, and grants 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.

2

Secure Installation and Configuration

This chapter outlines the planning process for a secure installation, describes several recommended deployment topologies for the systems, and includes the following topics:

Understanding 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 the database, file servers and the availability, performance, and 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?

  Resources belonging to PLM for Process should be protected from everyone on the Internet. Do you have suppliers that will be accessing the Supplier Portal? What level of access do you want to give to employees? What resources should they be able to access? Should the system administrators be able to access all data? You might consider giving access to highly confidential data or strategic resources to only a few well-trusted system administrators. Perhaps it would be best to allow no system administrators access to the data or resources.

- 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.

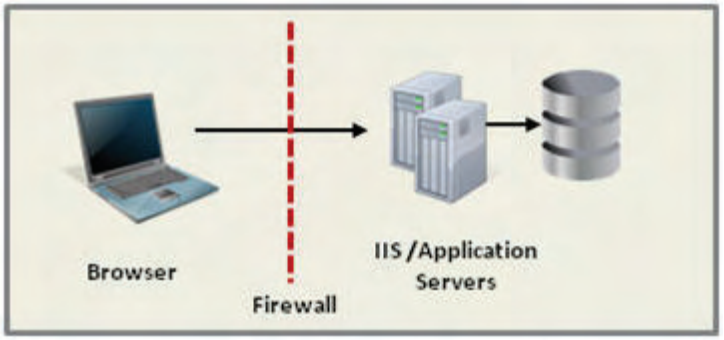
Recommended Deployment Topologies

This section describes recommended architecture for deploying Oracle Agile PLM for Process.

Core Applications

All applications, with the exception of the Supplier Portal, are deployed on a company's intranet. We recommend that the application server and database are deployed behind a firewall, to prevent direct access, as shown in Figure 2–1.

Figure 2–1 Single Firewall

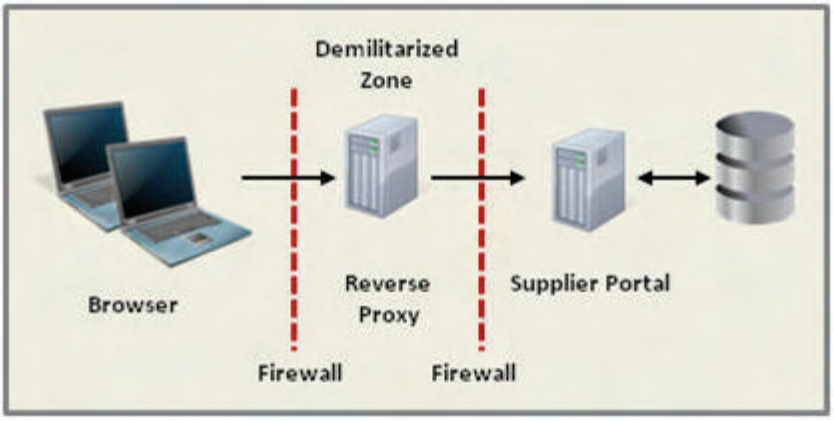


Supplier Portal

The Supplier Portal application should be accessible to the Internet. There are two recommendations for this deployment.

First is the well-known and generally accepted Internet-Firewall-DMZ-Firewall-Intranet architecture shown in Figure 2–2.

Figure 2–2 Traditional DMZ View



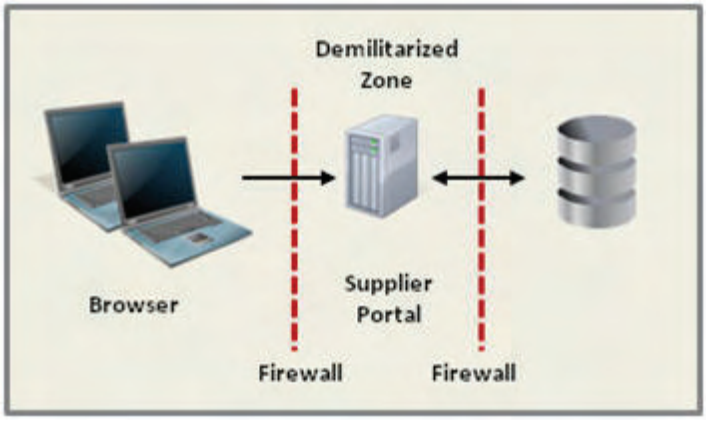
Note: The term demilitarized zone (DMZ) refers to a server that is isolated by firewalls from both the Internet and the intranet, thus forming a buffer between the two.

Firewalls separating DMZ zones provide two essential functions:

- Blocking any traffic types that are known to be illegal.
- Providing intrusion containment, should successful intrusions take over processes or processors.

The second option is deploying the Supplier Portal server in the DMZ and opening up the DB ports so the Supplier Portal can access it directly as shown in Figure 2–3.

Figure 2–3 Deploying Supplier Portal in DMZ



Installing Microsoft Windows 2003/2008 Server with IIS

This section describes how to install and configure Microsoft Windows 2003 and 2008 Server with IIS securely.

For an installation of Oracle Agile PLM for Process on Microsoft Windows 2003 Server or 2008 Server, modify the default configuration following the appropriate guideline found here: NSA Security Guides, with the following differences:

1. To properly run a PLM for Process application, the only application role required is IIS. For Microsoft Windows 2003, install IIS 6. For Microsoft Windows 2008, install IIS 7.
2. When configuring Application Pools for PLM for Process, avoid using Local System for the production environment. Local System prevents the use of Integrated SSPI when connecting to the database. Instead, a clear text username and password must be used in the environmentvariables.config configuration file. If Local System is not used, then Integrated SSPI can be used and the password is not exposed in the configuration file. Refer to the Install/Upgrade Guide for guidance.

   Example of DB configuration:

   ```
   Prodika.DB.URL=server=localhost;uid=user;pwd=pass;database=database
   ```

Installing Microsoft SQL Server Database 2005/2008/2012

This section describes how to install and configure SQL Server 2005, 2008, and 2012 securely.

For an installation of Oracle Agile PLM for Process on SQL Server 2005, 2008, or 2012, follow the appropriate guideline and modify the configuration with the following notes:

- SQL Server 2005 Security Best Practices
- Security Considerations for SQL Server 2008
- Choosing an Authentication Mode

By default, the application is configured to use Integrated SSPI. For this, only Windows Authentication is needed. However, you can choose to use SQL Server Authentication, as well. This method is less secure as it will require a username and password stored in clear text in the environmentvariables.config configuration file. SQL Server Authentication should not be used for production environments.

Installing Oracle Database 10g or 11g

For an installation of Oracle Agile PLM for Process on Oracle Database Server 10g Release 2, follow the Oracle Database Security Guide (10g Release 2) and make the necessary configuration changes.

For an installation of Oracle Agile PLM for Process on Oracle Database Server 11g, follow the Oracle Database Security Guide (11g Release 1) or Oracle Database Security Guide (11g Release 2) and make the necessary configuration changes.

Installing Oracle Agile PLM for Process

The solution is composed of five Media Packs that can be implemented individually:

1. Product Data Management
2. Formulation and Compliance
3. Product Supplier Collaboration
4. New Product Introduction and Development
5. Product Quality Management

The applications should only be installed on servers where they are needed. For example, if New Product Introduction and Development is only needed on one standalone server, do not install it on other servers that are part of the PLM for Process system. This reduces the attack surface area of your deployment.

Post-Installation Configuration

- The URLs for the application are set in the environmentvariables.config configuration file. By default, the URLs are set to HTTPS for a more secured connection. It is highly recommended that all environments where the client browser is on a different server than the application server use HTTPS to ensure that data travelling over the network is secure. If a customer decides not to use SSL, these URLs can be changed to HTTP.
- Export Encryption Key

The Data Admin application allows you to export an encrypted file of administrative data changes for import into a target environment. For increased security, this encryption key can be modified by an administrative user.

By default, the encryption keys are stored as key-value pairs in a database table called ConfigurationDictionary. To change these keys, you will need to update the values for the following two keys in the table:

- DataExchange.Encryption.KeyPassphrase
- DataExchange.Encryption.IVPassphrase

The encryption keys must be identical on both the export and import application environments. Depending on your security requirements, you may need to modify this table to store the keys, for example, in a restricted-access file. The storage and retrieval mechanism for the encryption keys can be modified by creating a custom class and modifying the application configuration.

- The Install/Upgrade Guide provides information for installing the application in a secure environment using Integrated SSPI as the DB connection method. For non-production and environments that do not contain sensitive or confidential information, you can choose to configure the following:
  - Remoting Container Service Run as Local System
  - Application Pools: Run as Local System
  - Connect string to use username and password

    ```
    Prodika.DB.URL=server=localhost;uid=user;pwd=pass;database=database
    ```

- For additional security, you may wish to lock down the application directory. To do this, follow these steps to secure your %PRODIKA_HOME%:

  Using Windows Explorer

  1. Right-click %PRODIKA_HOME%>Sharing and Security>Security Tab>Advanced.
  2. Uncheck "Allow inheritable permissions from the parent...".
  3. Choose Copy on the security pop-up.
  4. Remove all groups other than Administrators.
  5. Add the user that the application pool and remotecontainerservice service runs as.
  6. Give this user the following permissions to %PRODIKA_HOME%:
     a. Read & Execute
     b. List Folder Contents
     c. Read
  7. Also give this user the following permissions to %PRODIKA_HOME\XDocuments and %PRODIKA_HOME%\Logs:
     a. Read & Execute
     b. List Folder Contents
     c. Read
     d. Write
  8. Give this user the following permissions to the system temp directory:

You can find the path information located in your Windows environment variables under System variables. Typically, this is %WINDIR%\temp.

   a. Read & Execute
   b. List Folder Contents
   c. Read
   d. Write

9. Add the account chosen as the anonymous access user for the website.

   Typically, this is IUSR_<machinename> and can be found in IIS > <website> > properties > Directory Security > Authentication and access control > Edit.

10. Give that user "Read" permissions to the %PRODIKA_HOME% directory.

Configuring Firewall Access

Both Supplier Portal and eQ have applications that reside inside the firewall. Supplier Portal and Supplier eQ use a web service to interact with documents via DRL, and this web service must be accessible through the firewall.

To do this, you must:

- Allow standard port 80 or 443 from Supplier Portal to the DRL web service through your firewall.
- Modify your %PRODIKA_HOME%\config\environmentvariables.config as follows
  - Add Prodika.Server2.URL = http://server.domain.tld *
  - Change Prodika.DRLAttachment.URL = @@VAR:Prodika.Server2.URL@@/drl
  - Change Prodika.DRL.URL = @@VAR:Prodika.Server2.URL@@/drl

* This URL should match the URL configured in the intranet environmentvariables.config.

3

Security Features

This chapter outlines specific security mechanisms offered by Oracle Agile PLM for Process and includes the following topics:

Security Model

Application security arises from the need to protect company assets from unauthorized users.

The critical security features that provide protection are:

- 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

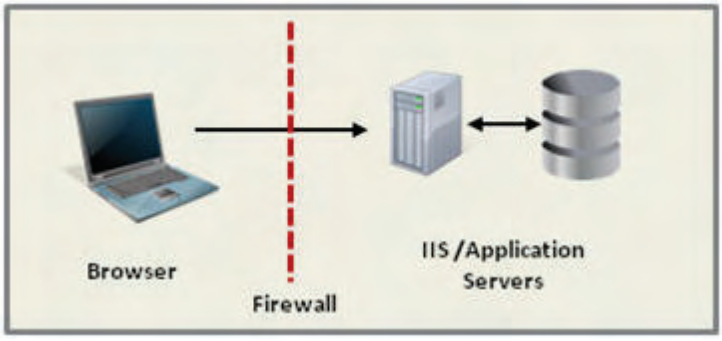
Oracle Agile PLM for Process can be configured to accommodate two kinds of authentication models. Each model has its benefit and is explained in the following sections:

- Basic Authentication
- Single Sign On Authentication

Basic Authentication

Basic authentication is the simplest form of authentication provided. It uses Oracle Agile PLM for Process' internal authentication capabilities. The authentication is performed by using the User ID and hashed password/User ID combination. A MD5 hashing algorithm is used and is not configurable. The hashed password/User ID combination is stored in the database with the user record.

Figure 3–1 Basic Authentication



If SSL is not used, the password is transmitted in clear text, so it is very important to use SSL in a production environment.

The application uses Basic Authentication by default.

Passwords

Password Policy

The password policy for Basic Authentication can be configured to meet the specific needs of each customer. In particular, you can configure these attributes:

- Password Expiration

  Purpose: Specifies the number of days a password is valid until it needs to be changed.

  Configuration File: EnvironmentSetting.config

  Element:

  ```
  <config key="PasswordExpiration" value="{days}" />
  ```

  {days}: Days until expiration, -1 means never expire

  Default: -1

- Password Length

  Purpose: Specifies the min and max length for the password

  Configuration File: CustomerSettings.config

  Element:

  ```
  <EnvironmentManager.configChildKey="key">
      <config.key="MinPasswordSize" value="{minlength}"/>
      <config.key="MaxPasswordSize" value="{maxlength}"/>
  </EnvironmentManager>
  ```

  {minlength}: Minimum length of password, Default:8

  {maxlength}: Maximum length of password, Default:15

- Required Characters

  Purpose: Specifies what characters are required

  Configuration File: ValidationSettings.xml

Element:

```
<rule type="userPassword">
    <condition event="save" minRequirement="{amounttomeet}:">
        <if type="ReflextiveRegExValidator" property="Text"
        expression="{a-z}+"/>
        <if type="ReflectiveRegExValidator" property="Text"
        expression="{A-Z}+"/>
        <if type="ReflextiveRegExValidator" property="Text"
        expression="{0-9}+"/>
        <if type="ReflectiveRegExValidator" property="Text"
        expression="{~!@#$%^&amp;*() :;&lt;&gt;?=\[\]\+\-]+"/>
    </condition>
</rule>
```

{amounttomeet}: Number of conditions that need to be met. For example, if it is set to 3, at least 3 of the regular expressions in the list have to be met.

Default: 3

Additional regular expression can be added.

Based on the specifications, the default password policy is as follows:

At least 8 characters and include 3 of the following: Upper Case (A-Z), Lower Case (a-z), Numbers (0-9) and/or Special Characters (~!@#$%^&*() -+[];:<>?). Password is set to never expire.

Passphrase Policy

A passphrase is provided to support the eSignature feature. Refer to the *Oracle Agile Product Lifecycle Management for Process Administrator Guide* for more information on this feature. The policy for this passphrase is configurable in the same way as the user password, same files just different elements. The default settings are also the same.

Passwords for Default Accounts

After installation there is a default user account and password available in the certified database to allow administration access to the applications. The user account information is as follows:

Username: prodikaadmin

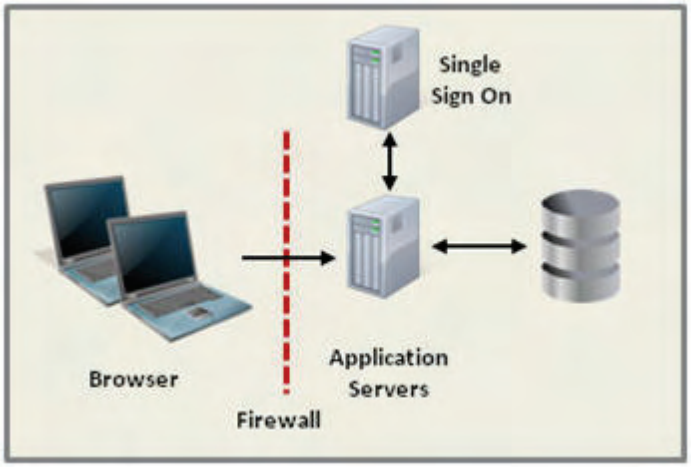
Password: agile

To help better secure the application, the user is required to change this password during the first login.

Single Sign On Authentication

Single Sign On (SSO) authentication allows companies to take advantage of their existing assets. Companies will be able to take advantage of the feature that their specific SSO solution offers, such as strong password enforcement.

Figure 3–2 Single Sign On Authentication



When a user logs in, the request is directed to the SSO server. Authentication is performed and the User ID or External ID is passed back in the response using HTTP Header Rewrite. The request is then forwarded to the application server which again authenticates the user with either the User ID or External ID.

It is important to secure the communication channel between the application server and the SSO server. Secure this channel with SSL.

Using the External ID to authenticate the user is more secure than using the User ID because the External ID is not publicly exposed. To configure the system to authenticate with the SSO, you must configure the SingleSignOn element in the EnvironmentSettings.config file.

```
<SingleSignOn
    xmlMergeKey='SingleSignOn'
    paramName='externalid'
    columnName='username'
    enabled='true'
/>
```

Key Name	Excepted Value	Description
paramName	Name of header key	The header key set by the SSO solution once it authenticates the user in the incoming request.
columnName	Name of the column in the user table	The name of the column in the Users table that contains the value to be compared to the value of the header key in the request.
enabled	true/false	Indicates if SSO is enabled.

The internal authentication mechanism must be set to use Raw Authentication in order for SSO to work properly. To enable this, you must modify the envvar element in the EnvironmentSettings.conf file as follows:

```
<envvar
    name='AuthenticationStrategy'
    id='Prodika'
    useRawAuthentication='true'
    configAttributeOverrideModifier='IsLocked'
/>
```

Configuring and Using Access Control

Oracle Agile PLM for Proces implements various authorization models which work together to provide secure and flexible access control. The following table is an overview of these security features:

General	
User Accounts	User accounts are managed in the User Group Management application. Refer to the *Oracle Agile Product Lifecycle Management for Process Administrator Guide* for more informatin.
Role Based Features	Many features across the product suite are enabled by the user's association to a Role. Users are associated to Roles through the use of User Groups in the User Group Management application. A complete list of Roles and their function can be found in Appendix A of the *Oracle Agile Product Lifecycle Management for Process Administrator Guide*.
Site Access	Users are granted access to specific applications within the applicatoin site through the Site Access Section in the User Group Management application. Refer to the *Oracle Agile Product Lifecycle Management for Process Administrator Guide* for more information.
GSM	
Business Unit Security	Read access to specifications within GSM can be controlled through BU Security. This allows users in a given Business Unit access to only specifications in the same Business Units. Note that this is different from Business Level Visibility. To enable this feature, set the Common.GSMBusinessUnitSecurity.Enabled configuration in the FeatureConfig section of the CustomerSettings.config file to true.
Workflow Security	Read access to GSM specifications can be controlled, based on the workflow step by using Workflow Security.
Section Level Editing	Custom validation rules can be created to control edit access of GSM sections. For example, a rule can be written to turn off editing of specific sections based on UGM user group and specification category, regardless of workflow status. When a section is read-only, all editing methods will be hidden; such as, Add New buttons and Edit icons. For more information, see the *Agile Product Lifecycle Management for Process Extensibility Guide*.

Object Level Security	Object Level Security permits or restricts read access to certain securable objects within a business object (specification, company, facility, sourcing approval, questionnaire, or PQM object). OLS does not determine access to the business object, but once the user does have access, OLS determines what securable objects within the business object the user has access to. These securable objects include: ■ Extended attributes ■ Custom sections ■ Sourcing approvals ■ Supporting documents ■ Supplier Document Management (SDM) documents
Private Smart Issue Requests	By default, all users with the [SMART_ISSUE_ READER] role will be able to read the smart issue request. If a request is marked as Private, only the users added to the Owner and Readers fields will be allowed to view the request.
Veto Plugin Handler	Custom security rules can be evaluated when determining GSM specification read permissions. The Specification Veto Plugin is an extension point available to all GSM specifications that allows a custom class to be accessed when the user opens a specification. The custom class evaluates the current specification and returns a true or false value giving read access to the specification or not.
Formula Classifications	Formula Classifications can be used to restrict access to % breakdowns on Ingredient specifications.
eSignature	Providing a signature for a Signature Document and advancing a spec in a workflow can be configured to require the user to enter a passphrase.
Printing	For all specifications printed, the following table shows how the items are secured. If you do not have access to them, they are not printed: **Secured Object** — **Security Respected** Attachments — OLS Custom Sections — OLS Sourcing Approvals — OLS and SCRM BU Security % Breakdowns — Formulation Classification All related specifications — WFA and BU Security
SCRM	
SCRM Business Unit Security	Access to Company and Facility data can be controlled by using SCRM Business Unit security. Refer to the *Oracle Agile Product Lifecycle Management for Process Supply Chain Relationship Management User Guide* for more information. To enable this feature, set the SCRMBusinessUnitSecurity.Enabled configuration in the FeatureConfig section of the CustomerSettings.config file to true.
NPD	

Private Projects	All projects are available to all NPD users by default. When the Private flag is checked on the project, only authorized team members will have access to the project. Refer to the *Oracle Agile Product Lifecycle Management for Process New Product Development User Guide* for more information.
	Supplier Portal
Supplier Portal Administration	Supplier access to the Supplier Portal is manged by using the Supplier Portal Administration application. Refer to the *Oracle Agile Product Lifecycle Management for Process Supplier Portal User Guid*e for more information.
Publishing Specifications to Supplier Portal	For a specification to be visible in the Supplier Portal, both the specification and the relevant sourcing approval must be in a workflow step on which the system action is set to "Publish to Supplier." Refer to the *Oracle Agile Product Lifecycle Management for Process Supplier Portal User Guide* for more information.
	eQuestionnaire
Questionnaire Security	There are two modes for eQuestionnaire security: Enabled—In this mode, the primary owner and those users defined in the Additional Administrators field have read and write access to this questionnaire. All other users are unable to access the questionnaire. Disabled—In this mode, all users with access to the eQuestionnaire application have read and write access to all questionnaires. To enable this feature, set the EQ.QuestionnaireSecurity.Enabled configuration in the FeatureConfig.config file to true.
	UGM
Import/Export	Customers maintain a staging environment where they add, update, and test administration data changes prior to deploying in a production environment. When ready to deploy to production, the data is exported into a file from the staging environment and then imported into production. Data that is confidential in nature will be exported to an encrypted file. the out-of-the-box functionality will allow the user to create a token on the target envrionment and used to create the export file. This file will now only be able to be imported in the target envrionment.

Default Access

General	
User Accounts	The following users with roles are available by default. **ProdikaAdmin** [ACCESS_LEVEL_EDITOR],[ADD_CUSTOM_SECTION],[ADD_EXT_ATT],[ARCHIVED_DWB_SPEC_CREATOR],[ARCHIVED_DWB_TO_GSM_SPEC_EXPORTER],[AVAILABLE_UOM_ADMIN],[CACHE_ADMIN],[CACHE_SERVER_VIEWER],[CAN_RERESOLVE_WORKFLOWS],[CAN_RERESOLVE_WORKFLOWS_SCRM],[COMPANY_CREATOR],[COMPLIANCE_REVIEWER],[CP_ACCESS_ADMIN],[CP_SYSTEM_ADMIN],[CREATE_FROM_TEMPLATE_1004],[CREATE_FROM_TEMPLATE_1005],[CREATE_FROM_TEMPLATE_1006], [CREATE_FROM_TEMPLATE_1009],[CREATE_FROM_TEMPLATE_1010],[CREATE_FROM_TEMPLATE_2076],[CREATE_FROM_TEMPLATE_2121],[CREATE_FROM_TEMPLATE_2147],[CREATE_FROM_TEMPLATE_2280],[CREATE_FROM_TEMPLATE_2283],[CREATE_FROM_TEMPLATE_5001],[CREATE_FROM_TEMPLATE_5002],[CREATE_FROM_TEMPLATE_5012],[CREATE_FROM_TEMPLATE_5019],[CREATE_FROM_TEMPLATE_5750],[CREATE_FROM_TEMPLATE_5816],[CREATE_FROM_TEMPLATE_6500],[CREATE_FROM_TEMPLATE_6501],[CREATE_FROM_TEMPLATE_7002],[[CREATE_FROM_TEMPLATE_7003],[CREATE_FROM_TEMPLATE_7004],[CSS_ADMIN],[CUSTOM_REPORTER], [CUSTOM_SECTION_DENORM_ENABLER],[DATA_ADMIN],[DENORMALIZED_CUSTOM_SECTION_EDITOR],[DEVELOPER],[DRL_CREATOR],[DRL_EDITOR],[DRL_VIEWER],[DUTCH_TRANSLATOR],[EA_SECTION_CREATOR],[ENGLISHUK_TRANSLATOR],[EQ_ACCESS_LEVEL_EDITOR],[EQ_TEMPLATE_CREATOR],[EXTERNALLY_MANAGED_CROSS_REF_ADMIN],[FACILITY_CREATOR],[FIC_CREATOR],[FIC_READER],[FRENCH_TRANSLATOR],[GERMAN_TRANSLATOR],[GLOBAL_CREATOR],[GLOBAL_EDITOR],[GLOBAL_PRINTER],[GLOBAL_READER],[GLOBAL_SA],[GLOBAL_TIP_ADMIN],[GSM_PRINT_ADMIN],[HIDDEN_SPEC_VIEWER],[HTML_POWERUSER],[ITALIAN_TRANSLATOR],[LIO_CREATOR],[LIO_READER],[LOCAL_USER],[NON_SPEC_SAC_CREATOR],[NPD_ADMIN],[NPD_FINANCIAL],[NPD_GLOBAL_DATA_MANAGER],[NPD_GLOBAL_FINANCIAL],[NPD_IDEA_DELETER],[NPD_ISP_CREATOR],[NPD_PACKAGE_COPY_ADMIN],[NPD_PROJECT_DELETER],[NPD_SA],[NPD_SA_READER],[NUTRIENT_ANALYSIS_CREATOR],[NUTRIENT_COMPARER],[NUTRIENT_COMPOSITE_CREATOR],[OUTPUT_DELETER],[PMA_GLOBAL_ADMIN],[PMA_GROUP_ADMIN],[PMA_USER_ADMIN],[POLISH_TRANSLATOR],[PORTUGESE_TRANSLATOR],[PQM_ADMIN],[PQM_COPIER],[PQM_CREATOR_7002],[PQM_CREATOR_7003],[PQM_CREATOR_7004],[PQS_ADMIN],[PQS_FINAL_SCORER_ROLE],[PQS_GUEST],[PQS_REPORTER],[PQS_SAMPLE_CREATOR],[PQS_SCORECARD_CREATOR],[PQS_SESSION_CREATOR],[PRINT_DEBUG],[REGULATORY_FILING_CREATOR],[REMOVE_CUSTOM_SECTION],[REMOVE_EXT_ATT],[SAC_CREATOR],[SCREEN_CREATOR],[SCRM_COMPANY_EDITOR],[SCRM_COMPANY_READER],[SCRM_FACILITY_EDITOR],[SCRM_FACILITY_READER],[SCRM_FACILITY_RELOCATOR],[SCRM_LOGIN],[SCRM_PRINCIPAL_EDITOR],[SCRM_SEARCH],[SMART_ISSUE_CREATOR],[SMART_ISSUE_EDITOR],[SMART_ISSUE_READER],[SPANISH_TRANSLATOR],[SPEC_ADMIN],[SPEC_COPIER],

[SPEC_CREATOR],[SPEC_CREATOR_1004],[SPEC_CREATOR_1005],[SPEC_CREATOR_1006],[SPEC_CREATOR_1009],[SPEC_CREATOR_1010],[SPEC_CREATOR_1011],[SPEC_CREATOR_2076],[SPEC_CREATOR_2121],[SPEC_CREATOR_2147],[SPEC_CREATOR_2280],[SPEC_CREATOR_2283],[SPEC_CREATOR_5750],[SPEC_CREATOR_5816],[SPEC_CREATOR_6500],[SPEC_CREATOR_6501],[SPEC_EDITOR],[SPEC_GRADUATOR],[SPEC_ISSUER],[SPEC_LOGIN],[SPEC_PRINT_CONTROLLER],[SPEC_PRINTER],[SPEC_READER],[SPEC_READER_1004],[SPEC_READER_2283],[SPEC_SEARCH],[SPEC_TARGET_REVISIONER],[SPEC_XML_VIEWER],[SUBSTITUTE_MATERIAL_DEFINER],[SUCCESSION_REQUEST_EDITOR],[SUCCESSION_REQUEST_READER],[SUPER_DATA_ADMIN],[TEMPLATE_CREATOR],[TEMPLATE_OVERRIDE],[TESTING_PROTOCOL_ADMIN],[TRANSLATION_APPROVER],[TSA_ADMIN],[UGM_GROUP_APPROVER],[UGM_USER_APPROVER],[UMP_ADMIN},[WFA_ADMIN],[WFA_GLOBAL_ADMIN],[WFA_USER]

System—used for system services like DRL and Remotingcontainer.

[ARCHIVED_DWB_TO_GSM_SPEC_EXPORTER],[CACHE_ADMIN],[CAN_RERESOLVE_WORKFLOWS],[COMPANY_CREATOR],[COMPLIANCE_REVIEWER],[CSS_ADMIN],[DATA_ADMIN],[DRL_CREATOR],[DRL_VIEWER],[DUTCH_TRANSLATOR],[ENGLISHUK_TRANSLATOR],[FACILITY_CREATOR],[FIC_CREATOR],[FIC_READER],[FRENCH_TRANSLATOR],[GERMAN_TRANSLATOR],[GLOBAL_CREATOR],[GLOBAL_EDITOR],[GLOBAL_PRINTER],[GLOBAL_READER],[GLOBAL_SA],[GLOBAL_TIP_ADMIN],[GSM_PRINT_ADMIN],[HTML_POWERUSER],[ITALIAN_TRANSLATOR],[LOCAL_USER],[NON_SPEC_SAC_CREATOR],[NPD_ADMIN],[NPD_FINANCIAL], [NPD_GLOBAL_DATA_MANAGER],[NPD_GLOBAL_FINANCIAL],[NPD_ISP_CREATOR],[NPD_PACKAGE_COPY_ADMIN],[NPD_PROJECT_DELETER],[NPD_SA],[NPD_SA_READER],[NUTRIENT_ANALYSIS_CREATOR],[NUTRIENT_COMPARER],[NUTRIENT_COMPOSITE_CREATOR],[PMA_GLOBAL_ADMIN],[PMA_GROUP_ADMIN],[PMA_USER_ADMIN],[POLISH_TRANSLATOR],[PORTUGESE_TRANSLATOR],[PQS_ADMIN],[PQS_GUEST],[PQS_REPORTER],[PRINT_DEBUG],[REGULATOR_FILING_CREATOR],[SAC_CREATOR],[SCREEN_CREATOR],[SCRM_COMPANY_EDITOR],[SCRM_COMPANY_READER],[SCRM_FACILITY_EDITOR],[SCRM_FACILITY_READER],[SCRM_LOGIN],[SCRM_SEARCH],[SPANISH_TRANSLATOR],[SPEC_ADMIN],[SPEC_CREATOR],[SPEC_CREATOR_1004],[SPEC_CREATOR_1005],[SPEC_CREATOR_1006],[SPEC_CREATOR_1009],[SPEC_CREATOR_1010],[SPEC_CREATOR_2076],[SPEC_CREATOR_2121],[SPEC_CREATOR_2147],[SPEC_CREATOR_2280],[SPEC_CREATOR_5750],[SPEC_CREATOR_6500],[SPEC_CREATOR_6501],[SPEC_EDITOR],[SPEC_LOGIN],[SPEC_PRINT_CONTROLLER],[SPEC_PRINTER],[SPEC_READER],[SPEC_READER_1004],[SPEC_SEARCH],[SPEC_XML_VIEWER],[SUCCESSION_REQUEST_EDITOR],[SUCCESSION_REQUEST_READER],[SUPER_DATA_ADMIN],[TESTING_PROTOCOL_ADMIN],[TRANSLATION_APPROVER],[TSA_ADMIN],[UMP_ADMIN],[WFA_ADMIN],[WFA_GLOBAL_ADMIN],[WFA_USER]

ProdikaUserGroupAdmins

[datareader], [datawriter]

Role Based Features	Many features across the product suite are enabled by the user's association to a Role. Users are associated to Roles thorugh the use of User Groups in the User Group Management application. A complete list of Roles and their function can be found in Appendix A of the *Oracle Agile Product Lifecycle Management for Process Administrator User Guide*.
Site Access	Users are granted access to specific applications within the application suite through the Site Access Section in the User Group Management application. Refer to the *Oracle Agile Product Lifecycle Management for Process Administrator User Guide* for more information.

Object Level Security

Object Level Security permits or restricts read access to certain securable objects within a business object (specification, company, facility, sourcing approval, questionnaire, or PQM object). OLS does not determine access to the business object, but once the user does have access, OLS will then determine what securable objects within the business object the user has access to. These securable objects include:

- Extended attributes
- Custom sections
- Sourcing approvals
- Supporting documents
- Supplier Document Management (SDM) documents

Each of these securable objects will have one associated security classification. You select a security classification when defining an extended attribute or custom section in the ADMN (Manage Core Data) application. For GSM supporting documents, you assign a security classification using the attachments Summary Information page. For SCRM SDM documents, assign security classifications using the Supplier Document Management page. Sourcing approvals have only one security classification, called Sourcing Approval, so no choice is required. For PQM, it only supports Non Contextual Security (simple security) in custom sections and supporting documents.

Object level security configuration is divided in two parts: Contextual and Non Contextual. It can be configured on or off per customer implementation. When both are configured off, these objects are unsecured and are accessible by all users who can access the specification or questionnaire.

Simple Security

Once the security classifications have been defined for the extended attributes or custom sections, you then define a privilege in user groups within UGM for each security classification. This security classification is referred to as Access Classification in the privilege list. These two terms can be used interchangeably. This privilege determines whether or not users within this group have access to these specific security classifications. If a privilege is not defined, then by default the users will not have access.

Contextual Security

Extended attributes, custom sections, and supporting documents support an additional security mode called "contextual security." This mode allows you to configure access based on context, i.e. the specification or questionnaire where the extended attribute, custom section, or supporting document exists. This means that a

given extended attribute, custom section, or supporting document can be visible in one specification but not visible in another. An example of this would be if you wanted a group of users to access financial data for all specifications except for those that are considered highly restricted. You might have a smaller group of users who can view this information on these highly restricted specifications.

Access Level

To set contextual security, an attribute of the specification or questionnaire called access level is used. Contextual security uses the access level to help determine if the user has access to the data based on the specific security classification. Access level is hierarchical, meaning that there is a ranking or level associated to each one. If users have access to a certain level for a security classification, they will also have access to all the levels below it. The access level is a combination of a description, such as "Highly Restricted," and a ranking, such as "500."

The way contextual security is defined is similar to that for simple security. Within the access privilege section of the user group in UGM, the Read column contains the security level that the group has access to for the corresponding security classification.

The security mode, "simple" or "contextual," is determined based on the security classification. Each security classification is defined as either non contextual (simple) or contextual. In the **Read** column of the Access Privilege list, the simple security classifications will have a drop-down list containing "Has Access" or "No Access." The contextual security classifications will have a drop-down list containing the access levels.

Note: Contextual Security is a legacy feature and not recommended for use. Please use Non-Contextual Security only.

User Access Privilege Resolution

The access privileges that a user inherits is a combination of access privileges from the user groups' hierarchies that they are members of. A user can be a member of multiple groups. A group can be a child of another group. The final user access privileges resolve based on the following rules:

- The list is a superset of privileges from the groups the user belongs to plus all the parents/grandparents of those groups. The resolution process climbs the group hierarchy until either the root node is reached or it encounters a group for which the Inherit Parent Privileges box is unchecked.
- If more than one group contains the same security classification, the user inherits the least restrictive one, i.e. the highest ranked one. For example, if the financial security classification was found in two groups, one with an access level of "Highly Restricted (500)" and one with a less restrictive access level of "Restricted (400)," the user would inherit the highly restricted (500) access level. This means the user will have access to data with a security classification of "Financial" that is contained on any specification or questionnaire that the user has access to, with an access level of highly restricted (500) or below.

The fully resolved privilege list for a user can be viewed in the Access Privilege section of a user's profile within UGM.

GSM Business Unit Security

When GSM BU security is enabled, read permissions are controlled by the business unit assigned to the specification in addition to WFA permissions. What business unit(s) the user has access to is defined on the UGM user profile.

GSM BU Security also restricts access to some objects that are linked to specifications. For example, if a sourcing approval is related to a specification the user does not have BU access to, the user will not have access to the sourcing approval. In addition, if a specification the user does not have access to is attached to an NSM object, the user will not have access to the NSM object.

If a user is associated to no business units in UGM they will have access to all business units.

SCRM Business Unit Security

When SCRM BU security is enabled, read permissions and visibility of company, facility, and sourcing approval objects is controlled by the business unit attached to the company and facility. What business unit(s) the user has access to is defined on the UGM user profile.

SCRM Business Units can be associated with a status on the company or facility profile. The combination of the business unit plus status creates the permission rule. For example, company A is attached to a BU ABC and BU ABC is set to "Inactive." Users not assigned to BU ABC can still see company A because BU ABC is inactive. This all depends on your configuration.

In addition to controlling read permissions, SCRM BU security also filters the business unit dialog box. The user will only see business units they have access to.

If a user is associated to no business units in UGM, they will have access to all business units.

BU Visibility Versus BU Security

It is important to understand the difference between business unit (BU) visibility and BU security.

BU Visibility

BU visibility feature helps reduce the number of specifications presented in a search result. Think of it as helper and not security.

1. When a user performs a search, GSM only presents specifications where the user and the specifications have common BUs either directly or indirectly. "Directly" represents an exact match and "Indirectly" would be a parent or child of a BU node.
2. The results returned will appear despite workflow permissions. Therefore you do not need read or write access to see a given specification in my search results.
3. However as soon as you click on the specification, then workflow permissions govern the ability to see and interact with the specification. If a user that is not assigned to the proper BU gains access to a specification, then workflow permissions govern security. Some examples of how users can gain access to specifications without the use of a search include:
   a. Automated email due to ownership, notification, signature
   b. A user provides a link to another user
   c. A user has access to Specification A which references Specification B. The user is not associated with a BU related to Specification B, i.e. Trade to Material, Formulation to Material…
4. An example follows:

a. Assume two users are both part of R&D.

b. We place both in a UGM group called "R&D" and assign each to their own BU; User A BU=NA, User B BU=CN.

c. Workflows are configured to allow anyone who is a member of "R&D" to read specifications.

d. Via a standard search, User A will only see specifications associated with BU = NA and User B will only see specifications associated with BU=CN.

e. But User A emails User B a link to a NA specification. Because workflow permissions govern read access and User B is a member of "R&D," User B will be able to read the NA specification.

BU Security

BU security basically changes how workflow permissions works in step 3 above as well as providing the various other forms of security described in this chapter. When BU security is turned on, then workflow permissions + BU govern read or write access. Therefore however a user finds a link to the specification they must be a member of both a proper BU and UGM group to see a specification.

Configuring and Using Auditing

There are two auditing features that can be used as part of a deployment:

1. Application level login attempt auditing
2. IIS level request auditing

Application Level Login Attempt Auditing

These logs should be periodically reviewed for suspicious failed login attempts.

The PLM for Process applications automatically log login attempts to the local server's Event Viewer, which can be found under System Tools in the Computer Management console on the server where the web application is running. A successful login will create an Information level event. A failed login attempt will create a Warning level event. The event log can filter the events by right-clicking the application in the Event Viewer and selecting Properties. On the Filter tab, the event types to be logged can be adjusted.

IIS Level Request Auditing

If a secure breach has been suspected, these logs can help determine which users viewed or edited data in question.

IIS can be configured to log every web request to any of the web applications deployed. To configure this, open IIS Manager. Right-click on the appropriate web site(s) on the tree on the left and choose Properties. On the Web Site tab, make sure Enable Logging is checked. To find the log file that is being used, select the Properties button. Another window opens. At the bottom of the General tab, the log file and directory are displayed.

4

Security Considerations for Developers

This chapter discusses information useful to developers extending the application or producing applications using the product as a platform and includes the following topics:

Extensibility Points

The PLM for Process suite includes numerous extensibility points—areas in the application suite used to extend functionality of the product suite. Several extensibility points can be leveraged to provide additional customized security within the application, including Section Level Editing and the Specification Veto Plugin. Other extensibility points allow for customized display of information in the application, either as user interface screen enhancements (Notification Panel, Spec Identity Plugins) or in print or report output.

Detailed documentation is available for each extensibility point, including class diagrams, configuration file examples, a working, compiled, reference implementation, and the related source code. The *Extensibility Guide* document contained in the Extensibility Pack release provides an overview of each extensibility point, as well as the locations of the reference implementations and documentation.

Custom Classes

To implement most extensibility points, application developers will typically write custom classes using C#, place the compiled code into the *bin* directories of the relevant web applications, and add a reference to their class in specific XML configuration files.

The application framework will call these custom classes and provide to each class relevant contextual data, such as the current specification data object. These data objects, however, do not contain security related business logic, so application developers must take care to implement various security checks as needed.

For instance, when viewing a Trade spec's related Material spec, you can use the "TrdMaterialSpecAssociationIdentityPlugin" extension to add information to the user interface display of the spec information, such as the Material spec's ingredient statement. If you want to ensure that only users that have read permission to that Material spec can read the ingredient statement, you would have to add specific code to perform that permission check.

Utility classes are available for determining spec permissions. See the Security section of the *Extensibility Guide* for more details.

Web Services

A set of over 40 PLM for Process web services, available in the Extensibility Pack, provide the ability to query, retrieve, and update data. When calling web services related to specific business objects, such as specifications, the user calling the web service is evaluated for security permissions. 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. For example, the GetSpecSummary web service—which returns the specification's name, status, and more—will not return a specification that the calling user does not have read permission for. See the *Oracle Agile Product Lifecycle Management for Process Application Programming Interface User Guide* for more details about the web services.

Printing

Printing the various system objects, such as specifications, NPD projects, etc., may be customized to meet various client needs. Clients may limit access to specific print templates (via print template Guard Conditions classes), limit visibility of specific data elements (via mapping file Guard Conditions classes), use custom data and field translations in the existing print templates, and create their own print templates. See the *Oracle Agile Product Lifecycle Management for Process Print Configuration Guide*, available in the Extensibility Pack, for more details.

Reporting

The Reporting application allows clients to organize, configure, secure, and launch custom reports. Clients can configure custom reports, specify the categorization of the reports, configure visibility rules via custom classes, and define the various report parameters to display. Reports are categorized by two grouping levels: Report Contexts and Report Groups, each of which can be secured by configuring security classes. Report parameters can use existing pop-ups found throughout the application, or use custom-defined parameters. See the *Oracle Agile Product Lifecycle Management for Process Custom Report Configuration Guide* for more details (Appendix B details how to apply security to reports).

Custom Portal

Custom Portal is an extensible web portal framework for customers to build web pages that query for Agile PLM for Process objects, display the search results, and print the result details in various formats. Access to the Custom Portal pages is secured through PLM for Process administration. The search results screens, however, are custom built. They can be implemented in various ways, from web service calls, which enforce security permission checks, to completely custom SQL code, which

would then require custom security checks to be written. See the *Custom Portal Implementation Guide* in the Extensibility Pack for more details.

Site Navigation

The site navigation menu allows for overriding the existing menu items and icon buttons or adding new menu items that are not part of the core product. Each menu item or icon's visibility can be restricted by modifying the configuration entries as indicated in the *Navigation Configuration Guide*. For instance, the Edit icon on a specification can be limited to certain user groups or roles. A custom class can also be called to evaluate visibility permissions for the icon.

A

Secure Deployment Checklist

This appendix contains the Secure Deployment Checklist to help secure your database.

Secure Deployment Checklist

The following security checklist includes guidelines that help secure your database:

1. Install only what is required.
2. Lock and expire default user accounts.
3. Enable data dictionary protection.
4. Practice the principle of least privilege.
   a. Grant necessary privileges only.
   b. Revoke unnecessary privileges from the PUBLIC user group.
   c. Restrict permissions on run-time facilities.
5. Enforce access controls effectively and authenticate clients stringently.
6. Restrict network access.
   a. Use a firewall.
   b. Never poke a hole through a firewall.
   c. Monitor listener activity.
   d. Monitor who accesses your systems.
   e. Check network IP addresses.
   f. Encrypt network traffic.
   g. Harden the operating system.
7. Apply all security patches and workarounds.