Oracle® Retail Predictive Application Server

Installation Guide

Release 13.3.1

E35408-02

September 2012

ORACLE®

Oracle Retail Predictive Application Server Installation Guide, Release 13.3.1

E35408-02

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

Primary Author: Melissa Artley

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

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

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

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

This software or hardware and documentation may provide access to or information 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.

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

(i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.

(ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.

(iii) the software component known as **Access Via™** licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.

(iv) the software component known as **Adobe Flex™** licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.

Contents

4 Installing on a Windows Environment

5 Installing the RPAS Fusion Client

List of Tables

List of Figures

Send Us Your Comments

Oracle Retail Predictive Application Server Installation Guide, Release 13.3.1

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

> **Note:** Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Technology Network Web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at `http://www.oracle.com`.

Preface

Oracle Retail Installation Guides contain the requirements and procedures that are necessary for the retailer to install Oracle Retail products.

Audience

This Installation Guide is for the following audiences:

- Database administrators (DBA)
- System analysts and designers
- Integrators and implementation staff

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.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/support/contact.html` or visit `http://www.oracle.com/accessibility/support.html` if you are hearing impaired.

Related Documentation

For more information, refer to the following documents in the Oracle Retail Predictive Application Server Release 13.3.1 documentation set:

- *Oracle Retail Predictive Application Server Release Notes*
- *Oracle Retail Predictive Application Server Administration Guide for the Classic Client*
- *Oracle Retail Predictive Application Server Administration Guide for the Fusion Client*
- *Oracle Retail Predictive Application Server Configuration Tools Guide*
- *Oracle Retail Predictive Application Server Licensing Information*
- *Oracle Retail Predictive Application Server Online Help for the Fusion Client*
- *Oracle Retail Predictive Application Server User Guide for the Classic Client*
- *Oracle Retail Predictive Application Server User Guide for the Fusion Client*

Supplemental Documentation at My Oracle Support

The following document is available through My Oracle Support. Access My Oracle Support at the following URL:

`https://support.oracle.com`

Oracle Retail Fashion Planning Bundle Reports Documentation (Note ID 1132783.1)

The Oracle Retail Fashion Planning Bundle Reports package includes role-based Oracle Business Intelligence (BI) Enterprise Edition (EE) reports and dashboards that provide an illustrative overview highlighting the Fashion Planning Bundle solutions. These dashboards can be leveraged out-of-the-box or can be used along with other dashboards and reports that may have already been created to support a specific solution or organizational needs. This package includes dashboards for the Assortment Planning, Item Planning, Item Planning Configured for COE, Merchandise Financial Planning Retail Accounting, and Merchandise Financial Planning Cost Accounting applications.

The Oracle Retail Fashion Planning Bundle Reports documentation set includes the following documents that describe how you can install and use the reports and dashboards:

- *Oracle Retail Fashion Planning Bundle Reports Installation Guide* – This guide describes how you can download and install the Fashion Planning Bundle reports. This guide is intended for system administrators and assumes that you are familiar with the Oracle Retail Predictive Application Server (RPAS) and Oracle BI EE.
- *Oracle Retail Fashion Planning Bundle Reports User Guide* – This guide describes the reports and dashboards included for the Oracle Retail Fashion Planning Bundle solutions.

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

`https://support.oracle.com`

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 13.3) or a later patch release (for example, 13.3.1). If you are installing the base release, additional patch, and bundled hot fix releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch and bundled hot fix releases can contain critical information related to the base release, as well as information about code changes since the base release.

Oracle Retail Documentation on the Oracle Technology Network

Documentation is packaged with each Oracle Retail product release. Oracle Retail product documentation is also available on the following Web site:

`http://www.oracle.com/technology/documentation/oracle_retail.html`

(Data Model documents are not available through Oracle Technology Network. These documents are packaged with released code, or you can obtain them through My Oracle Support.)

Documentation should be available on this Web site within a month after a product release.

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

Introduction

Welcome to the *Oracle Retail Predictive Application Server Installation Guide*. This chapter outlines the contents of this guide, discusses the updated components with respect to the previous version, lists hardware and software requirements, and defines commonly used notations and terms.

Check for the Current Version of the Installation Guide

Corrected versions of Oracle Retail Installation Guides may be published whenever critical corrections are required. For critical corrections, the rerelease of an installation guide may not be attached to a release; the document will simply be replaced on the Oracle Technology Network Web site.

Before you begin installation, check to be sure that you have the most recent version of this installation guide. Oracle Retail installation guides are available on the Oracle Technology Network at the following URL:

`http://www.oracle.com/technology/documentation/oracle_retail.html`

An updated version of an installation guide is indicated by part number, as well as print date (month and year). An updated version uses the same part number, with a higher-numbered suffix. For example, part number E123456-02 is an updated version of an installation guide with part number E123456-01.

If a more recent version of this installation guide is available, that version supersedes all previous versions. Only use the newest version for your installation.

About This Document

This document contains information for full and patch installations:

- Full Installation. Refer to this section if you are performing a full installation of RPAS 13.3.1.
- Patch Installation. Refer to this section if you are performing a patch installation of RPAS 13.3.1.

> **Note:** Only RPAS base releases have installers. Patch releases and hot fixes do not have installers. If you are installing a base release, refer to Full Installation for installer instructions. If you are installing a patch, refer to Patch Installation for patch instructions.

Read this entire guide before beginning the installation process to ensure you understand the installation process and have all the necessary documentation, hardware, and software available.

Hardware and Software Requirements

Table 1–1 describe the hardware and software requirements for the RPAS Server, RPAS Configuration Tools, and ODBC and JDBC servers and clients.

RPAS Server and Components

For information on installing the RPAS Server, refer to either Chapter 3, "Installing on UNIX and Linux Environments" or Chapter 4, "Installing on a Windows Environment".

Table 1–1 RPAS Server and Components Hardware and Software Requirements

Component	Details
Supported Operating Systems for the RPAS Server, Compilers, ODBC Server, and ODBC Client	AIX 5.3 (POWER) – TL12 SP1: GCC 4.1.1 (64 bit)
	AIX 6.1 (POWER) – TL6: GCC 4.3.3 (64 bit)
	Oracle Linux 5, Update 8 (5.8): GCC 4.1.2 (64 bit)
	Oracle Solaris 10 (SPARC) Update 5, with time zone patch 122032-01 and libc patch 119689-07: Solaris Studio 12.2
	HP-UX Itanium 11.31, Sept. 2010 Quality Pack: ACC 6.20 (64 bit)
	Note: The RPAS ODBC Client is supported on the previously listed operating systems, as well as 32-bit Windows.
Supported Operating Systems for RPAS Configuration Tools	Microsoft Windows 7
	Microsoft Windows XP
	Note: The server aspect of the RPAS Configuration Tools (rpasInstall, which is used to install and patch domains) is supported on the same operating systems as the previously listed RPAS Server.
Required Software	JDK 1.6 is required to support the RPAS Configuration Tools, server machines, and JDBC Client. There are specific JDK versions supported for each of the following operating systems: ■ AIX 5.3 (POWER) TL12: IBM JDK 1.6 SR9 (64-bit) ■ IBM AIX 6.1 (POWER) TL6: IBM JDK 1.6 SR9 (64-bit) ■ Oracle Linux 5 Update 8: Oracle JDK 1.6 Update 29 (64-bit) ■ Oracle Solaris 10 Update 5: Oracle JDK 1.6 Update 29 (64-bit) ■ HP-UX 11.31 Itanium: HP JDK 1.6_09 (64-bit) **Note:** When installing Java, avoid enabling AutoUpdate because it may update the Java version without prompting

RPAS Classic Client

Table 1–2 describe the hardware and software requirements for the RPAS Classic Client. For information on installing the RPAS Classic Client, refer to Chapter 6, "Installing and Configuring the RPAS Classic Client". For information about Single Sign-On, refer to "Appendix D: Oracle Single Sign-On (SSO)".

Table 1–2 RPAS Classic Client Hardware and Software Requirements

Component	Details
Supported Operating Systems	Microsoft Windows XP Professional SP3 with Microsoft Office 2003
	Microsoft Windows 7 Professional (Service Pack 1) with Microsoft Office 2007
Client System Requirements	**All components are required:** ■ 800x600 or higher display resolution ■ 1GHz or higher processor ■ 512 MB or higher memory ■ Intranet network connectivity with at least 10Mbps data rate
RPAS Classic Client Web Deployment and Single Sign-On (SSO) Requirements	**Note:** Classic Client Web Deployment, along with SSO, is optional.
	Server options (only one of these options is required): ■ Oracle WebLogic Server 11gR1 (Release 10.3.5) with Oracle Application Development Framework (11g (11.1.1.5) and JDK 1.6. If Oracle SSO is used, the Web Tier Utilities 11.1.1.5 must be installed. ■ Apache Tomcat 6.0 with JDK 1.6
	Web browser requirements: ■ Microsoft Internet Explorer 6.0 or 7.0 ■ Oracle JVM plug-in of Java version 1.6
	Single Sign-On (SSO) WebLogic requires both of these components: ■ Oracle Web Tier Utilities (11.1.1.5) ■ Oracle Identity Management 11g (11.1.1.5)
	RPAS Classic Client Web Deployment is certified for SSO using Oracle Access Manager 11g (OAM). This is available in the Oracle Identity and Access Management 11g package (11.1.1.5).
	OAM works with a wide variety of LDAP-based identity stores. RPAS Classic Client Web Deployment has been verified to work with Oracle Internet Directory 11g (OID 11.1.1.5).
	OAM-based SSO needs a web server. RPAS Classic Client Web Deployment has been verified to work with Oracle HTTP Server (OHS) 11.1.1.5.
	A web server plug-in (OAM Webgate) communicates with an OAM instance and to create the SSO cookie. OAM Webgate 11.1.1.5 is required.
	In summary, the following Oracle Fusion Middleware packages are utilized in the solution: ■ Oracle Web Tier Utilities (11.1.1.5) ■ Oracle Identity Management 11g (11.1.1.5) ■ Oracle Identity and Access Management 11g (11.1.1.5) ■ Oracle Access Manager Webgate 11g (11.1.1.5)

RPAS Fusion Client

Table 1–3 describe the hardware and software requirements for the RPAS Fusion Client. For information on installing the RPAS Fusion Client, refer to Chapter 5, "Installing the RPAS Fusion Client".

Table 1–3 RPAS Fusion Client Hardware and Software Requirements

Component	Details
Supported Operating Systems for the Fusion Client	Microsoft Windows XP Professional SP3 with Microsoft Office 2003
	Microsoft Windows 7 Professional (Service Pack 1) with Microsoft Office 2007
Supported Web Browsers	**Note:** All browsers must have Adobe Flash Player 9.0 (or later).
	Microsoft Windows XP ■ Microsoft Internet Explorer 7.0, 8.0 ■ Mozilla Firefox 4.0 (or later)
	Microsoft Windows 7 ■ Google Chrome 7.0 (or later) ■ Microsoft Internet Explorer 8.0 ■ Mozilla Firefox 7.0 (or later)
Application Server Requirements	All components required: ■ Oracle WebLogic Server 11g Release 1 (Release 10.3.5) ■ Oracle Application Development Runtime (11.1.1.5) ■ My Oracle Support patch 13849867
Supported Operating Systems for the Application Server	**Note:** The operating systems you choose for the RPAS server and the application server for the RPAS Fusion Client do not need to be the same.
	AIX 6.1 (POWER) – TL6 (64 bit)
	Oracle Linux 5, Update 8 (5.8) (64 bit)
	Oracle Solaris 10 (SPARC) Update 5, with time zone patch 122032-01 and libc patch 119689-07
	HP-UX Itanium 11.31, Sept. 2010 Quality Pack (64 bit)
Required Software	JDK 1.6 is required to support the Fusion Client on an application server. There are specific JDK versions supported for each of the following operating systems: ■ IBM AIX 6.1 (POWER) TL6: IBM JDK 1.6 SR10 (64-bit) ■ Oracle Solaris 10 Update 5: Oracle JDK 1.6 Update 30 (64-bit), or Oracle Jrockit 6 - R28.2.2 (64-bit) ■ Oracle Linux 5 Update 8: Oracle JDK 1.6 Update 30 (64-bit), or Oracle Jrockit 6 - R28.2.2 (64-bit) HP-UX 11.31 Itanium: HP JDK 1.6_13 (64-bit)

Table 1–3 (Cont.) RPAS Fusion Client Hardware and Software Requirements

Component	Details
Supported Oracle Software for Single Sign-On (SSO)	**Note:** SSO is optional.
	RPAS Fusion Client is certified for SSO using Oracle Access Manager 11g (OAM). This is available in the Oracle Identity and Access Management 11g package (11.1.1.5).
	OAM works with a wide variety of LDAP-based identity stores. RPAS Fusion Client in SSO deployment has been verified to work with Oracle Internet Directory 11g (OID 11.1.1.5).
	OAM-based SSO needs a web server. RPAS Fusion Client has been verified to work with Oracle HTTP Server (OHS) 11.1.1.5.
	A web server plug-in (OAM Webgate) communicates with an OAM instance and to create the SSO cookie. OAM Webgate 11.1.1.5 is required.
	In summary, the following Oracle Fusion Middleware packages are utilized in the solution: ■ Oracle Web Tier Utilities (11.1.1.5) ■ Oracle Identity Management 11g (11.1.1.5) ■ Oracle Identity and Access Management 11g (11.1.1.5) ■ Oracle Access Manager Webgate 11g (11.1.1.5)

Hardware and Software Requirement Notes

The following notes pertain to the RPAS hardware and software requirements:

- Once the RPAS server and client are installed, you must build and set up an RPAS domain or install an RPAS solution. For more information on setting up an RPAS domain, refer to either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*. For more information on installing an RPAS solution, refer to the relevant installation guide included with the RPAS solution package.
- If you are installing only the Oracle RPAS Fusion Client without any additional applications supported by the Oracle Application Development Runtime, you do not need to install the Oracle Database and MetaData Services (MDS) repository schema specified by the Oracle Application Development Runtime installation instructions.
- If you are installing the RPAS Server on Windows, you must install Cygwin to emulate UNIX commands (required for starting the RPAS Server on Windows). You can find more information about downloading this product at `http://www.cygwin.com`. If running the RPAS Server on Windows, use Windows XP or Windows 7. Perl is an interpreted language that is included on all supported UNIX platforms (included with Cygwin for Windows). Perl is used by the patch sets, which are used to install an RPAS patch.
- An application for unzipping (.zip) components on UNIX must be installed and used for extracting the RPAS Configuration Tools. Unzip is an open source software package that can be used for this process.

Table 1–4 indicates which software components are needed for each task. The reference to Windows refers to either Windows XP or Windows 7.

Table 1–4 Software Requirements Notes

Task	Typical User	Platforms	RPAS Server	RPAS Clients	Configuration Tools	Java
Log in to an existing (built) RPAS domain for the primary purpose of building workbooks	End User	Windows	No	Yes	No	No
Use the Configuration Tools to create or modify solutions.	Solution/ Product Administrator	Windows	Yes	No	Yes	Yes
Use the Configuration Tools to build configured solutions.	Solution/ Product Administrator	Windows UNIX Linux	Yes	No	Yes	Yes

Java can be acquired from `www.java.com` for Oracle Solaris and Microsoft Windows or from the respective vendor's Web site for IBM and HP.

Environment variables are automatically set when using the Oracle Retail Installer to install the RPAS components on a UNIX environment.

Supported Oracle Retail Products

For information on the version of the RPAS platform that an RPAS application uses, refer to that application's documentation.

Terms

The following table lists terms that are used in this guide.

Term	Definition
RPAS	The Oracle Retail Predictive Application Server provides the foundation for Oracle Retail solutions such as Oracle Retail Demand Forecasting (RDF), Merchandise Financial Planning (MFP), and Advanced Inventory Planning (AIP). RPAS does not include any business logic, but it enables the solutions to store, manipulate and retrieve data. It provides the solutions with a standard interface based on wizards, templates, workbooks, and batch processes.
RPAS solution	The software that uses RPAS. RPAS solutions are added on to RPAS domains as separate modules. All the business logic is encapsulated in the solution. An RPAS domain can support multiple solutions.
RPAS domain	The collection of server-side directories and files containing data and procedures that comprise the RPAS solution. For additional information, refer to the *Oracle Retail Predictive Application Server Configuration Tools User Guide* and the Classic Client and Fusion Client versions of the *Oracle Retail Predictive Application Server Administration Guide*.
RPAS Classic Client	The Windows-based client interface for end users and system administrators of an RPAS domain. An administrator may perform maintenance work in a domain using the RPAS Classic Client, server-side RPAS utilities.
RPAS Fusion Client	The Web-based Rich Client for end users and system administrators of an RPAS domain. An administrator may perform maintenance work in a domain using the RPAS Fusion Client in a browser. This Retail Predictive Application Server (RPAS) platform is developed using the Oracle Application Development Framework (ADF).
RPAS Configuration Tools	The tools used to configure an RPAS solution. For more information, refer to the *Oracle Retail Predictive Application Server Configuration Tools User Guide*.

Part I

Full Installation

Part I of this guide details the steps needed to perform a full installation of RPAS.

Part I contains the following chapters:

For information about a patch installation, refer to Patch Installation.

2

Getting Started

This chapter provides:

- An overview of the RPAS platform
- Typical installation scenarios
- An overview of the installation contents

RPAS Platform Overview

RPAS 13.3.1 is comprised of many components. In addition, there are solutions that have been developed using the RPAS 13.3 foundation. These solutions must be installed separately. Examples of these solutions include Oracle Retail Merchandise Financial Planning (MFP) and Oracle Retail Advanced Inventory Planning (AIP).

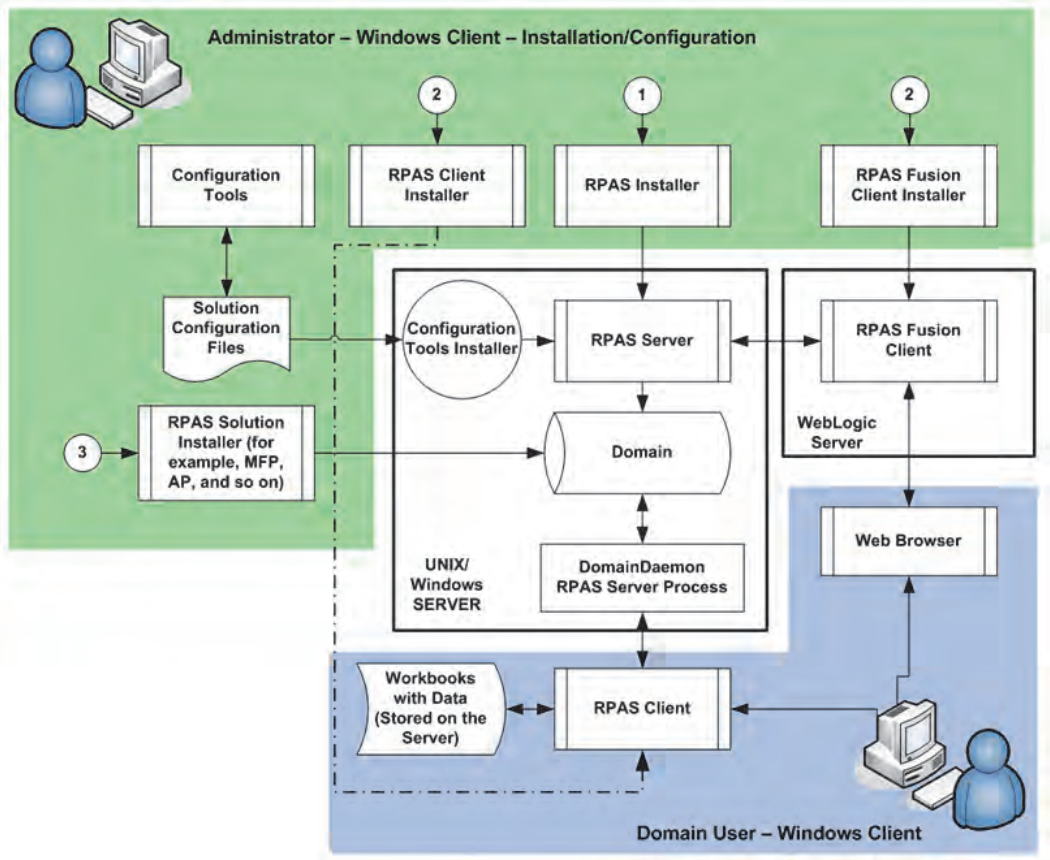
The components of the RPAS software include the following:

- RPAS Server and related utilities
- RPAS Classic Client
- RPAS Fusion Client
- RPAS Configuration Tools
- Sample configurations (Curve and Grade)
- Documentation
- Supported Translations

Installation Process Flow

A typical RPAS Server-based installation is illustrated in Figure 2–1. For instructions on installing on a Windows machine, refer to Chapter 4, "Installing on a Windows Environment".

Figure 2–1 Installation Process Flow



RPAS Environment

Figure 2–1 displays a typical RPAS Server-based installation and provides the following information:

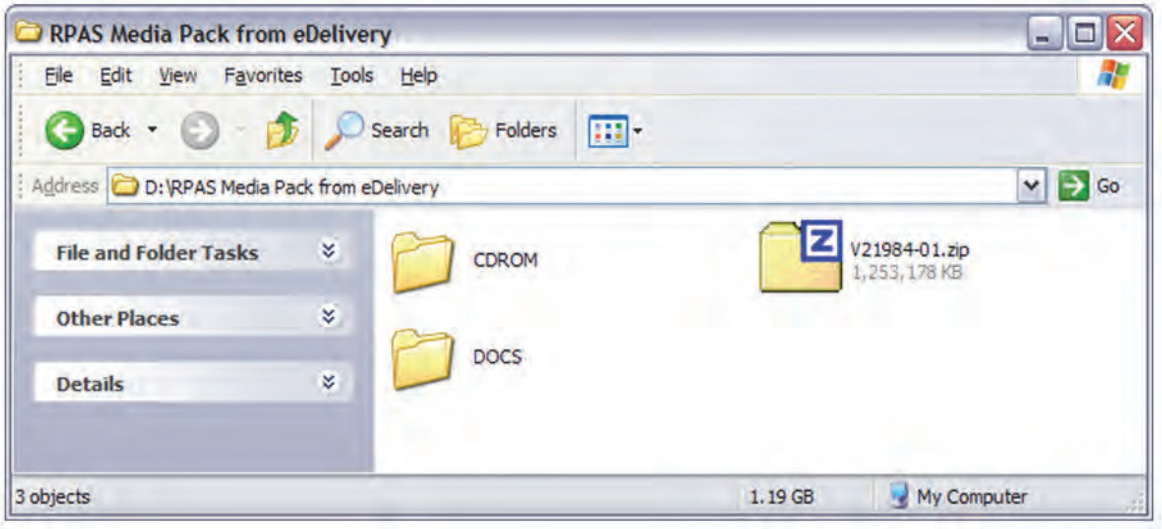
- RPAS and the Configuration Tools may also be installed on a single Windows stand-alone machine.
- Numbers represent the order in which you must install the RPAS components.
- The RPAS Classic Client Installer and RPAS Fusion Client Installer processes have the same number. This indicates that you can choose to install the RPAS Classic Client on the domain user systems or the RPAS Fusion Client on an Oracle WebLogic Server instance.
- Before you install an RPAS solution, you must have the RPAS Server and RPAS Clients installed. The RPAS solution installers include the taskflow configuration and online help files that require the RPAS Fusion Client to be already installed.
- A domain user can log on to an RPAS domain/solution using the RPAS Classic Client or by logging on to the RPAS Fusion Client through a Web browser.

Downloading and Extracting the RPAS Media Pack

The following procedure provides information about extracting the RPAS Media Pack and its contents.

1. Create a directory to store the RPAS Media Pack and download the media pack to this location.
2. Extract the media pack to this location. Once extracted, two folders appear, CDROM and DOCS.

Figure 2–2 Example of CDROM and DOCS Folder Created by Extracting Media Pack ZIP File



The CDROM folder contains the ZIP files listed in Table 2–1.

Table 2–1 ZIP File Contents

File	Contents
FusionClient.zip	The RPAS Fusion Client installer.
RPAS-13.3.1-unix.zip	All the RPAS components to be installed on your UNIX server.
RPAS-13.3.1-windows.zip	The RPAS components that can be installed on a Windows environment. Refer to the chapters, "Installing on UNIX and Linux Environments" and "Installing on a Windows Environment" for information on performing installations.

The DOCS folder has folders within it that contain the RPAS documentation in PDF format.

RDF Packaging

The scripts for Oracle Retail Demand Forecasting (RDF) are packaged within the RPAS/RDF server installation. For more information, refer to the RDF documentation.

The Curve and Grade documentation sets which were previously included in the DOCS folder are now combined with the RDF documentation. This documentation is available within the RDF package and on the following Web site:

`http://www.oracle.com/technology/documentation/oracle_retail.html`

3

Installing on UNIX and Linux Environments

The installation of the server-side RPAS components on UNIX or Linux operating systems is accomplished by using a Java-based installation program that is included with the installation package.

This program automates the following:

- Installation of the RPAS Server
- Installation of Configuration Tools on the server
- Creation of sample domains
- Definition of DomainDaemon port

Preparation

The RPAS components included in this installation process are available inside the media pack of the solution downloaded from Oracle's E-Delivery Web site, http://edelivery.oracle.com/.

There are two RPAS archives inside the media pack: one RPAS archive for UNIX and Linux and one for Windows.

Java Environment

Ensure that Java Development Kit (JDK) has been installed on the machine where RPAS will run and that the JAVA_HOME environment variable is properly set.

Note: Avoid enabling AutoUpdate when installing Java because it may update the Java version without prompting.

The following commands are examples based on common Java installation structures. These commands are automatically setup by the retaillogin.ksh script. After this script has run, compare your environment variables to the appropriate subsequent examples to ensure that it is correct. To ensure the path is correct, use the UNIX find command to locate libjvm.so (find $JAVA_HOME -name libjvm.so) and adjust the following paths as appropriate.

Linux

Example 3–1 shows a sample of common Java installation structures for Linux.

Example 3–1 Linux

```
export LD_LIBRARY_PATH="$JAVA_HOME/lib:$JAVA_HOME/jre/lib/amd64/server:
$LD_LIBRARY_PATH"
```

If JROCKIT instead of JDK is used as JAVA_HOME, then the settings should be:

```
LD_LIBRARY_PATH="$JAVA_HOME/lib:$JAVA_HOME/jre/lib/amd64/jrockit:
$LD_LIBRARY_PATH

export PATH="$JAVA_HOME/bin:$PATH"
```

AIX

Example 3–2 shows a sample of common Java installation structures for AIX.

Example 3–2 AIX

```
export LIBPATH="$JAVA_HOME/lib:$JAVA_HOME/bin/classic:$LIBPATH"
export PATH="$JAVA_HOME/bin:$PATH"
```

> **Note:** Linux and AIX are compatible with only a 64-bit version of Java.

Solaris

Example 3–3 shows a sample of common Java installation structures for Solaris.

Example 3–3 Solaris

```
export LD_LIBRARY_PATH="$JAVA_HOME/lib:$JAVA_HOME/jre/lib/sparcv9/server:$JAVA_
HOME/jre/lib/sparc: $LD_LIBRARY_PATH"
```

If JROCKIT instead of JDK is used as JAVA_HOME, then the settings should be:

```
export LD_LIBRARY_PATH="$JAVA_HOME/lib:$JAVA_HOME/jre/lib/sparcv9/jrockit:$JAVA_
HOME/jre/lib/sparcv9: $LD_LIBRARY_PATH"
export PATH="/usr/xpg4/bin:$JAVA_HOME/bin:$PATH"
```

> **Note:** The PATH variable on Solaris operating systems must have /usr/xpg4/bin in the path, and there can be no other occurrence of /bin or /usr/bin to its left. Otherwise, the scripts use the incorrect versions of grep, sed, awk, tail, and so on.

HP-UX Itanium

Example 3–4 shows a sample of common Java installation structures for HP-UX Itanium.

Example 3–4 HP-UX Itanium

```
export SHLIB_PATH="$JAVA_HOME/lib:$JAVA_HOME/jre/lib/IA64W/server:$JAVA_
HOME/jre/lib/IA64W/:$SHLIB_PATH"
export PATH="$JAVA_HOME/bin:$PATH"
export RIDE_OPTIONS=-d64
```

Note: Solaris and HP Itanium do not release separate 32-bit and 64-bit versions of Java. Therefore, you must set the 64-bit Configuration Tools environment variable for Java as shown:

```
export RIDE_OPTIONS=-d64
```

RPAS_JAVA_CLASSPATH

The RPAS_JAVA_CLASSPATH variable is used by RPAS applications that use the RPAS Java Special Expression functionality. This variable tells RPAS where to find the Java Special Expression implementations. It should contain a list of the locations of any Java code that is needed to execute a Java Special Expression. The list must also include the RpasJavaUtils.jar located in the applib subdirectory of RPAS_HOME. For information about exporting RPAS_JAVA_CLASSPATH through Cygwin, refer to Cygwin Path Settings.

Example 3–5 RPAS_JAVA_CLASSPATH

In the following example, the absolute path to RpasJavaUtils.jar file name is listed as well as an example of a Java Special Expression implementation.

```
export RPAS_JAVA_
CLASSPATH="/Oracle/RPAS/applib/RpasJavaUtils.jar;/Oracle/RPAS/applib/customJavaExp
ression.jar"
```

Note: Certain RPAS applications may have additional uses for the RPAS_JAVA_CLASSPATH environment variable. To determine if you need to set this variable in a different way, refer to that application's Installation Guide.

Ride Options

The RIDE_OPTIONS environmental variable has been defined to allow users to pass information into the rpasInstall process. Unlike the regular arguments passed on the command line to rpasInstall (such as -fullinstall and -updatestyles), arguments defined in RIDE_OPTIONS are passed to every rpasInstall instance that runs in the environment.

There are the three supported properties for use with RIDE_OPTIONS:

- **Xmx** – used for Java
- **HP 64-bit mode Java (-d64)** – used for HP Itanium and Solaris
- **Drpas.maxProcesses** – used for RPAS

For Java

Xmx - By default, the Java Virtual Machine requests on the order of 268 MB of RAM from the OS to allocate for its heap. Large domains that are built from complex configurations can potentially exhaust this limited amount of memory. This is even more of an issue in patch installations than in builds since a patch installation requires two different versions of a configuration to be held in memory simultaneously.

By using the -Xmx option, you can instruct the Java Virtual Machine to request more memory from the OS to prevent situations when all allocated memory is exhausted. The syntax of the property is:

`-Xmx###m`, where ### is the amount, in megabytes, of memory the JVM is to request. Common values for this argument are `-Xmx512m` or `-Xmx1024m`.

For HP Itanium and Solaris

HP 64-bit mode Java (-d64) - The HP distribution of Java does not consist of separate executables for 32-bit and 64-bit operating systems. Instead, there is a single distribution of Java that can run in either 32-bit or 64-bit mode. By default, the HP Java runs in 32-bit mode. Because RPAS is built as a 64-bit executable on the Itanium OS, the RPAS libraries are unable to link with Java if it is running in 32-bit mode.

By adding the -d64 property to RIDE_OPTIONS, the HP Java distribution is 64-bit mode enabled and the RPAS libraries link successfully.

It is often the case that users may want to use other properties in conjunction with RIDE_OPTIONS. When this is the case, all desired properties should be included within the environmental variable definition separated by white space with the entire definition enclosed in double quotes. An example of this is shown as:

```
export RIDE_OPTIONS="-d64 -Xmx1024m -Drpas.maxProcesses=8"
```

For RPAS

Drpas.maxProcesses - Several RPAS server utilities are designed to take advantage of multi-processor hardware to improve their performance. These utilities attempt to perform operations in parallel, each process running on a distinct processor.

The -Drpas.maxProcesses argument is used to instruct RPAS how many processors it should attempt to run in parallel when executing one of the server utilities that has multi-processor support when that utility is executed as a part of the rpasInstall process.

Note that the -Drpas.maxProcesses argument only affects those calls to server utilities made from within the rpasInstall process and does not affect calls to server utilities made from the command line or as part of a batch job. The syntax of the property is:

`-Drpas.maxProcesses=###`, where ### is the number of sub-processes the RPAS server utility should attempt to run in parallel. The number of processes to use should be determined by the administrator of the hardware system based on the physical number of processors available and the amount of load that is acceptable for the rpasInstall process to place on the system.

Before You Begin

Before starting the RPAS Installer, the following software must be installed on your system:

- Java 1.6
- Unzip utility

Running the RPAS Installer

Perform the following procedure to run the RPAS Installer.

1. Locate and extract RPAS-13.3.0-unix.zip into the current directory, which is referred to in this document as [RPAS_Installer].
2. Begin the Installer by changing to the [RPAS_Installer] directory and running the following command:

   ```
   ./install.sh
   ```

   Note: The command must be executed with the preceding period and forward slash.

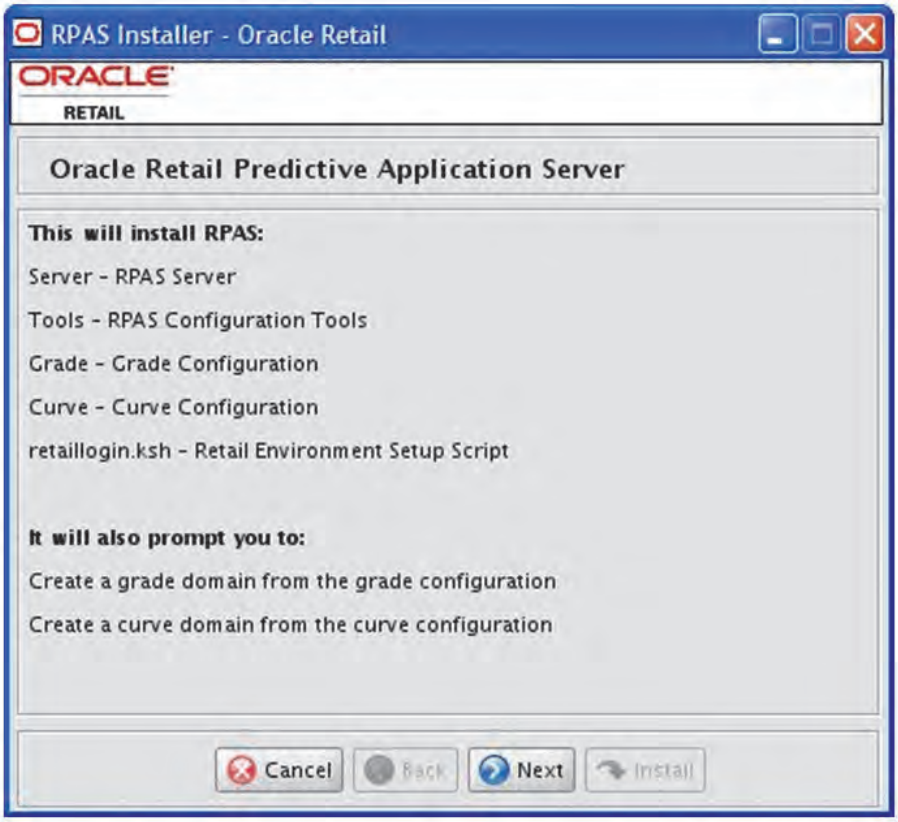
   If this process is being run on an X-Windows emulator (such as Exceed), a graphical user interface (GUI) to the Installer opens. If you are running in console mode through a terminal emulator, a text interface to the Installer opens.

   In both cases, the requested information is identical, but displayed differently. In the GUI, a checkbox may appear to indicate whether you want a component installed. In text mode, you are prompted for a response of either *Yes* or *No*.

   Note: In text mode, the default value appears in square brackets. To use the default value and continue, press **Enter**. If you want to use a different value, enter the new value. When prompted to create a directory, respond with *Yes* and press **Enter**.

3. The RPAS Installer window opens and displays the components that can be installed to your system. Click **Next**.

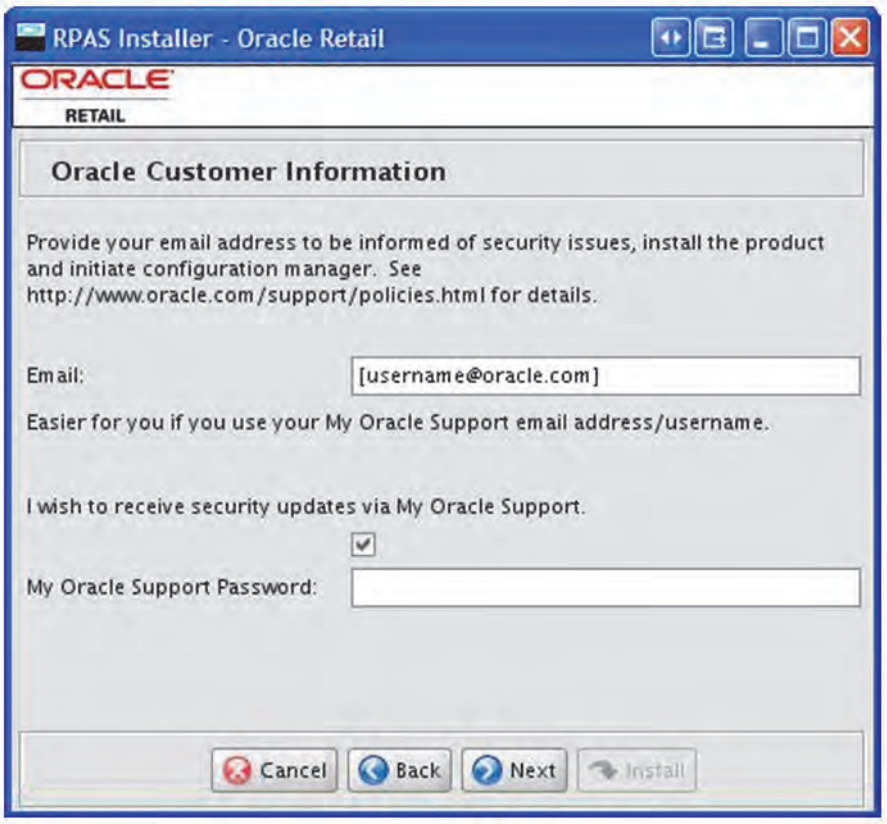
Figure 3–1 RPAS Installer



4. The Oracle Customer Information window opens.

   If you want to receive e-mails from My Oracle Support about security updates, enter your e-mail address and My Oracle Support password and ensure that the check box is selected. Click **Next** to continue.

Figure 3–2 Oracle Customer Information



The security updates are provided through Oracle Configuration Manager (OCM). The Oracle Retail OCM collector is included in the installer and is shown in Figure 3–2. The collector only needs to be installed once per ORACLE_HOME, WAS_HOME, or installation root directory. After the initial installation, the OCM collector automatically performs self-updates.

For more information about Oracle Retail OCM, refer to the following guide:

Oracle Configuration Manager Installer Guide (Note ID: 1071030.1)

This guide describes the procedures and interface of the Oracle Retail OCM collector that is a part of Oracle Retail full releases.

This document is available through My Oracle Support. Access My Oracle Support at the following URL:

`https://support.oracle.com`

The OCM documentation is located at the following URL:

`http://www.oracle.com/technology/documentation/ocm.html`

Note: If you select to receive security updates but do not provide e-mail and password information or lack an internet connection, addition windows appear. For more information about these windows, refer to the *Oracle Configuration Manager Installer Guide*.

---

5. The Install Requirements window opens.

   This window displays the software required to complete this installation. You should already have installed this software on your system. If you have not installed these items, perform the necessary installations before continuing.

   Click **Next** to continue.

Figure 3–3 Install Requirements

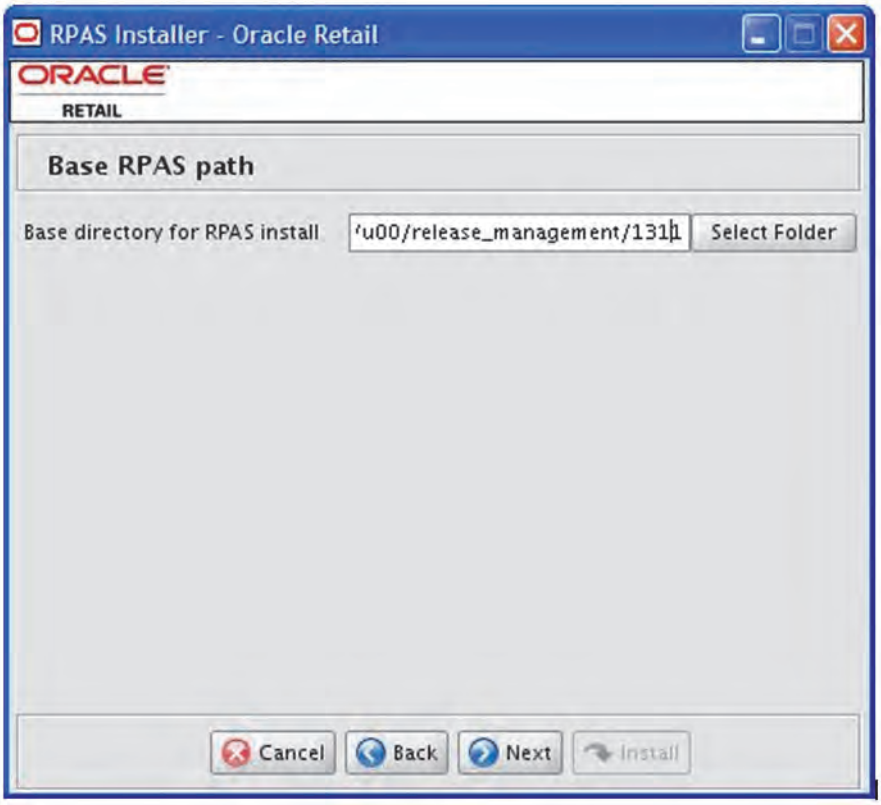
6. The Base RPAS Path window opens.

   Enter the path where the RPAS Server and components will be installed, and click **Next**. This path is used when creating your domains, should you choose to create them.

   Note: Ensure that the installation path is located outside of the installer directory [RPAS_Installer].

   If this directory does not exist, the Installer prompts you to create it.

Figure 3–4 Base RPAS Path



7. The RPAS Installations Paths window opens.

   Enter the following path information and click **Next**:

Field	Description
RPAS Server path	Enter the target directory for your RPAS Server.
RPAS Tools path	Enter the target directory for your RPAS Configuration Tools.
Grade Config path	Enter the target directory for your Grade configuration.
Curve Config path	Enter the target directory for your Curve configuration.
Directory for Retail login script	Enter the target path where the retaillogin.ksh file will be created on your system.

8. The Install Tasks window opens.

   Select the options to be performed by the RPAS Installer, enter the DomainDaemon port number, and click **Next**.

   - To create the domains for Grade and Curve, select the appropriate options on the Install tasks window. These options are selected by default, meaning that they will be created.
   - Enter the port where the RPAS DomainDaemon will run. This port needs to be configured for use with the RPAS Clients.

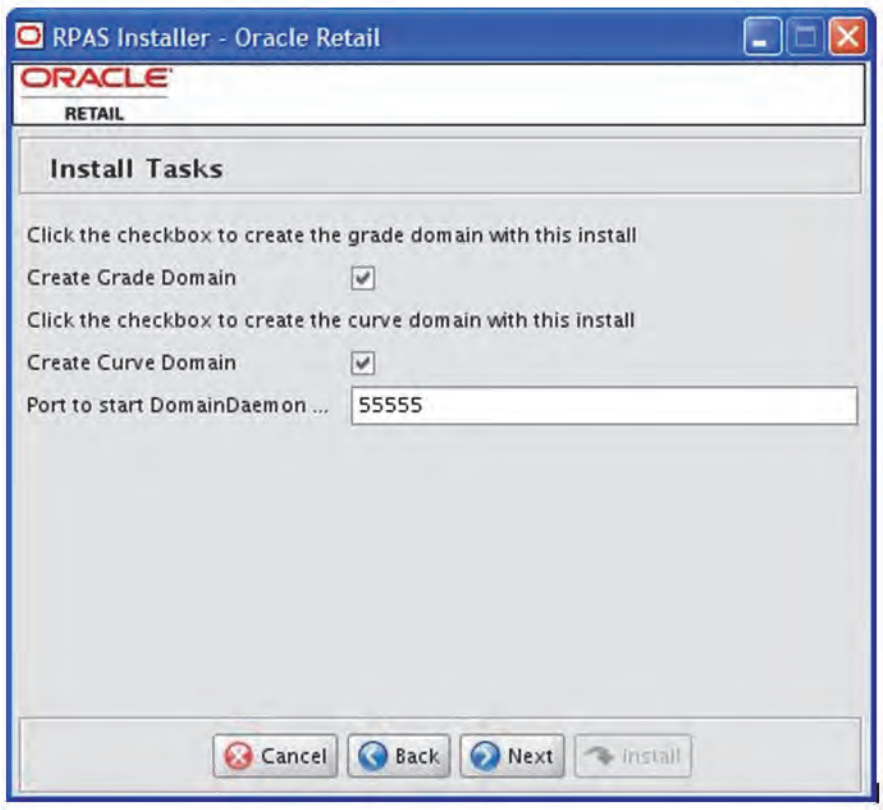
For the RPAS Classic Client, this is done with the EConfigure utility as documented in Chapter 6, "Installing and Configuring the RPAS Classic Client".

For the RPAS Fusion Client, this is done during the RPAS Fusion Client installation as documented in Chapter 5, "Installing the RPAS Fusion Client".

The Installer will validate that this port is not in use. The DomainDaemon will not be running at the end of this installation process, but can be started by using the startrpas alias created in the environment setup script.

Note: If you choose to create domains, they are created in a directory called domains under the **Base directory path** you defined on the Base RPAS path window.

Figure 3–5 Install Tasks



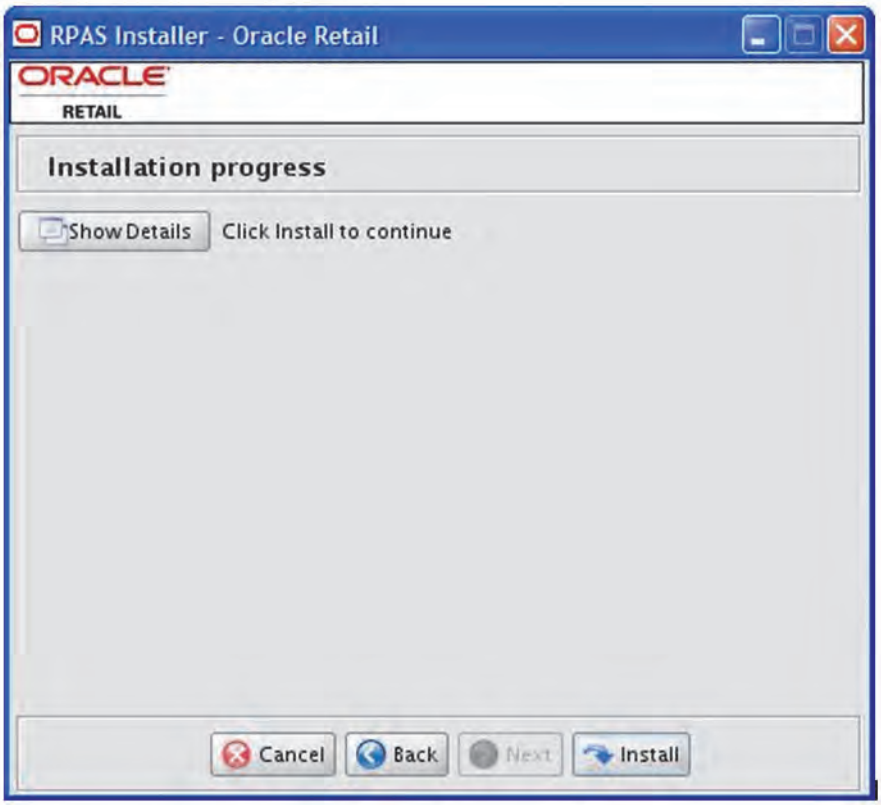
9. The Installation Progress window opens.

   To display the progress of the components and tasks being performed by the Installer, select **Show Details**. Click **Install** to start the installation process.

   You can view the detailed mode at any time during or after the installation.

Note: The installation process can vary depending on your environment. If you chose to create the domains, installation time might take 10 to 30+ minutes depending on server.

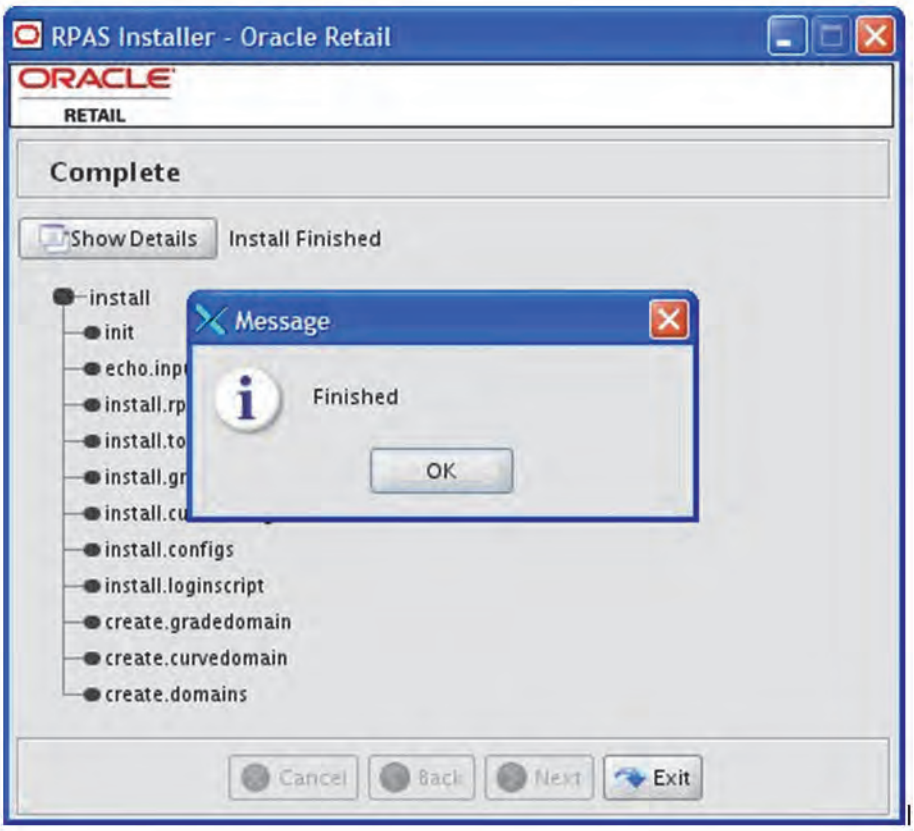
Figure 3–6 Installation Progress



10. When the installation process is complete, the Complete window opens with a *Finished* Message dialog box.

    Click **OK** to close the dialog box.

Figure 3–7 Complete



11. To view the installation details, click **Show Details**. The window displays two tabs: the Output tab and the Error tab. It is recommended that you review these tabs for any issues that may have occurred during the installation process.

    If you want to view the log again at a later date, a text copy was saved in the directory [RPAS_Installer]. The log file will be named based on the product, platform, and a timestamp, followed by the .log extension.

12. Click **Exit** to close the Installer.

Environment Variable Setup Script

To begin using RPAS, run the retaillogin.ksh script. The script is located in the root of the base directory where RPAS was installed unless the default was overwritten when specifying directory paths.

Source the script from inside the directory where the script is located:

```
. ./retaillogin.ksh
```

Or, include the full path after the period ".":

```
. /<base_directory>/retaillogin.ksh
```

Note: The preceding period and space (". ") must be included at the beginning of the command when executing the script.

Include this path and script in the .profile in your home directory (~/.profile) if you want to have this environment setup script run during login.

This script will set up environment variables, such as RPAS_HOME and RIDE_HOME, which are required for RPAS to run properly.

Installing ODBC Server and Client Components

After the RPAS Server has been installed and the RPAS_HOME environment variable has been set, the RPAS ODBC Server can be installed. The ODBC Server is required only if you have ODBC or JDBC applications that use the RPAS domain as data source, or if you want an SQL interface to the RPAS domain.

To install the ODBC Server, change directory to RPAS_HOME/odbc and run the shell script customInstall.sh. Although the installation script customInstall.sh works for non-root users, it is strongly suggested that the script be run by a root user so that the RPAS ODBC Agent can utilize the OS logon authentication method.

For information about the ODBC server configuration, refer to either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*.

Both 32-bit and 64-bit ODBC Clients are available. They are delivered in zip files named odbcclient32.tar.zip and odbcclient64.tar.zip respectively. To install, copy the appropriate zip file to your preferred location. Unzip and untar the file. For more information about the ODBC Client configuration, refer to either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*.

Installing JDBC Client

Perform the following procedure to install the JDBC client driver.

Unzip and untar the jdbcclient.tar.zip from the RPAS_HOME directory.

For additional information on the JDBC Server, refer to either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*.

Determine the Path for the Domains

Perform the following procedure to Determine the Path for the Domains.

1. Determine the locations of the domains to be installed.

Note: Domain paths cannot contain spaces. In addition, symbolic links cannot be used for domain paths.

2. Create a directory at the root of the domain to be installed.

DomainDaemon

The RPAS DomainDaemon is the process that must be running on the server for a user to log into an RPAS domain. Before beginning the installation process, a port was specified where the DomainDaemon will run.

Use the aliases `startrpas` and `stoprpas` to start and stop the DomainDaemon on the port specified before installation. This alias is an automated mechanism of starting the DomainDaemon. Alternatively, you can start the DomainDaemon manually. Instructions for the DomainDaemon are included in the Classic Client and Fusion Client versions of the *Oracle Retail Predictive Application Server Administration Guide*.

4

Installing on a Windows Environment

This chapter describes how to install RPAS on a Windows environment.

RPAS Server and Tools Installation on Windows

Note: You must install the RPAS Server on Windows to use the RPAS Configuration Tools on Windows. The RPAS Configuration Tools application is supported on Windows XP and Windows 7.

For the purposes of this section, / is used to delineate directories and files in paths. Users in a Windows Command Prompt environment will need to either use \ as the delineation character or use double quotes around paths.

Note: Paths on Windows are case-sensitive when using Cygwin.

Extracting the RPAS Package

Unzip the RPAS-13.3.1-windows.zip to a newly created directory on the Windows machine. The RPAS-13.3.1-windows.zip contains all the RPAS components.

Once extracted, the following directories appear:

Directory	Description
ClassicClient	This directory contains the setup.exe used to install the RPAS Classic Client.
Curve	This directory contains the Curve base configuration file provided with RPAS.
FusionClient	This directory contains the installer used to install the RPAS Fusion Client.
Grade	This directory contains the Grade base configuration file provided with RPAS.
OCM	This directory contains the stand-alone OCM installer.
ODBC	This directory contains the JDBC and ODBC client drivers.
RPAS	This directory will be referred to later in this document as **RPAS_HOME**.
Tools	This directory will be referred to later in this document as **RIDE_HOME**.
Translations	This folder contains the files for the various languages supported by RPAS.
Web	This directory contains the files required for an RPAS Web deployment.

Java Environment

During the Java installation, a directory is created to store the Java software. This directory is referred to later in this document as **JAVA_HOME**.

Install ODBC Server Components (Optional)

Perform the following procedure to install the ODBC server:

1. Run setup.exe from Rpas/ODBCServerInstall/iwinnt folder where you extracted the RPAS-13.3.1-windows.zip file.
2. Follow the installation wizard to proceed to the Server Setup window. In this window, enter the destination folder path.
3. The Server Configuration window opens. If the default values need to be modified, enter the agent service name, agent service port, and the Windows username used to administer this installation of the server.
4. Proceed to the next window, Service Configuration. In this window, enter the service name and service port if the default values need to be modified.
5. Follow the rest of the installation wizard to finish the installation process.

Note: If the installation fails on Windows 7, try installing again in compatibility mode. To do this, perform the following steps:

Right-click the setup.exe file and select the **Troubleshoot compatibility** option. Then, select the **Try recommended settings** option and click **Start the program**. Follow the installation wizard to complete the installation process.

For additional information on the ODBC Server, refer to either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*.

Install ODBC or JDBC Client Components (Optional)

ODBC Client Driver

Perform the following procedure to install the ODBC client driver.

- To install the ODBC client software, run setup.exe from the ODBC\ODBCClient directory where you extracted the RPAS-13.3.1-windows.zip file.
- Follow the installation wizard to proceed to the Oracle RPAS ODBC Driver Setup window. Enter the destination folder if the default values need to be modified.
- Click **Next**. The Data Source Configuration window opens. If the default values need to be modified, enter the data source name, description, service host name, service port, and service data source name.
- Follow the rest of the installation wizard to finish the installation process.

JDBC Client Driver

Perform the following procedure to install the JDBC client driver.

1. Unzip and untar the jdbcclient.tar.zip from the ODBC/JDBC Client directory where you extracted the RPAS-13.3.1-windows.zip file to a target destination directory.

For additional information on the ODBC Server, refer to either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*.

Install Cygwin

Cygwin is required if the RPAS Server is to be installed on Windows operating systems. You can find more information about downloading this product at:

`http://www.cygwin.com`.

For installation guidance, refer to the following note on My Oracle Support (`https://support.oracle.com`):

Cygwin Setup Guide for RPAS (Note 1333398.1)

This document details necessary options you should select when installing Cygwin to make it function properly with RPAS.

Cygwin Path Settings

To export PATH through Cygwin, use colons (:) and to export RPAS_JAVA_CLASSPATH through Cygwin, use semicolons (;). If you are using Java in Cygwin, use semi-colons to seperate Java class paths. Do not use colons because Java.exe runs on Windows and it expects a semi-colon. For this instance, using a colon is incorrect as it is already used in the Windows file paths. Cygwin is a UNIX like environment and as the command line interface for Windows it expects colons for path settings.

Note: To setup this variable, refer to Step 6 in Creating the Required Environment Variables.

Example 4–1 Cygwin Path

```
export PATH=/usr/bin:/usr/local/bin:/cygdrive/c/java/32bit/jdk1.7.0_20/bin
export RPAS_JAVA_CLASSPATH= "c:/rpas_home/13.3/rpas/applib/aaijni.jar;
                             c:/rpas_home/13.3/rpas/applib/aaiReplenOpt.jar"
```

Determine the Path for the Domains

Perform the following procedure to determine the path for the domains.

1. Determine the locations of the domains to be installed.

Note: Domain paths cannot contain spaces. In addition, symbolic links cannot be used for domain paths.

---

2. Create a directory at the root of the domain to be installed.

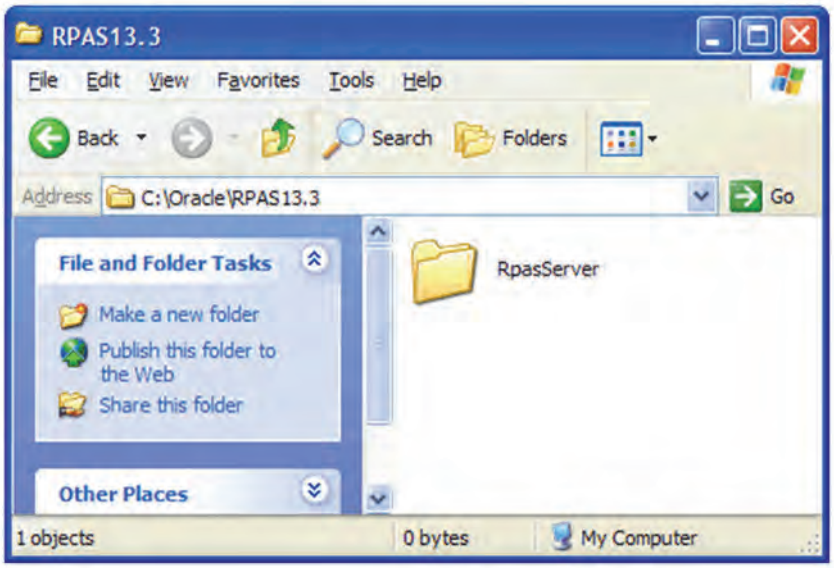
Installing the RPAS Server

The following procedures provide information about creating the necessary folders on your Windows PC and copying the RPAS Server components to them.

1. On your C drive, create a folder named **Oracle**.
2. Open the Oracle folder and create a folder named **RPAS13.3.1**.

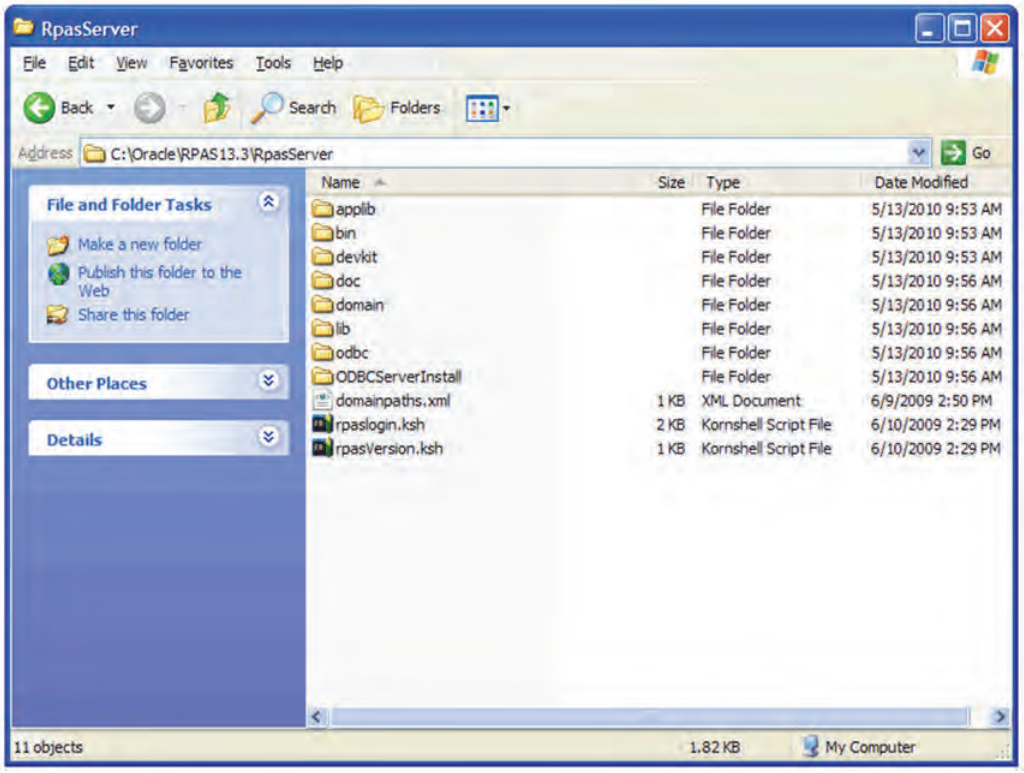
3. Open the RPAS13.3.1 folder and create a folder named **RpasServer**.

Figure 4–1 Example of RpasServer Folder Path



4. Copy all files and folders from the Rpas folder where you extracted the Media Pack to the C:\Oracle\RPAS13.3.1\RpasServer folder.

Figure 4–2 RpasServer Folder with All RPAS Server Components



This location is referred to as RPAS_HOME. An environment variable is defined on your Windows PC to point to this location so that RPAS will function correctly. Refer to Creating the Required Environment Variables for information on creating the necessary RPAS variables.

Note: When installing on Windows 7, update the permissions for $RPAS_HOME/bin directory to include execute permissions.

In a Cygwin session, enter the following commands:

```
cd $RPAS_HOME
chmod +x -R bin
```

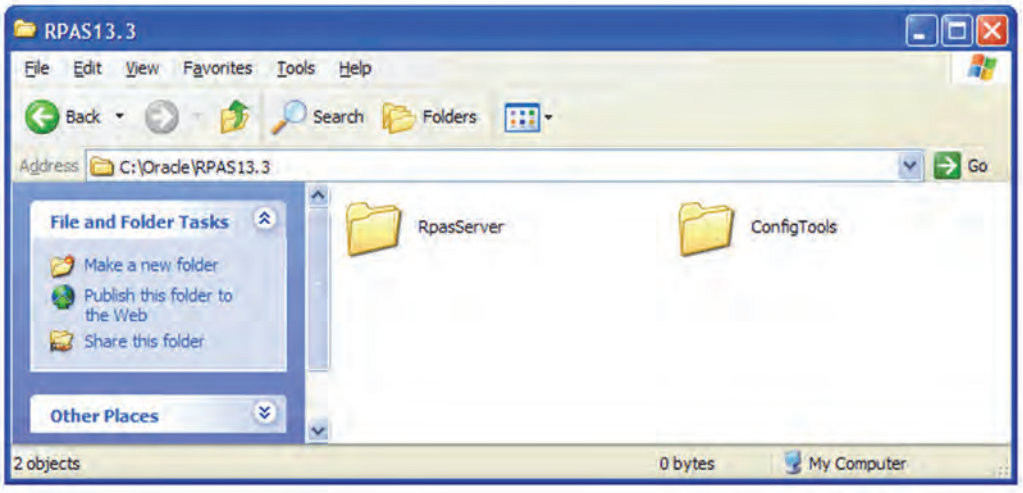
where RPAS_HOME is set to the correct directory and is in the proper Cygwin format.

Installing Configuration Tools

The following procedures provide information about creating the necessary folders on your Windows PC and copying the Configuration Tools components to them.

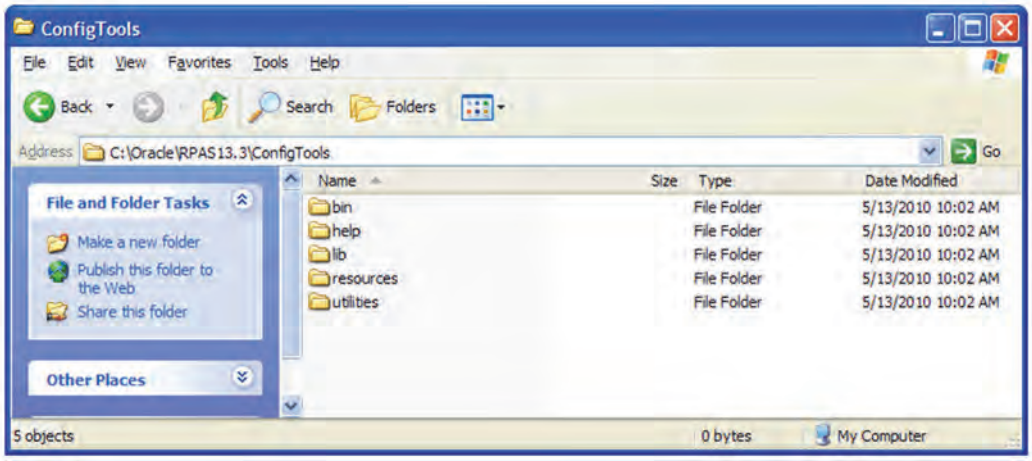
1. Using Windows Explorer, navigate to your C drive, create a folder named **Oracle\RPAS13.3.1**, which you created in the Installing the RPAS Server section.
2. Create a folder named **ConfigTools**.

Figure 4–3 Example of ConfigTools Folder Path



3. Copy all files and folders from the CDROM\Tools folder where you extracted the Media Pack to the C:\Oracle\RPAS13.3.1\ConfigTools folder.

Figure 4–4 ConfigTools Folder with All Configuration Tools Components



This location is referred to as RIDE_HOME. An environment variable will be defined on your Windows PC to point to this location so that RPAS will function correctly. Refer to the Creating the Required Environment Variables section for information on creating the necessary RPAS variables.

Note: If you plan to use the Curve or Grade functionality, ensure that you copy the plugin folders to the ConfigTools folder. For instructions, refer to the section, Building the Domain on your Windows PC.

Oracle Configuration Manager (OCM)

The Oracle Retail OCM installer is packaged in the CDROM\OCM directory. The collector only needs to be installed once per ORACLE_HOME, WAS_HOME, or installation root directory. After the initial installation, the OCM collector automatically performs self-updates.

For more information about Oracle Retail OCM, refer to the following guide: *Oracle Configuration Manager Installer Guide* (Note ID: 1071030.1)

This guide describes the procedures and interface of the Oracle Retail OCM collector that is a part of Oracle Retail full releases.

This document is available through My Oracle Support. Access My Oracle Support at the following URL:

`https://support.oracle.com`

OCM Documentation Link:

`http://www.oracle.com/technology/documentation/ocm.html`

Creating Start Menu Shortcuts to RPAS Applications and Utilities

This section provides information on creating shortcuts to these applications:

- Configuration Tools
- Configuration Converter

Procedure to Create Start Menu Shortcuts to RPAS Applications and Utilities

Perform the following procedure to create start menu shortcuts to RPAS applications and utilities

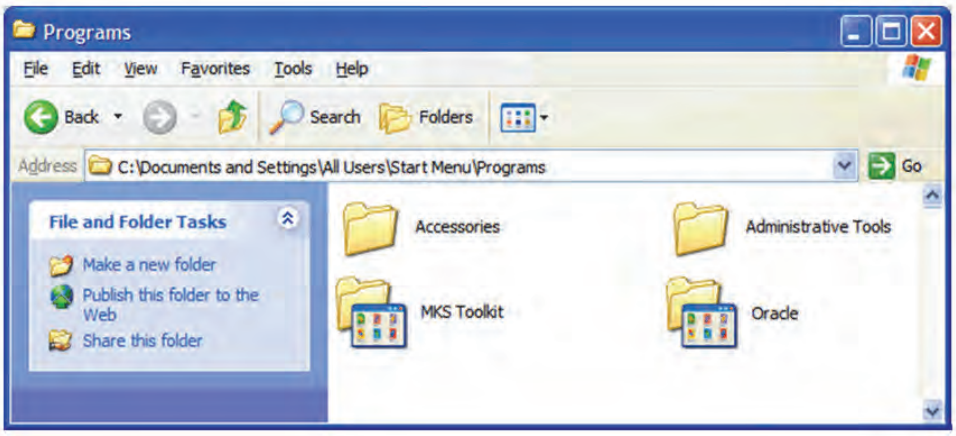
1. Open Windows Explorer and navigate to the appropriate path for your operating system.

Operating System	Path
Windows XP	C:\Documents and Settings\All Users\Start Menu\Programs
Windows 7	C:\ProgramData\Microsoft\Windows\Start Menu\Programs

   The Programs window displays all applications and shortcuts available to all users accessing the PC.

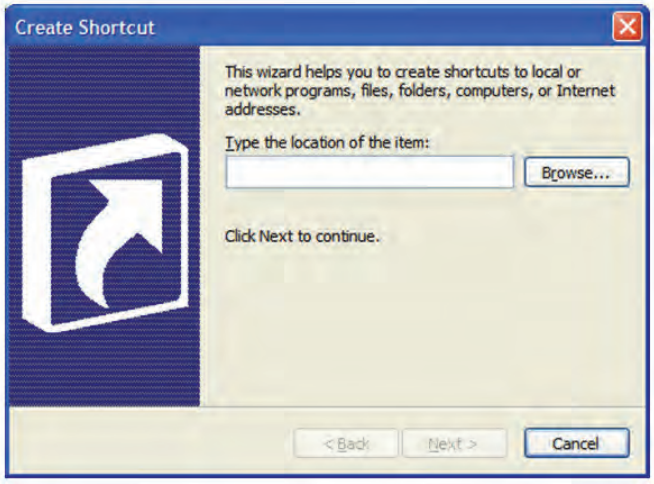
2. Right-click the window and select **New – Folder**. Name this folder **Oracle**.

Figure 4–5 Programs Windows with Oracle Folder



3. Double-click the Oracle folder. The folder opens in Windows Explorer.
4. Right-click the Oracle window and select **New – Folder**. Name the folder **RPAS 13.3.1**.
5. Create a shortcut to Configuration Tools:
   a. Double-click the RPAS 13.3.1 folder, right-click in the folder window, and select **Shortcut**. The Create Shortcut Wizard Dialog Box opens.

Figure 4–6 Create Shortcut Wizard Dialog Box



b. Click **Browse** and navigate to the Oracle\RPAS13.3.1\ConfigTools\bin folder on your C drive.

c. Select **ConfigTools.exe** and click **OK**. The selected path appears in the Create Shortcut wizard.

d. Click **Next**. The Select a Title for the Program wizard window opens. By default, this window displays the file name and extension selected.

e. In the text field, enter **Configuration Tools** as the shortcut name and click **Finish**. The shortcut wizard closes and the Oracle window displays the shortcut to the Configuration Tools.

6. Create a Utilities folder in the Oracle window. Right-click the window and select **New – Folder**. Name this folder **Utilities**.

7. Double-click the **Utilities** folder. The folder opens in Windows Explorer.

8. Create a shortcut for the Configuration Converter:

   a. Right-click the Utilities folder window and select **Shortcut**. The Create Shortcut wizard dialog box opens.

   b. Click **Browse** and navigate to the Oracle\RPAS13.3.1\ConfigTools\utilities folder on your C drive.

   c. Select **RpasConverter.exe** and click **OK**. The selected path appears in the Create Shortcut wizard.

   d. Click **Next**. The Select a Title for the Program wizard window opens.

   e. In the text field, enter **Configuration Converter – g** as the shortcut name and click **Finish**. The **–g** after the name is required to display the Windows interface for the converter. The shortcut wizard closes and the Oracle window displays the shortcut to the Installer.

9. Verify your shortcuts appear in the Start menu. From the Start menu, select **All Programs – Oracle – RPAS 13.3.1.** The Configuration Tools and Installer shortcuts should appear. Select the **Utilities** folder and verify that the Configuration Converter shortcut appears.

   Now that the necessary files and shortcuts are defined, you need to create the necessary environment variables in order to open the applications

Creating the Required Environment Variables

The following steps outline the process to follow and environment variables required to support the RPAS installation and domain install.

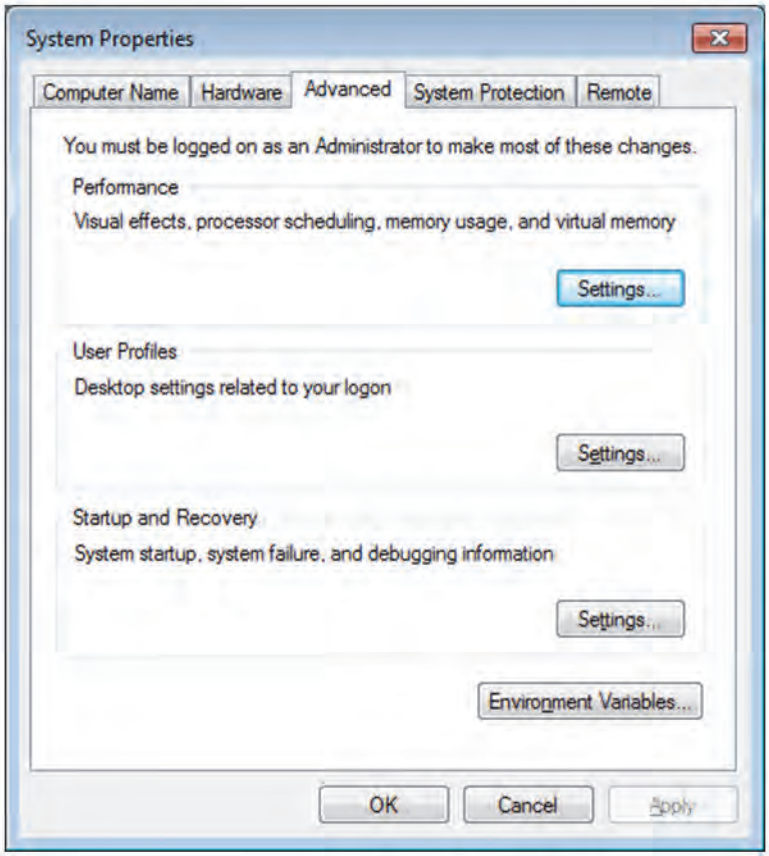
1. From the Control Panel, open the System window.
   a. If your system is using Category view, from the Windows 7 Start menu, go to **Control Panel**, select **System and Security**, select **System**, and then select **Advanced System Settings**.

      The System Properties window opens on the Advanced tab.

   b. Select the **Advanced** tab.

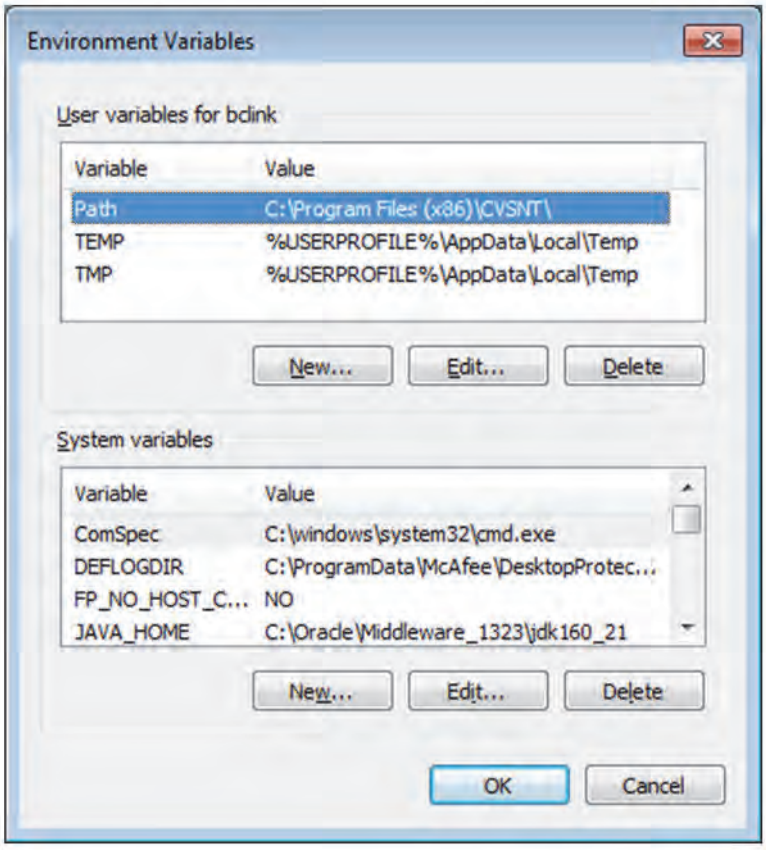
   c. At the bottom of the window, click **Environment Variables**.

Figure 4–7 System Properties - Advanced Tab



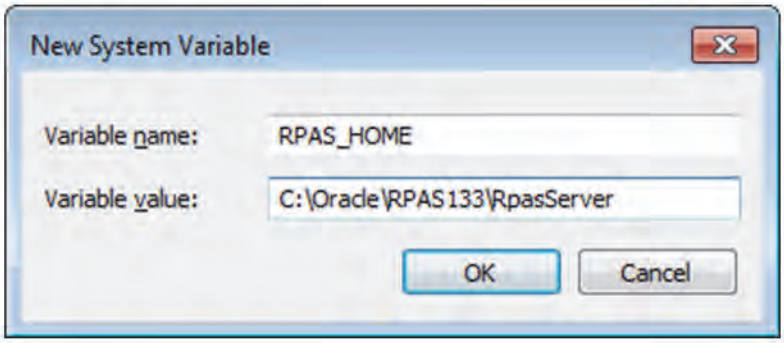
   d. The Environment Variables window opens.

Figure 4–8 Environment Variables



2. Create the **RPAS_HOME** environment variable.
   a. Under the System variables box, click **New**. The New System Variable dialog box opens.
   b. Enter **RPAS_HOME** in the **Variable** name field.
   c. Enter the path the RPAS Server folder in the **Variable value** field.

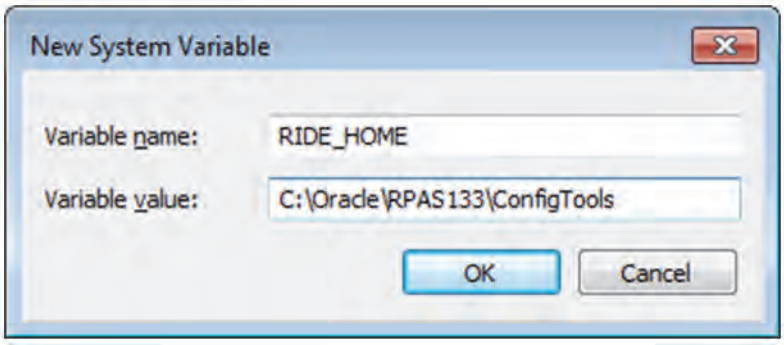
Figure 4–9 Example of RPAS_HOME Variable



   d. Click **OK**. **RPAS_HOME** now appears in the Variable name box.

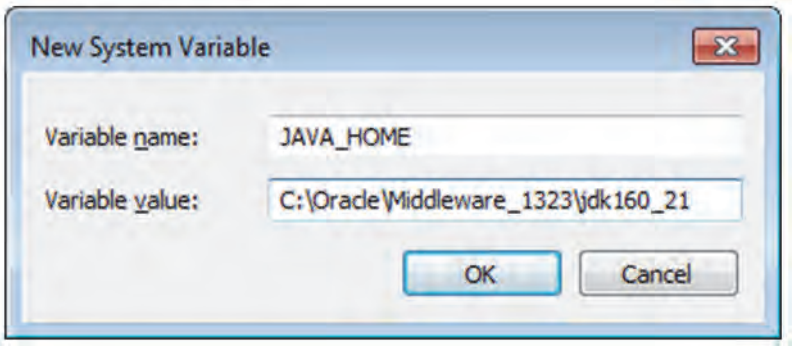
3. Create the **RIDE_HOME** environment variable.
   a. Under the System variables box, click **New**. The New System Variable dialog box opens.
   b. Enter **RIDE_HOME** in the **Variable name** field.
   c. Enter the path the ConfigTools folder in the **Variable value** field.

Figure 4–10 Example of RIDE_HOME Variable



   d. Click **OK**. **RIDE_HOME** now appears in the Variable name box.
4. Create the **JAVA_HOME** environment variable.
   a. Under the System variables box, click **New**. The New System Variable dialog box opens.
   b. Enter **JAVA_HOME** in the **Variable name** field.
   c. Enter the path the Java folder under Program Files in the **Variable value** field.

Figure 4–11 Example of JAVA_HOME Variable



   d. Click **OK**. **JAVA_HOME** now appears in the Variable name box.
5. Update the Path variable.
   a. Under the System variables section, select the **Path** environment variable and click **Edit**.
   b. Insert the complete paths for **RPAS_HOME, RIDE_HOME**, and **JAVA_HOME** as shown:

      %RPAS_HOME%\bin;%RPAS_HOME%\applib;%RPAS_HOME%\lib;

      %RIDE_HOME%\bin;%RIDE_HOME%\lib;

%JAVA_HOME%\bin;%JAVA_HOME%\bin\client;%JAVA_HOME%\lib;
%JAVA_HOME%\jre\bin\client

Note: Remember to separate all path statements with semicolons (;).

c. Select **OK** to save your changes.

6. Update the **RPAS_JAVA_CLASSPATH** environment variable.
   a. Under the System variables box, click **New**. The New System Variable dialog box opens.
   b. Enter **RPAS_JAVA_CLASSPATH** in the **Variable name** field.
   c. Enter the path the Java folder under Program Files in the **Variable value** field.

Figure 4–12 Example of RPAS_JAVA_CLASSPATH Variable

   d. Click **OK**. **RPAS_JAVA_CLASSPATH** now appears in the Variable name box.

7. Close all open windows.

Create a Global Domain Configuration Directory (Optional)

If installing a Global Domain environment, an xml file may be created to determine how the domains will be partitioned and the label of each domain. The following is an example of the structure of the globaldomainconfig.xml file. The items in Example 4–2 are as follows:

Item	Description
Path	The location of the root of the domain.
Partitiondim	The partition dimension. Using the following example, pgrp (Group) is the dimension in which the local domains are partitioned. There can only be one partition dimension.
Subpath	The path and name of the local (sub-domain) that contains a specific partition position. ldom+# is the default name given by RPAS to local domains.
Subposition	The position from the partition dimension that is located in the local domain. For example, ldom0 includes all product positions at or below pgrp 1100.

Example 4–2 File Structure

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<rpas>
    <globaldomain>
        <path>/Domains/RDF133/D01</path>
        <partitiondim>pgrp</partitiondim>
        <subdomain>
            <subpath>/Domains/RDF133/ldom0</subpath>
            <subpositions>1100</subpositions>
        </subdomain>
        <subdomain>
            <subpath>/Domains/RDF133/ldom1</subpath>
            <subpositions>1300</subpositions>
        </subdomain>
        <subdomain>
            <subpath>/Domains/RDF133/ldom2</subpath>
            <subpositions>2500</subpositions>
        </subdomain>
    </globaldomain>
</rpas>
```

Configure the RPAS Clients to Use the Domain

The RPAS Clients must be configured to point to the newly created domains.

For instructions on how to configure the RPAS Clients, refer to either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*.

Using Multiple Versions of RPAS on the Same Windows Machine

If you have multiple versions of RPAS installed on your PC, it is important to note that the environment variables will reference RPAS 13.3.1 after the installation process is complete.

> **Note:** Previously set environment variables for other versions or installations of RPAS will still exist in the Path System variable, but Windows uses the first set of variables defined in the path, which is where the installation process places them.

To switch to a different version of RPAS that is installed on your machine, you will need to manually update the environment variables each time you want to switch. You can either insert the path to the version you want to use and leave the path to 13.3.1, or delete the path and either reinstall the 13.3.1 components or manually reinsert the paths when you want to revert to 13.3.1.

Base Configuration Installation

There are three base configurations available with the RPAS archive that can be used to build a domain. These configurations are initially stored in the following folders that were created in the CDROM folder when you extracted the RPAS-13.3.1-windows.zip file in the location where you downloaded the RPAS Media Pack.

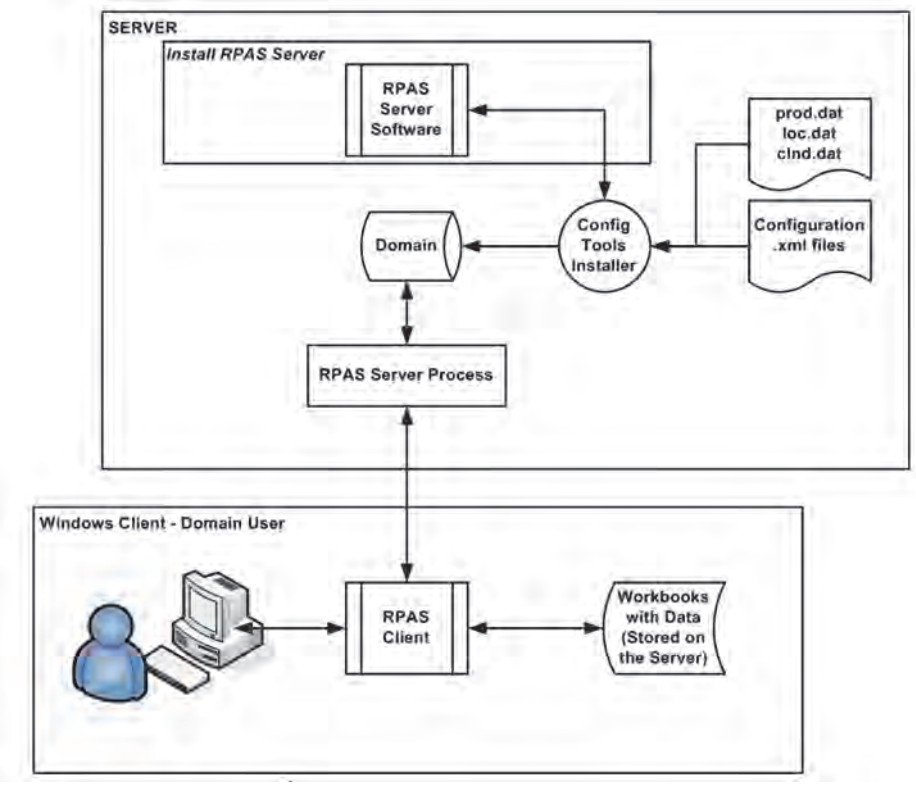
- **Grade** – Grade is a clustering tool that provides insight into how various parts of a retailer's operations can be grouped together.
- **Curve** – Curve is a profile generation tool used to produce ratios (profiles) from historical data at user-specified intersections.

The following section describes how to use these configurations to build a domain.

Build a Domain Process Overview

Figure 4–13 shows an overview of the steps involved in using a configuration to build and an RPAS domain. This section describes each of the steps in this diagram.

Figure 4–13 Build a Domain Process Overview Diagram



Verify the Environment Variable Settings

Prior to beginning the domain build process you should have installed RPAS and the Configuration Tools on your server. During that process, you should have set up the necessary environment variables for RPAS and the Configuration Tools.

Perform the following steps to verify that environment variables have been successfully configured.

Open a Cygwin zsh window. Use the following commands to verify your environment settings:

```
echo $RPAS_HOME
echo $RIDE_HOME
echo $JAVA_HOME
echo $PATH
```

Note: The path for the RPAS_HOME variable may change from release to release.

If you make any changes to the environment variable settings, remember to exit and restart your UNIX session in order to execute your .profile and make the changes effective. This step is very important before you continue to the remaining steps.

Note: The paths for your RIDE_HOME and RPAS_HOME variables cannot have spaces in them, unless short file naming conventions are utilized. Given this restriction, do not place your Tools build, Tool Configurations or RPAS installation under Program Files or My Documents. If you do, define all RPAS related environment variables using short (8dot3) file names.

Setting Up Base Configuration Files

Locate and copy/move the desired configuration zip file to a location on your machine. For the purposes of these instructions assume that location is called:

C:/root/testenv/<Configuration>.

The following subfolders will be created in: C:/root/testenv/<Configuration>:

- data/ – hierarchy and sample data files (this path is used in conjunction with the –in [input] option of the `rpasInstall` command)
- configuration/<Configuration_Name> – Configuration files for use in building the domains where <Configuration_Name> will be Sample_Configuration, Grade, or Curve.

  Do not change the directory name for the configuration or alter the contents in any way.
- scripts – Scripts used to complete the domain build process.
- resources – Contains the plug-ins for the Configuration Tools. When this resource directory is supplied, it must be copied in its entirety to the RIDE_HOME location. This must be done in order for the Configuration Tools to build domains.

Building the Domain on your Windows PC

This section provides instructions for how to create a domain from the base configurations.

Because building an RPAS domain on Windows is currently a manual process, the person building the domain should be skilled in administering UNIX or Windows servers and should have scripting skills.

Note: The Configuration Tools are supported on all platforms (HP-UX, AIX, and Windows); however, they require Java 1.6. Make sure that the server you will be using has this version of Java.

1. Create a testenv (test environment) folder on your C drive.
2. Copy the Curve and Grade plugin folders to the ConfigTools\resources\plugins folder. These Curve and Grade plugin folders are located in the folder where you extracted the RPAS-13.3.1-windows.zip file to the testenv folder:

   `testenv\Curve\resources\plugins`

   `testenv\Grade\resources\plugins`

Sample Data Files

The domain build process requires the following data files to be available:

- prod.dat
- loc.dat
- clnd.dat
- input data files for measures (<measure>.ovr)

These files should be located in the C:/root/testenv/<Configuration>/data directory. This directory path will be used during the domain build process as the input directory.

Domain Environment Setup

The path that the domain will be created must exist prior to running the domain build process.

For the domain, manually create the directory structure:

C:/root/testenv/domain

The name of the domain will automatically be created under the domain path based on the configuration name. So, for the previously listed domain path, the full path to the domain will be as follows once the domain build process is completed.

C:/root/testenv/domain/<Configuration>

Build the Domain

Use the Tools Installer, the rpasInstall script, to build the domain. This executable is located in bin directory of your Tools installation. There are different scripts to run based on which configuration is being used to build a domain.

For more information on the Tools Installer and the specific options available when using the rpasInstall command, refer to the *Oracle Retail Predictive Application Server Configuration Tools User Guide*.

Note: The `rpasInstall` script only loads the hierarchy files and builds the domain. It does not load any measure data. The hierarchy files are copied to the /input/processed directory of the domain and appended with a time-date stamp.

Grade

Perform this procedure to build the domain for Grade.

1. Copy the plugins folder from the Grade/resources directory and paste it in the RIDE_HOME/resources directory.
2. Enter the following command to build a domain for the Grade configuration:

   ```
   rpasInstall -fullinstall -dh <path to the domain> -cn Grade
   -ch <path to the configuration> -in <path to the data files>
   -log <path to the location and name of the installation log>
   -rf AppFunctions –rf ClusterEngine –p pgrp
   ```

3. After the domain installation has completed, the sales data must be loaded into the domain using the loadmeasure utility. Open a command prompt from the master domain (/Grade) and type the following commands:

   ```
   loadmeasure -d . -measure dpos

   loadmeasure -d . -measure rsal

   loadmeasure -d . -measure csal

   loadmeasure -d . -measure psal
   ```

4. Open a command prompt from the local domain (/Grade/ldom0) and type the following command:

   ```
   mace -d . -run -group common_batch
   ```

   Repeat this step for each of the remaining local domains (/Grade/ldom1, /Grade/ldom2).

Curve

Perform this procedure to build the domain for Curve.

1. Copy the plugins folder from the Curve/resources directory and paste it in the RIDE_HOME/resources directory.
2. Enter the following command to build a domain for the Curve configuration:

   ```
   rpasInstall -fullinstall -dh <path to the domain> -cn Curve
   -ch <path to the configuration> -in <path to the data files>
   -log <path to the location and name of the installation log>
   -rf AppFunctions –rf ClusterEngine –p pgrp
   ```

3. After the domain installation has completed the sales data must be loaded into the domain using the `loadmeasure` utility. Open a command prompt from the master domain (/Curve) and type the following commands:

   ```
   loadmeasure -d . -measure dpos

   loadmeasure -d . -measure rsal

   loadmeasure -d . -measure csal

   loadmeasure -d . -measure psal
   ```

4. Open a command prompt from the local domain (/Curve/ldom0) and type the following command:

   ```
   mace -d . -run -group common_batch
   ```

   Repeat this step for each of the remaining local domains (/Curve/ldom1, /Curve/ldom2).

Start the RPAS Server (DomainDaemon)

In order to use the domains built from the sample configurations, the RPAS Server must be running on the server/machine where the domain is located.

The RPAS Server is started by executing the RPAS DomainDaemon executable, which provides a centralized process for managing domain connections between the client and the server.

Following is an example of running the DomainDaemon, which allows you to connect to the RPAS Server and a domain using the RPAS Clients. When running the DomainDaemon, RPAS requires the Secure Socket Layer (SSL) settings to be defined. Different settings are required depending on the client being used. This example is a simple case of using the Classic Client with no-SSL. Complete information about the Domain Daemon and the different SSL options is located in the Classic Client and Fusion Client versions of the *Oracle Retail Predictive Application Server Administration Guide*.

Execute the following command from a UNIX command line (or using Cygwin on Windows). If the environment variables paths have been properly set, this command can be run from any directory.

Example 4–3 Running the DomainDaemon

```
DomainDaemon -port <port_number> -start –ssl <option> [-wallet <path_to_wallet>]
```

Where `<port_number>` is an integer between 1025 and 65535.

Where `<option>` is the type of SSL you are using.

Where `<path_to_wallet>` is the path to the Oracle Wallet containing the server side SSL certificates. This is optional depending on which SSL option you are using.

This port number is used when configuring the client connection. Refer to the "Installing and Configuring the RPAS Classic Client" and "Installing the RPAS Fusion Client" chapters for additional information.

For additional information about setting up SSL wallets, refer to Setup SSL

SSL Options

DomainDaemon lets you set up SSL with these options:

Table 4–1 SSL Option Values and Recommendations

Value	Description	Application	Usage	Recommendation
0	Disable SSL support.	Classic Client	No authentication, no encryption.	Least secure - not recommended.
1	One-way SSL with server authentication.	Classic Client	One-way authentication and encrypted data transfer.	Most secure -recommended.

Table 4–1 (Cont.) SSL Option Values and Recommendations

Value	Description	Application	Usage	Recommendation
2	Two-way SSL with client and server authentication.	Fusion Client	Two-way authentication and encrypted data transfer.	Most secure -recommended.
3	SSL without authentication.	Classic Client	Encrypted data transfer without authentication.	Vulnerable to man in the middle attacks - not recommended.
4	Two-way SSL authentication only.	Fusion Client	Two-way authentication but unencrypted date transfer.	Least secure - not recommended except for users that deploy everything behind a firewall.

5

Installing the RPAS Fusion Client

The RPAS Fusion Client is the Web-based Rich Client for the Retail Predictive Application Server (RPAS) platform developed using the latest Oracle Application Development Framework (ADF).

This chapter describes typical installations of the RPAS Fusion Client. It includes these sections:

- Road Map for Installing the RPAS Fusion Client
- Pre-Installation Tasks
- Installation Tasks
- Post-Installation Tasks
- Troubleshooting

> **Note:** The RPAS Fusion Client is different from the RPAS Web Deployment. For more information, refer to Chapter 7, "RPAS Classic Client Web Deployment".

Road Map for Installing the RPAS Fusion Client

This section explains how to install and set up the RPAS Fusion Client application, along with the required and optional software.

These instructions assume knowledge of application servers, databases, and application installation or administration, and are intended for system administrators and experienced IT personnel. Before carrying out any of these activities, ensure that you understand UNIX commands (including shell configuration and scripting), directory operations, and symbolic links.

In order to install RPAS Fusion Client for production, you must perform the following tasks listed in Road Map Tasks.

Road Map Tasks

To install the RPAS Fusion Client, there are three phases and tasks within each phase as listed in Table 5–1.

Table 5–1 Road Map Phases and Tasks

Phase	Task	Additional Information
Pre-Installation Tasks	Plan your environment, based on your business needs.	For more information on the planning process and the supported configurations, refer to Chapter 2, "Getting Started" and the section, Planning.
	Install and set up the RPAS Infrastructure.	For more information, refer to Chapter 3, "Installing on UNIX and Linux Environments" or Chapter 4, "Installing on a Windows Environment".
	Set up the WebLogic server.	For more information, refer to Setting Up the WebLogic Server.
	Access the RPAS Fusion Client installation software.	For more information, refer to Accessing the Fusion Client Installation Media.
	Set up the install.properties file.	For more information, refer to Setting Up Your Installation Properties File.
	Set the environment variables.	For more information, refer to Setting Up Environment Variables.
	Optional: Validate the WebLogic and ADF versions.	For more information, refer to Validating WebLogic and Oracle Application Development Framework Versions (Optional).
	Create credentials in the Oracle Wallet.	For more information, refer to Creating User Credentials in an Oracle Wallet.
Installation Tasks	Install the Fusion Client in silent mode or text/graphical mode.	For more information, refer to Silent Mode or Graphical or Text Mode.
Post-Installation Tasks	Clear the browser cache.	For more information, refer to Clear the Browser Cache.
	Configuring External Authentication.	For more information, refer to Configuring External Authentication.
	Setup SSL between the RPAS server and the RPAS Fusion Client.	For more information, refer to Setup SSL.
	Review the RPAS configuration property files.	This task is only necessary when installing the RPAS Fusion Client over an existing RPAS Fusion Client environment. For more information, refer to Review the RPAS Configuration Property Files.
	Optional: Set up SSO.	For more information, refer to Set Up Single Sign-On (SSO).
	Optional: Set up the configuration properties file, pivot table styles, and layout and formatting.	For more information, refer to the *Oracle Retail Predictive Application Server Administration Guide for the Fusion Client*.
	Install and set up the RPAS solution to work with the RPAS Fusion Client.	For more information, refer to the Installation Guide of the relevant RPAS solution.

Pre-Installation Tasks

The pre-installation process includes these tasks that must be performed in order:

Table 5–2 Order of Pre-Installation Tasks

Order	Task
1.	Planning
2.	Install and Set Up the RPAS Infrastructure
3.	Setting Up the WebLogic Server
4.	Accessing the Fusion Client Installation Media
5.	Setting Up Your Installation Properties File
6.	Setting Up Environment Variables
7.	Validating WebLogic and Oracle Application Development Framework Versions (Optional)
8.	Creating User Credentials in an Oracle Wallet

Planning

This is the first pre-installation task.

Before installing the RPAS Fusion Client, you must first determine the performance and availability goals for your business, and then plan the hardware, network, and storage requirements accordingly. This section provides some basic considerations for the installation. It also includes the list of hardware and software requirements.

This section includes the following topics:

- Planning Your Environment
- Supported Configurations

Planning Your Environment

Planning your implementation prior to an installation also gives you a better understanding of the environment, and enables you to adapt faster to any future changes in the environment setup.

Use the following steps to plan and prepare the product environment:

1. Plan and design the infrastructure, based on your business needs, for the installation. This includes:
   - Meeting the hardware and associated software requirements.
   - Acquiring the prerequisite software (and licensing).
   - Determining the external authorization strategy. For more information, refer to Configuring External Authentication.
   - Setting up the load balancers and clusters. For more information, refer to Considerations for Setting Up Load Balancers.
   - Gathering the capacity data.
   - Planning the data security policies.
   - Designing the backup and recovery strategies.
2. Determine the size of the implementation.

3. Identify source systems. Identify the systems that will exchange data with RPAS Fusion Client.

Considerations for Setting Up Load Balancers

You can choose to implement a software load balancer or network-based load balancer hardware.

Before you start setting up a load balancer, you must consider the items listed in Table 5–3. These considerations are relevant for an external load balancer used in a multple managed application server deployment featuring standalone authentication. If using Oracle SSO 11g, the mod_wl_ohs Web Tier plugin performs the application server level load balancing function.

An external load balancer can still be beneficially used in an SSO deployment. This would be deployed in front of multiple web tier servers. The advantage is in avoiding single point of failure (at the web server), and optionally, providing Secure Sockets Layer (SSL) termination, compression, and static content caching at the load balancer.

Table 5–3 External Load Balancer Considerations - Non-SSO Deployment

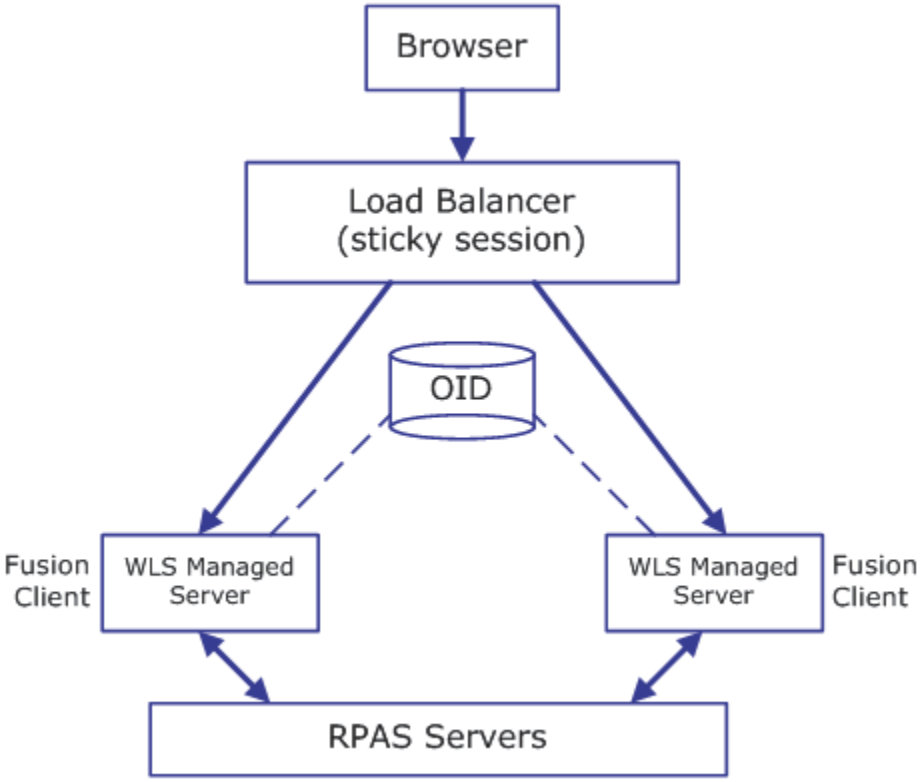
Item	Description
SSL Termination at the load balancer	This establishes a Secure Sockets Layer (SSL) protocol at the load balancer and replaces the need for the Web server to set up the SSL. To set up SSL Termination at the load balancer, ensure that it is configured with an SSL certificate (self generated or signed by a certificate authority).
Load Balancing Method	It is recommended to use a Round Robin load balancing method, coupled with session affinity. In the Round Robin method, requests are balanced across a list of available servers and servers are selected sequentially. By coupling with session affinity, subsequent requests from a specific user are redirected to the same server assigned for the previous requests from the user. Session affinity is necessary because there is no application state replication between the servers. This will avoid the excessive need for the application state to be replicated between the servers.
KeepAlive	The load balancer uses the KeepAlive feature to test the servers before directing the users to an active server. This test typically involves setting up a keepalive page (such as index.html) or a custom page that the load balancer will attempt to load as per the test. You can choose to set up this feature or set up a monitor that checks the ports on the servers ensuring that they are active. Setting up a monitor is the preferred method.

Non-SSO deployment

The considerations listed in Table 5–3 apply in case of non-SSO deployment. Figure 5–1 shows a load balancer for a non-SSO deployment.

Using a load balancer is recommended for scenarios where you need to use multiple servers because one server may not be able to handle the load. The RPAS Fusion Client can be installed and used without implementing a load balancer.

Figure 5–1 Load Balancer for a Non-SSO Deployment

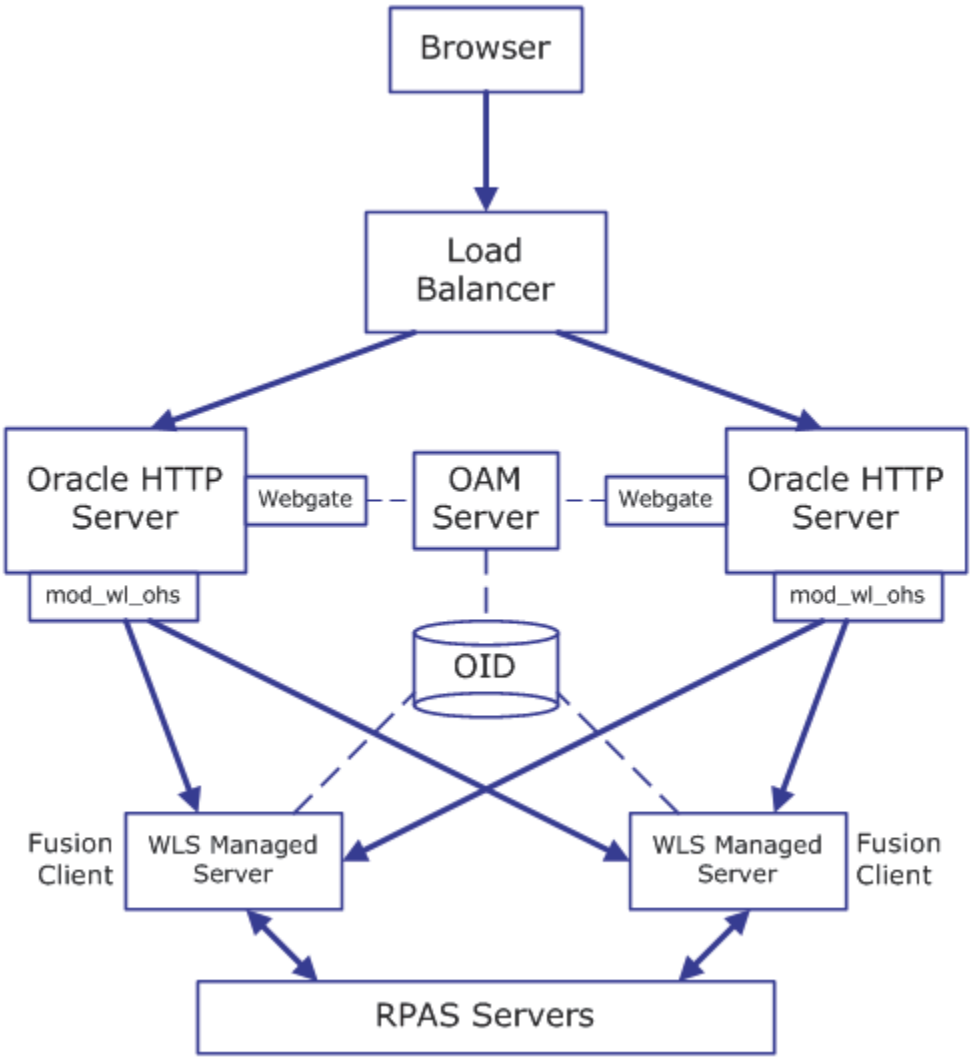


SSO deployment

These considerations apply in case of an SSO deployment. Figure 5–2 shows a load balancer for an SSO deployment.

In a deployment that uses Oracle Single Sign On for authentication, you must use the mod_wl_ohs Oracle HTTP server module to distribute requests with session affinity across multiple Weblogic managed servers. Single Sign On is enforced by an Oracle Access Manager 11g WebGate module plugged into the Oracle HTTP server. Scalability on the application server is achieved through the use of multiple managed servers. Single point of failure can be avoided by deploying multiple Oracle HTTP servers with a load balancer in front. The load balancer can also bring in other performance benefits such as SSL termination, content compression, caching, and so on.

Figure 5–2 Load Balancer for an SSO Deployment



For more information on setting up load balancers, refer to the documentation included with the Load Balancer.

Supported Configurations

For more information on the software and hardware requirements, refer to Table 1–3, " RPAS Fusion Client Hardware and Software Requirements" in Chapter 1, "Introduction".

Note: RPAS Fusion Client is included with the RPAS installation media and requires that the RPAS Server and Configuration Tools are upgraded to Release 13.3.1.

Install and Set Up the RPAS Infrastructure

This is the second pre-installation task, ensure that all previous pre-installation tasks are complete.

Install and set up the RPAS Infrastructure. For more information, refer to Chapter 3, "Installing on UNIX and Linux Environments" or Chapter 4, "Installing on a Windows Environment".

Setting Up the WebLogic Server

This is the third pre-installation task, ensure that all previous pre-installation tasks are complete.

The RPAS Fusion Client is a Web-based client for RPAS. When you run the Fusion Client installer, the installer will require a domain set up over the WebLogic Server to deploy the Fusion Client as an application.

Before installing the RPAS Fusion Client, you must install the WebLogic Server and set up a domain for the Fusion Client. This chapter describes how you can set up the WebLogic Server for the Fusion Client. It includes the following sections:

- Installing the WebLogic Server
- Installing the Oracle ADF Run Time Patch
- Setting Up a WebLogic Domain

> **Note:** Once you set up the WebLogic server and domain, you must take note of the location where you installed the WebLogic domain. You will need to set up this location as an environment variable, WEBLOGIC_DOMAIN_HOME, before running the Fusion Client installer.

Installing the WebLogic Server

Install the Oracle WebLogic Server and Application Development Runtime. For Weblogic Server installation instructions, refer to the Oracle WebLogic Server Documentation for guidance. For Application Development Runtime installation, refer to the *Oracle Fusion Middleware Installation Guide for Application Developer*.

> **Note:** The Oracle RPAS Fusion Client does not require the Oracle Database Server & MDS repository schema specified by the Oracle Application Development Runtime installation instructions.

In the following sections, the WebLogic installation directory is referred to as the <MW_HOME> directory.

Installing the Oracle ADF Run Time Patch

Before you set up a WebLogic domain, you must apply the Oracle Application Development Framework (ADF) Run Time Patch 13849867 on top of ADF 11.1.1.5.0.

To download and apply the patch:

1. Log on to the My Oracle Support Web site and download the patch 13849867. To download this patch:
   a. In a Web browser, open the My Oracle Support Web at this URL:

https://support.oracle.com/

b. Select a language and sign on to the Web site by clicking **Sign In**.

c. Once signed in, the **My Oracle Support | Dashboard** window opens.

d. Click the **Patches & Updates** tab.

e. On the **Patch & Updates** window, under **Patch Search**, click **Patch ID** or **Number**.

f. In the **Patch ID** or **Number** field, enter *13849867*.

g. Optionally, you can also choose a platform from the Platform drop-down list.

h. Click **Search**. The **Patch Search Results** window opens.

i. In the **Patch Search Results** window, under **Patch ID**, click the relevant patch.

j. On the next window, click **Download**. It is located on the left side of the window.

Note: On the **Patch Search Result**s window, you can also select the row that matches the patch description, and then click **Download** on the toolbar that appears under the selected row.

---

2. Unpack the ZIP file to a temporary directory and navigate to this location.
3. Set the ORACLE_HOME and PATH environment variables using the following commands:

```
export $ORACLE_HOME=$MW_HOME
export PATH=$PATH:$MW_HOME/oracle_common/OPatch
```

4. At the command prompt, run the following command to apply the patch:

```
opatch apply
```

5. Follow the prompts to complete the patch installation. For detailed instructions, refer to the README.txt file included in the patch directory.

You can now set up your WebLogic domain. For more information, refer to Setting Up a WebLogic Domain.

Setting Up a WebLogic Domain

Use the WebLogic Configuration Wizard to create and set up a domain on the WebLogic Server. This section describes how you can create and set up a domain. It also introduces the steps to configure the managed servers and clusters on the application server. For more information on the WebLogic Configuration Wizard and customizing the domain environments with managed servers and 0s, refer to the Oracle Fusion Middleware Creating Domains Using the Configuration Wizard.

Note: For headless installations, ensure that you set up the WebLogic Startup script with the java.awt.headless parameter. For more information, refer to Troubleshooting.

To set up a WebLogic domain:

1. Navigate to the **<MW_HOME>/common/bin** directory, and run the following command to start the WebLogic Configuration Wizard in the graphical mode:

```
sh config.sh
```

2. On the WebLogic Configuration Wizard, follow the steps listed in Table 5–4:

Table 5–4 Steps to Setup a WebLogic Domain

Step	Window	Task
1.	Welcome Window	Click the Create a new WebLogic domain option, and then click Next.
2.	Select Domain Source Window	Click the Generate a domain configured automatically to support the following products option, select the Oracle JRF - 11.1.1.0 [oracle_common] check box, and click **Next**. Notes: ■ If the JRF option is not available, you must exit the installation, install the Application Development Runtime, and then restart the domain configuration. ■ The **Basic WebLogic Server Domain - 10.3.5.0 [wlserver_10.3]** check box is automatically selected and grayed out.
3.	Specify Domain Name and Location Window	Enter a domain name in the Domain Name field. In the **Domain location** field, specify the location where you want to install the domain. This location is referred to as the WEBLOGIC_DOMAIN_HOME all through this document.
4.	Configure Administrator User Name and Password Window	Set up an administrative user name and password. Important: Keep a note of the user name and password. You must specify this user name and password in the ant.install.properties file. The Oracle Installer uses this user to connect to the WebLogic Server during the RPAS Fusion Client installation.
5.	Configure Server Start Mode and JDK Window	Under WebLogic Domain Startup Mode, click Production Mode. Under JDK Selection, select the relevant JDK. Click **Next**.
6.	Select Optional Configuration Window	Select the configurations you want to customize and click **Next**. Go to Step 7 (Configure the Administration Server Window) or proceed directly to creating your domain by skipping the following steps and going to Step 15 (Configuration Summary Window).
7.	Configure the Administration Server Window	Enter relevant information in the following fields: ■ Name - Valid server name. (String of characters that can include spaces.) ■ Listen address - Listen address for a server instance. ■ Listen port - Valid value for the listen port. ■ SSL listen port - Valid value to be used for secure requests. ■ SSL enabled - Select this check box to enable SSL. You can enter values in the SSL listen port field once you select this check box. Click **Next**.
8.	Configure Managed Servers Window	Click **Add**, and then enter relevant information in the following fields: ■ Name - Valid server name. (String of characters that can include spaces.) ■ Listen address - Listen address for a server instance. ■ Listen port - Valid value for the listen port. ■ SSL listen port - Valid value to be used for secure requests. Repeat this step to add more managed servers. Click **Next**.

Table 5–4 (Cont.) Steps to Setup a WebLogic Domain

Step	Window	Task
9.	Configure Clusters Window	This window opens, once you specify the managed servers. Click **Add**, and then enter relevant information in the following fields: ■ Name - Valid cluster name. (String of characters that can include spaces.) ■ Multicast address - Address used by the cluster members to communicate with each other. ■ Multicast port - Port used by the cluster members to communicate with each other. ■ Cluster address - Address that identifies the Managed Servers in the cluster. Repeat this step to specify more clusters. Click **Next**.
10.	Assign Servers to Clusters Window	Use the arrow buttons and assign the servers to the clusters specified in the domain. Click **Next**.
11.	Configure Machines Window	Click **Add**, and then add the machine (UNIX-based) information where the Fusion Client will be deployed. If you need to specify a local host because one of your target managed server is on the local host (meaning that it is the same as your admin server host), enter any of the following: ■ localhost ■ 127.0.0.1 ■ the DNS name Do not enter an IP address of the local host because it will try to use SSH to copy files to the local host. This is not only unnecessary but may not work depending on the SSH environment and on whether you specified SSH properties. In a clustered installation involving multiple machines, this includes all the systems where the RPAS Fusion Client will be deployed. In other words, the installer looks for all machines defined in this section in order to copy files to each of them. If you do not want to install the product on a host, do not specify that host here. **Note:** Only define machines where you plan to run managed servers. Any additional machine definitions may unnecessarily cause the installer to copy configuration files to that machine. Click **Next**.
12.	Assign Servers to Machines Window	Use the arrow buttons and assign the managed servers to the machines specified in the domain. Click **Next**.
13.	Target Deployments to Clusters or Servers	In the left pane, select the clusters or servers, and then select the relevant application check boxes in the right pane to target them to the specific cluster or managed server. For each cluster and managed server, select the **Library** check box. The WebLogic domain must be set up in such a manner that all the clusters and the relevant managed servers include all the libraries included with the WebLogic server.
14.	Target Services to Clusters or Servers	In the left pane, select the clusters or servers, and then select the relevant services check boxes in the right pane to target them to the specific cluster or managed server.
15.	Configuration Summary Window	Review and confirm the configuration summary. Click **Next**.
16.	Creating Domain Window	Displays the domain configuration progress. After the configuration is complete, click **Done**.

Setting Up the Maximum Heap Size

After you have set up the WebLogic domain, ensure that you set up the maximum heap size for the WebLogic server. Setting a maximum heap size depends on your implementation.

For more information on heap sizing, refer to the Oracle Java documentation on Java Performance Tuning and the *Oracle Fusion Middleware Performance and Tuning for Oracle WebLogic Server*.

Configuring the Node Manager for Clusters-based Installation

When setting up a WebLogic cluster with multiple physical machines, ensure that you have completed the following tasks:

- Installed WebLogic Server and the ADF Runtime libraries on identical paths on each machine. For example, the identical path could be:

  ```
  /u00/webadmin/Oracle/Middleware
  ```

  This path must exist on each machine's filesystem. If this is not done, the essential ADF runtime libraries will not deploy and the application will not run.

- Copy the WebLogic domain structure from the Admin Server machine to all the managed server machines, ensuring identical filesystem locations. You can use the pack.sh and unpack.sh utilities to perform the copy. This process also copies the startWebLogic.sh script, which can be found in the domain directory. This script can be used to start up the managed servers.

  Note: The previously listed considerations do not apply if the WebLogic Server and the domain are installed on a shared filesystem.

There are two startup options for customizing managed server startup parameters: manual startup and Node Manager startup. These options are described in the following sections.

Manual Startup

The managed servers in a WebLogic cluster can be started manually by using the startManagedWebLogic.sh script in the WebLogic domain directory. You can modify this script to customize server startup parameters such as JVM heap size, garbage collection settings, and so on.

Node Manager-Based Startup

Using NodeManager, choose one of the following options for server startup customization:

- Setup custom server startup parameters for each managed server on the WebLogic Administration Console. These parameters can be accessed on the Server Start tab under **Home -> Servers -> <managed-server-name>**.
- Specify startup parameters in the startup.properties file located in the following filesystem path:

  ```
  <domain-home>/servers/<managed-server-name>/data/nodemanager
  ```

  This file must exist on each server machine's filesystem.

Note: If a shared filesystem is in use, all the startup.properties files must reside on that filesystem.

- Make NodeManager use a start script. The script on each server can be modified as needed, as described in Manual Startup. Use startWebLogic.sh as the base script and then modified as needed.

For more information about cluster-based installation, including information on installing a WebLogic server and setting up WebLogic clusters, refer to the *Oracle Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server*.

Accessing the Fusion Client Installation Media

This is the fourth pre-installation task, ensure that all previous pre-installation tasks are complete.

The RPAS Fusion Client installation media is included with the RPAS installation media. The installation files for the RPAS Fusion Client are available at the following location in the <RPAS_CD_IMAGE> directory:

```
<RPAS_CD_IMAGE>/fusion/
```

Note: <RPAS_CD_IMAGE> is the temporary location where the RPAS installation media files were unpacked.

Setting Up Your Installation Properties File

This is the fifth pre-installation task, ensure that all previous pre-installation tasks are complete.

To install the RPAS Fusion Client, it is recommended that you set up the installation properties file (ant.install.properties) before running the installer.

Note: For an installation in silent mode, you must set up the installation properties file before running the installer. For an installation in graphical or text mode, this is optional.

To set up your install.properties file:

1. Navigate to the RPAS Fusion Client directory, copy the ant.install.properties.template file to the same directory, and rename it ant.install.properties.
2. Edit the ant.install.properties file using any text editor, specifying values as described within the file, and save it. For more information on the parameters, refer to Installation Properties File Parameter Reference.

Note: Ensure that the ant.install.properties file is available in the same directory with the install.sh script.

Installation Use Cases

The following use cases can help you understand what to specify for various installation properties which have values that depend on how your domain is

configured and whether you are installing for the first time. Your installation may be similar to one or multiple use cases. If your installation is a combination of use cases, all properties from the relevant use cases apply.

Use Case 1: Installation on a Single Managed Server, Same Host as Admin Server

Installation on a single managed server located on the same physical host as the admin server:

- Set `input.appserver.host` to either:
  - `localhost`
  - `127.0.0.1`.
- Since the managed server is on the same physical host as the admin server, set `input.is.multiple.hosts` to **No**.
- Any property that begins with `input.ssh` (SSH-related properties) is inconsequential and can be set to either **Yes** or **No**.

Use Case 2: Installation on the Admin Server

Use the same guidelines as described in Use Case 1: Installation on a Single Managed Server, Same Host as Admin Server.

Use Case 3: Installation on a Single Managed Server, Different Host from Admin Server

Installation on a single managed server that is located on a different physical host as the admin server host:

- Set `input.is.multiple.hosts` to **Yes**.
- If using silent install, then you must set `input.retrieve.credentials` to **Yes** and prepare the wallet with weblogic and SSH credentials, before install. Set it to **No** if you do not have SSH credentials stored in the wallet and need to specify the credentials yourself.

> **Note:** Setting `input.retrieve.credentials` to **Yes** implies that you have also saved the WebLogic admin credentials in the wallet. Either all user credentials are to be retrieved from the wallet (for Weblogic and SSH) or they are to be entered manually by the user in the installer UI.
>
> If using the silent mode installer, then you must set `input.retrieve.credentials` to **Yes** and prepare the Wallet with WebLogic and SSH credentials, before installing.

All other SSH-related properties that begin with input.ssh must be set or ignored appropriately, so that files can be copied to the managed server host from the current host which is the admin server host.

> **Note:** It is required that all machines have the same SSH userid and password.
>
> Because the installer uses SCP to migrate files to remote hosts, you should ensure that you can copy files from the installation host to the target server using SCP and the specified parameters. If you cannot, the installer will fail.

Use Case 4: Installation on a Cluster of Managed Servers, Same Host as Admin Server

Installation of a cluster of managed servers, where all managed servers are located on the same physical host as the admin server:

Use the same guidelines as described in Use Case 1: Installation on a Single Managed Server, Same Host as Admin Server.

Use Case 5: Installation on a Cluster of Managed Servers, Different Host as Admin Server

Installation onto a cluster of managed servers, where at least one of the managed servers is located on a different physical host as the admin server host:

Use the same guidelines as described in Use Case 3: Installation on a Single Managed Server, Different Host from Admin Server

Use Case 6: Installation on Multiple Standalone Managed Servers, Same Host as Admin Server

Installation on multiple standalone managed servers that are not part of a cluster, where all managed servers are on the same physical host as the admin server host:

Use the same guidelines as described in Use Case 1: Installation on a Single Managed Server, Same Host as Admin Server

Use Case 7: Installation on Multiple Standalone Managed Servers, Different Host as Admin Server

Installation on multiple standalone managed servers that are not part of a cluster, where at least one managed server is located on a different physical host as the admin server host:

Use the same guidelines as described in Use Case 3: Installation on a Single Managed Server, Different Host from Admin Server.

Installation Properties File Parameter Reference

The following table describes the parameters in the ant.install.properties file that you must set up before you install the RPAS Fusion Client application:

Note: When the installation starts, values set for all the user credentials will be encrypted and stored in the Oracle Wallet, and then cleared from the ant.install.properties file. Therefore, you will have to change the installation parameters to retrieve the credentials before attempting to re-install.

Table 5–5 Installation Properties File Parameter Reference

Parameter Name	Description
Retrieve Credentials	
input.retrieve.credentials	As mentioned previously, this applies to GUI mode of install. For silent, you must set it to **Yes**. You should set the value to **Yes** if you have stored user credentials to retrieve them later. If you do not have user credentials stored in the secure wallet, or if you want to overwrite the existing credentials or store new credentials, set the value to **No**. If using the silent mode installer, then you must set `input.retrieve.credentials` to **Yes** and prepare the Wallet with WebLogic and SSH credentials, before installing.
Target Installation Directory	
input.install.target.dir	Specify the location where you want to install the RPAS Fusion Client.
Logs and Temporary Directories	
input.wallet.dir	Specify the location of the Oracle Wallet where the user credentials are to be saved or retrieved. This cannot be in or under the same temporary directory indicated by input.install.tmp.dir.
input.app.log.dir	Specify the location for the application log files.
input.install.log.dir	Specify the location for the installation log files.
input.install.tmp.dir	Specify the location for the temporary file directory used during installation.
WebLogic Admin Server Information	
input.appserver.host	Specify the host name where the application server is running. If the application server is running on the same host as the installer. If you need to specify a local host because one of your target managed server is on the local host (meaning that it is the same as your admin server host), enter any of the following: ■ localhost ■ 127.0.0.1 ■ the DNS name If the application server is running on a different host as the installer, enter the DNS name or IP address of the host where the application server is running. You must also specify values for appropriate parameters starting with input.ssh.
input.admin.server.port	Specify the port number associated with the application server.
input.admin.username	Specify the administrative user name for the application server.
input.admin.username.alias	Specify an alias name for the administrative user. Specifying an alias name for the administrative user enhances the security for the application. When left blank, the alias name will default to the administrative user name.
Application Configuration Information	
input.is.multiple.hosts	To specify that your domain contains at least one managed server machine that is different from the admin server machine, set the value to yes. If all the managed server machines are on the same machine as the admin server machine, then set the value to no. In other words, even if you have a cluster with multiple managed servers or have multiple standalone managed servers, the value should be no if all of these managed servers are on the same machine as the admin server machine.

Table 5–5 (Cont.) Installation Properties File Parameter Reference

Parameter Name	Description
input.sso.enabled	Specify whether you want to install the application to be SSO enabled (set the value to yes). To install the application without configuring SSO, set the value to no. For more information on setting up SSO, refer to the *Oracle Retail Application Server Administration Guide for the Fusion Client*.
SSH Credentials Applies to cluster-based installations only.	
input.ssh.authentication.mode	Specify one of the following authentication methods: ▪ password - Use the specified password (associated with the SSH User Name) to connect to the remote hosts for copying the files. ▪ passphrase - Use the specified passphrase (associated with the SSH User Name) along with the SSH Key to connect to the remote hosts. ▪ default - Connect to the remote hosts without a user name, password, or passphrase. This is only applicable if you are copying files to a remote host (meaning that at least one managed server is on a different physical host than the admin server host).
input.ssh.username	Specify the SSH user name to connect to the remote hosts. This is only applicable if you are copying files to a remote host (meaning that at least one managed server is on a different physical host than the admin server host).
input.ssh.username.alias	Specify the alias name associated with the SSH user name. This is used to store or retrieve the SSH credentials (SSH username, and either SSH password or passphrase) to and from the Oracle Wallet. This is only applicable if you are copying files to a remote host (meaning that at least one managed server is on a different physical host than the admin server host).
input.ssh.keyfile	Enter the location of the SSH key file. When left blank, the installer retrieves the file from `${user.home}/.ssh/id_dsa` directory, where `user.home` is your home directory. To use this default location, ensure that you have the private DSA key stored at this location. This is only applicable if you are copying files to a remote host (meaning that at least one managed server is on a different physical host than the admin server host).
Application Server Information	
input.target.server.name	Specify the cluster or managed application server names where you want to install the RPAS Fusion Client.

Table 5–5 (Cont.) Installation Properties File Parameter Reference

Parameter Name	Description
User Information	
input.security.principal1 input.security.principal2 input.security.principal3 input.security.principal4 input.security.principal5	Enter up to five enterprise users or groups for SSO, LDAP/WebLogic (supported), and WebLogic attached (for demos/development) authentication. These users and groups refer to the User IDs and user groups that are created in the ID store. The users (user or group names) you list here inform the installer which users and user groups are allowed to access the Fusion Client. The users listed in the SSO ID store must be users of the RPAS solution deployed on the RPAS Fusion Client. To support SSO, the Web deployment descriptors need to be configured to allow access pages to SSO-authenticated requests. During the application installation, the names entered here are added to the Web deployment descriptor file (weblogic.xml) as <principal-user> under <security-role-assignment> tag. **Note**: Using group names is preferred over user names as it allows you to add new users to the group without making changes to the deployment descriptor. The RPAS Fusion Client application roles are mapped to the enterprise roles or groups in this deployment descriptor file. For more information on setting up SSO, refer to the Appendix D: Oracle Single Sign-On (SSO).
Application Deployment Information	
input.app.name	Specify an application name. The RPAS Fusion Client will be deployed over the WebLogic Server with this name.
input.app.context.root	Specify the context root for the application. Once deployed, the RPAS Fusion Client will be available on the Web browser using this context path. For example, in case you set the context root to rav, you can access the application using the URL: `http://<hostname>:<port>/rav`.
input.app.image.repository	Specify the location or a network path where the images used in the application are located.
RPAS Information	
input.rpas.solution.details.known	Specify whether you know the details of the RPAS solution infrastructure and domain.
input.rpas.solution.id	The RPAS Solution ID for your RPAS application.
input.rpas.solution.desc	Specify the RPAS solution description which is displayed in the fusion client to let you select the solution.
input.rpas.server.name	Specifies the host name of the DomainDaemon from the RPAS Server installation.
input.rpas.server.port	Specifies the port number of the DomainDaemon from the RPAS Server installation.
input.rpas.domain.path	Specify the location where the RPAS domain is installed.

Setting Up Environment Variables

This is the sixth pre-installation task, ensure that all previous pre-installation tasks are complete.

Before you start the installation, ensure that the following environment variables are set in the system:

- WEBLOGIC_DOMAIN_HOME – Location where the WebLogic domain is installed. For more information, refer to Setting Up the WebLogic Server.
- ORAINST_HOME – An absolute path to the file containing the central inventory information. This file must define the `inventory_loc` and `inst_group` variables in it. The `inst_group` value should be the UNIX group for the opatch utility.

  For example:

  ```
  inventory_loc=/home/weblogic/oraInventory
  inst_group=users
  ```

> **Note:** You do not need to set JAVA_HOME or ORACLE_HOME. Regardless of your JAVA_HOME, JAVA_HOME is set by the installer to the one used by the WebLogic domain pointed by WEBLOGIC_DOMAIN_HOME. The same is true for ORACLE_HOME, which is set by the installer to the value needed during installation.

Although it is recommended that these variables be set up in relevant bash shell startup files (.bash_profile) of the system, you can also set up the variables using the EXPORT command at the UNIX prompt. For more information on setting up these variables in the startup files, refer to the operating system documentation.

To set up the environment variables for the current session, at the UNIX prompt type the following commands in sequence:

```
export WEBLOGIC_DOMAIN_HOME=<path where the WebLogic domain is installed>
For example, /u01/app/oracle/middleware/user_projects/domains/base_domain
```

Validating WebLogic and Oracle Application Development Framework Versions (Optional)

This is the seventh pre-installation task and it is optional, ensure that all previous pre-installation tasks are complete.

When you launch the installer, it attempts to validate the version of WebLogic and the associated Oracle Application Development Framework version for this release. You may want to run these validations without launching the installer in a standalone fashion prior to running the installer. There are two shell scripts that you can run to do this. In the `<installer>/common` directory, there are two files:

- `validateWls.sh` for validating the WebLogic version
- `validateAdf.sh` for validating the Oracle Application Development Framework version

You can run each of these scripts independently without any argument:

- `sh validateWls.sh`
- `sh validateAdf.sh`

If the validation is successful, the scripts print a success message: *Found supported version of WebLogic Server x.x.x*. Or, it exits with an error message that describes the issue. After addressing the issue, you may want to run the scripts again.

Creating User Credentials in an Oracle Wallet

This is the eighth and final pre-installation task, ensure that all previous pre-installation tasks are complete.

As part of the Oracle Software Security Assurance (OSSA), sensitive information such as user credentials required for the RPAS Fusion Client installation is encrypted and stored in a secure location called the Oracle Wallet.

When the installation starts, all the necessary user credentials are retrieved from the Oracle Wallet based on the alias name associated with the user credentials.

Note: Before installing the RPAS Fusion Client in silent mode, you must create user credentials in an Oracle Wallet. This step is optional when installing in text or graphical mode.

Storing Credentials

There are two kinds of credentials that the silent-mode installer demands to be stored in the wallet before it starts:

- **Weblogic admin userid and password**: Stored against the alias *wlAdmin* (or whatever alias is configured within the ant.install.properties file against the *input.admin.username.alias* property. username: *WebLogic admin user name*.
- **Client-side SSL keystore access password**: The userNameAlias must be *fckey*, however, the username can be anything as it is ignored. At runtime, this password is accessed from the Weblogic domain credential store and used to read the SSL key stores deployed on the Fusion Client.

The respective passwords are prompted for by the `save_credential.sh` script

Creating Credentials

The following steps describe how to create the user credentials:

1. Set and export the JAVA_HOME variable.
2. Cd to `<installer>/retail-public-security-api/bin`.
3. Run `sh save_credential.sh <userNameAlias> <username> <locationOfWalletDir>`.

   The following table describes the field options to run the script in Step 3.

Field Option	Description
`<userNameAlias>`	The keyname for which the credentials need to be stored.
`<username>`	The username to be stored in a secure credential wallet for the specified userNameAlias.
`<locationOfWalletDir>`	The directory where the wallet will be created. This is an optional parameter. If omitted, it creates the wallet under: `<installer>/retail-public-security-api/secure-credential-wallet`.

Installation Tasks

After you have completed the steps in the Pre-Installation Tasks section, you can start installing the RPAS Fusion Client.

The RPAS Fusion Client Installation media includes an Oracle installer that you must run to install the RPAS Fusion Client. The installer installs the application based on the parameters specified in an installation properties file.

You can install the application in either of these modes:

- Silent Mode - In silent mode, the installer processes the values set in the properties file with no manual intervention required.
- Graphical or Text Mode- In graphical or text mode, the Oracle Installer will prompt you to enter or modify the value of properties specified in the installation properties file.

Silent Mode

This section describes how to install RPAS Fusion Client in silent mode. Silent mode is non-interactive.

> **Note:** If you are reinstalling the Fusion Client after installing an RPAS application, you must backup the rgbu_planning_home/Help/ohwconfig.xml file and restore it after the installation. Otherwise, access to the application's help files is lost.

To install RPAS Fusion Client in silent mode:

1. Ensure that you have completed Setting Up Your Installation Properties File.

   > **Note:** Ensure that the ant.install.properties file is available in the same directory with the install.sh script.

2. Ensure that you have saved these user credentials in an Oracle Wallet:
   - Weblogic domain admin user credential (the entry alias is configurable)
   - Client-side SSL keystore credential (the entry alias is *fckey* and it is not configurable)

   The silent mode installer does not ask for user credentials. Instead it retrieves them from the Oracle Wallet.

   For more information, refer to Creating User Credentials in an Oracle Wallet.

   > **Note:** The installation property `input.retrieve.credentials` must be **Yes**.

3. Ensure that the RPAS Domain and WebLogic Server are running.
4. Navigate to the RPAS Fusion Client installation folder, enter the following command:

   ```
   ./install.sh silent
   ```

install.sh

The install.sh command enables you to install RPAS Fusion Client.

Syntax

```
./install.sh <mode name>
```

Arguments

Use any arguments listed as needed:

Argument	Description
a.	Argument
b.	Description
c.	<mode name>
d.	Use this argument to specify the installation mode. You can specify the following: ■ swing – to launch a graphical installer. This is the default installation mode. In case you do not specify a mode, the installer defaults to swing mode. ■ text – to launch the installer with instructions that appear as text on the screen. ■ silent – to start the installation based on the parameters set up in the ant.install.properties file. No manual intervention is required.

Output

The RPAS Fusion Client installation creates the application directory structure, populates it with appropriate files, and when the installation finishes, it generates a log file and two properties files.

Graphical or Text Mode

If you prefer to use a guided user interface, you can use the Oracle Installer in the graphical or text mode. Although this section describes how you can install the RPAS Fusion Client in graphical mode, the same on-screen instructions appear as text instructions in the text mode.

Note: Although you do not have to set up the installation properties file when installing in graphical or text mode, it is helpful. If you set up values in the properties file, those values will be the default values in the graphical or text mode dialog.

For instructions on setting up this file, refer to Setting Up Your Installation Properties File.

If you are reinstalling the Fusion Client after installing an RPAS application, you must backup the rgbu_planning_home/Help/ohwconfig.xml file and restore it after the installation. Otherwise, access to the application's help files is lost.

To install RPAS Fusion Client using the Graphical Mode:

1. Ensure that the RPAS Domain and WebLogic server are running.

2. If you are viewing the installer from a Windows client:
   - On the Windows client, start an Xserver program that enables you to emulate the X terminal.
   - On the application server, set the display for the Windows client where you want the Oracle Installer to display as follows:

     ```
     export DISPLAY=<IP address>:0.0
     ```

3. From your application server machine, enter the following command:

   ```
   ./install.sh
   ```

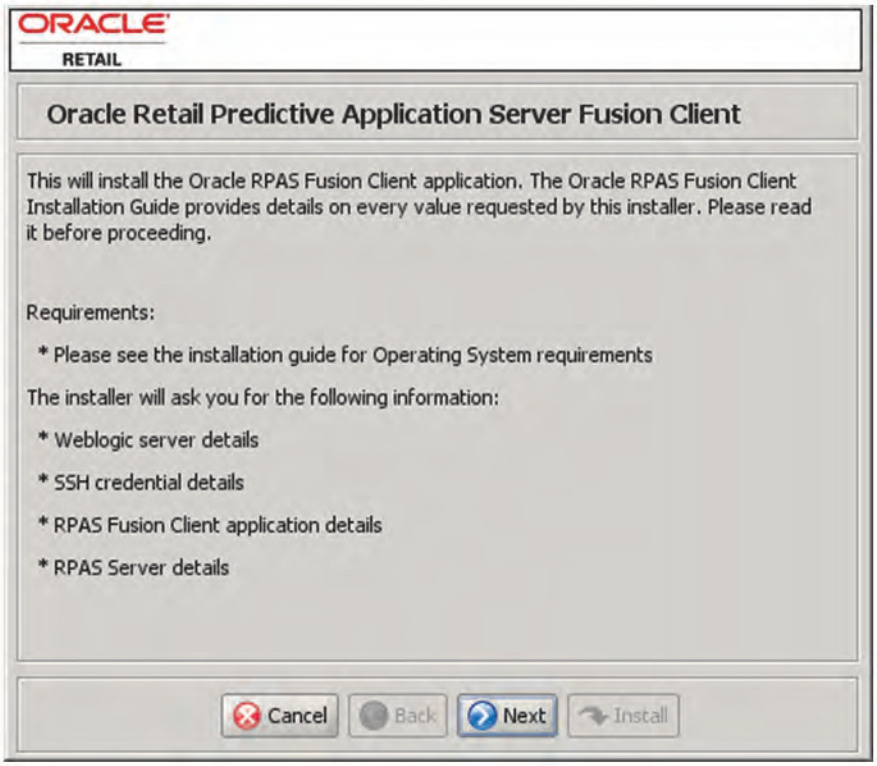
   When the installer runs, it attempts to validate the version of WebLogic and the associated Oracle Application Development Framework that are used by the WebLogic domain. If you encounter a validation error, fix the problem and try again.

   Note: If you want, you can skip these validations by setting and exporting `SKIP_FC_VALIDATION=1` before running the installer.

   For more information about the install.sh command refer to the section, Silent Mode.

4. The Oracle Retail Predictive Application Server Fusion Client window opens. Click **Next**.

Figure 5–3 Oracle Retail Predictive Application Server Fusion Client

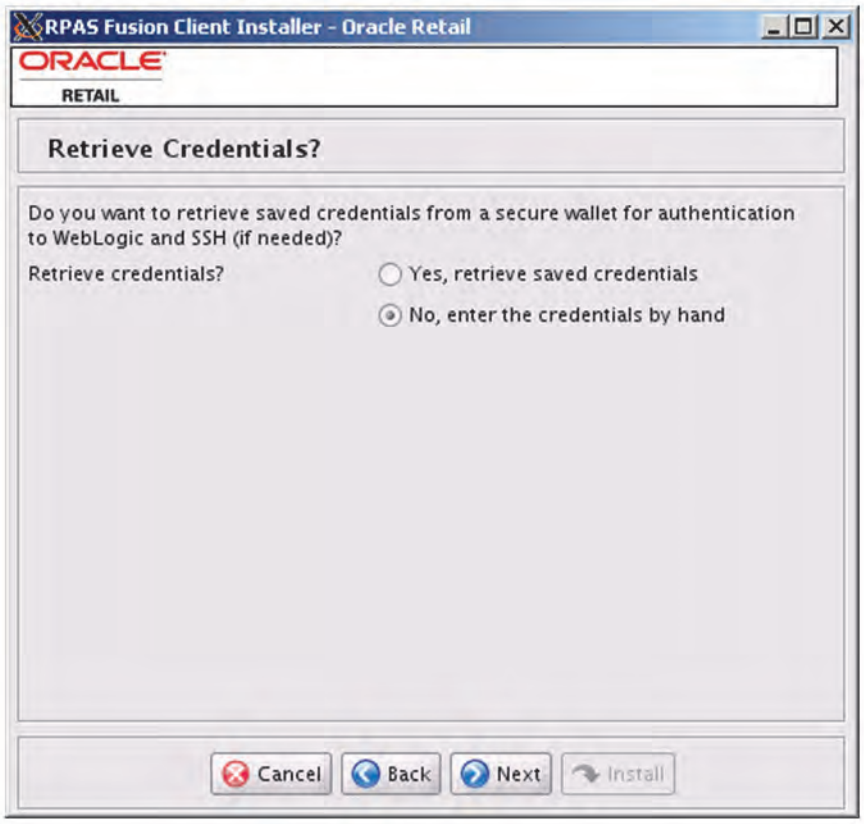


5. The Retrieve Credentials? window opens. Select whether to retrieve user credentials from the Oracle Wallet:

   - Select **Yes** to indicate that the installer will read the user credentials from an Oracle Wallet
   - Select **No** to indicate that you will enter the user credentials in the user interface.

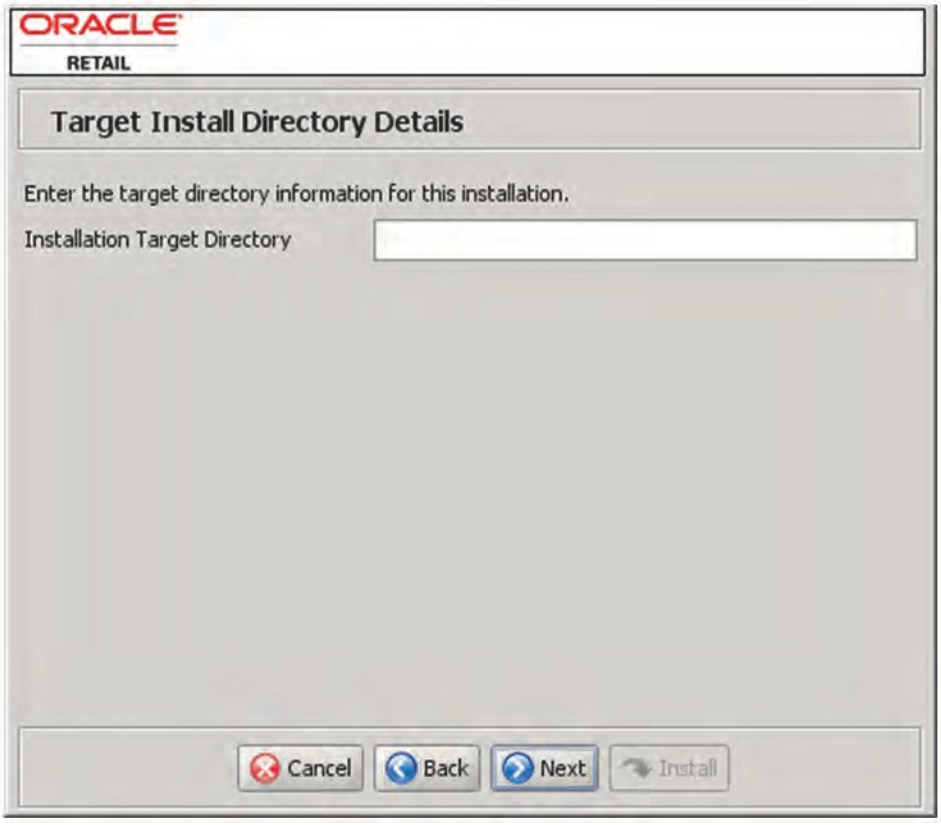
   Click **Next**.

Figure 5–4 Retrieve Credentials?



6. The Target Install Directory Details window opens. In the Installation Target Directory field, specify the location where you want to install the RPAS Fusion Client. Click **Next**.

Figure 5–5 Target Install Directory Details

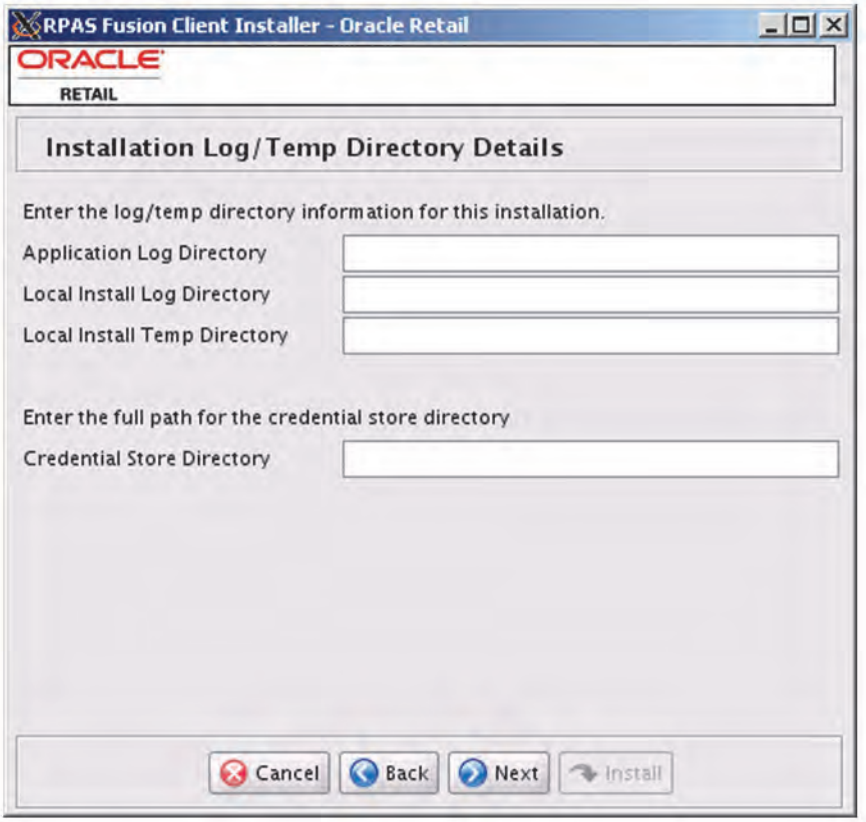


7. The Installation Log/Temp Directory Details window opens. Enter the relevant information in the following fields and click **Next**:

Field	Description
Application Log Directory	Specify the location for the application log files.
Local Install Log Directory	Specify the location for the installation log files.
Local Install Temp Directory	Specify the location for the temporary file directory used during installation.
Credential Store Directory	Specify the location of the Oracle Wallet you want to use to save or retrieve user credentials. This cannot be in or under the same temporary directory named in the Local Install Temp Directory field.

Note: By default, all fields (except Credential Store Directory) are pre-populated based on the installation directory you specified in theTarget Install Directory Details window.

Figure 5–6 Installation Log/Temp Directory Details



8. The Weblogic Admin Server Details window opens. On the WebLogic Admin Details window, enter appropriate information for the following fields and click **Next**:

Field	Description
Admin Server Host Name	Specify the host name of the application server.
Admin Server Port Number	Specify the port number associated with the application server.
Admin User Name	Specify the administrative user name for the application server.
Admin User Name Alias	Specify an alias name for the administrative user. Specifying this name enhances the security for the application. When left blank, the alias name defaults to the administrative user name. Refer to the note following this table.
Admin Password	Specify the password associated with administrative user name.
Test admin server connection?	Select **Yes** if you want to test the connection to the admin server. Select **No** if you want to advance to the next screen without testing the connection

Note: As part of the Oracle Software Security Assurance, sensitive information such as user credentials for the RPAS Fusion Client are encrypted and stored in a secure location in the application installation directory. This location is called the Oracle Wallet.

When the installation starts, if you have chosen to retrieve the user credentials from an Oracle Wallet, the administrative user credentials are retrieved.

Figure 5–7 Weblogic Admin Server Details

9. The Application Configuration window opens.

   a. Specify whether or not you are installing to more than one host:

Option	Description
Yes	This indicates an installation where at least one managed server is running on a remote machine (remote to the admin server machine). Go to Step 10.

Option	Description
No	This indicate an installation where all of the managed servers for deploying the Fusion Client are running on the same machine as the admin server machine, or if you are deploying to the admin server only. Go to Step 11.

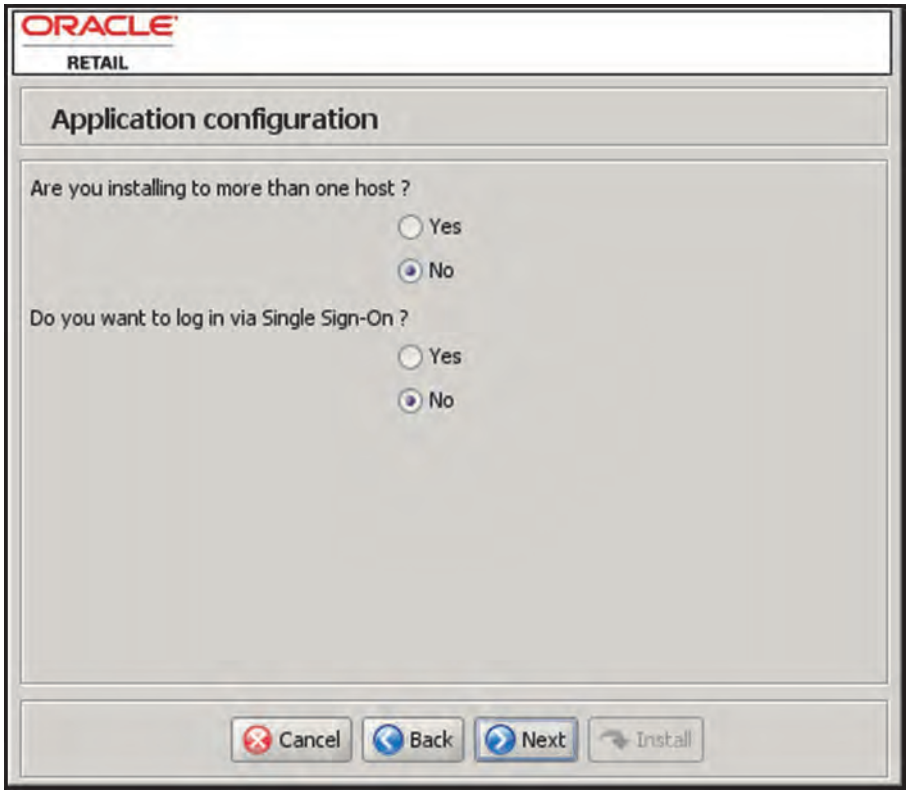
b. Specify whether you want to use the Single Sign-On (SSO) feature to log on to the application.

- Select **Yes** to indicate that you want use this feature. Go to Step 12.

Click **Next**.

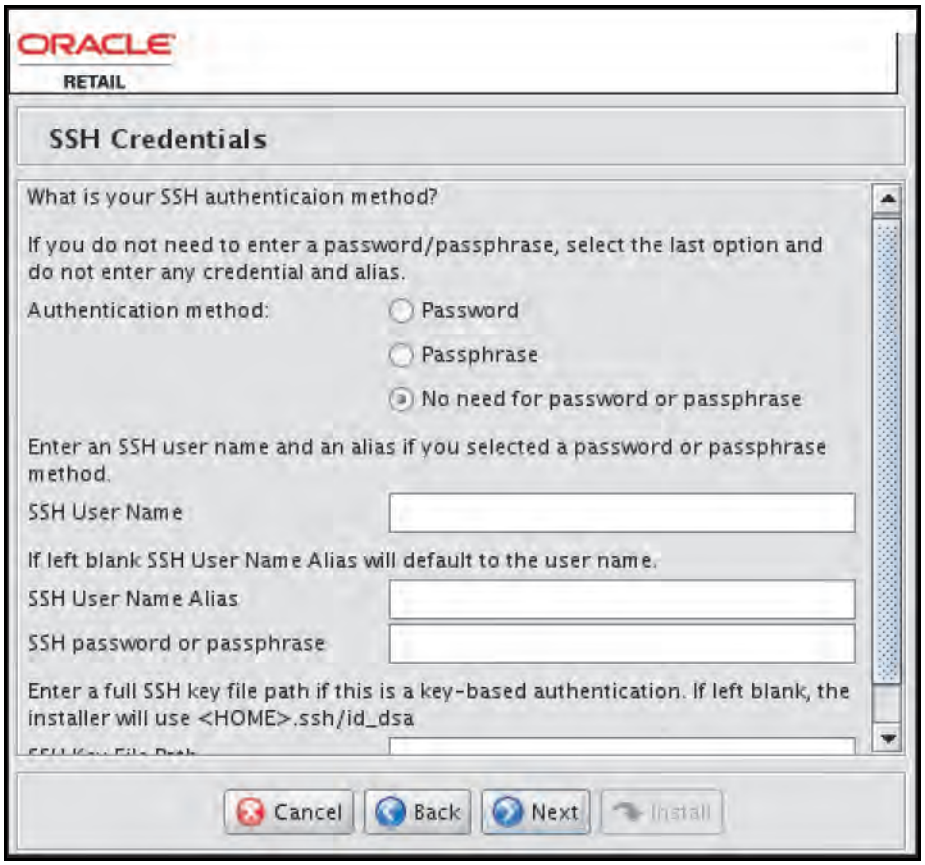
Note: For more information on the setting up SSO, refer to the section, Set Up Single Sign-On (SSO).

Figure 5–8 Application Configuration



10. The SSH Credentials window opens if you selected **Yes** on the Application Configuration window, otherwise continue to Step 11

Figure 5–9 SSH Credentials



Enter the relevant information in the following fields and click **Next**:

Field	Description
Authentication method	Select one of the following authentication methods: ▪ **Password** - Use the specified password (associated with the SSH User Name) to connect to the remote hosts for copying the files. ▪ **Passphrase** - Use the specified passphrase (associated with the SSH User Name) along with the SSH Key to connect to the remote hosts. ▪ **No need for password or passphrase** - Default option; connect to the remote hosts without a user name, password, or passphrase.
SSH User Name	Specify the SSH user name to connect to the remote hosts.
SSH User Name Alias	Specify the alias name associated with the SSH user name. Specifying an alias name enhances the security for the application. When left blank, the alias name will default to the administrative user name. Refer to the first note following this table.
SSH password or passphrase	Based on the authentication method you selected, enter the relevant SSH password or passphrase.

Field	Description
SSH Key File Path	In case you selected the Passphrase option in the **Authentication Method** field, enter the location of the SSH key file. When left blank, the installer will retrieve the file from `${user.home}/.ssh/id_dsa` directory, where `user.home` is your home directory. To use this default location, ensure that you have the private DSA key stored at this location. Refer to the second note following this table.

Note: As part of the Oracle Software Security Assurance, sensitive information such as user credentials are encrypted and stored in a secure location in the application installation directory. This location is called the Oracle Wallet.

When the installation starts, the SSH user credentials will be retrieved from the Oracle Wallet based on the alias name specified on this window.

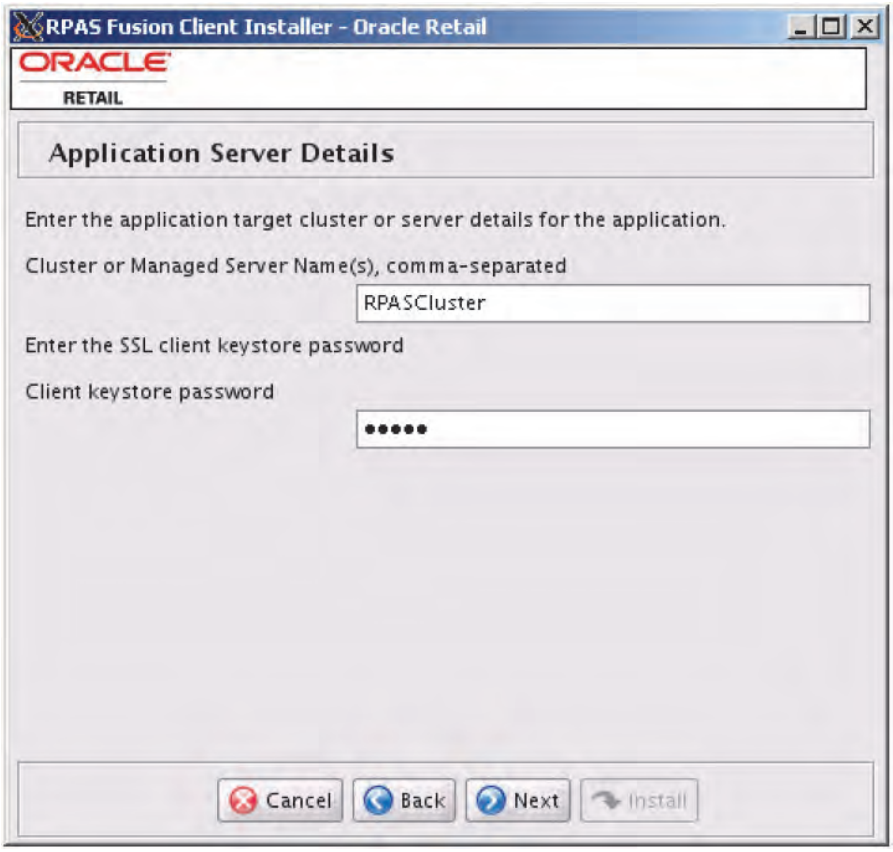
Note: The **SSH User Name** and **SSH password or passphrase** fields do not appear when you choose to retrieve the existing SSH credentials (the **Yes, retrieve saved credentials** option in the Retrieve Credentials? window).

The existing SSH user credentials will be retrieved based on the alias name for the SSH user.

11. The Application Server Details Window window opens. Enter relevant information for the following fields and click **Next**:.

Field	Description
Cluster or Managed Server Name(s), comma-separated	Enter the cluster or managed server names where you want to deploy the fusion client.
Client keystore password	Enter the client keystore password which will be used for client authentication. For additional information about the client keystore password , refer to Setting Up a Trust Store in the JKS Format.

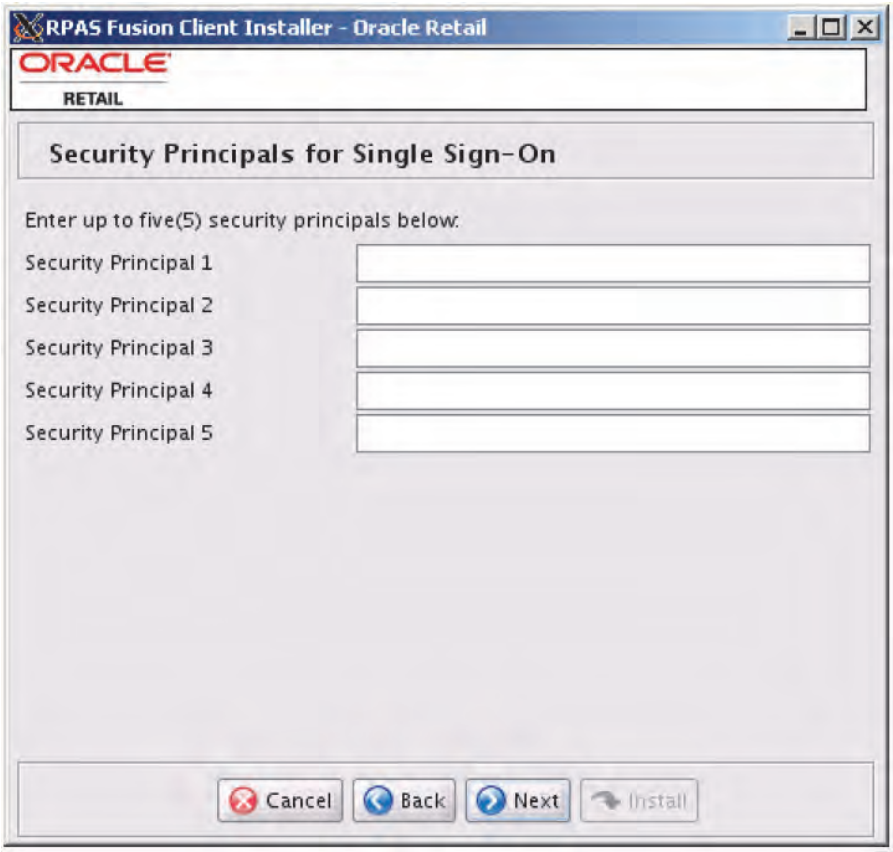
Figure 5–10 Application Server Details Window



12. The Security Principals for Single Sign-On window opens. Enter up to five enterprise user account names or user group names as described in Table 5–5. For additional information, refer to User Information.

Note: The Web deployment descriptors need to be configured to allow access pages to authenticated requests. During the application installation, the names entered here will be added to the Web deployment descriptor file (weblogic.xml) as `<principal-user>` under `<security-role-assignment>` tag. The RPAS Fusion Client application roles are mapped to the enterprise roles or groups in this deployment descriptor file.

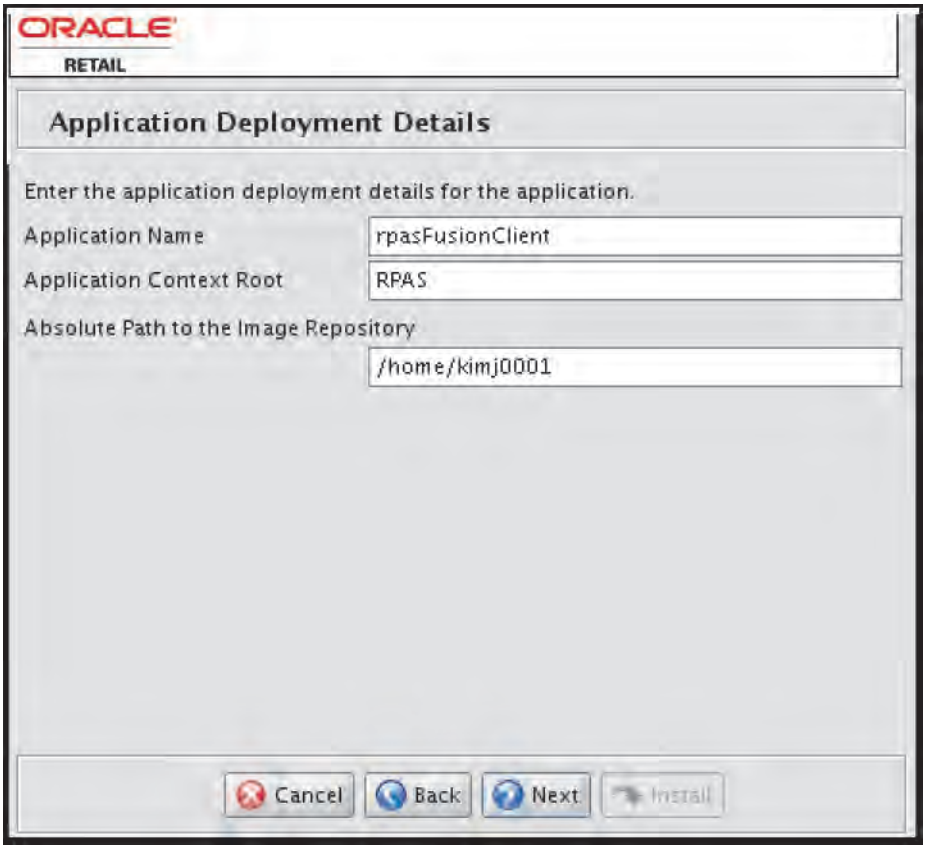
Figure 5–11 Security Principals for Single Sign-On



13. The Application Deployment Details window opens. Enter relevant information for the following fields and click **Next**:

Field	Description
Application Name	Specify an application name. The RPAS Fusion Client will be deployed over the WebLogic Server with this name.
Application Context Root	Specify the context root for the application. Once deployed, the RPAS Fusion Client will be available on the Web browser using this context path. For example, if you set the context root to rav, you can access the application using the URL: `http://<hostname>:<port>/rav`.
Absolute Path to the Image Repository	Specify the location or a network path where the images used in the application are located.

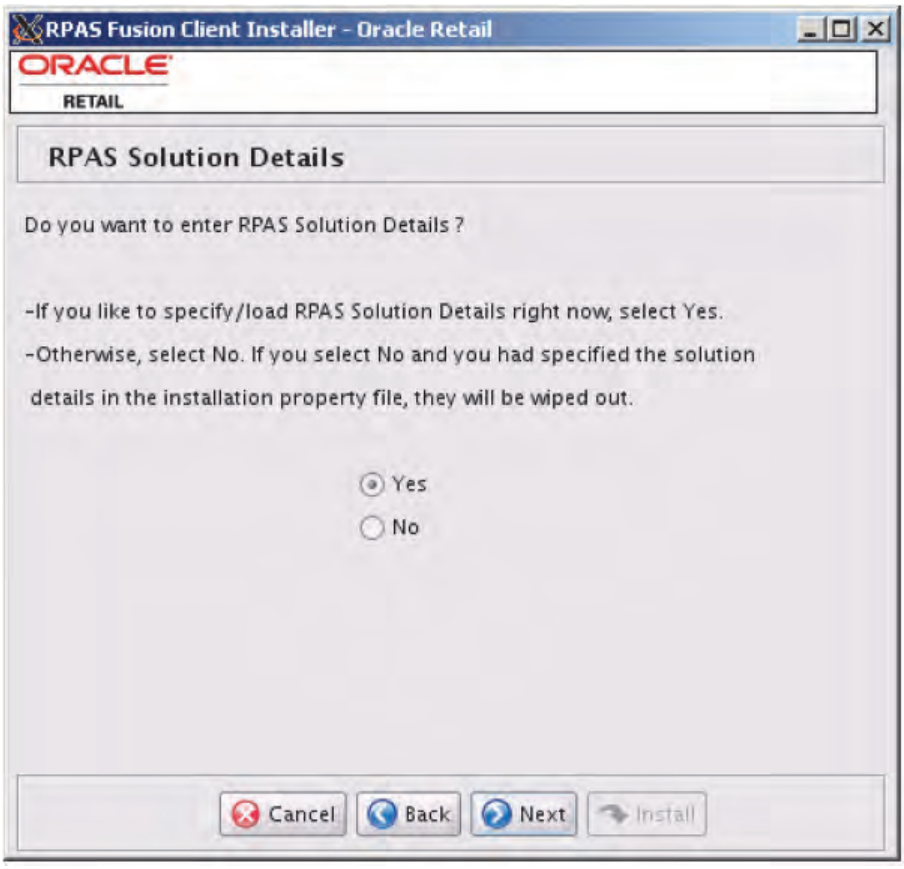
Figure 5–12 Application Deployment Details



14. The RPAS Solution Details (1) window opens. Select one of the following options and click **Next**:

    - Select **Yes** to enter RPAS Server and Domain details in the Installer. During the installation, the relevant RPAS Fusion Client configuration files will be updated based on the information you enter here. Go to Step 15.
    - Select **No** to skip adding the RPAS Server and Domain details and add them later manually. For more information on adding this configuration manually, refer to the *Oracle Retail Predictive Application Server Administration Guide for the Fusion Client*. Go to Step 16.

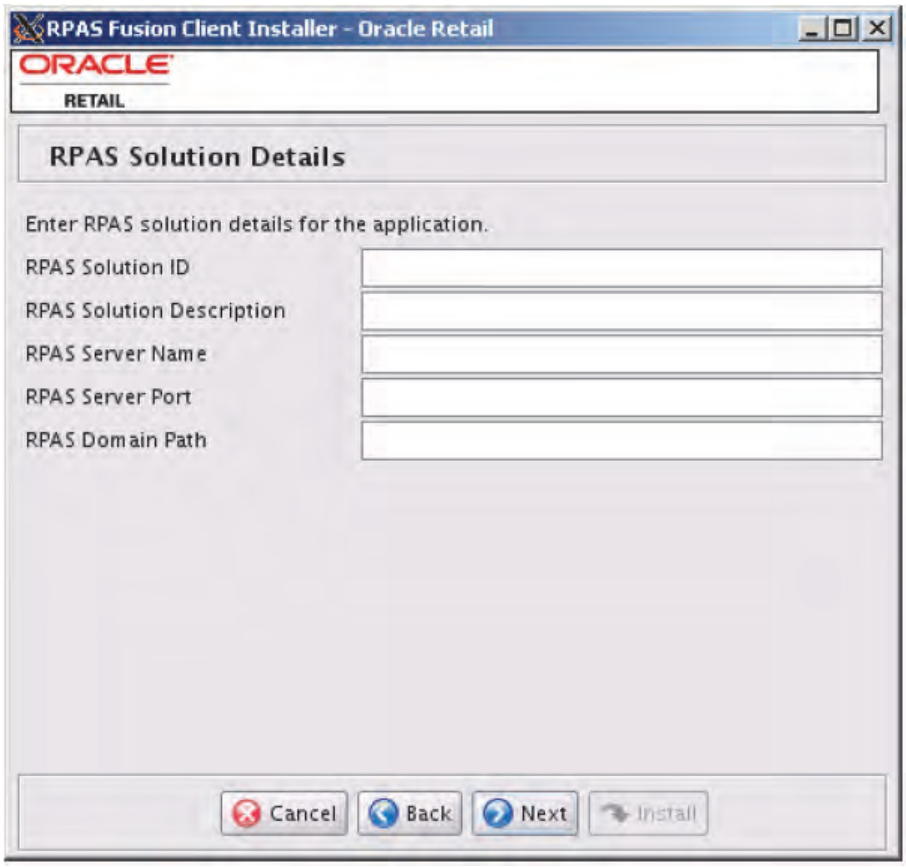
Figure 5–13 RPAS Solution Details (1)



15. The RPAS Solution Details (2) window opens with fields to collect RPAS Solution information. Enter relevant information for the following fields and click **Next**.

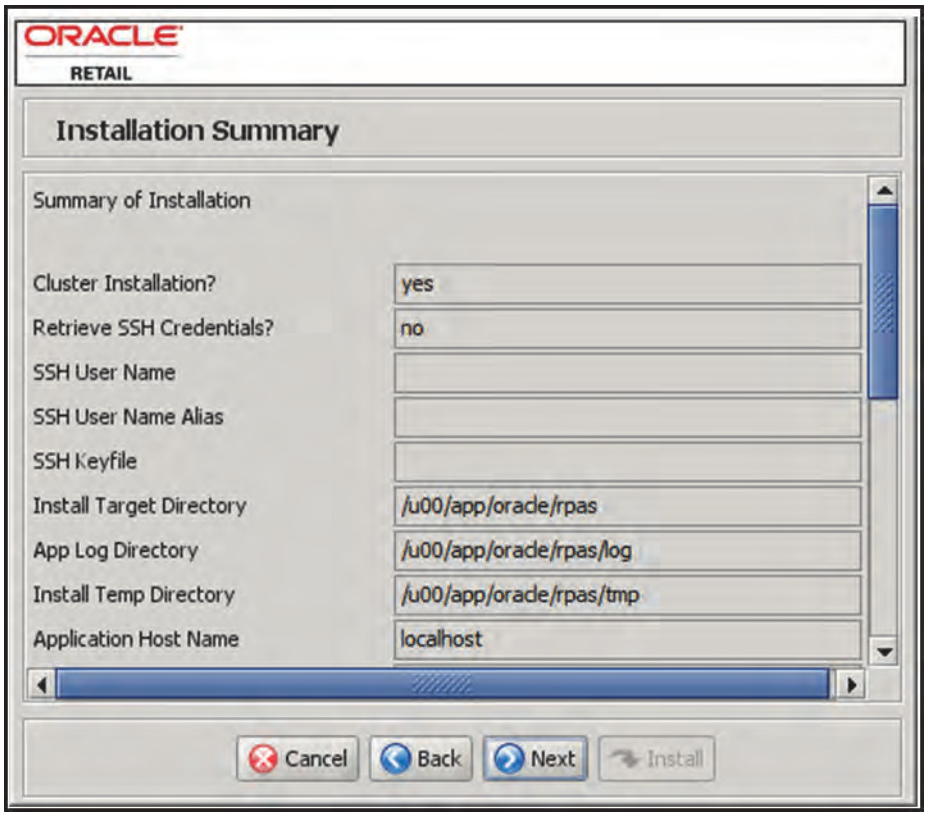
Field	Description
RPAS Solution ID	Specify the RPAS Solution ID for your RPAS application.
RPAS Solution Description	Specify the RPAS Solution Description which is displayed within the RPAS Fusion Client.
RPAS Server Name	Specify the host name where the RPAS infrastructure is installed.
RPAS Server Port	Specify the post associated with the RPAS installation.
RPAS Domain Path	Specify the location where the RPAS domain is installed. **Note:** This must be a simple domain or a global domain. You should not specify a local domain within a global domain environment.

Figure 5–14 RPAS Solution Details (2)



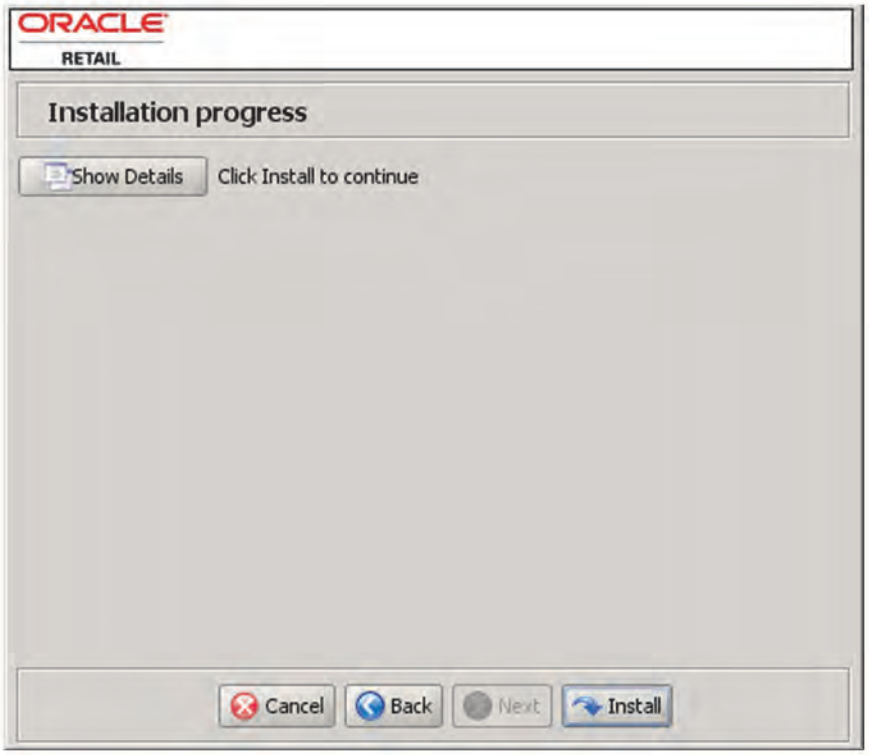
16. The Installation Summary window opens. Review the installation summary and click **Next**.

Figure 5–15 Installation Summary



17. The Installation Progress Window window opens. Click **Install** to start the installation.

Figure 5–16 Installation Progress Window



18. After the installation is complete, click **Exit** to close the Installer.
19. Restart the WebLogic server, and then verify that the application is accessible over the network. In a Web browser, enter the following URL in the Address bar, and press **Enter**:

    `http://<hostname>:<portnumber>/<contextroot>`

    Note: In the previously listed URL, `<hostname>`, `<portnumber>`, and `<contextroot>` represent the host name, port, and context root you set up for the application during the installation. You must specify the relevant values in the Address bar.

Post-Installation Tasks

Note: Refer to chapter, "Creating a Multi-solution Taskflow" in the *Oracle Retail Predictive Application Server Configuration Tools User Guide* for information about the Multi-solution Taskflow.

Before you log on to the application, you must set up the Fusion Client based on your business need. This includes the following tasks:

- Configuring External Authentication
- Setup SSL
- Clear the Browser Cache

- Review the RPAS Configuration Property Files (optional)
- Set Up Single Sign-On (SSO) (optional)
- Review any Troubleshooting issues
- Set up the configuration properties file, pivot table styles, and layout and formatting. For more information, refer to the *Oracle Retail Predictive Application Server Administration Guide for the Fusion Client*.
- Set up the RPAS solution to work with the RPAS Fusion Client. For more information, refer to the installation guide of the relevant RPAS solution.

Configuring External Authentication

There are three types of external authentication, one that supports SSO and the other is standalone authentication (non-SSO). The Weblogic Server can be attached to a standalone user management system such as Oracle Internet Directory (OID), or it can be configured to use an SSO system.

The third type of external authentication also has Weblogic attached and is not used for production, but is useful for development and demonstration purposes.

Authentication (SSO)

The RPAS Fusion Client is certified for perimeter authentication using Oracle SSO 11g

Standalone Authentication (Non-SSO)

Users and groups can be set up in a user management system such as OID or even Weblogic's embedded LDAP server. The corresponding authentication provider needs to be configured within the Weblogic Server default security realm called *myrealm*.

Weblogic has out of the box support for several LDAP-based authentication systems including OID. The configuration of the authentication provider can be conveniently done within the Weblogic Admin Console. This configuration provides Weblogic with information about the user management system. For example, in the case of OID one must specify its host name and port, userid and password needed to access it, and the root location in the LDAP directory tree where users and groups can be found. When users access the application for the first time, Weblogic redirects the user to a login page. The entered User ID and Password are validated by the authentication provider within Weblogic against the user management system.

The enterprise users and groups specified during the Fusion Client installation need to be created within the user management system.

Note: For more information, refer to the Weblogic documentation for details on configuring authentication providers.

External Authentication Process

The following table provides high level process steps for configuring external authentication and whether or not it applies to SSO, non-SSO, or both.

Process Steps	Authentication Type
Create an 11g WebGate definition in Oracle Access Manager. Specify the base URL that points to the Oracle HTTP Server (OHS) instance that has the WebGate module plugged in. Ensure that certain application URLs are excluded from authorization as listed in "URL Protection Rules". **Note:** For performance and high availability reasons it may be necessary to deploy multiple OHS instances with a load balancer in front. In this case specify the base URLs for all the OHS instances in the WebGate definition.	SSO
Configure the mod_wl_ohs module on the OHS instance to tunnel requests to the application servers on which the Fusion Client is deployed. (Do it on each of the OHS instances, if using multiples.)	SSO
Configure the OAM identity asserter and the OID authentication provider on the default security realm on the application servers to communicate with the OID instance.	SSO
Create the same users in the Oracle Identity Management (IdM) as in RPAS domain. These are referred to as *enterprise* users.	SSO and non-SSO
Define an RPAS specific enterprise role or group. This assists in providing all your enterprise users with RPAS access at one go (since the user principal mapping done during the install becomes much simpler). Make all the users members of this role or group.	SSO and non-SSO
Configure an authentication provider in Weblogic. Specify *sufficient* as the control flag value. This provider should be of a type that is capable of interacting with the IdM. Weblogic comes with out of the box support for several IdM types, for example OID.	Non-SSO

URL Protection Rules

By default the following URLs are protected:

Protected URLs
/
/.../*

Exclude the following URLs:

URLs to Excude
/.../*.gif
/.../*.png
/.../images/*
/.../rpas_exit.jsp
/.../*.js
/.../*.css
/.../*.html

Setup SSL

This section describes two-way SSL configuration on the RPAS server.

About SSL and RPAS

RPAS supports all SSL configurations which include:

- One-way SSL
- Two-way SSL
- SSL without authentication

> **Note:** The Fusion Client only supports two-way SSL.

One-way and two-way SSL require key store, trust store, or both to manage certificates. A key store contains a private key and its corresponding public certificate chain. A trust store contains trusted public certificates and certificate chains.

The RPAS server uses Oracle Wallet for its key store and trust store. The same wallet is used for both the Key Store and Trust Store. Oracle Wallet is managed by a command line utility called orapki which is included in the RPAS installation.

The Fusion Client uses a Java Key Store (JKS) to act as its Key Store and Trust Store. The Certificate Store and Trust Store may be stored in separate JKS files. JKSs are managed by the keytool utility which is included in the standard JDK.

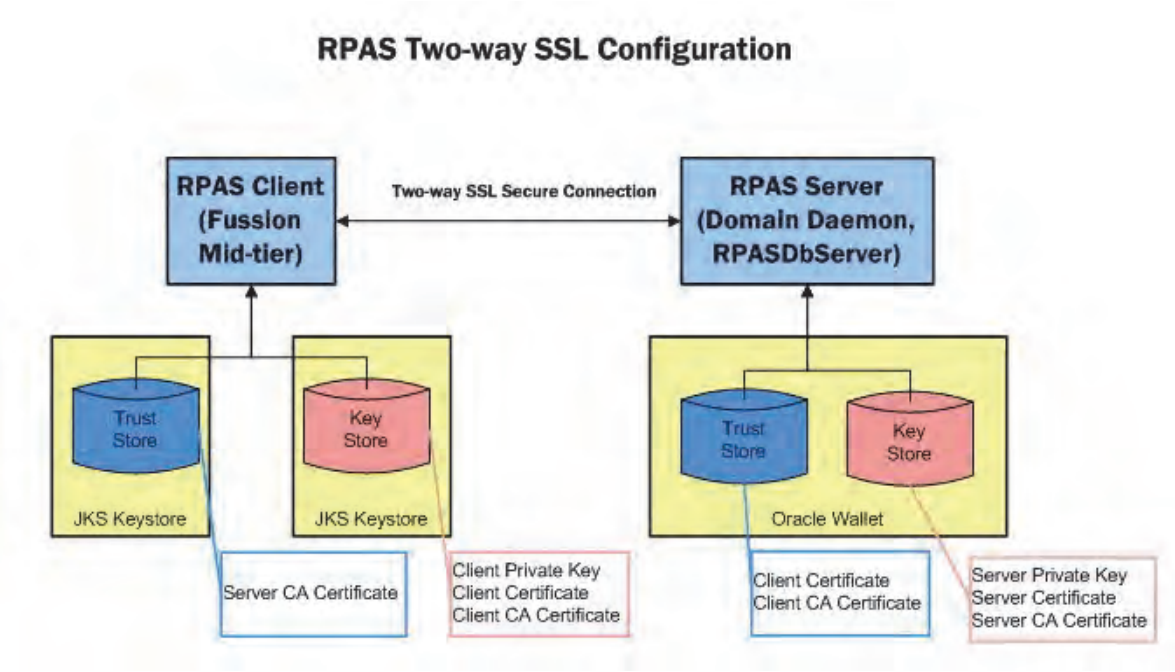
Oracle Wallet and JKS stores cannot be used interchangeably, though the orapki tool can be used to convert between them.

To enable SSL in RPAS, two command line options are provided for the Domain Daemon. One is for the SSL type and the other is for the Oracle Wallet location which is optional for some SSL types. When the RPAS Classic Client or the mid-tier process of the Fusion Client connects to the Domain Daemon, it detects the type of SSL for the connection and automatically chooses the appropriate handshake protocol. The client may need to configure its own certificate store in advance. RPAS DB Server inherits the SSL setup from the Domain Daemon and no additional configuration is needed.

Two-way SSL

This section describes two-way SSL as illustrated in Figure 5–17.

Figure 5–17 Configuration of Two-way SSL for RPAS



Two-way SSL authenticates both the server and the client. Both sides must have a key store and a trust store. RPAS server uses one Oracle Wallet for both stores. Two-way SSL is not supported in the Classic Client. For Fusion client mid-tier, both the trust store and the key store are in the JKS format.

The trust store must contain the CA certificate or self-signed root certificate for the other side so as to enable mutual authentication. In addition, the trust store of the server must contain the client certificate so that it can recognize and authorize that particular client.

Note: For additional information on SSL, refer to the *Oracle Retail Predictive Application Server Administration Guide for the Fusion Client*.

Creating a Self-signed Root Certificate

Perform the following steps to create a self-sign root certificate. The same root certificate can be used to generate both server and client certificates.

Note: Under Cygwin environments on Windows, the path of the wallet must be in Windows format and not Cygwin format. For example, it must be:

`C:/wallets/root, not /cygdrive/c/wallets/root`.

---

1. Create an Oracle wallet using this format: orapki wallet create -wallet {root_wallet_directory} -pwd {root_wallet_password}

Example 5–1 Oracle Wallet

```
orapki wallet create -wallet C:/wallets/root -pwd rootpass1
```

2. Generate a private key and a self-signed root certificate using this format: orapki wallet add -wallet {root_wallet_directory} -keysize {key_len} -dn {root_dn} -self_signed -validity {validity_days} -pwd {root_wallet_password}

> **Note:** Oracle OSSA requires that the minimum key size is 2048.

Example 5–2 Private Key and a Self-signed Root Certificate

```
orapki wallet add -wallet C:/wallets/root -keysize 2048 -dn "cn=rpas_qa_
ca,dc=us,dc=oracle,dc=com" -self_signed -validity 3650 -pwd rootpass1
```

3. Export the root certificate chain to a file for later use using this format: orapki wallet export_trust_chain -wallet {root_wallet_directory} -certchain {root_cert_chain_file} -dn {root_dn} -pwd {root_wallet_password}

Example 5–3 Root Certificate Chain

```
orapki wallet export_trust_chain -wallet C:/wallets/root -certchain
C:/wallets/root_chain.txt -dn "cn=rpas_qa_ca,dc=us,dc=oracle,dc=com" -pwd
rootpass1
```

Two-way SSL Setup

The process of two-way SSL configuration on the RPAS server is described in the following table.

Step	Process	Reference
1.	Set up a server key store. One Oracle wallet can act as both key and trust stores.	Setting Up a Server Key Store
2.	Import certificates.	Import Certificates
3.	Start the Domain Daemon with the appropriate options.	Start Domain Daemon with Two-way SSL Options
4.	Set up a client key store. One Oracle wallet can act as both key and trust stores.	Setting Up a Client Key Store
5.	Set up a trust store in the JKS format.	Setting Up a Trust Store in the JKS Format

Setting Up a Server Key Store

Use the following instructions to set up a server key store.

1. Create an Oracle Wallet with Auto Login using this format: orapki wallet create -wallet {server_wallet_directory} –auto_login -pwd {server_wallet_password}

   Auto-login means that the wallet can be read without a password. It is generally protected by file system permission. The default file permission of the wallet is 0300 which means that it is only accessible by the owner.

> **Note:** Oracle OSSA requires that the minimum key size is 2048.

Example 5–4 Oracle Wallet with Auto Login

```
orapki wallet create -wallet C:/wallets/server –auto_login -pwd serverpass1
```

2. Generate a private key using this format: orapki wallet add -wallet {server_wallet_directory} -keysize {key_len} -dn {server_dn} -pwd {server_wallet_password}

   Note: Oracle OSSA requires that the minimum key size is 2048.

Example 5–5 Private Key

```
orapki wallet add -wallet C:/wallets/server -keysize 2048 -dn "cn=rpas_qa_
server,dc=us,dc=oracle,dc=com" -pwd serverpass1
```

3. Export a certificate request using this format: orapki wallet export -wallet {server_wallet_directory} -dn {server_dn} -request {server_cert_req_file} -pwd {server_wallet_password}

Example 5–6 Certificate Request

```
orapki wallet export -wallet C:/wallets/server -dn "cn=rpas_qa_
server,dc=us,dc=oracle,dc=com" -request C:/wallets/server_cert_req.txt -pwd
serverpass1
```

4. Create the server certificate.

   Note: For additional information, refer to the section, "Creating a Self-signed Root Certificate".

   a. If a third-party Certificate Authority (CA) is used, send the server certificate request file ({server_cert_req_file}) to the CA. The CA sends back a certificate for the server (referred to as {server_certificate_file}) along with the public certificate of the CA (referred to as {root_cert_chain_file}).

   b. If the self-signed root certificate is used, run the following command:

      orapki cert create -wallet {root_wallet_directory} -request {server_cert_req_file} -cert {server_certificate_file} -validity {validity_days} -pwd {root_wallet_password}

Example 5–7 Self-signed Root Certificate

```
orapki cert create -wallet C:/wallets/root -request C:/wallets/server_cert_req.txt
-cert C:/wallets/server_cert.txt -validity 3650 -pwd rootpass1
```

5. Import the CA or self-signed certificate into the wallet using this format: orapki wallet add -wallet {server_wallet_directory} -trusted_cert -cert {root_cert_chain_file} -pwd {server_wallet_password}

Example 5–8 Import Certificate

```
orapki wallet add -wallet C:/wallets/server -trusted_cert -cert C:/wallets/root_
chain.txt -pwd serverpass1
```

   Note: For third-party CA, the public certificate chain may contain more than one certificate. These certificates need to be imported one by one starting from the top of the chain.

6. Import the server certificate into the wallet using this format: orapki wallet add -wallet {server_wallet_directory} -user_cert -cert {server_certificate_file} -pwd {server_wallet_password}

Example 5–9 Import the Server Certificate

```
orapki wallet add -wallet C:/wallets/server -user_cert -cert C:/wallets/server_
cert.txt -pwd serverpass1
```

Now the key store is ready for the server.

Import Certificates

For every client connecting to the RPAS server using two-way SSL, their certificates must be imported into the server wallet as trusted certificates. Use the following command:

```
orapki wallet add -wallet {server_wallet_directory} -trusted_
cert -cert {client_cert_file} -pwd {server_wallet_password}
```

> **Note:** If the client certificates are from different CA other than the ones already in the server wallet, the CA certificates must be imported first.

Start Domain Daemon with Two-way SSL Options

To start the Domain Daemon with two-way SSL support, use the following command line options:

DomainDaemon -port portNum -ssl 2 -wallet file:<walletLocation> start

The <walletLocation> is the absolute path to the directory of the Oracle Wallet. It cannot be a relative path.

Example 5–10 Domain Daemon with Two-way SSL Support

```
DomainDaemon -port 12348 -ssl 2 -wallet file:C:/wallets/server start
```

> **Note:** There is an `-ssl 4` option, whereby the SSL certificates are used only for mutual authentication but no encryption of data is done. This is an option provided for customers who have deployed all the applications behind a firewall and are not concerned about unauthorized interception of the data exchanged between the Fusion Client and the RPAS Server.
>
> The syntax for starting up DomainDaemon is the same; just replace `-ssl 2` with `-ssl 4`.
>
> For additional infomation on SSL options, refer to SSL Options.

Setting Up a Client Key Store

Use the following instructions to set up a client key store.

1. Create an Oracle Wallet with Auto Login using this format: orapki wallet create -wallet {client_wallet_directory} –auto_login -pwd {client_wallet_password}

Example 5–11 Oracle Wallet with Auto Login

```
orapki wallet create -wallet C:/wallets/client –auto_login -pwd clientpass1
```

2. Generate a private key using this format: orapki wallet add -wallet {client_wallet_directory} -keysize {key_len} -dn {client_dn} -pwd {client_wallet_password}

> **Note:** Oracle OSSA requires that the minimum key size is 2048.

Example 5–12 Private Key

```
orapki wallet add -wallet C:/wallets/client -keysize 2048 -dn "cn=rpas_qa_
client,dc=us,dc=oracle,dc=com" -pwd clientpass1
```

3. Export a certificate request using this format: orapki wallet export -wallet {client_wallet_directory} -dn {client_dn} -request {client_cert_req_file} -pwd {client_wallet_password}

Example 5–13 Certificate Request

```
orapki wallet export -wallet C:/wallets/client -dn "cn=rpas_qa_
client,dc=us,dc=oracle,dc=com" -request C:/wallets/client_cert_req.txt -pwd
clientpass1
```

4. Create the client certificate.

> **Note:** For additional information, refer to the section, "Creating a Self-signed Root Certificate".

   a. If a third-party Certificate Authority (CA) is used, send the client certificate request file ({client_cert_req_file}) to the CA. The CA sends back a certificate for the client (referred to as {client_certificate_file}) along with the public certificate of the CA (referred to as {root_cert_chain_file}).

   b. If the self-signed root certificate is used, run the following command:

      orapki cert create -wallet {root_wallet_directory} -request {client_cert_req_file} -cert {client_certificate_file} -validity {validity_days} -pwd {root_wallet_password}

Example 5–14 Self-signed Root Certificate

```
orapki cert create -wallet C:/wallets/root -request C:/wallets/client_cert_req.txt
-cert C:/wallets/client_cert.txt -validity 3650 -pwd rootpass1
```

5. Import the CA or self-signed certificate into the wallet using this format: orapki wallet add -wallet {client_wallet_directory} -trusted_cert -cert {root_cert_chain_file} -pwd {client_wallet_password}

Example 5–15 Import Certificate

```
orapki wallet add -wallet C:/wallets/client -trusted_cert -cert C:/wallets/root_
chain.txt -pwd clientpass1
```

> **Note:** For third-party CA, the public certificate chain may contain more than one certificate. These certificates need to be imported one by one starting from the top of the chain.

6. Import the client certificate into the wallet using this format: orapki wallet add -wallet {client_wallet_directory} -user_cert -cert {client_certificate_file} -pwd {client_wallet_password}

Example 5–16 Import the Client Certificate

```
orapki wallet add -wallet C:/wallets/client -user_cert -cert C:/wallets/client_
cert.txt -pwd clientpass1
```

Setting Up a Trust Store in the JKS Format

A trust store in the JKS format must be created. Then the CA or self-signed root certificate of the server certificate should be imported into the trust store.

Use the following instructions to set up a a trust store in the JKS format.

1. Import the CA or self-signed certificate for the server certificate into the wallet using this format: orapki wallet add -wallet {client_wallet_directory} -trusted_cert -cert {root_cert_chain_file_for_the_server} -pwd {client_wallet_password}

> **Note:** This step can be skipped if both client and server certificates are issued by the same CA or generated from the same self-signed root certificate.

Example 5–17 Import the CA or Self-signed Certificate

```
orapki wallet add -wallet C:/wallets/client -trusted_cert -cert C:/wallets/root_
chain.txt -pwd clientpass1
```

2. Convert the Oracle Wallet to JKS format using this format: orapki wallet pkcs12_to_jks -wallet {client_wallet_directory} -pwd {client_wallet_password} -jksKeyStoreLoc {key_store_file} -jksKeyStorepwd {key_store_password} -jksTrustStoreLoc {trust_store_file} -jksKeyStorepwd {trust_store_password}

> **Note:** The password, `jksKeyStorepwd`, must be the same as what was entered into the Weblogic domain credential store using the credential entry alias *fckey*.

Example 5–18 Convert the Oracle Wallet to JKS Format

```
orapki wallet pkcs12_to_jks -wallet C:/wallets/client -pwd clientpass1
-jksKeyStoreLoc testkey.jks -jksKeyStorepwd welcome1 -jksTrustStoreLoc
testtrust.jks -jksTrustStorepwd welcome1
```

3. Finally, copy the files `testkey.jks` and `testtrust.jks` as `fckey.jks` and `fctrust.jks` into the *idstores* directory under the Fusion Client installation.

> **Note:** The `fckey.jks` password is the client keystore password as requested in Figure 5–10, "Application Server Details Window".

Now the client key store setup is complete.

Clear the Browser Cache

After the Fusion Client has been upgraded, ensure that all users clear their browser cache.

Review the RPAS Configuration Property Files

If you install the RPAS Fusion Client over an existing RPAS Fusion Client environment, the installer updates the existing `config/config.properties` and `config/rpas/rpasConfig.properties` files. If you modified any property values in these files, they are overwritten by the files found in the installer. However, the installer backs up the existing files and creates a report on the changed property values and any new properties added that did not exist in the previous version.

Example 5–19 RPAS Configuration Property Files

Following is an example of the config.properties.

```
-rw-r--r--  1 build users  375 Jun  7 17:18 config.properties
-rw-r--r--  1 build users  401 Jun  7 16:44 config.properties.201106071642
-rw-r--r--  1 build users  258 Jun  7 16:44
config.properties.201106071642.mergeReport
```

In this example are the following components:

- `config.properties` is the new file
- `config.properties.201106071642` is the backup of the previous version of config.properties
- `config.properties.201106071642.mergeReport` contains what was added, updated, or removed between `config.properties.201106071642` and `config.properties`.

You can review the changes and restore any property value if needed.

Set Up Single Sign-On (SSO)

RPAS can be set up on an Oracle SSO infrastructure that enables users who are already connected and authenticated to the Oracle SSO to directly access the RPAS Fusion Client or RPAS Classic Client Web Deployment. For more information about SSO, refer to "Appendix D: Oracle Single Sign-On (SSO)".

To set up SSO, perform the following steps:

1. Set up the Identity Management Infrastructure for SSO. Install the following components:
   - Oracle Identity Management (OID) LDAP server. For more information, refer to the *Oracle Fusion Middleware Installation Guide for Oracle Identity Management 11g Release 1 (11.1.1)*.

2. An Oracle Internet Directory repository configured to be used by the LDAP server. (OID uses an Oracle Database as the back end.) Ensure that you have a WebLogic domain extended with the JRF template. This was already done before you installed the RPAS Fusion Client. For more information, refer to Setting Up the WebLogic Server.
3. Skip this step if you are setting up SSO for RPAS Classic Client Web Deployment.

   During the RPAS Fusion Client installation, specify that you want to use the SSO feature to log on to the application and specify the SSO users or groups. For more information, refer to the Installation Properties File Parameter Reference section or see Steps 12, 17, and 18 in the section, Graphical or Text Mode.
4. Install the Oracle Fusion Middleware 11g Web Tier Utilities referring to the *Oracle Fusion Middleware Installation Guide for Oracle Web Tier* guide.

If you are setting up an SSO environment, continue to Setting Up an SSO Environment.

Setting Up an SSO Environment

For additional information, refer to "Appendix D: Oracle Single Sign-On (SSO)" and specifically, Figure D–1, "Single Sign-On Topology".

Perform the following steps if you are setting up an SSO environment:

1. Register the Oracle HTTP server (Web Tier) with the Oracle Access Manager server by configuring a Webgate plug-in. To do this, perform the following steps:
   a. From the Webgate installation, copy certain essential files over to the Web Tier installation. For more information, refer to the instructions at this address: `http://download.oracle.com/docs/cd/E14571_01/install.1111/e12002/webgate004.htm`.

      Note: Webgate needs operating system specific Gnu C Compiler (GCC) libraries to be available on the library load path. For Linux and Solaris you can obtain the library from `http://gcc.gnu.org/`. More details on this requirement can be found at the following address: `http://docs.oracle.com/cd/E14571_01/install.1111/e12002/webgate002.htm#CACGIGBB`.

   b. Create a Webgate definition using the Oracle Access Manager console (`http://<host-ip-addr>:<OAM-domain-port>/oamconsole`). The Webgate's base URL must point to the Web Tier server. This creates files under `<OAM Domain dir>/output` directory (`cwallet.sso` and `ObAccessClient.xml`).
   c. Copy those files from the web tier to: `Oracle_WT1/instances/instance1/config/OHS/ohs1/webgate/config`.
2. From the Oracle SSO server administrator, obtain the OID information, such as the TCP/IP address and port, whether SSL is used as a transport mechanism, and the realm name. In addition, obtain an administrative login and password, such as the one used by the orcladmin user.
3. Configure authentication providers in your Weblogic domain for SSO, by performing the following steps:
   a. If not already present, then copy `oamAuthnProvider.jar from the $MW_HOME/oracle_common/modules/oracle.oamprovider_11.1.1`

directory to the `/u00/webadmin/Oracle/Middleware/wlserver_10.3/server/lib/mbeantypes` directory.

b. Configure the OAM identity asserter using the instructions at the following address: `http://docs.oracle.com/cd/E14571_01/core.1111/e10043/osso.htm#CHDCDAIC`. Specifically, refer to the section "9.3.5.2.4 - Setting up providers for identity assertion."

c. Configure an OID authenticator so that all the roles are retrieved from OID for the user logged in through SSO. Following are the key parameters you need to enter in the provider-specific configuration tab:

Parameter	Enter:
Group Search Base	cn=Groups, dc=us,dc=*yrcmpny*,dc=com
User Search Base	cn=Users, dc=us,dc=*yrcmpny*,dc=com
User name attribute	uid
location	ipaddress:portnumber, for example 10.10.10.10:2345
bind dn	cn=<LDAP admin user name>
password	<LDAP admin user's password>

Note: Where *yrcmpny* is your company's name.

a. Ensure the three asserters are configured in the following order:

- OAM Identity Asserter: OPTIONAL
- OID Authenticator: SUFFICIENT
- DefaultAuthenticator: SUFFICIENT

b. Save and activate the changes.

c. Restart the WebLogic server.

4. Update the mod_wl_ohs.conf file to send requests to the WebLogic server. To update the mod_wl_ohs.conf file, perform the following steps:

a. Navigate to the location where the mod_wl_ohs_conf file exists and open it for editing. For example,

```
$ORACLE_INSTANCE/ config/ <COMPONENT_TYPE>/ <COMPONENT_NAME>
```

b. Update the file based on Example 5–20 and Example 5–21.

Example 5–20 Single WebLogic Instance

For a single WebLogic instance, specify:

```
<Location /console>
   SetHandler weblogic-handler
   WebLogicHost server1
   WeblogicPort 7001
</Location>
```

This forwards `/console` from the HTTP server to `/console` on the WebLogic Server with the host name and port number, server1:7001.

Example 5–21 WebLogic Instances in a Cluster

For WebLogic instances in a cluster, specify:

```
<Location /myServerURL>
   SetHandler weblogic-handler
   WebLogicCluster server1:7010,server2:7010
</Location>
```

This forwards `/myServerURL` from the HTTP server to `/myServerURL` on the WebLogic Clusters with the host names and port numbers, server1:7010 and server2:7010.

Note: In Example 5–20 and Example 5–21, server1 and server 2 are the host names used for illustrative purposes. Ensure that you use relevant host names, port numbers, and context roots based on your implementation.

Oracle Linux on x86 Architecture

There is a known issue with the JDK running on an Oracle Linux server with Intel x86 processors. For the steps to avoid this error, refer to StringIndexOutOfBoundsException in Oracle Linux on x86 Architecture.

Troubleshooting

This section lists possible solutions for some issues that may occur when using the application.

WebLogic Ulimit Error

An error may occur when starting the WebLogic server if the limit for open files is set too low:

```
<Log Management> <BEA-170019> <The server log file /u01/Oracle/Middleware/user_
projects/domains/domain1/servers/AdminServer/logs/AdminServer.log is opened. All
server side log events will be written to this file.>
Unhandled exception
Type=Segmentation error vmState=0x00040000
J9Generic_Signal_Number=00000004 Signal_Number=0000000b Error_Value=00000000
Signal_Code=00000033
Handler1=09001000A049F450 Handler2=09001000A0495F70
R0=0000000000000001 R1=000000011757E200 R2=09001000A0340048 R3=09001000A0340178
R4=0000000000000234 R5=0000000000000000 R6=800000000000F032 R7=3000000000000000
R8=000000000012F7D0 R9=0000000000000000 R10=0000000000000000 R11=F0000000301D3600
R12=090000000154ABB0 R13=0000000117588800 R14=0000000116635CA0
R15=0000000116599D00
```

To avoid this issue, set the ulimit to a larger number, at least 8192, by issuing the following command:

```
ulimit -u 8192
```

Error Occurs When Users Access the Charting Feature in the RPAS Fusion Client

If users attempt to access the application from a system that does not have a connected Display/Video card, they may encounter the following error message when they try using the charting feature for the first time:

```
Sun.awt.X11GraphicsEnvironment (initialization failure)
For more information, please see the server's error log for an entry beginning
with: Server Exception during PPR, #
```

To avoid this issue, edit the WebLogic Startup script with the java.awt.headless parameter using the following steps:

1. Navigate to the following location on the system where the application server is installed:

   ```
   <WEBLOGIC_DOMAIN_HOME>/bin/
   ```

2. In a text editor, open the startWebLogic.sh script for editing.

3. Append the following parameters to the set JAVA_OPTIONS = %SAVE_JAVA_OPTIONS% statement:

   ```
   -Djava.awt.headless=true
   ```

   After it is set up, the JAVA_OPTIONS statement appears as in the following example:

   ```
   set JAVA_OPTIONS=%SAVE_JAVA_OPTIONS% -Djava.awt.headless=true
   ```

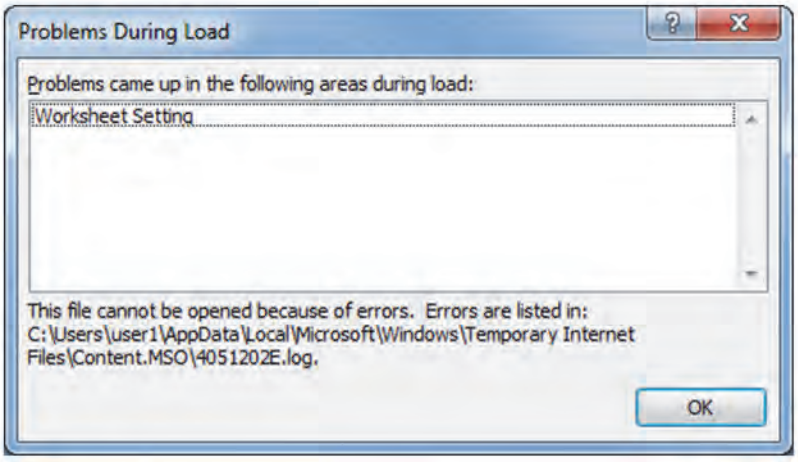
4. Save and close the file.

5. For the changes to take effect, restart the WebLogic Server.

Error Occurs When Users Export to Microsoft Excel in the RPAS Fusion Client

If users attempt to export to Microsoft Excel in the Fusion Client, they may encounter the error message shown in Figure 5–18

Figure 5–18 Microsoft Excel Error Message



This error message means that the Excel export file is corrupt due to a headless environment. In the server logs, the error message appears as follows:

```
ERROR view - java.lang.NullPointerException
java.lang.NullPointerException
        at javax.swing.MultiUIDefaults.getUIError(MultiUIDefaults.java:133)
        at javax.swing.UIDefaults.getUI(UIDefaults.java:741)
        at javax.swing.UIManager.getUI(UIManager.java:1002)
        at javax.swing.JPanel.updateUI(JPanel.java:109)
        at javax.swing.JPanel.<init>(JPanel.java:69)
        at javax.swing.JPanel.<init>(JPanel.java:92)
        at javax.swing.JPanel.<init>(JPanel.java:100)
```

To avoid this issue, edit the WebLogic Startup script with the java.awt.headless parameter using the following steps:

1. Navigate to the following location on the system where the application server is installed:

   `<WEBLOGIC_DOMAIN_HOME>/bin/`

2. In a text editor, open the startWebLogic.sh script for editing.
3. Append the following parameters to the set `JAVA_OPTIONS = %SAVE_JAVA_OPTIONS%` statement:

   `-Djava.awt.headless=true`

   After it is set up, the JAVA_OPTIONS statement appears as the following example:

   `set JAVA_OPTIONS=%SAVE_JAVA_OPTIONS% -Djava.awt.headless=true`

4. Save and close the file.
5. For the changes to take effect, restart the WebLogic Server.

StringIndexOutOfBoundsException in Oracle Linux on x86 Architecture

If users attempt to access the application from a system that does not have a connected Display/Video card, they may encounter the following error message when they try using the charting feature for the first time:

```
StringIndexOutOfBoundsException in
org.apache.myfaces.trinidadinternal.style.util.CSSGenerationUtils
```

To avoid this issue, you must set up the WebLogic Startup script with the JVM option

-XX:-UseSSE42Intrinsics parameter. To do this, perform the following steps:

1. Navigate to the following location on the system where the application server is installed:

   `<WEBLOGIC_DOMAIN_HOME>/bin/`

2. In a Text Editor, open the startWebLogic.sh script for editing.
3. Append the following parameters to the set JAVA_OPTIONS = $SAVE_JAVA_OPTIONS statement:

   `-XX:-UseSSE42Intrinsics`

   After set up, the JAVA_OPTIONS statement appears like the following example:

   `set JAVA_OPTIONS=$SAVE_JAVA_OPTIONS -XX:-UseSSE42Intrinsics`

4. Save and close the file.

5. Remove the cached CSS file, for example:

   ```
   $APP_TMP_
   FOLDER/public/adf/styles/cache/blafplus-desktop-ezog8j-en-ltr-gecko-1.9.1.8-cmp
   .css
   ```

6. For the changes to take effect, restart the WebLogic Server.
7. Clear the browser cache.

6

Installing and Configuring the RPAS Classic Client

This section describes the installation of the RPAS Classic Client on Windows machines, and describes how to configure the client to connect to a domain.

Make RPAS Classic Client Files Generally Accessible

Perform the following procedure to make the RPAS Classic Client available.

1. Create a directory on the network from where users will install the RPAS Classic Client.

   The location and the name of the directory are up to the system administrator's preferences. This directory is henceforth referred to as the `[RPASCLIENT]` directory.

2. Copy the files from the following directory on the server:

   `[RPAS Installation]/Client`

   to the `[RPASCLIENT]` directory.

Installing the RPAS Classic Client

The RPAS Classic Client installation procedure is the same for all of the RPAS applications. Perform the following procedures to install the application on a PC.

1. Run the setup.exe file located in the [RPASCLIENT] directory on the network.
2. The welcome page is displayed. Follow the installation procedures as prompted.

   The setup program exits after the installation is complete.

Configuration

After creating an RPAS domain and starting the DomainDaemon (refer to the *Oracle Retail Predictive Application Server Administration Guide for the Classic Client*), you must configure the RPAS Classic Client to connect to the domain on a server. The eConfigure utility is used to create this connection.

For information about eConfigure, refer to the eConfigure section in the *Oracle Retail Predictive Application Server Administration Guide for the Classic Client*.

Part II

Patch Installation

Part II of this guide details the steps needed to perform a patch installation of RPAS.

Part II contains the following chapters:

Chapter 8, "RPAS Package Extraction"

Chapter 9, "RPAS Server Patch Installation"

Chapter 10, "RPAS Fusion Client Patch Installation"

Chapter 11, "RPAS Classic Client Patch Installation"

For information about a full installation, refer to Full Installation

Upgrading Process

Releases earlier than RPAS 13.3 have special considerations that need to be followed when upgrading. Previous upgrade instructions do not apply. It is very important that you follow the process as detailed in the following table.

The RPAS Upgrade process is dependent upon your current RPAS version.

Current Version	Upgrade Process
Pre-12.1	At the time of the 13.3.1 release, Oracle Retail is aware of customer implementations that are still lower than version 12.1. Oracle Retail advises such customers to be sure to follow the process outlined in the 12.1 version of the *Oracle Retail Predictive Application Server Installation Guide* to convert their pre-12.1 domain to a post-12.1 domain. Fundamental changes have been made to RPAS's storage layer, and pre-12.1 domains are not upgradable to 13.3 domains simply with the use of the upgradeDomain utility. After following the upgrade instructions to convert the environment to 12.1, customers can then continue with an upgrade to 13.3.1, which also has special instructions as listed in the following row.
Pre-13.3	RPAS 13.3.1 requires a special upgrade process even if you are on major version 13. After installing the code described in "Part II: Patch Installation" of this guide, proceed to either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*. The chapter, "Building and Upgrading Domains ", details the full process to convert and upgrade your domain environment to be compatible with RPAS 13.3.1.
13.3 and later	If you are already using RPAS 13.3, there is no special upgrade process to follow. Continue the regular patch installation as described in "Part II: Patch Installation" of this guide.

7

RPAS Classic Client Web Deployment

The RPAS Classic Client can be deployed through traditional installation or through Web-based environments. This chapter describes the RPAS Web deployment installation process.

> **Note:** Accessing RPAS through a Web-based deployment is different from the RPAS Fusion Client. For more information on the Fusion Client, refer to Chapter 5, "Installing the RPAS Fusion Client".

Web-based deployment allows you to perform the following:

- Use a Web browser to install the RPAS Classic Client application to the user's computer.
- Launch the RPAS Classic Client when it has already been installed.
- Reinstall the RPAS Classic Client when an updated version is available.
- Use the RPAS Web Launch applet to facilitate In-Context Launch integration.

For the supported components used for web deployment of the Classic Client, refer to Table 1–2, " RPAS Classic Client Hardware and Software Requirements" .

These instructions assume that the previously specified software has been properly installed and configured. Consult the documentation of each component for installation and configuration information, as well as hardware and software requirements.

For the RPAS Web deployment to function properly, users must have sufficient access to their PCs (typically administrator rights) which allow them to install software, unless the administrator configures the applet to launch only preinstalled RPAS Classic Client. Specifically, they need permission to write into the Windows Registry.

Installation and Configuration Process Overview

The following is an overview of the process that must be followed to install RPAS for Web deployment.

- Install the RPAS Web Application. This installation is completed onto the Web server and involves two components that are included with the RPAS archive (RPAS.war or RPAS_osso.war, and RPASWebData.tar).
- Install multiple versions of RPAS Classic Client files on Web server (as needed).
- Configure the RPAS Servlet by using the deployment descriptor web.xml to specify servlet properties.

- Configure Oracle SSO for RPAS Web application (if Oracle SSO is used).
- Start the RPAS Web Configuration Utility. Using the URL of the RPAS Web Launch application, administrators and users follow this process to log in to the system.
- Configure Web Launch and Web Tunneling: using the Enterprise Configuration component of the Administration Console, the administrator indicates whether Web tunneling is to be used.
- Perform other Web client administration activities. Once the Web deployment environment is prepared, additional configuration and administration activities, such as domain configuration and managing administrative users, may need to be performed.

Installing the RPAS Web Application

Installing the RPAS Web Application consists of the following procedures:

- Preparing Your Environment
- Installing the necessary files and configuring the environment based on your type of installation. Three different processes may be used for RPAS Web deployment:
  - Installing on Oracle Application Server with SSO Support
  - Installing on Oracle Application Server without SSO Support
  - Installing on WebLogic Server with SSO Support
  - Installing on WebLogic Server without SSO Support
  - Installing on Apache Tomcat (a standalone server that is not part of the SSO infrastructure)
- Configuring the RPAS Servlet
- Configuring and Administering the Web Application

Preparing Your Environment

Perform the following procedure to prepare your environment to install t he RPAS web application.

1. Log in to the UNIX server and determine where the RPAS Web files will be installed. A minimum of 50 MB disk space available is required for the application installation files. More space may be needed if multiple versions of RPAS Classic Client are supported on the Web server.
2. Copy the RPAS Web files (RPAS.war, RPAS_osso.war and RPASWebData.tar), located in [RPAS Installation]/Web/ directory, to a newly created staging directory on the UNIX server. This directory will be referred to as STAGING_DIR.
3. Extract the RPASWebData.tar to the appropriate location. This location is referred to as [RPAS_WEB_DATA_DIR] in this document. If the Web server is running in a load balance environment with multiple servers, the RPASWebData files must be deployed to a network drive accessible to all Web server instances. A new directory RPASWebData/ and three subdirectories (client/, db/, and logs/) are created. Verify that the client directory has read permissions and that the db and logs directories have read and write permissions.
4. For each release of RPAS Classic Client, there are two files: buildNumber.txt and client.zip. These files are not part of RPAS Web files. They generally come with RPAS release package. The default installation location for the files is [RPAS_

WEB_DATA_DIR]/RPASWebData/client. If multiple client versions are to be supported, both files of each version must be placed under [RPAS_WEB_DATA_DIR]/RPASWebData/client/[VERSION] where [VERSION] is the version number of that release (for example, 13.3, 12.0.10).

5. Perform the necessary procedures based on your type of implementation.

Installing on Oracle Application Server with SSO Support

Perform the following procedure if you are implementing RPAS Web on an Oracle Application Server with SSO Support. This process consists of several steps:

Step 1: Meet the Prerequisites for RPAS Web Deployment Using Oracle Single Sign-On (OSSO)

Step 2: Deploying WAR File

Step 3: Configuring RPAS Web Launch

Step 4: Protect RPAS Root

Step 5: Setting RPAS Role for OSSO Logins

Step 1: Meet the Prerequisites for RPAS Web Deployment Using Oracle Single Sign-On (OSSO)

Make sure the following procedures have been performed before installing RPAS Web using OSSO:

1. Install the Oracle Identity Management 10g Infrastructure server, including the Oracle Internet Directory (OID) LDAP and OSSO components.
2. Register the RPAS HTTP server with the OSSO server with the ssoreg.sh script. The output of this command will be a binary file, denoted here as the osso.conf file. Copy osso.conf to the RPAS HTTP server:

   ```
   ORACLE_HOME/Apache/Apache/conf/osso/osso.conf
   ```

   Then, configure the RPAS HTTP Server to enable the mod_osso module. For further details, refer to the Oracle SSO documentation.
3. Obtain the OID information (TCP/IP address and port, whether SSL is used as a transport mechanism and the realm name) from Oracle SSO server administrator. You will also need an administrative login and password, such as that used by the orcladmin user.
4. Set the instance security provider for the RPAS OC4J to Oracle Identity Management (the OID server). You will need to use the information gathered in Step 3. Verify this by checking the file:

   ```
   ORACLE_HOME/j2ee/<RPAS_OC4J_INSTANCE>/config/jazn.xml
   ```

   An example file is shown in Example 7–1, "RPAS OC4":

Example 7–1 RPAS OC4

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<jazn xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://xmlns.oracle.com/oracleas/schema/jazn-10_
0.xsd" schema-major-version="10" schema-minor-version="0" provider="LDAP"
location="ldap://myhost.mycompany.com:636" default-realm="us">
      <property name="ldap.cache.purge.initial.delay" value="1200000"/>
      <property name="ldap.password"
value="{903}lDjczxpuY0o2BQg2MqM0YReAax9p+Po0wuU0oKU67as="/>
      <property name="ldap.cache.initial.capacity" value="20"/>
      <property name="ldap.user"
value="orclApplicationCommonName=jaznadmin2,cn=JAZNContext,cn=products,cn=OracleCo
ntext"/>
      <property name="ldap.cache.policy.enable" value="true"/>
      <property name="ldap.cache.purge.timeout" value="1200000"/>
      <property name="ldap.cache.realm.enable" value="true"/>
      <property name="ldap.cache.session.enable" value="true"/>
</jazn>
```

Note: Only LDAP specific properties are listed inExample 7–1. Your values of these may also differ. for additional details, refer to the Oracle Application Server administration documentation.

5. Restart the RPAS OC4J to incorporate your changes.

Step 2: Deploying WAR File

Perform the following procedure to deploy the WAR file to the Oracle Application Server.

1. Log on Oracle Enterprise Manager/Application Server Control as oc4jadmin.
2. Select the intended application group for your deployment.
3. Click **Deploy**.
4. Select **Archive is already present on the server where Application Server Control is running** (second option) and type the following in Location on Server field:

   `[STAGING_DIR]/RPAS_osso.war`
5. Click **Next**.
6. In the Application Name field, type **RPAS Web Launch**.
7. In the Context Root field, type **RPAS** (or anything you choose). This name is referred to as [CONTEXT_ROOT] in this document. Click **Next**.
8. Click the pen icon for Select Security Provider, and select Oracle Identity Management from the list.
9. Select **Enable SSO Authentication** check box. Click **OK.**
10. Click **Deploy**.

Step 3: Configuring RPAS Web Launch

To configure RPAS Web Launch, you need to modify one property file (propfile). This file is located in the following path; where [OAS_INSTALL_DIR] is the installation location of the OAS server:

[OAS_INSTALL_DIR]/j2ee/home/applications/RPAS Web Launch/[CONTEXT_ROOT] /WEB-INF/config

1. Locate the following information in propfile and replace [RPAS_WEB_DATA_DIR] with the actual location and [HOSTNAME] with the host name of the server)

```
dbPath=[RPAS_WEB_DATA_DIR]/RPASWebData/db
clientSourceDir=[RPAS_WEB_DATA_DIR]/RPASWebData/client
tunnelLogFile=[RPAS_WEB_DATA_DIR]/RPASWebData/logs/tunnel.[HOSTNAME].log
webLogFile=[RPAS_WEB_DATA_DIR]/RPASWebData/logs/rpasPortal.[HOSTNAME].log
isOSSO=true
debug=false
classicMode=false
launchPreinstalledOnly=false
supportMultipleVersions=true
```

   The isOSSO flag must be set to True. Set launchPreinstalledOnly to true if only pre-installed RPAS Client can be launched. Set classicMode to true to support RPAS Client release 9.4. To support multiple versions of RPAS Client, set supportMultipleVersions to True.

2. Restart the RPAS Web Launch Application from the Oracle Enterprise Manager/Application Server Control screen.

Step 4: Protect RPAS Root

Perform the following to protect the RPAS root location in the Oracle HTTP Server configuration.

1. In the file ORACLE_HOME/Apache/Apache/conf/mod_osso.conf, add the following protected resource to <IfModule mod_osso.c> section.

```
<Location /[CONTEXT_ROOT]/web>
require valid-user
AuthType Basic
</Location>
```

2. Restart the Oracle HTTP Server to ensure the modification is applied.

> **Note:** Protect /[CONTEXT_ROOT]/web instead of /[CONTEXT_ROOT] to let through /[CONTEXT_ROOT]/tunnel for Web tunneling.

Step 5: Setting RPAS Role for OSSO Logins

There are two types of roles for RPAS Web Launch users:

- RPAS_ADMIN_ROLE
- RPAS_USER_ROLE

Both roles can launch the RPAS Client and connect to a domain. Only RPAS_ADMIN_ROLE has the privilege to access the ADMIN interface.

It is recommended that RPAS_USER_ROLE be assigned to most OSSO users (such as planner) and RPAS_ADMIN_ROLE be assigned for a few power users (such as executive). This needs to be performed on the LDAP server storing the OSSO user information.

The roles can be created manually by using the OID DAS application. The oidadmin application or LDIF scripts may also be used to create users and roles. For more details, refer to the OID documentation.

Creating a Group Using the DAS Application

Use the following procedure to use the DAS application to create the RPAS_USER_ROLE and RPAS_ADMIN_ROLE accounts.

1. Access the DAS application.

   The DAS application is found in the following location; where `<host>` and `<port>` are the infrastructure or Oracle Identity Management OAS:

   `http://<host>:<port>/oiddas`

   Example: `http://hostname.example.com:7778/oiddas`

2. Click **login** and log in as **orcladmin** or another privileged user.
3. On the right-side of the page, select the **Directory** tab, and on the left side, select the **Groups** link.
4. Click **Create**.
5. Enter the name of the group to create (for example, RPAS_ADMIN_ROLE), the Display name, and a description.
6. Ensure the Group Visibility option is set to **Public**.
7. If needed, add additional users. Scroll to the Members section and select **Add User** to add users to this group. You can also nest other groups as well. Members can be added at a later time as needed.
8. When all members have been added, click **Submit**.

Creating Groups from an LDIF Script

Alternatively, you can create the groups using an LDIF script. A template is shown in Example 7–2. Note that the following token `@BASE_REALM_DN@` needs to be replaced with installation specific value of the Realm Distinguished Name. Also, this script creates the group with a single member, orcladmin, as part of the group. Additional members may be added with more `uniquemember` attributes. You can execute the script with the `ldapadd` command supplied with the Oracle Identity Management infrastructure OAS server.

Example 7–2 LDIF Script

```
# The LDIF template for creating RPAS_ADMIN_ROLE and RPAS_USER_ROLE groups in OID.
# RPAS_USER_ROLE
dn: cn=RPAS_USER_ROLE,cn=groups,@BASE_REALM_DN@
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
cn: RPAS_USER_ROLE
displayname: RPAS user role
description: RPAS user role
orclisvisible: true
owner: cn=orcladmin,cn=users,@BASE_REALM_DN@
uniquemember: cn=orcladmin,cn=users,@BASE_REALM_DN@

# RPAS_ADMIN_ROLE
dn: cn=RPAS_ADMIN_ROLE,cn=groups,@BASE_REALM_DN@
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
cn: RPAS_ADMIN_ROLE
displayname: RPAS Administrator role
description: RPAS Administrator role
orclisvisible: true
owner: cn=orcladmin,cn=users,@BASE_REALM_DN@
uniquemember: cn=orcladmin,cn=users,@BASE_REALM_DN@
```

Once the RPAS groups have been created with the LDIF script, you could use the OID DAS application to add more members to them.

For more information about SSO, refer to "Appendix D: Oracle Single Sign-On (SSO)".

Installing on Oracle Application Server without SSO Support

Perform the following procedure if you are implementing RPAS Web on an Oracle Application Server without SSO Support. This process consists of several steps:

- Step 1: Deploying the WAR File
- Step 2: Configuring RPAS Web Launch

Step 1: Deploying the WAR File

Perform the following procedure to deploy the WAR file to the Oracle Application Server without SSO.

1. Log on Oracle Enterprise Manager/Application Server Control as oc4jadmin.
2. Select the intended application group for your deployment and click **Deploy**.
3. Select **Archive is already present on the server where Application Server Control is running** (second option).
4. In the Location on Server field, type:

   `[STAGING_DIR]/RPAS.war`
5. Click **Next**.
6. In the Application Name field, type **RPAS** (or anything you choose).
7. In the Context Root field, type **RPAS** (or anything you choose).
8. This name is referred to as [CONTEXT_ROOT] in this document.

9. Click **Next**.
10. Click **Deploy**.

Step 2: Configuring RPAS Web Launch

To configure RPAS Web Launch, you need to modify one property file (propfile). This file is located in the following path; where `[OAS_INSTALL_DIR]` is the installation location of the OAS server:

```
[OAS_INSTALL_DIR]/j2ee/home/applications/RPAS Web
Launch/[CONTEXT_ROOT] /WEB-INF/config
```

1. Locate the following information in propfile and replace `[RPAS_WEB_DATA_DIR]` with the actual location and `[HOSTNAME]` with the host name of the server)

```
dbPath=[RPAS_WEB_DATA_DIR]/RPASWebData/db
clientSourceDir=[RPAS_WEB_DATA_DIR]/RPASWebData/client
tunnelLogFile=[RPAS_WEB_DATA_DIR]/RPASWebData/logs/tunnel.[HOSTNAME].log
webLogFile=[RPAS_WEB_DATA_DIR]/RPASWebData/logs/rpasPortal.[HOSTNAME].log
isOSSO=false
debug=false
classicMode=false
launchPreinstalledOnly=false
supportMultipleVersions=true
```

> **Note:** The `isOSSO` flag must be set to `False`. Set `launchPreinstalledOnly` to `true` if only pre-installed RPAS Client can be launched. Set `classicMode` to `True` to support RPAS Client release 9.4. Set `supportMultipleVersions` to `True` to support multiple versions of RPAS Client.

2. Restart RPAS Web Launch Application from the Oracle Enterprise Manager/Application Server Control window.

Installing on WebLogic Server with SSO Support

Perform the following procedure if you are implementing RPAS Web on a WebLogic server with SSO support. This process consists of these steps:

- Step 1: Set Up SSO
- Step 2: Configure the Oracle Access Manager
- Step 3: Set Up the WAR File
- Step 4: Deploy the WAR File
- Step 5: Set RPAS Role for Oracle SSO Logins

Step 1: Set Up SSO

This SSO configuration is the same as it is for SSO for the RPAS Fusion Client. Follow the procedure as described in the section, Set Up Single Sign-On (SSO).

Step 2: Configure the Oracle Access Manager

Configure the Oracle Access Manager using the following steps:

1. Log in to the OAM console.
2. Set URL access control rules within Webgate instance as follows:

   ```
   Protection Level: Excluded

   /.../tunnel
   ```

3. Under Policy configuration in the left pane, select Shared Components > Authentication Schemes > Select LDAP Scheme.

   The LDAPScheme window opens in the right pane.

   In the Challenge Parameter field, enter: **ssoCookie=disablehttponly**.

Step 3: Set Up the WAR File

Perform the following procedure to set up and deploy the WAR file to the WebLogic Server.

1. **Configure the Application for the OSSO Identity Asserter** - The WebLogic Server supports adding multiple authentication-methods. If you are setting up an OSSO Identity Asserter in the WebLogic Application Console, the Web application using the OSSO Identity Asserter must have its auth-method set to CLIENT-CERT. After deploying the application on the WebLogic Server, all web.xml files in the application EAR file must include CLIENT-CERT in the element auth-method for the appropriate realm. To edit web.xml for the OSSO Identity Asserter:

   a. Locate the web.xml file in the application WAR file. For example:

      ```
      WEB-INF/web.xml
      ```

   b. Locate the auth-method for the appropriate realm and enter CLIENT-CERT. For example:

      ```
      <login-config>
        <auth-method>CLIENT-CERT</auth-method>
        <realm-name>myrealm</realm-name>
      </login-config>
      ```

   c. Save the file.

d. Create a new weblogic.xml file with the following contents (replace [CONTEXT_ROOT] with the actual context root):

```
<?xml version='1.0' encoding='UTF-8'?>
<weblogic-web-app xmlns="http://xmlns.oracle.com/weblogic/weblogic-web-app"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://xmlns.oracle.com/weblogic/weblogic-web-app
http://xmlns.oracle.com/weblogic/weblogic-web-app/1.0/weblogic-web-app.xsd"
>

<context-root>[CONTEXT_ROOT]</context-root>

<security-role-assignment>
     <role-name>RPAS_ADMIN_ROLE</role-name>
     <principal-name>RPAS_ADMIN_ROLE</principal-name>
</security-role-assignment>

<security-role-assignment>
     <role-name>RPAS_USER_ROLE</role-name>
     <principal-name>RPAS_USER_ROLE</principal-name>
</security-role-assignment>

</weblogic-web-app>
```

e. Save the weblogic.xml file to the same location of the web.xml file in the WAR file.

2. **Configure the RPAS Web Launch** - To configure RPAS Web Launch, you need to modify one property file (propfile) located within the WEB-INF/config directory of the RPAS_osso.war file.

a. Locate the following information in propfile and replace [RPAS_WEB_DATA_DIR] with the actual location and [HOSTNAME] with the host name of the server)

```
dbPath=[RPAS_WEB_DATA_DIR]/RPASWebData/db
clientSourceDir=[RPAS_WEB_DATA_DIR]/RPASWebData/client
tunnelLogFile=[RPAS_WEB_DATA_DIR]/RPASWebData/logs/tunnel.[HOSTNAME].log
webLogFile=[RPAS_WEB_DATA_DIR]/RPASWebData/logs/rpasPortal.[HOSTNAME].log
isOSSO=true
debug=false
classicMode=false
launchPreinstalledOnly=false
supportMultipleVersions=true
```

Note: The `isOSSO` flag must be set to `True`. Set `launchPreinstalledOnly` to `true` if only pre-installed RPAS Classic Client can be launched. Set `classicMode` to `True` to support RPAS Classic Client release 9.4. To support multiple versions of RPAS Classic Client, set `supportMultipleVersions` to `True`.

---

b. Save the file and the WAR archive.

Step 4: Deploy the WAR File

Perform the following procedure to deploy the WAR file to the WebLogic Server:

1. Log on to the WebLogic Administration Console.
2. Under the Domain Structure (left navigation pane), select Deployments. The Summary of Deployments window opens.

3. On the Summary of Deployments window, click Install. The Install Application Assistant window opens.
4. On the Install Application Assistant window, navigate to the location where you extracted the RPAS_osso.war ([STAGING_DIR]/RPAS_osso.war), select the file, and click **Next**.
5. Click the Install this deployment as an application option and then click **Next**. The next window displays optional settings. You can choose to set them up or accept the default values and proceed.
6. Optional. Enter relevant information for the optional settings.
7. Click **Finish**. The WAR file is deployed and it appears listed in the Summary of Deployments window.
8. On the Summary of Deployments window, click the deployment you just added. The Settings for <deployment-name> window opens.
9. On the Configuration tab, under General, enter a relevant value in the **Context Root** field. You can choose to type RPAS or any other context root. This name is referred to as [CONTEXT_ROOT] in this document.
10. Click **Save**. The Save Deployment Plan Assistant window opens.
11. Enter or select a location for the deployment plan, and click **OK**.
12. Restart your deployment for the changes to take effect.

Step 5: Set RPAS Role for Oracle SSO Logins

There are two types of roles for RPAS Web Launch users: RPAS_ADMIN_ROLE and RPAS_USER_ROLE.

Both roles can launch the RPAS Classic Client and connect to a domain. Only RPAS_ADMIN_ROLE has the privilege to access the ADMIN interface.

It is recommended that RPAS_USER_ROLE be assigned to most OSSO users (such as planner) and RPAS_ADMIN_ROLE be assigned for a few power users (such as executive). This needs to be performed on the LDAP server storing the OSSO user information.

The roles can be created manually by using the OID DAS application. The oidadmin application or LDIF scripts may also be used to create users and roles. For more details, refer to the OID documentation.

Creating a Group Using the DAS Application

Use the following procedure to use the DAS application to create the RPAS_USER_ROLE and RPAS_ADMIN_ROLE accounts.

1. Access the DAS application.

   The DAS application is found in the following location:

   `http://<host>:<port>/oiddas`

   where `<host>` and `<port>` are the infrastructure or Oracle Identity Management OAS.

   Example: `http://hostname.example.com:7778/oiddas`
2. Click **login** and log in as orcladmin or another privileged user.
3. On the right-side of the page, select the **Directory** tab, and on the left side, select the **Groups** link.

4. Click **Create**.
5. Enter the name of the group to create (for example, RPAS_ADMIN_ROLE), the Display name, and a description.
6. Make sure the Group Visibility option is set to **Public**.
7. If you would like, add additional users. Scroll to the Members section and click **Add User** to add users to this group. You can also nest other groups as well. Members can be added at a later time as needed.
8. When all members have been added, click **Submit**.

Creating Groups from an LDIF Script

Alternatively, you can create the groups using an LDIF script. A template is shown in Example 7–3. Note that the following token @BASE_REALM_DN@ needs to be replaced with installation specific value of the Realm Distinguished Name. Also, this script creates the group with a single member, orcladmin, as part of the group. Additional members may be added with more `uniquemember` attributes. You can execute the script with the `ldapadd` command supplied with the Oracle Identity Management infrastructure OAS server.

Example 7–3 LDIF Script

```
# The LDIF template for creating RPAS_ADMIN_ROLE and RPAS_USER_ROLE groups in OID.
# RPAS_USER_ROLE
dn: cn=RPAS_USER_ROLE,cn=groups,@BASE_REALM_DN@
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
cn: RPAS_USER_ROLE
displayname: RPAS user role
description: RPAS user role
orclisvisible: true
owner: cn=orcladmin,cn=users,@BASE_REALM_DN@
uniquemember: cn=orcladmin,cn=users,@BASE_REALM_DN@

# RPAS_ADMIN_ROLE
dn: cn=RPAS_ADMIN_ROLE,cn=groups,@BASE_REALM_DN@
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
cn: RPAS_ADMIN_ROLE
displayname: RPAS Administrator role
description: RPAS Administrator role
orclisvisible: true
owner: cn=orcladmin,cn=users,@BASE_REALM_DN@
uniquemember: cn=orcladmin,cn=users,@BASE_REALM_DN@
```

Once the RPAS groups have been created with the LDIF script, you could use the OID DAS application to add more members to them.

For more information about SSO, refer to "Appendix D: Oracle Single Sign-On (SSO)".

Installing on WebLogic Server without SSO Support

Perform the following procedure if you are implementing RPAS Web on a WebLogic Server instance without SSO Support. This process consists of several steps:

- Step 1: Configuring RPAS Web Launch
- Step 2: Deploying the WAR File

Step 1: Configuring RPAS Web Launch

To configure RPAS Web Launch, you need to modify one property file (propfile) located within the WEB-INF/config directory of the RPAS.war file.

1. Locate the following information in **propfile** and replace `[RPAS_WEB_DATA_DIR]` with the actual location and `[HOSTNAME]` with the host name of the server).

```
dbPath=[RPAS_WEB_DATA_DIR]/RPASWebData/db
clientSourceDir=[RPAS_WEB_DATA_DIR]/RPASWebData/client
tunnelLogFile=[RPAS_WEB_DATA_DIR]/RPASWebData/logs/tunnel.[HOSTNAME].log
webLogFile=[RPAS_WEB_DATA_DIR]/RPASWebData/logs/rpasPortal.[HOSTNAME].log
isOSSO=false
debug=false
classicMode=false
launchPreinstalledOnly=false
supportMultipleVersions=true
```

> **Note:** The `isOSSO` flag must be set to `False`. Set `launchPreinstalledOnly` to `true` if only pre-installed RPAS Classic Client can be launched. Set `classicMode` to `True` to support RPAS Classic Client release 9.4. Set `supportMultipleVersions` to `True` to support multiple versions of RPAS Classic Client.

2. Save the file and WAR archive.

Step 2: Deploying the WAR File

Perform the following procedure to deploy the WAR file to the Oracle Application Server without SSO.

1. Log on to the WebLogic Administration Console.
2. Under the Domain Structure (left navigation pane), select **Deployments**. The Summary of Deployments window opens.
3. On the Summary of Deployments window, click **Install**. The Install Application Assistant window opens.
4. On the Install Application Assistant window, navigate to the location where you extracted the RPAS.war ([STAGING_DIR]/RPAS.war), select the file, and click **Next**.
5. Click the Install this deployment as an application option and then click **Next**. The next window displays optional settings. You can choose to set them up or accept the default values and proceed.
6. Optional. Enter relevant information for the optional settings.
7. Click **Finish**. The WAR file is deployed and it appears listed in the Summary of Deployments window.

8. On the Summary of Deployments window, click the deployment you just added. The Settings for <deployment-name> window opens.
9. On the Configuration tab, under General, enter a relevant value in the **Context Root** field. You can choose to type RPAS or any other context root. This name is referred to as [CONTEXT_ROOT] in this document.
10. Click Save. The Save Deployment Plan Assistant window opens.
11. Enter or select a location for the deployment plan, and click **OK**.
12. Restart your deployment for the changes to take effect.

Installing on Apache Tomcat

Perform the following procedure if you are deploying RPAS Web launch on a standalone Apache Tomcat server, which implies a non-SSO environment.

Installing RPAS Web Launch on Apache Tomcat consists of two steps:

- Step 1: Deploying the RPAS WAR File
- Step 2: Configuring RPAS Web Launch on Apache Tomcat

Step 1: Deploying the RPAS WAR File

Refer to your Apache Tomcat documentation for more details of how to deploy a Web archive.

1. Log on to the Tomcat Web server URL: `http://server:port/manager/html`.
2. Scroll to **Deploy directory or WAR file** located on server section.
3. In the Context Path field, type **/RPAS** (or anything else you choose).

   This location is referred to (without the "/") as [CONTEXT_ROOT] in this document.
4. In the WAR or Directory URL field, type **[STAGING_DIR]/RPAS.war**.
5. Click **Deploy**.

The display name should show RPAS Web Launch for a successful deployment. In the event you need to a re-deploy RPAS Web Launch, it is recommended that the following be performed:

- Undeploy the Web application.
- Restart the Web server to clear any caching.
- Re-deploy the Web application.

Step 2: Configuring RPAS Web Launch on Apache Tomcat

To configure RPAS Web Launch, you need to modify one property file (propfile). This file is located in the following path; where `[TOMCAT_INSTALL_DIR]` is the installation location of the Tomcat Web server. If the Web server is running in a load balance environment with multiple servers, this file must be modified for all Web server instances:

```
[TOMCAT_INSTALL_DIR]/webapps/[CONTEXT_ROOT]/WEB-INF/config
```

1. Locate the following information in propfile and replace [RPAS_WEB_DATA_DIR] with the actual location and [HOSTNAME] with the host name of the server.

```
dbPath=[RPAS_WEB_DATA_DIR]/RPASWebData/db
clientSourceDir=[RPAS_WEB_DATA_DIR]/RPASWebData/client
tunnelLogFile=[RPAS_WEB_DATA_DIR]/RPASWebData/logs/tunnel.[HOSTNAME].log
webLogFile=[RPAS_WEB_DATA_DIR]/RPASWebData/logs/rpasPortal.[HOSTNAME].log
isOSSO=false
debug=false
classicMode=false
launchPreinstalledOnly=false
supportMultipleVersions=true
```

> **Note:** The `isOSSO` flag must be set to `false`. Set `launchPreinstalledOnly` to `true` if only pre-installed RPAS Classic Client can be launched. Set `classicMode` to `true` to support RPAS Classic Client release 9.4. Set `supportMultipleVersions` to `true` to support multiple versions of RPAS Classic Client.

2. Restart the RPAS Web Launch application.

Migrating from Previous Versions

If you have been running an older version of RPAS Web Launch, here are the steps to migrate old data to the new deployment.

1. Migrate client binary:

   Copy buildNumber.txt and client.zip files to the location specified by property `clientSourceDir`. If multiple versions are supported, they should be copied to `clientSourceDir`/[VERSION] where [VERSION] is the version number of that release (12.1.2, 11.1.15, and so on).

2. Migrate admin user data:

   Copy userdata.dat file to the location specified by property `dbPath`.

3. Migrate domain registration data:

   Copy domaindata.dat to the location specified by property `dbPath`.

4. Restart Web application RPAS Web Launch.

> **Note:** After the migration, if an admin user fails to log on, that would indicate that the userdata.dat file is corrupt. Remove the file, and log on the administration interface using default user, **adm** (default password **adm**), and re-create all admin users.

Configuring the RPAS Servlet

The class for the RPAS servlet is com.retek.mdap.servlet.ServletManager. The servlet properties have been configured in the deployment descriptor web.xml that is originally archived in RPAS_osso.war or RPAS.war.

This deployment descriptor provides two sets of initialization parameters to the RPAS servlet.

Note: The deployment descriptor should not be modified. All of the servlet initialization parameters should not be modified, except the "time-out" and "sleep" parameters (which specify the time in seconds) for Web tunneling.

After the servlet is configured, load it into your Web server. You might be required to reload your Web server to activate the new servlet.

Configuring and Administering the Web Application

The following topics provide information on accessing the RPAS Web Administration console to perform administrative tasks such as defining the RPAS enterprise configuration, and adding, modifying and deleting domain configurations.

Start the RPAS Web Configuration Utility – Administration Console

Perform the following procedure to start the RPAS Web Configuration utility.

1. To access the RPAS Web configuration utility, start a Web browser (Internet Explorer recommended) and go to the following location; where `WEB_SERVER_ADDRESS` is the address you use to access your Web server and`CONTEXT_NAME` is the value you defined for the Context Root field as described in each of the three installation processes listed in the Installing the RPAS Web Application section:

   `http://[WEB_SERVER_ADDRESS]/[CONTEXT-NAME]/web`

   Note: The Web application support internationalization. It uses the locale from the browser to determine the appropriate language to display in the Web interface. The default language is English.

   Example: `http://rpasweb.oracle.com:13085/RPAS/web`

   Depending the type of RPAS deployment being implemented (with SSO or without SSO), one of the following windows opens.

Figure 7–1 Login Window after OSSO Authentication

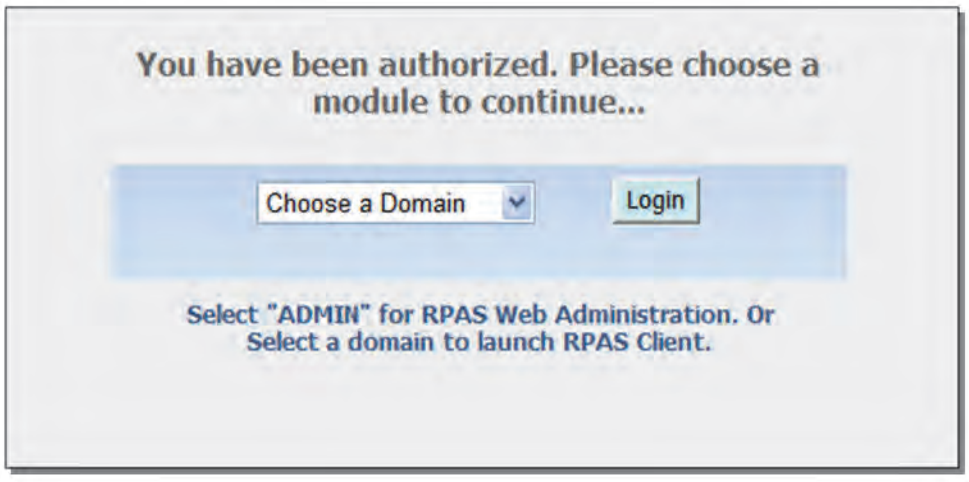


Figure 7–2 Login Window for non-OSSO Configuration

Note: If there is a very long list of domains, use URL `http://[WEB_SERVER_ADDRESS]/[CONTEXT-NAME]/web?app=[AppID]` to filter domains on the login page. Only domains with an application ID field matching `AppID` will be displayed in the list.

2. Perform one of the following:
   - If you are using an SSO environment, select **ADMIN** as the domain and click **Login** to access the Administration Console.
   - If you are not using an SSO environment, enter an Administrator user name and password (the initial administration user name is **adm** and the password is **adm**). Select **ADMIN** as the domain and click **Login** to access the Administration Console.

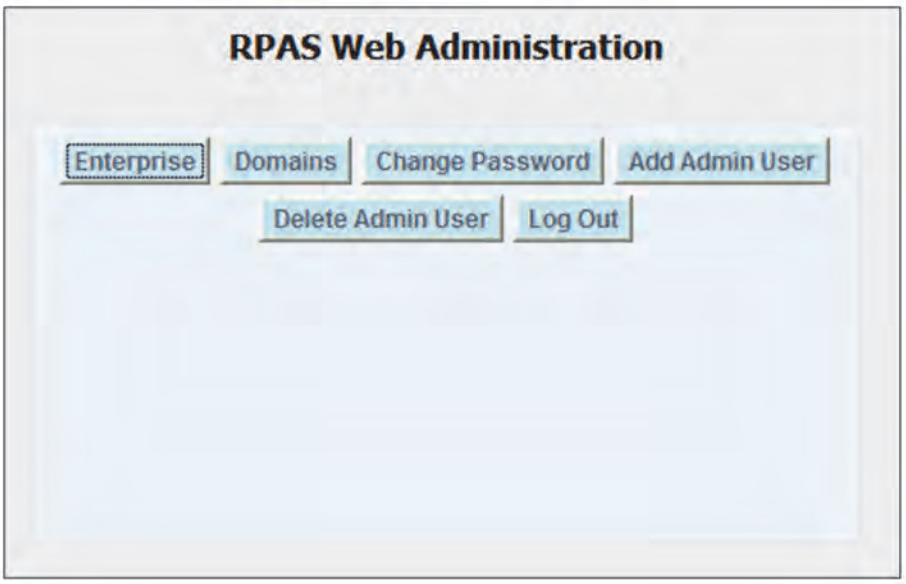
   A security warning dialog box opens.

Figure 7–3 Security Warning on Internet Explorer

3. Click **Run**. To avoid seeing this message in the future, make sure **Always trust content from this publisher** option is selected. The RPAS Web Administration console opens.

Figure 7–4 RPAS Web Administration Console in SSO Environment

Figure 7–5 RPAS Web Administration Console without SSO



4. Refer to the following topics to configure RPAS Web Launch or perform other administration activities.

Configure Web Launch and Web Tunneling – Enterprise Configuration

The following section describes how to configure the use of the Web launch or the Web tunneling architecture. Both the Web launch and Web tunneling architectures allow domain location setup, client application installation, and application launch processes to be initiated from a Web browser. The difference between the two architectures is in how data is communicated between the RPAS Classic Client application that runs on a user's PC and the RPAS domain that runs on the database server.

The Web tunneling architecture sends all data through the Web server as it travels from a user's PC to the database server. This method allows PCs that are located outside a company's network to communicate through the Internet to a database server that is located inside a company's network.

The Web launch architecture sends all data directly from a user's PC to the database server. This architecture assumes that the database server is on a network directly accessible by each user's PC (that is, the company's LAN).

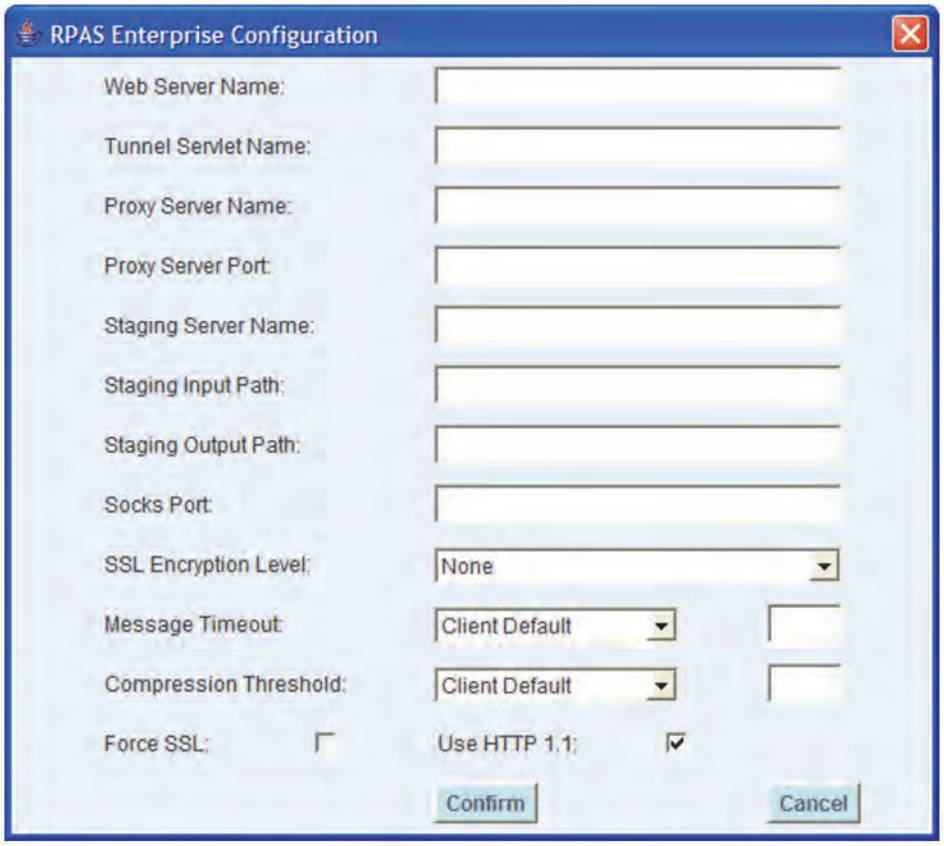
1. Click **Enterprise** to open the RPAS Enterprise Configuration window.

   This dialog allows you to define the communications architecture that connects client PCs to the database server.

   From a configuration perspective the key differentiator, between the two options is in the value of the Web Server Name field. To use the Web tunneling architecture, this field must be populated; if it is empty, the Web launch architecture is used.

2. To configure the Web launch architecture, make sure the **Web Server Name** field in the RPAS Enterprise Configuration dialog is empty, and click **Confirm**. All other fields in this window are ignored.

Figure 7–6 RPAS Enterprise Configuration Window

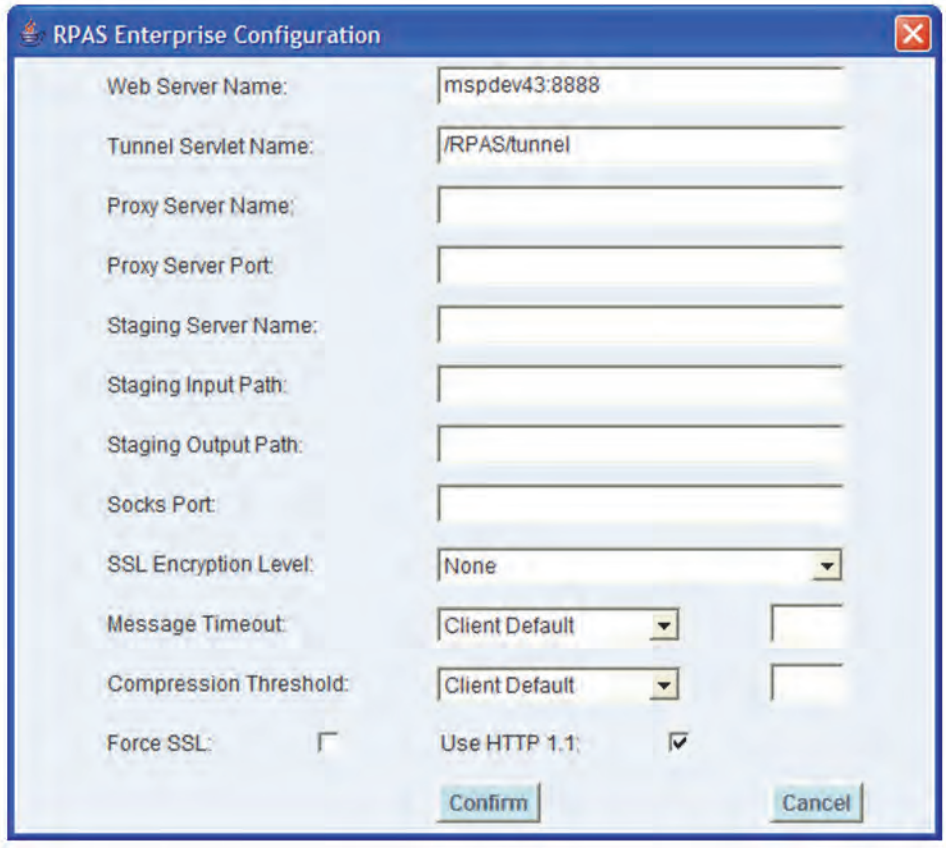


3. To configure the Web tunneling architecture, the RPAS Enterprise Configuration window must be filled with appropriate values in the following table.

Field Name	Value Description
Web Server Name	The hostname or the IP address of the Web server and the port number of the Web server. They must be entered sequentially with a colon in between. If the **Force SSL** check box is checked, replace the port with the SSL port number. Required.
Tunnel Servlet Name	The path to the servlet that tunnels the information between the client and server. Formatting: /**[CONTEXT_NAME]**/tunnel. Required.
Proxy Server Name	The hostname or the IP address of the proxy server.
Proxy Server Port	The port number on which the proxy server is active. Must be an integer between 1 and 65535.
Staging Server Name	Leave blank. Not currently used.
Staging Input Path	Leave blank. Not currently used.
Staging Output Path	Leave blank. Not currently used.
Socks Port	If HTTP 1.1 is being used along with a proxy server, then the proxy server must enable SOCKS protocol. Must be an integer between 1 and 65535.
SSL Encryption Level	If SSL is to be used, this value should be 128 Bit US, or 64 Bit International encryption level. 128 bit encryption should be preferred.

Field Name	Value Description
Message Timeout	Used in HTTP 1.1 to specify the number of milliseconds of inactive communication after which the client will timeout and reconnect. Must be an integer between 1 and 65535.
Compression Threshold	The number of bytes above which client and server will be using compression.
Force SSL	This is a check box that specifies whether SSL is used for transferring data between client and server.
Use HTTP 1.1	This is a check box that specifies whether HTTP 1.1 should be used. If not selected, HTTP 1.0 will be used.

Figure 7–7 Sample Web Tunneling Configuration



Other Web Client Administration Activities

The following sections provide instructions for these other Web Client Administration activities:

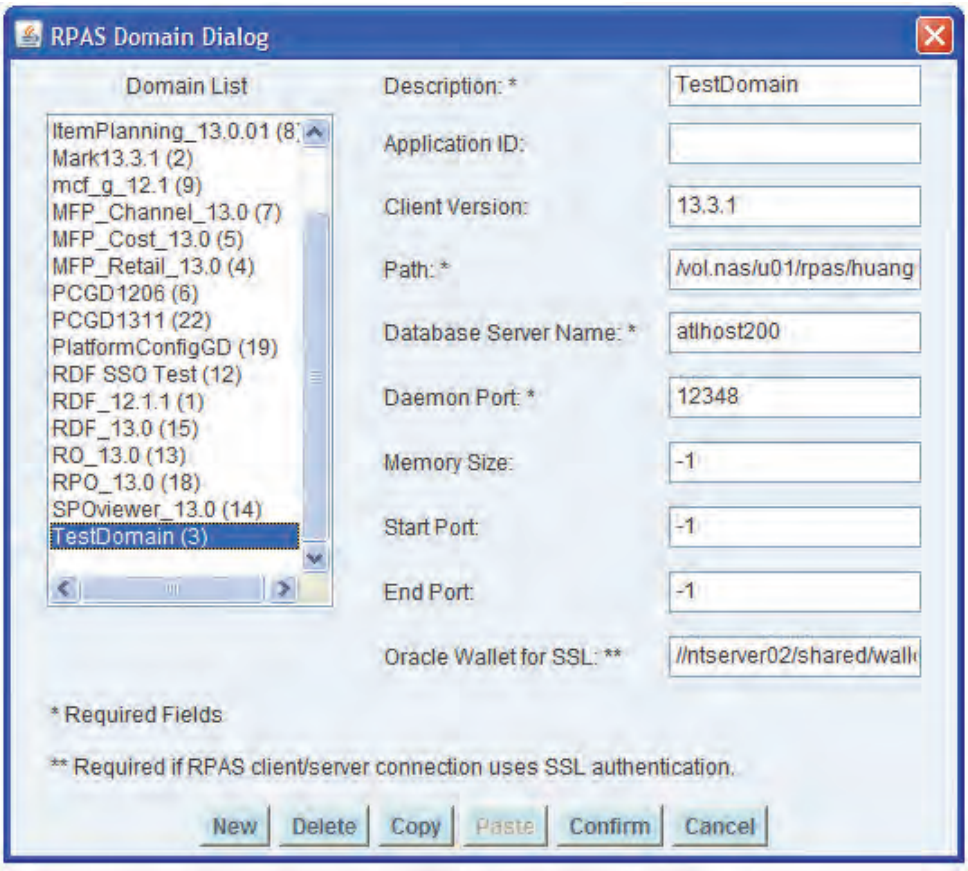
- Adding, Modifying and Deleting Domain Configuration
- Changing Administrator Password
- Adding a New Administrator Account
- Deleting an Administrator Account
- Logging Out

Adding, Modifying and Deleting Domain Configuration

Perform the following procedure to add, modify, and delete domain configuration.

1. Click **Domains** in the RPAS Web Administration Console. The RPAS Domain Dialog opens. This dialog is used to specify the location of RPAS domains. Each domain that can be accessed by a user must be specified with the dialog.

Figure 7–8 RPAS Domain Dialog



2. To add a new domain, click **New**, enter the following information, and click **Confirm**.

Field Name	Value Description	Use
Description	This is displayed to users when they are selecting a domain to log in to.	Required.
Application ID	Used in domain filtering.	Can be any string without spaces. Leave blank if preferred.
Client Version	The version number of the RPAS Classic Client to launch.	It must match exactly the version number in the path of the client files on the Web server. Leave blank if multiple version support is not enabled.
Path	The full path to the directory containing the domain on the database server.	Required.

Field Name	Value Description	Use
Database Server Name	The hostname of the database server containing the domain.	Required.
Daemon Port	The port number of the DomainDaemon process running on the database server. The port must be between 1025 and 65535 (inclusive).	Required.
Memory Size	Not currently used.	Leave blank.
Start Port	Start of the range of ports used by a client PC (Web launch architecture) or the Web server (Web tunneling architecture) to connect to the database server.	This value must be great than (>) 1025. If it not specified, the RPAS database server attempt to find a free port whenever a client connects.
End Port	End of the range of ports used by a client PC (Web launch architecture) or the Web server (Web tunneling architecture) to connect to the database server.	This value cannot be greater than 65535.
Oracle Wallet for SSL	The wallet location that passes to the Classic Client in order to support one-way SSL.	Required.

3. To change an existing domain configuration, select the domain from the **Domains List**, modify the fields as necessary, and click **Confirm**. Select **Cancel** to discard any changes that have been made.
4. To remove a domain, select a domain from the **Domains List** and click **Delete**. The selected domain configuration is removed.
5. To copy all of the domain settings of a domain, perform the following:
   a. Select the domain from the **Domains List** and click **Copy**.
   b. Selecting another domain from the **Domains List** and click **Paste**. The domain is updated the domains settings you have copied.
   c. Click **Confirm** to save the updated information.

Changing Administrator Password

Perform the following procedure from the RPAS Web Administration Console.

1. Click **Change Password**. The RPAS Change Password window opens. This allows the currently logged in administrator to change his/her password that allows access to the administrative console.
2. Enter the current password in the **Old Password** field. Passwords should not exceed 30 characters in length.
3. Enter the new password in the **New Password** and **Confirm New Password** fields.
4. Click **Confirm** to save the new password.

Adding a New Administrator Account

Perform the following procedure from the RPAS Web Administration Console.

1. Click **Add Admin User** to open the RPAS Add Admin User window. This window is used to add another RPAS administrative user.
2. Enter the administrative user's name in the **User Name** field. The user name must not be used by other people.

   If the user name has been used, an error dialog opens. Click **OK** on this error dialog if this occurs, and enter another name for this new administrative user.
3. Enter the initial password in the **Password** and **Confirm Password** fields.
4. Click **Confirm** to create the new administrator account.

Deleting an Administrator Account

Perform the following procedure from the RPAS Web Administration Console.

1. Click **Delete Admin User** to open the RPAS Delete Admin User window. This allows you to delete an RPAS administrative user.
2. Select the administrative user's name from the list in the window, and click **Confirm** to delete the user.

Logging Out

From the RPAS Web Administration Console, click **Logout** to exit the administrative console. This returns you to the Login window.

Install and Launch the RPAS Classic Client Application

Perform the following procedure the install the RPAS Classic Client and log in to a domain using RPAS Web Launch:

1. Start a Web browser (Internet Explorer 7 is recommended) and go to the following location/URL: `http://[WEB_SERVER_ADDRESS]/[CONTEXT_NAME]/web`

   Example: `http://rpasweb.oracle.com:13085/RPAS/web`

   This address is established during the initial installation and configuration. Administrators must provide this location/URL to end users. The `[WEB_SERVER_ADDRESS]` portion of the URL is the host address where the Java application service is running. This address may also include an alternate TCP/IP port number to communicate on (for instance, for port 8080, webss:8080). The login window opens.

   Note: If using Windows 7, start the web browser in *Run as administrator* mode the first time you use RPAS Web Launch.

   This ensures that the browser has privileges to install the RPAS Classic Client. After the first time, run the web browser in regular mode for better security.

2. Perform one of the following based on your environment:

   - If your environment is not using Oracle SSO, enter a user name and password, select a domain from the list, and then click **Login**.
   - If you are using SSO, enter your SSO credentials for authentication. A drop-down list appears, displaying a list of domains you can choose from. Select a domain. The RPAS Classic Client login page opens. Log in with your RPAS solution username and password.

   Note: When using SSO, you can by-pass the login page by specifying the domain in the URL:
   `http://[WEB_SERVER_ADDRESS]/[CONTEXT_NAME]/web?domain=[Desc].`

   The domain with a description field matching Desc will be launched automatically after the authentication. No spaces are allowed in the description field if this direct triggering mechanism feature is used.

   When**Login** is selected, the **DomainDaemon** on the database server is contacted to verify that the specified user is allowed to access the selected domain. Ensure that the **DomainDaemon** process is running on the database server before clicking **Login**.

   If access to the domain is allowed, a security dialog window may appear.

3. If the security window opens, click **Run**.

   After you click **Run** in the security window, a check is made to see if the RPAS Classic Client application needs to be installed on the user's PC. The Web server administrator is able to define a common installation location of the RPAS Classic Client for all users' PCs.

   This is accomplished by setting the appropriate value in the server-side clientPath.txt file (note the mixed-case filename) under the `clientSourceDir/[VERSION]` directory where the optional `[VERSION]` is the client version number if multiple versions are supported. The file clientPath.txt is an optional file which must reside under the same directory as buildNumber.txt does. RPAS Web installation files do not contain it. The administrator, or person responsible for installing RPAS Server components, must decide whether or not to define the installation location on user's PC by creating this file and specifying the full path of installation directory in the first line of the file. If `launchPreinstalledOnly` flag is set to `True`, the Web Launch applet will try to launch RPAS Classic Client from that location without downloading and installing the client. It will fail if the RPAS Classic Client has not been installed, and the applet will display an error message. If `launchPreinstalledOnly` flag is set to `False` and the user has not previously installed the RPAS Classic Client, or a newer version has become available on the server, the RPAS Classic Client will be downloaded and installed. If launchPreinstalledOnly flag is set to false and the RPAS Classic Client path is not specified, the user is prompted for an installation location for the RPAS Classic Client. The RPAS Classic Client installation directory must have at least 50 MB storage space.

4. If necessary, select a directory that has at least 50 MB of free storage for installing RPAS Classic Client, and click **OK**. A status dialog box opens as files are copied from the server to the user's PC. After the files have been copied, a RPAS installation program runs, and the RPAS Classic Client starts. If everything is successful, the user sees a **Login Successful** message in the bottom left corner of the RPAS Classic Client window.

Note: If the RPAS Classic Client does not need to be installed on the user's PC after you click **Login**, the RPAS Classic Client immediately starts and connects the user to the selected domain.

Troubleshooting

If a problem is encountered when using RPAS Web Launch, review any log files and record the output to determine the causes. Any support ticket submitted to Oracle must have the logging output attached.

On the server side, the log files are specified by the properties `webLogFile` and `tunnelLogFile`. On the client side, logging output is written to Java Console which can be opened by right-clicking the Java icon in the Windows system tray and choosing **Open Java Console**.

If the browser fails to launch the client without displaying an error message or behaves abnormally, we recommend that the user clear all browser cookies and try again.

If an instance of RPAS Classic Client is already running when the Web Launch applet is trying to install RPAS Classic Client, the installation may fail. We recommend that the user stop all RPAS Classic Client processes and try again.

Note: You can turn on the `debug` flag to obtain additional logging information by setting `property debug` to `true` in property file propfile and restarting the web application.

RPAS Web Launch and Web-based Applications

If you plan to implement RPAS Web Launch (including In-Context Launch) in conjunction with web-based applications, refer to either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide* for more information.

8

RPAS Package Extraction

The first step in upgrading to the most recent installation is to download the 13.3.1 release from the My Oracle Support Web site (https://support.oracle.com) to a staging folder (such as $PACKAGEDIR) that is accessible to all components of your current RPAS environment.

Example Package Extraction

The following example describes a sample upgrade installation. These sample commands are provided to guide you through the file extraction process and to identify the files provided in this upgrade.

```
$ mkdir packagedir
$ cp rpas.zip packagedir
$ cd packagedir
$ export PACKAGEDIR=`pwd`
$ unzip rpas.zip
```

The following items may be extracted to the current directory:

- ARPOPlatform-13.3.1.aix53.tar.zip
- ARPOPlatform-13.3.1.aix61.tar.zip
- ARPOPlatform-13.3.1.sun10.tar.zip
- ARPOPlatform-13.3.1.linux.tar.zip
- ARPOPlatform-13.3.1.nt.zip
- ARPOPlatform-13.3.1.clients.zip
- Curve13.3.1.zip
- Grade13.3.1.zip
- FusionClient.zip
- README.html
- DOCS folder

Note: ARPOPlatform-13.3.1.clients.zip is an archive of the RPAS Classic Client and ODBC Client for all platforms.

The Curve and Grade documentation sets which were previously included in the DOCS folder are now combined with the Oracle Retail Demand Forecasting (RDF) documentation. This documentation is available within the RDF package and on the following Web site:

http://www.oracle.com/technology/documentation/oracle_retail.html

At this point, you must choose which package you wish to extract, based on your current server platform and version. AIX 6.1 is used for the purpose of the following example.

Next, run the following commands.

```
$ unzip ARPOPlatform-13.3.1.aix61.tar.zip
$ tar -xf ARPOPlatform-13.3.1.aix61.tar
```

Now the package directory should contain a subdirectory named ARPOPlatform. You have successfully completed extracting the upgrade.

9

RPAS Server Patch Installation

This chapter describes how to patch the RPAS Server on UNIX or Windows. For instructions on patching the server on Windows, refer to Appendix C, "Appendix C: rsp_manager Usage".

RPAS Upgrade Prerequisites

In order to upgrade RPAS, first verify the following criteria for the RPAS system:

- Verify that RPAS is currently installed.
- Verify that UNIX operating system is updated to the currently supported version, which can be found in the section, Hardware and Software Requirements.
- Verify that the environment variables are correctly set; if they are not, follow these instructions to set them:
  - On Windows, update the environment variables using the instructions in the section, Creating the Required Environment Variables.
  - On UNIX, change directories to the original RPAS installation directory (such as the one created by the most recent installer), and execute retaillogin.ksh to set all environment variables. For example:

```
$ cd /retail
$ . ./retaillogin.ksh
```

Note: Once you have run the script, verify that the environment variables all point to the correct locations on your environment.

If you have updated Java since the last installation of RPAS, verify that the JAVA_HOME path is correct. If not, update your RIDE_HOME/toolslogin.ksh script and source your retaillogin.ksh again as previously outlined.

For Windows: Install Cygwin

Cygwin is required if the RPAS Server is to be installed on Windows operating systems. You can find more information about downloading this product at `http://www.cygwin.com.`

For installation guidance, refer to the following note on My Oracle Support (`https://support.oracle.com`):

Cygwin Setup Guide for RPAS (Note 1333398.1)

This document details necessary options you should select when installing Cygwin to make it function properly with RPAS.

Java Environment

Ensure that Java Development Kit (JDK) has been installed on the machine where RPAS will run and that the JAVA_HOME environment variable is properly set.

For detailed Java environment information, refer to the section, Java Environment, in the Installing on UNIX and Linux Environments chapter.

Ride Options

The RIDE_OPTIONS environmental variable has been defined to allow users to pass information into the rpasInstall process. Unlike the regular arguments passed on the command line to rpasInstall (such as -fullinstall and -updatestyles), arguments defined in RIDE_OPTIONS are passed to every rpasInstall instance that runs in the environment.

There the three supported properties for use with RIDE_OPTIONS:

Property	Used for
Xmx	Java
HP 64-bit mode Java (-d64)	HP Itanium and Solaris
Drpas.maxProcesses	RPAS

For Java

Xmx

By default, the Java Virtual Machine requests on the order of 268 MB of RAM from the OS to allocate for its heap. Large domains that are built from complex configurations can potentially exhaust this limited amount of memory. This is even more of an issue in patch installations than in builds since a patch installation requires two different versions of a configuration to be held in memory simultaneously.

By using the `-Xmx` option, you can instruct the Java Virtual Machine to request more memory from the OS to prevent situations when all allocated memory is exhausted. The syntax of the property is:

`-Xmx###m`, where ### is the amount, in megabytes, of memory the JVM is to request. Common values for this argument are `-Xmx512m` or `-Xmx1024m`.

For HP Itanium and Solaris

HP 64-bit mode Java (-d64)

The HP distribution of Java does not consist of separate executables for 32-bit and 64-bit operating systems. Instead, there is a single distribution of Java that can run in either 32-bit or 64-bit mode. By default, the HP Java runs in 32-bit mode. Because RPAS is built as a 64-bit executable on the Itanium OS, the RPAS libraries are unable to link with Java if it is running in 32-bit mode.

By adding the `-d64` property to RIDE_OPTIONS, the HP Java distribution is 64-bit mode enabled and the RPAS libraries link successfully.

It is often the case that users may want to use or more different properties in conjunction with RIDE_OPTIONS. When this is the case, all desired properties should be included within the environmental variable definition separated by white space with the entire definition enclosed in double quotes. An example of this is shown as:

```
export RIDE_OPTIONS="-d64 -Xmx1024m -Drpas.maxProcesses=8"
```

For RPAS

Drpas.maxProcesses

Several RPAS server utilities are designed to take advantage of multi-processor hardware to improve their performance. These utilities attempt to perform operations in parallel, each process running on a distinct processor. The

The `-Drpas.maxProcesses` argument is used to instruct RPAS how many processors it should attempt to run in parallel when executing one of the server utilities that has multi-processor support when that utility is executed as a part of the rpasInstall process.

Note that the -Drpas.maxProcesses argument only affects those calls to server utilities made from within the rpasInstall process and does not affect calls to server utilities made from the command line or as part of a batch job. The syntax of the property is:

`-Drpas.maxProcesses=###`, where ### is the number of sub-processes the RPAS server utility should attempt to run in parallel. The number of processes to use should be determined by the administrator of the hardware system based on the physical number of processors available and the amount of load that is acceptable for the rpasInstall process to place on the system.

RPAS Upgrade Process

The following process outlines how to upgrade the RPAS server environment to the current version.

1. In a command prompt, change to location of the base directory of this upgrade.

   ```
   $ cd $PACKAGEDIR/ARPOPlatform/13.3.1
   ```

2. Run RSP Manager to upgrade your environment:

   If the platform is Linux, use the following command:

   ```
   $ ./rsp_manager.linux –install –sp linux –no_domain
   ```

   For all other platforms, use the following command:

   ```
   $ ./rsp_manager –install –sp [PLATFORM] –no_domain
   ```

   Note: If using rsp_manager to install an RPAS 13.3.1 patch, do not use the `-domain` option. You should use the `-no_domain` option.

Note: [PLATFORM] represents your current platform and should be replaced with the correct label, such as aix53.

`-no_domain` indicates that there no domain in need of upgrading.

If you want to upgrade a single domain, include `-domain` with the full name or path of the domain. If you want to upgrade multiple domains at the same time, you must include `-domain` and pass on a file that contains a list of all domains that need to be upgraded.

For instructions on upgrading domains, refer to the "Building and Upgrading Domains" chapter in either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*.

3. Verify that none of the files failed during the upgrade; this can be determined based on the output of RSP Manager. For example, a successful output message would read:

```
Validation complete...
Files Checked: 106
Files Passed: 106
Files Failed: 0
```

The RPAS upgrade process is complete.

Domain Upgrade Process

After you have upgraded/patched RPAS server, you should upgrade any individual domains to be synchronized with that version. For information about upgrading domains, refer to the Domain Administration chapter in either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*.

ODBC/JDBC Upgrade Process

This section describes how to save and migrate your existing ODBC/JDBC configurations to the new version. If you do not have any existing configurations to migrate, you can remove the old version and install the new one.

ODBC Server

The following sections describe how to update your existing ODBC server to the new version.

Upgrading from 13.0.x

On all platforms, the 13.0.x ODBC Server configurations are stored in openrda.ini and oadrd.ini.

1. Before upgrading $RPAS_HOME, save a copy of openrda.ini and oadrd.ini to a temporary location.
2. Remove the 13.0.x version of the ODBC Server. To do this on Windows, run setup.exe and choose the Remove option. On UNIX platforms, the ODBC directory should be automatically overlaid when you upgrade your $RPAS_HOME.

3. Install the new version (13.1.2 or later) of the ODBC Server. Use the following information to migrate the 13.0.x configuration to the new ODBC Server.

Migrating Server Configuration

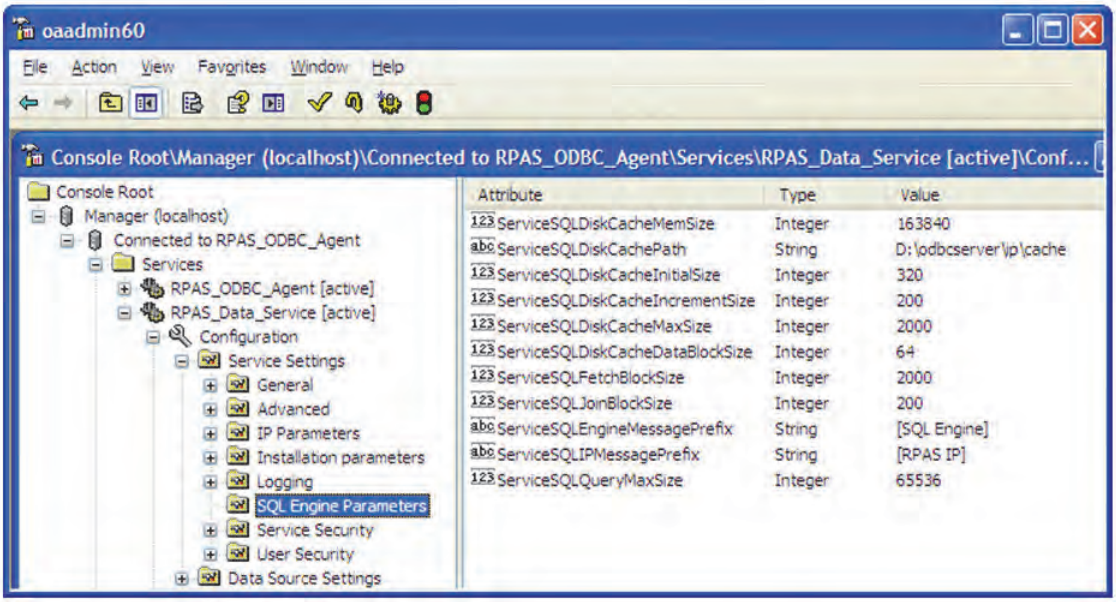
Table 9–1 shows the mapping of the configurations between 13.0.x and the new version (13.1.2 or later) of the ODBC Server

Table 9–1 Mapping Server Configuration

13.0.x Server Configurations	Corresponding Server Configurations (13.1.2 and Later)
INITIAL_SIZE	ServiceSQLDiskCacheInitialSize
INCREMENT_SIZE	ServiceSQLDiskCacheIncrementSize
MAX_SIZE	ServiceSQLDiskCacheMaxSize
DATABLOCK_SIZE	ServiceSQLDiskCacheDataBlockSize
CacheMemSize	ServiceSQLDiskCacheMemSize
FETCHBLOCK_SIZE	ServiceSQLFetchBlockSize
JOINBLOCK_SIZE	ServiceSQLJoinBlockSize
QueryMaxSize	ServiceSQLQueryMaxSize

Figure 9–1 shows the new ODBC Manager with the configuration attributes that are listed in Table 9–1.

Figure 9–1 Server Configuration Attributes (Versions13.1.2 and Later)



Migrating Data Source Information

A data source in oadrd.ini looks like this sample:

```
ADDRESS=hostname.example.com
PORT=1710
CONNECT_STRING=/vol.nas/u08/Position_parent/croad_SR
TYPE=BTREE
```

```
SCHEMA_PATH=
REMARKS=
```

The attributes that you need to migrate are ADDRESS, PORT, and CONNECT_STRING. CONNECT_STRING in 13.0.x maps to DOMAIN_PATH in the new version. Figure 9–1 and Figure 9–2 show where they are in the new Server configuration.

Figure 9–2 Server Address and Port Number (Versions13.1.2 and Later)

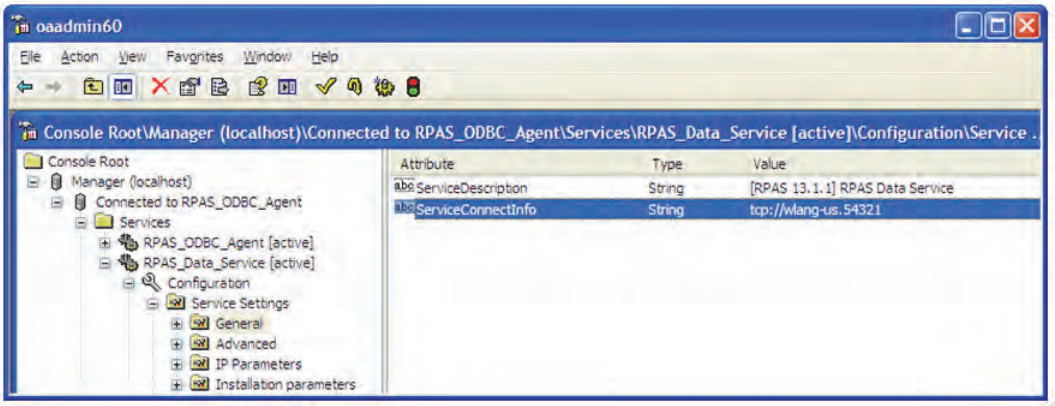
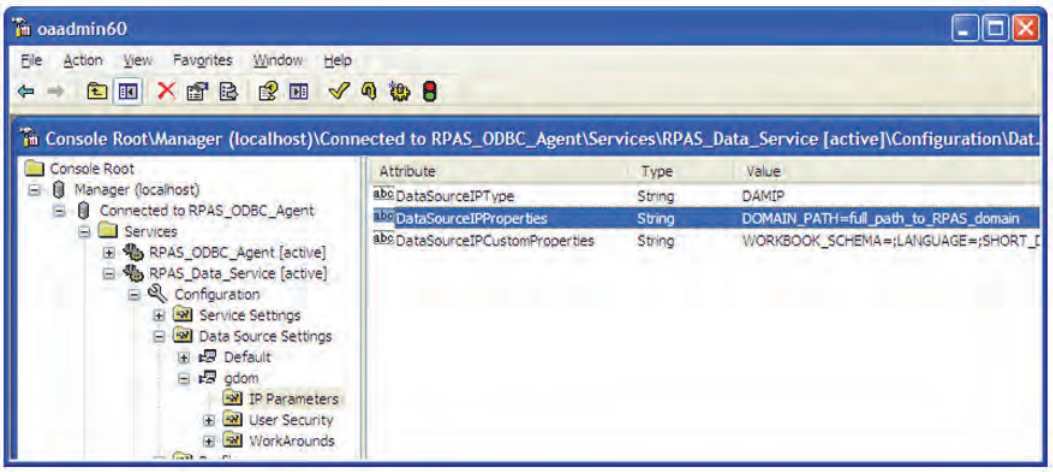


Figure 9–3 DOMAIN_PATH (Versions13.1.2 and Later)



Upgrading from 13.1.1.x

Perform the following procedure when upgrading from 13.1.1.x.

1. Before removing 13.1.1.x, take screenshots of the server configuration and server address as shown in these previous figures:
   - Figure 9–1, "Server Configuration Attributes (Versions13.1.2 and Later)"
   - Figure 9–2, "Server Address and Port Number (Versions13.1.2 and Later)"
   - Figure 9–3, "DOMAIN_PATH (Versions13.1.2 and Later)"

   These figures show the server's connecting and configuration information as well as the data sources you have.

2. Remove 13.1.1.x ODBC Server. To do this on Windows platform, run setup.exe in the server installation package and choose the **Remove** option. On UNIX platforms, delete the ODBC directory under $RPAS_HOME.
3. Install the new version (13.1.2 or later) ODBC Server. Use the information saved in the screenshots created in Step 1 to complete the server and data source configuration.

ODBC Client

The following sections describe how to update your existing ODBC client to the new version.

UNIX Platform

In 13.0.x, the client configuration information to be migrated is stored in oadrd.ini and odbc.ini. Note that odbc.ini is not required by the 13.0.x version of the RPAS ODBC Client, but it may be required by your ODBC application (such as OBIEE).

Following is a sample data source definition in oadrd.ini.

```
ADDRESS=hostname.example.com
PORT=54321
REMARKS=
```

To migrate SampleDataSource to the new version (13.1.2 or later) of the ODBC Client, create an entry for SampleDataSource in odbc.ini:

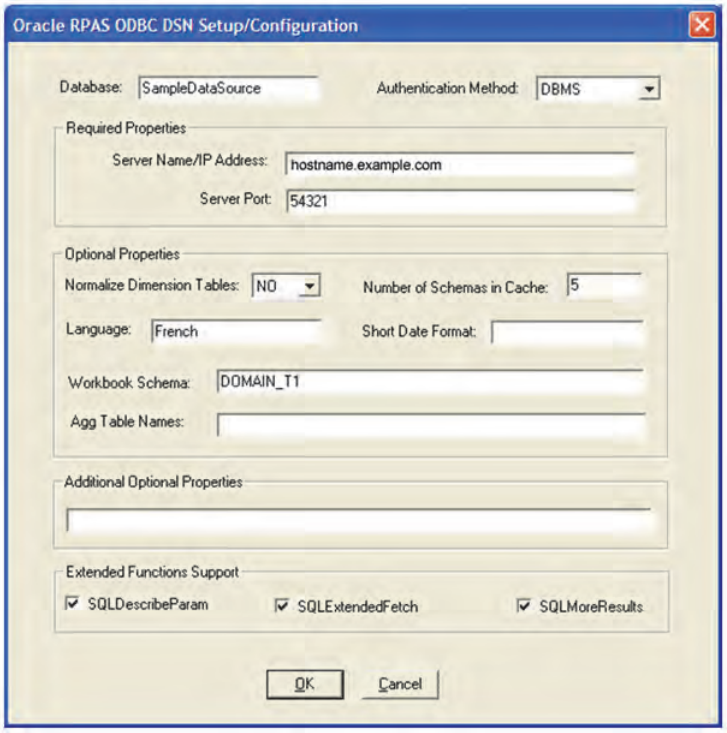
```
[ODBC Data Sources]
SampleDataSource=Oracle Retail RPAS ODBC Driver

[SampleDataSource]
Driver=PATH_TO_ODBC_CLIENT/odbcclient32/lib/ivoa22.so
Description=Oracle Retail RPAS ODBC Driver
Host=hostname.example.com
Port=54321
ServerDataSource=gdom
UseLDAP=0
DistinguishedName=
Encrypted=0
LoadBalancing=0
AlternateServers=
ConnectionRetryCount=0
ConnectionRetryDelay=3
CustomProperties=
```

The customProperties entry in odbc.ini can be copied to the same entry in the new version of odbc.ini.

Windows Platform

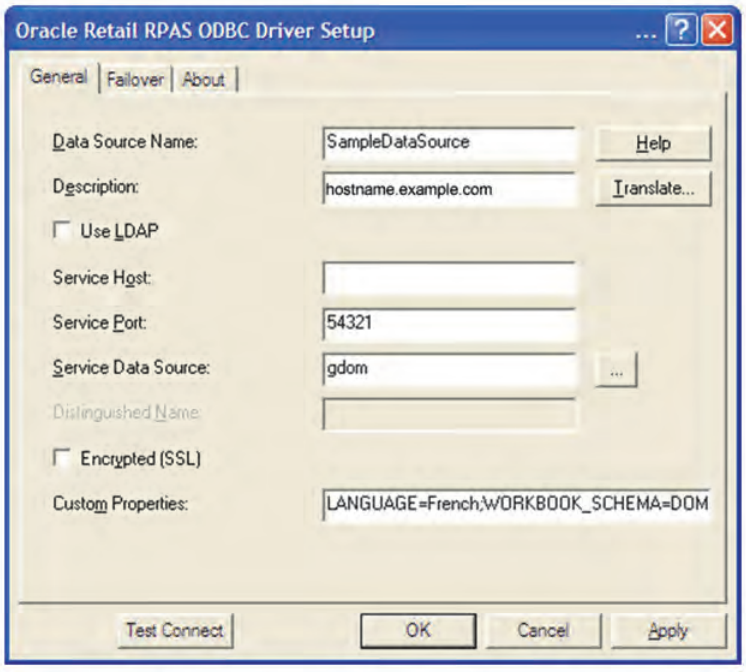
Figure 9–4 shows a sample data source in the 13.0.x version of the ODBC Client.

Figure 9–4 RPAS ODBC DSN Setup/Configuration for 13.0.x



In 13.3 and later versions, the Microsoft ODBC Administrator is used for creating and configuration the ODBC data source.

Figure 9–5 RPAS ODBC Driver Setup (Versions13.1.2 and Later)



All properties in Optional Properties and Additional Optional Properties in 13.0.x map to the Custom Properties in the new version (13.1.2 or later).

The properties are:.

- NORMALIZE_DIM_TABLES
- SCHEMA_IN_CACH
- LANGUAGE
- WORKBOOK_SCHEMA
- AGG_TABLE_NAMES
- SHORT_DATE_FORMAT
- DEFAULT_SCHEMA
- LOG_FILE
- RPAS_LOG_LEVEL

JDBC Client

The following sections describe how to update your existing JDBC client to the new version.

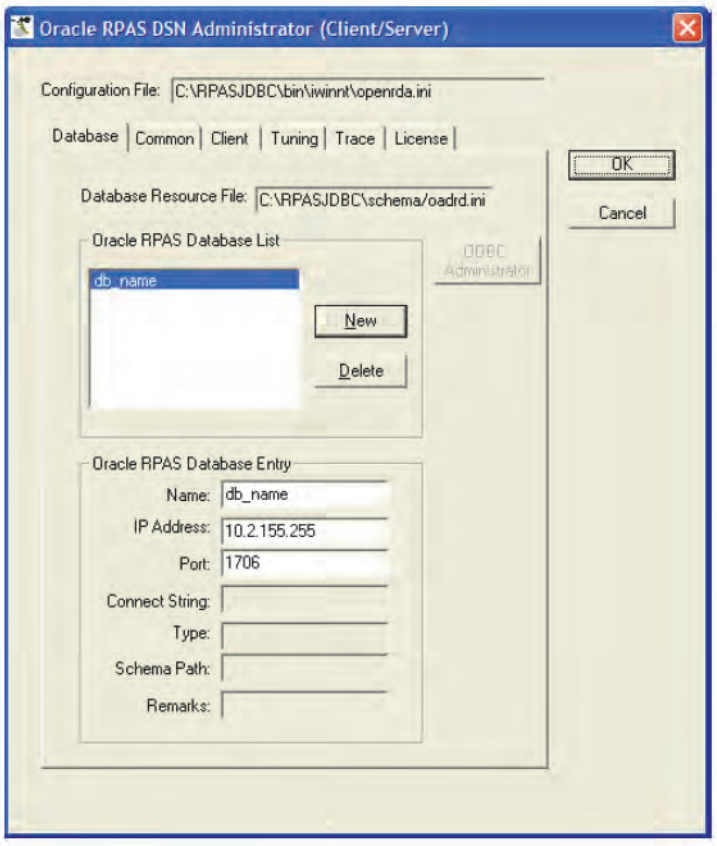
Upgrading from 13.0.x

Perform the following procedure when upgrading from 13.0.x

1. Before removing the 13.0.x JDBC Client, record the data sources that you want to migrate to the new version (13.1.2 or later).
   - To do this on Windows platforms, open the Admin Tool (shown in Step 3), gather the name, IP address, and port (of the server).
   - On UNIX platforms, use the command line Admin utility rpasjdbcclientadmin to gather the same information.

   You should also collect the optional custom connection properties that may exist in your JDBC URLs if you use URL in your JDBC applications.
2. Remove the 13.0.x JDBC Client.
   - To do this on Windows, run setup.exe and choose the **Remove** option.
   - On UNIX, delete the jdbcclient directory.
3. Install the new version (13.1.2 or later) of the JDBC Client. For instructions, refer to the RPAS ODBC/JDBC Driver chapter in either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*. Then use the information gathered in Step 1 to construct the URLs for your JDBC applications.

Figure 9–6 RPAS DSN Administrator (Client/Server) Window



Upgrading from 13.1.1.x

Perform the following procedure when upgrading from 13.1.1.x.

1. Gather the information for the server's IP address, port number, data source name, and any custom connection properties in the 13.1.1.x JDBC URLs.
2. Remove the 13.1.1.x version of the JDBC Client.
3. Install the new version (13.1.2 or later) JDBC Client.
4. Use the information gathered in Step 1 to construct the JDBC URLs for the new JDBC Client.

10

RPAS Fusion Client Patch Installation

The Fusion Client patch process follows the same process as the full installation. For detailed instructions, refer to the section, "Installation Tasks" in Chapter 5, "Installing the RPAS Fusion Client". Before applying the patch, ensure that you backup the Fusion Client installation as a precaution.

When applying a Fusion Client patch, the existing configuration files are backed up and applied to the new installation. Ensure that the configuration files are restored correctly and that the Foundation.xml file is correct. For more information on the configuration files, refer to the *Oracle Retail Predictive Application Server Administration Guide for the Fusion Client*.

Note: After applying any Fusion Client patch, ensure that all users clear their browser cache.

The patch installation will create a Foundation.xml file based on the information provided in the installation properties file (ant.install.properties).

If the Solution ID is the same as the one already in the Foundation.xml, the patch installation will update the Solution ID parameters with the ones specified in the ant.install.properties file.

11

RPAS Classic Client Patch Installation

The RPAS Classic Client can be installed through either of the following methods:

- Windows Installer Method
- Classic Client Web Deployment

The following sections describe the installation processes for these two methods.

Windows Installer Method

This section describes the installation of the RPAS Classic Client on Windows machines, and describes how to configure the client to connect to a domain.

Make RPAS Classic Client Files Generally Accessible

Perform the following procedure to make the RPAS Classic Client available.

1. Create a directory on the network from where users will install the RPAS Classic Client.

   The location and the name of the directory are up to the system administrator's preferences. This directory is henceforth referred to as the [RPASCLIENT] directory.

2. Extract the client from the ARPOPlatform-13.3.1.clients.zip included in the main package to the [RPASCLIENT] directory.

Installing the RPAS Classic Client

The RPAS Classic Client installation procedure is the same for all of the RPAS applications. Perform the following procedures to install the application onto a PC.

1. Run the setup.exe file located in the [RPASCLIENT] directory on the network.
2. The welcome page is displayed. Follow the installation procedures as prompted.

   The setup program exits after the installation is complete.

Configuration

After creating an RPAS domain and starting the DomainDaemon (refer to the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide*.), you must configure the RPAS Classic Client to connect to the domain on a server. This section provides instructions for configuring the RPAS Classic Client on a local computer using a Microsoft Windows operating system.

The EConfigure Utility

EConfigure is a Windows application that configures the client-server communication for RPAS. EConfigure lets you specify communication parameters and produces a file that is used as input to the client. These files must be in FCF (Foundation Configuration File) format/extension. The files contain the necessary information for the client to start up the communication with the server. These files can be stored on the client machine or on the network.

When the client is executed, a file named Foundation.FCF is expected in the same directory. If the file has a different name or if it is stored somewhere on the network, the path to this file must be passed in as an argument to the client.

EConfigure consists of a menu bar, a main view, and the advanced settings dialog box. Passwords saved in the FCF file are encrypted. To launch EConfigure, double-click the EConfigure.exe file, which is by default located in the root directory of the RPAS Classic Client.

Menu Bar

The files produced by EConfigure may contain multiple connections. Each connection will be specific for a server with certain communication settings. Connections need to have unique descriptions, and they can be added and deleted using the menu bar.

Figure 11–1 EConfigure Menu Bar

Main View

The main view has the basic connection parameters. On this view, three groups of controls are available:

- The connection group
- The domains group
- The Advanced Settings dialog

The Connection Group

The connection group has these fields:

Field	Description
Database Server	The hostname or the IP address of the server, for example, atldev03 or 10.2.1.23. This value should be localhost when running the RPAS Server on a Windows machine.
Daemon Port	The port number on which the domain daemon is listening. This must be an integer between 1025 and 65535 (for example, 55278).

The Domains Group

The domains group has these fields:

Field	Description
Domain	The name of the domain that is displayed to the user when logging in. Select a domain from the list or type the name of a new domain and click **Add Domain**. You can delete a domain from the list by selecting it and then clicking **Delete Domain**.
Domain Path	The full path to the directory containing the domain, for example, /root/testenv/domain/Sample_Project
User	Provide the user ID if you do not want to force the user to provide it when logging in. The user ID must be defined in the associated domain.
Password	Provide the password for the user if you do not want to force the user to provide it when logging in. This password must match the password defined in the domain for the associated user.

The Advanced Settings Dialog

The Advanced Settings Dialog has these fields for the default database login:

Field	Description
User	The database user that is used by the client if a domain specific user has not been entered, for example, adm.
Password	Like the default database user, default database password is used if a domain specific password has not been entered, for example, adm.
Database Port Range	Port range is used to specify the range of ports on which the RPAS Server processes is started by the DomainDaemon (the rpasDbServer processes). The port Start and port End fields are the lower and upper limits of this range respectively. These fields must be integers between 1025 and 65535, which are also the default values if values are not specified, for example, Start: 40000, End: 45000.
Compression Threshold	The number of bytes above which client and server are using compression. Only advanced users should manipulate this number.
Web Tunneling	The configuration of Web tunneling.
Proxy Settings	The configuration of the RPAS Classic Client to support a proxy server is not completed in this utility.

Classic Client Web Deployment

For instructions on Classic Client web deployment for patch installations, refer to Chapter 7, "RPAS Classic Client Web Deployment" in the Full Installation section. If the web environment needs to upgrade, the web deployment instructions for full installations and patch installations are the same. If the web environment is unchanged, simply install the new WAR file after the same preparation.

A

Appendix A: Bandwidth Requirements

Understanding Bandwidth Requirements

The bandwidth requirements for a Web-based deployment of the RPAS Classic Client are minimal. The only large data transfer that occurs in this configuration is installation of the RPAS Classic Client to a PC (approximately 5 MB of data). This happens very infrequently. The client software is installed the first time a PC tries to connect to a domain or if the PC has an older version of the software that needs to be upgraded.

B

Appendix B:RPAS Sizing and Partitioning Considerations

This appendix provides guidelines and information on what to consider when sizing and partitioning RPAS domains. This appendix is not specific to any one solution. It is meant to give general information that will help you size and partition your solutions to achieve optimal performance.

RPAS Sizing

The number of positions within the hierarchies of a solution has an effect on the on-line and batch performance of a domain. When using a global domain, the positions along the partitioned hierarchy will be split among local domains. This partitioning will help in certain areas but is not a reason to include large numbers of positions in a single global domain environment.While there is no hard limit on how big a single global domain environment should be, the number of positions within the lowest level of each hierarchy should not be excessive. There are certain batch operations (loading hierarchies, reshaping arrays, repartitioning data between domains) that will be affected no matter how many local domains are created.

For example, assume that there is a solution that has a product, location and calendar hierarchy. In one environment, you have a single global domain instance with the product hierarchy having 1 million positions at the lowest level, the location hierarchy having 100 positions and the calendar hierarchy having 5 years. In a second environment, you have two global domain instances each with 500,000 product positions, 100 locations and 5 years of data. The loading of the product hierarchy in the first environment will be longer in than the second environment no matter how the local domains are partitioned.

Partitioning Considerations

The purpose of using a global domain and partitioning data across multiple domains is to help reduce contention, provide smaller domains for most users to interact with and to allow for parallel processing during batch. If the partitioning is not done correctly, it can lead to unnecessary contention or poor performance. Here are some key considerations to make when determining how to partition a global domain environment.

- The hierarchy that you partition on should allow the users the ability to work in a single local domain. If users require access to all positions within a hierarchy, that is not a good candidate for partitioning. For example, it does not make sense to partition on the location hierarchy if your business process requires all users to include all locations in each workbook.

- The partition level should also be above the level at which most of the data is stored. If most data is stored at the division level or below in the product hierarchy, the partition level should be at the division level or above. When data is based above the partition level of the domain, the data will be stored in the master domain. All users across the local domains that require this data will have contention from all of the users and not just the users of the local domain they are working in.
- The partitioning should be set such that the business requirements do not require high usage of the master domain. The performance of a workbook built from the master domain will never match that of a local domain workbook. The heavy usage of workbooks should take place across the local domains. For example, if most of the users only need to see data within a division then the partitioning should not be done below that level.
- The number of users that are in a single local domain should be evenly distributed across all the domains in a global domain environment. If there are a larger number of users in a single local domain than others, it will not matter how many partitions you create. The domain with the largest user group will always have the potential to experience more contention issues and poor performance. If possible, create more domains and separate more users across those domains.

Workbook Sizing Considerations

The impact of size for the end user is not limited to just the size of the domain or where they are building a workbook from. The size of the individual workbooks will have a direct affect on the performance they experience. The workbook size is a result of the number of measures and number of positions from each of the hierarchies included in the built workbook.

Note: The Fusion Client user interface hides the distinction between local and global domains and implicitly establishes user interaction with the domains to which the user has access. A user does not have to explicitly select a domain (through a profile selection during login) to work in the RPAS Fusion Client. For additional information, refer to the *Oracle Retail Predictive Application Server User Guide for the RPAS Fusion Client*.

The number of measures for a workbook template is static based on what is configured. The more measures that are configured in a template the larger the workbook becomes. As workbooks get larger, workbook operations will take longer. Specifically, operations like save and open are directly related to the overall size of the workbook.

Since the number of measures in a given workbook template are static based on what is configured, the number of positions in each hierarchy is the only factor that the end user controls from workbook to workbook using the same template. Two workbooks for the same template may have completely different performance based on how many positions are included.

The simplest way to compare the size of two workbooks for the same template is to multiply the number of positions for each hierarchy at the base intersection of the template and the measures. For example, assume that there is a workbook that has the majority of measures based at the week/style-color/channel. This workbook always contains 500 measures so that is a constant. If there is one workbook that contains 52 weeks (One year), 300 style colors and 3 channels, the total possible positions at the

base level would be slightly over 23 million cells. This does not include any aggregate values a user may view. If a user built the same workbook for two years (104 weeks), the total possible positions double to over 46 million cells. Going back to the first example and just including 450 style colors instead of 300, the total possible base level cells would increase to over 35 million.

Although there is no maximum number of cells that should be contained in a workbook, the number does have an impact on performance and therefore should be considered during design. If workbooks contain a total possible number of positions at the base level in the hundreds of millions, not only will the workbook performance be less than ideal but also the user will not be able to manage that level of detail.

C

Appendix C: rsp_manager Usage

The rsp_manager (Retail Service Pack Manager) is a Perl script tool that is capable of currently patching the following:

- RPAS
- Configuration Tools
- Domains
- Solution Environments (AIP_HOME, SCI_HOME, and so on)

This system will automatically run any creates, scripts, or procedures that need to be run when a patch is applied.

Prerequisites

You must have Perl 5.005 or later installed on your system. Most UNIX variants will have this installed by default. On Windows, an installation of Cygwin is required.

Applying a Service Pack

The following instructions describe how to install a service pack.

1. Copy component`-ver.os.tar.zip`

   Note: This component will be named `-ver.os.zip` for Windows.

   The service pack is shipped as a compressed .tar or .zip, depending on the platform. The file will be named based on the release level of the code contained within. Copy the service pack .tar.zip or .zip file to a standard service pack directory that you have previously set up.

Example C–1 Service Pack Directory

Create a service pack directory at:

```
/files1/service_packs
```

Then, copy the service pack file to (where `/service_packs` is a user-created directory for archived service packs):

```
cp ./ARPOplatform-13.3.1.sun.tar.zip /service_packs
```

In Windows, this directory would resemble the directory `C:\service_packs`.

2. Unpack the service pack from the .tar.zip or .zip file from Step 1.

Example C–2 UNIX Commands

The following are example UNIX commands to unpack the service pack.

```
cd /service_packs
unzip ARPOplatform-13.3.1.sun.tar.zip
tar -xvf
```

This will create a subdirectory in your service pack directory named the same as the service patch/pack version, which contains a directory for the platform. In this directory, you will see subdirectories for each of the modules this service pack is updating. For example, if this service pack has updates to RPAS, domains, and tools, the following module directories could be created:

```
/service_packs/ARPOplatform/13.3.1/sun/rpas
/service_packs/ARPOplatform/13.3.1/sun/domain
/service_packs/ARPOplatform/13.3.1/sun/tools
```

Additionally, this document, Release Notes, and a copy of any service pack installation scripts/libraries will be copied to a location such as:

```
/service_packs/ARPOplatform/13.3.1
```

Note: In Windows, you may use WinZip or a similar unzipping tool for this step.

---

3. Apply the service pack on a staging or production server. After extracting the service pack, you will have to apply the service pack to the installed components and any domains that have been built. Note that the service pack installation should be carried out on the same operating system as that on which the product resides.

   The syntax of applying a service pack with *rsp_manager* is:

   ```
   rsp_manager –install –sp <sp path> -domain <domain path>
   ```

Example C–3 Commands to Apply Service Pack 13.3.1 for ARPOplatform and domain

To apply service pack 13.3.1 for ARPOplatform and domain /domain1, use the following commands:

```
cd /service_packs/ARPOplatform/13.3.1/
./rsp_manager –install –sp sun –domain /domain1
```

Example C–4 Commands to Turn on File Logging

To turn on file logging of the output and store the results of the application in domain1.log, use the following commands:

```
cd /service_packs/ARPOplatform/13.3.1/
./rsp_manager –install –sp sun –domain /domain1 –log domain1.log
```

Following installation, a validation process will be run against your patched install.

Applying Service Packs on Multiple Domains

If you have more than one domain running off the same ARPOplatform, it is possible to create a domain list file and supply that file path, instead of the domain path, as an argument. This will be a text file with a full path to a domain on each line.

The additional syntax of rsp_manager is:

```
rsp_manager -install -sp <sp path> -domain <domain_list_file>
```

Example C–5 Applying Service Packs

To install service pack 13.3.1 for ARPOplatform and all domains listed in /files/domain_list.txt, use the following commands:

```
cd /service_packs/ARPOplatform/13.3.1/
./rsp_manager -install -sp sun -domain /files/domain_list.txt
```

…where /files/domain_list.txt looks similar to this:

```
cat /files/domain_list.txt
/domains/domain1
/domains/domain2
/domains/domain3
```

Note: Logging will work with multiple domains, but only one file will be created and written to. This single log will contain the output from all updated modules and domains.

Optional Arguments or Commands for rsp_manager

rsp_manager has optional arguments that will allow you to perform tasks such as an installation version report, install or patch validation, and patch application forcing. The following sections provide details on these arguments.

-no_rpas

This flag stops your RPAS_HOME from being patched. This can be used in conjunction with -no_tools, but still passing domains, in order to upgrade a domain to your RPAS_HOME code level without performing an RPAS upgrade.

-no_tools

This flag stops your RIDE_HOME from being patched. This can be used in conjunction with -no_rpas, but still passing domains, in order to upgrade a domain to your RPAS_HOME code level without performing a tools upgrade.

-no_domain

This flag stops the patch from being applied to any domains.

-log <logfile>

Although logging is done by default, the log will be saved to the current working directory as a date-stamped filename. This flag allows you to change the name of the log file created to the argument you pass.

-force

This flag enforces the application of the patch/pack regardless of the versions that the components report. This allows you to reapply a patch that has already been applied, while also running any update scripts that might have already been run.

Example C–6 -force Flag

To force reinstallation of the 13.3.1 service patch onto your installation and a single domain, with logging:

```
cd /service_packs/ARPOplatform/13.3.1/
./rsp_manager -install -sp sun -domain /domain1 -log domain1.log -force
```

-validate

This flag is run by default at the end of all -install processes. The purpose of this flag is to validate components of the service patch/pack against your installation. Currently, this will only check your core binaries and libraries in both RPAS_HOME and RIDE_HOME. Tests include permissions comparisons and file checksum validation, which are represented in the output as "P" or "C" respectively upon errors.

Example C–7 -validate Flag

To validate the 13.3.1 Sun service patch against your installation any time after patching:

```
cd /service_packs/ARPOplatform/13.3.1/
./rsp_manager -validate -sp sun
Validating your updated install against the service pack/patch -
.....................................................................................
.....................
Validation complete...
Files Checked: 106
Files Passed: 106
Files Failed: 0
```

Note: The number of files checked might not match the previous number, as it changes quantity based on platform and patch version. If any files fail, a listing of those failed files will be presented, each being preceded by flags ("C" or "P") to indicate which checks failed.

Optional Environment Variables

Note: The following process is not a suggested installation process, but Oracle Retail acknowledges that it may be more efficient in some limited cases.

Since rsp_manager relies on the Retek.pm library, this file must normally be in the same directory as the one you run rsp_manager from. You may use an environment variable to point to the path that contains the library so that they can be split from each other. A useful instance would be setting up a directory in your path and placing rsp_manager inside, while using the RSP_HOME environment variable to point to the

directory that contains the Retek.pm file. This would allow you to run rsp_manager from anywhere on the system.

Example C–8 Running rsp_manager

To be able to run rsp_manager from anywhere:

```
> cd /service_packs/ARPOplatform/13.3.1/
> ls
rsp_managerRetek.pm
> mkdir ~/bin
> cp ./rsp_manager ~/bin/
> export PATH=~/bin:$PATH
> export RSP_HOME=/service_packs/ARPOplatform/13.3.1
```

At this point, you can change directories to anywhere on the disk and run rsp_manager.

Keep in mind that if you do choose to split these files, when you obtain new copies of the script and library, you will need to place them into the locations you reference in $PATH and $RSP_HOME.

D

Appendix D: Oracle Single Sign-On (SSO)

Oracle Single Sign-On Overview

This appendix provides a basic description of Oracle Single Sign-On (SSO).

What is Single Sign-On?

SSO is a term for the ability to sign onto multiple Web applications through a single user ID/Password. There are many implementations of SSO. Oracle currently provides three different implementations:

- Oracle SSO (OSSO)
- Java SSO (with the 10.1.3.1 release of OC4J)
- Oracle Access Manager (OAM 11g)

> **Note:** OAM 11g provides more comprehensive user access capabilities. For additional support information, refer to Hardware and Software Requirements.

Most, if not all, SSO technologies use a session cookie to hold encrypted data passed to each application. The SSO infrastructure has the responsibility to validate these cookies and, possibly, update this information. The user is directed to log on only if the cookie is not present or has become invalid. These session cookies are restricted to a single browser session and are never written to a file.

Another facet of SSO is how these technologies redirect a user's Web browser to various servlets. The SSO implementation determines when and where these redirects occur and what the final window shown to the user is.

Most SSO implementations are performed in an application's infrastructure and not in the application logic itself. Applications that leverage infrastructure managed authentication (such as deploying specifying Basic or Form authentication) typically have little or no code changes when adapted to work in an SSO environment.

What Do I Need for Oracle Single Sign-On?

The nexus of an Oracle SSO system is the Oracle Identity Management Infrastructure installation. This consists of the following components:

- An Oracle Internet Directory (OID) LDAP server, used to store user, role, security, and other information. OID uses an Oracle database as the back-end storage of this information.

- An Oracle HTTP Server 11g Release 1 as a front end to the Oracle WebLogic Server. The Oracle HTTP Server is included in the Oracle Web Tier Utilities 11g Release 1 (11.1.1).
- An Oracle SSO Plug-in (OAM 11g WebGate) is used to authenticate the user and create the OSSO session cookie. This is available in the Oracle Fusion Middleware 11g Identity and Access management 11g package.
- The users and group information may also be loaded or modified through standard LDAP Data Interchange Format (LDIF) scripts.
- Additional administrative scripts for configuring the OSSO system and registering HTTP servers.

For more information on setting up SSO, refer to either the Classic Client or Fusion Client version of the *Oracle Retail Predictive Application Server Administration Guide.*

Additional WebLogic managed servers are needed to deploy the business applications leveraging the OSSO technology.

Oracle SSO Terms and Definitions

This section lists the terms and definitions used in Oracle SSO.

Authentication

Authentication is the process of establishing a user's identity. There are many types of authentication. The most common authentication process involves a user ID and password.

Identity Management Infrastructure

The Identity Management Infrastructure is the collection of product and services which provide Oracle SSO functionality. This includes the Oracle Internet Directory, an Oracle HTTP server, and the Oracle SSO services. The Oracle Application Server deployed with these components is typically referred as the Infrastructure instance.

mod_wl_ohs

mod_wl_ohs operates as a module within the HTTP server that allows requests to be proxied from the Apache HTTP server to the WebLogic server.

Oracle Internet Directory

Oracle Internet Directory (OID) is an LDAP-compliant directory service. It contains user IDs, passwords, group membership, privileges, and other attributes for users who are authenticated using Oracle SSO.

Partner Application

A partner application is an application that delegates authentication to the Oracle Identity Management Infrastructure. One such partner application is the Oracle HTTP Server (OHS) supplied with the Oracle Application Server. OHS uses the OAM 11g WebGate module to configure this functionality.

All partner applications must be registered with the Oracle Access Manager.

Realm

A Realm is a collection of users and groups (roles) managed by a single password policy. This policy controls what may be used for authentication (for example, passwords, X.509 certificates, and biometric devices). A Realm also contains an

authorization policy used for controlling access to applications or resources used by one or more applications.

A single OID can contain multiple Realms. This feature can consolidate security for retailers with multiple banners or to consolidate security for multiple development and test environments.

What SSO is Not

SSO is not a user ID/password mapping technology.

However, some applications can store and retrieve user IDs and passwords for non-SSO applications within an OID LDAP server. An example of this is the Oracle Forms Web Application framework, which maps OSSO user IDs to a database logins on a per-application basis.

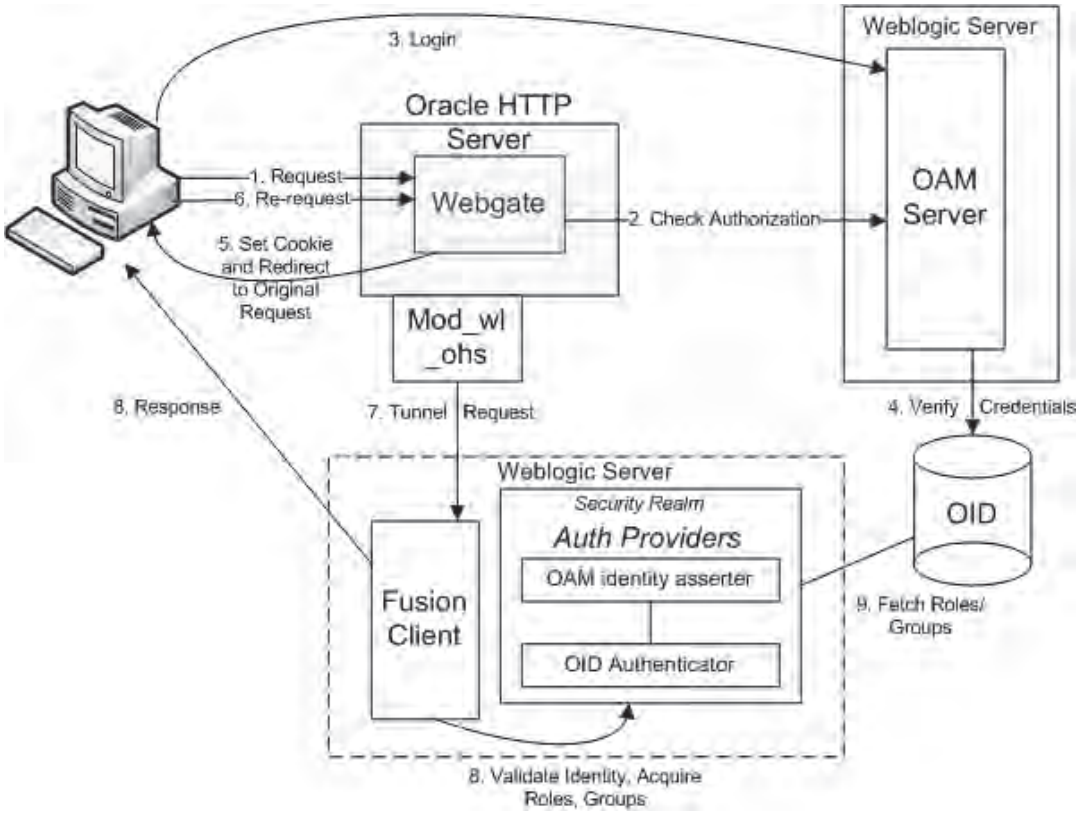
Single Sign-On Topology

RPAS usernames are case sensitive. Therefore, when setting up an SSO environment, ensure that the case sensitivity is maintained.

> **Note:** For additional information, refer to the chapter, "Configuring Single Sign-On with Oracle Access Manager 11g" in the *Oracle Fusion Middleware Application Security Guide*.

Figure D–1 illustrates the SSO topology.

Figure D–1 Single Sign-On Topology



Installation Overview

For Oracle SSO installation, refer to the Oracle Fusion Middleware Application Security Guide 11g Release 1 (11.1.1)Part Number E10043-09.

The section, Deploying the Oracle Access Manager 11g SSO Solution (http://docs.oracle.com/cd/E21764_01/core.1111/e10043/osso_b_oam11g.htm#BABHHABA), provides information on how to implement OAM 11g with the Authentication Provider when you have applications that are (or will be) deployed in a WebLogic container.

User Management

User Management consists of displaying, creating, updating or removing user information. There are two basic methods of performing user management: LDIF scripts and the Delegate Administration Services (DAS) application.

OID DAS

The DAS application is a Web-based application designed for both administrators and users. A user may update their password, change their telephone number of record, or modify other user information. Users may search for other users based on partial strings of the user's name or ID. An administrator may create new users, unlock passwords, or delete users.

The DAS application is fully customizable. Administrators may define what user attributes are required, optional or even prompted for when a new user is created.

Furthermore, the DAS application is secure. Administrators may also what user attributes are displayed to other users. Administration is based on permission grants, so different users may have different capabilities for user management based on their roles within their organization.

LDIF Scripts

Script based user management can be used to synchronize data between multiple LDAP servers. The standard format for these scripts is the LDAP Data Interchange Format (LDIF). OID supports LDIF script for importing and exporting user information. LDIF scripts may also be used for bulk user load operations.

User Data Synchronization

The user store for Oracle SSO resides within the Oracle Internet Directory (OID) LDAP server. Oracle Retail applications may require additional information attached to a user name for application-specific purposes and may be stored in an application-specific database. Currently, there are no Oracle Retail tools for synchronizing changes in OID stored information with application-specific user stores. Implementers should plan appropriate time and resources for this process. Oracle Retail strongly suggests that you configure any Oracle Retail application using an LDAP for its user store to point to the same OID server used with Oracle SSO.

E

Appendix E: Installation Order

This appendix provides a guideline for the order in which the Oracle Retail applications should be installed. If a retailer has chosen to use only some of the applications, the order is still valid, less the applications not being installed.

> **Note:** The installation order is not meant to imply integration between products.

Enterprise Installation Order

1. Oracle Retail Merchandising System (RMS), Oracle Retail Trade Management (RTM), Oracle Retail Sales Audit (ReSA), Optional: Oracle Retail Fiscal Management (ORFM)

   > **Note:** ORFM is an optional application for RMS if you are implementing Brazil localization.

2. Oracle Retail Service Layer (RSL)
3. Oracle Retail Extract, Transform, Load (RETL)
4. Oracle Retail Active Retail Intelligence (ARI)
5. Oracle Retail Warehouse Management System (RWMS)
6. Oracle Retail Allocation
7. Oracle Retail Invoice Matching (ReIM)
8. Oracle Retail Price Management (RPM)

   > **Note:** During installation of RPM, you are asked for the RIBforRPM provider URL. Since RIB is installed after RPM, make a note of the URL you enter. If you need to change the RIBforRPM provider URL after you install RIB, you can do so by editing the remote_service_locator_info_ribserver.xml file.

9. Oracle Retail Central Office (ORCO)
10. Oracle Retail Returns Management (ORRM)
11. Oracle Retail Back Office (ORBO) or Back Office with Labels and Tags (ORLAT)

12. Oracle Retail Store Inventory Management (SIM)

> **Note:** During installation of SIM, you are asked for the RIB provider URL. Since RIB is installed after SIM, make a note of the URL you enter. If you need to change the RIB provider URL after you install RIB, you can do so by editing the remote_service_locator_info_ribserver.xml file.

13. Oracle Retail Predictive Application Server (RPAS)
14. Oracle Retail Demand Forecasting (RDF)
15. Oracle Retail Category Management (CM)
16. Oracle Retail Replenishment Optimization (RO)
17. Oracle Retail Analytic Parameter Calculator Replenishment Optimization (APC RO)
18. Oracle Retail Regular Price Optimization (RPO)
19. Oracle Retail Merchandise Financial Planning (MFP)
20. Oracle Retail Size Profile Optimization (SPO)
21. Oracle Retail Assortment Planning (AP)
22. Oracle Retail Item Planning (IP)
23. Oracle Retail Item Planning Configured for COE (IP COE)
24. Oracle Retail Advanced Inventory Planning (AIP)
25. Oracle Retail Integration Bus (RIB)
26. Oracle Retail Point-of-Service (ORPOS)
27. Oracle Retail Markdown Optimization (MDO)
28. Oracle Retail Clearance Optimization Engine (COE)
29. Oracle Retail Analytic Parameter Calculator for Markdown Optimization (APC-MDO)
30. Oracle Retail Analytic Parameter Calculator for Regular Price Optimization (APC-RPO)
31. Oracle Retail Promotion Intelligence and Promotion Planning and Optimization (PI-PPO)
32. Oracle Retail Analytics
33. Oracle Retail Workspace (ORW)