Oracle® Retail Integration Bus

Security Guide Release 14.0 E49331-01

December 2013



Oracle Retail Integration Bus Security Guide, Release 14.0

E49331-01

Copyright © 2013, Oracle and/or its affiliates. All rights reserved.

Primary Author: Sanal Parameswaran

Contributing Author: Gloreen Soans

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 is software or related documentation that 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.

Contents

end Us Your Comments		
Preface	vii	
Audience	vii	
Documentation Accessibility	vii	
Related Documents	vii	
Customer Support	viii	
Review Patch Documentation	viii	
Improved Process for Oracle Retail Documentation Corrections	viii	
Oracle Retail Documentation on the Oracle Technology Network		
Conventions	ix	

1 Security Overview

Physical Deployment Model	1-1
Dependent Applications	1-2
Oracle Retail Integration Bus Administration User Interface	1-2
General Security Principles	1-2
The Foundations of Security	1-2
Oracle Credential Store Framework API Principles	1-3
Oracle Retail Recommended Security Approach	1-3
Oracle Software Security Assurance (OSSA)	1-3
OSSA compliance	1-4

2 RIB Secure Installation and Configuration

Security in RIB Application Builder		
Security in RIB Deployment Configuration File Editor	2-2	
Security During RIB Deployment Process	2-2	
Security During RIB Runtime	2-2	
RIB Administration Security	2-2	
Security in RIHA	2-3	
Security in RDMT	2-3	
Security in PL/SQL Application API Stubs	2-3	
Security in Integration Gateway Services	2-3	
Secure Sockets Layer Configuration	2-3	
Security in Injector Service	2-4	
• •		

RIB-OMS Security Configuration	
RIB-OMS to RSB-OMS Routing Service Security Configuration	2-5

3 Secure IGS Web Services Using Administration Console

Server-side Setup for Username and Password Authentication	3-1
Attach the Policy File to the Web Service	3-1
Create Roles and Users	3-8
Client-side Setup for Username and Password Authentication	3-17
Server-side Setup for Encrypted Username and Password Token Authentication	3-18
Client-side Setup for Encrypted Username and Password Token Authentication	3-21

4 Security Feature Overview

Securing Sensitive Data	4-1
Cardholder Data	4-1
Communication with web service Application	4-1
Securing the Application	4-1
Passwords	
Default Accounts and Passwords	4-2
Tools	4-2
Securing the Application Environment and Configuration	4-2
Database	4-2

A Credential Store Framework

Oracle Retail RIB CSF Implementation A	\-1
--	-----

B Keytool Utility

Creating a Self-Signed Certificate	
Creating a Certificate Signing Request	B-1
Exporting and Importing Certificates	B-1

C Secure Web Services

WS-Security	C-1
Web Service Security Implementation	C-1
Oracle Retail Management System Web Service	C-1

Glossary

Send Us Your Comments

Oracle Retail Integration Bus Security Guide, Release 14.0

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

This document serves as a guide for administrators, developers, and system integrators who securely administer, customize, and integrate applications using Oracle Retail Integration Bus (RIB). Installation and configuration for each product are covered in more detail in the each product's Installation Guide.

Audience

This document is intended for administrators, developers, and system integrators who perform the following functions:

- Document specific security features and configuration details for the Oracle Retail Integration Bus products, in order to facilitate and support the secure operation of the Oracle Retail product and any external compliance standards.
- Guide administrators, developers, and system integrators on secure product implementation, integration, and administration.

It is assumed that the readers have general knowledge of administering the underlying technologies and the application.

Documentation Accessibility

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit

http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are
hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Retail documentation set:

- Oracle Retail Integration Bus Implementation Guide
- Oracle Retail Integration Bus Installation Guide
- Oracle Retail Integration Bus Release Notes

- Oracle Retail Integration Bus Hospital Administration Guide
- Oracle Retail Integration Bus Operations Guide
- Oracle Retail Integration Bus Support Tools Guide
- Oracle Retail Enterprise Integration Guide
- Oracle Retail Functional Artifacts Guide
- Oracle Retail Integration Bus Integration Gateway Services Guide
- Oracle Retail Functional Artifact Generator Guide
- Oracle Retail Service-Oriented Architecture Enabler Tool Guide
- Oracle Retail Integration Bus Data Model
- Oracle Retail PL-SQL Payload Mapper Guide (ID 1590674.1)

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, 14.0) or a later patch release (for example, 14.0.1). If you are installing the base release and additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times not be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Technology Network Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

This process will prevent delays in making critical corrections available to customers. For the customer, it means that before you begin installation, you must verify that you have the most recent version of the Oracle Retail documentation set. Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

http://www.oracle.com/technetwork/documentation/oracle-retail-100266.ht

ml

An updated version of the applicable Oracle Retail document is indicated by Oracle 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 a document with part number E123456-01.

If a more recent version of a document is available, that version supersedes all previous versions.

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.	

Security Overview

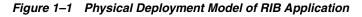
Security in the integration layer is a big concern for every retail enterprise. The security system should be open enough to allow trusted remote applications to integrate easily and, at the same time, lock down unauthorized remote access. To address security concerns, RIB utilizes the security modules available in the Oracle middleware and database systems.

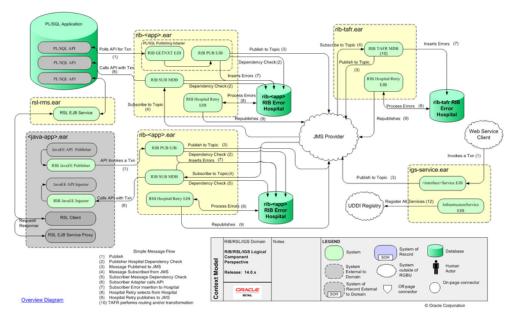
This chapter provides an overview of the security features in Oracle Retail Integration Bus. It includes the following sections:

- Physical Deployment Model
- Dependent Applications
- General Security Principles
- Recommended Approach

Physical Deployment Model

The following figure illustrates the physical deployment model of the RIB application.





The Web-based RIB Administrator user interface is accessed using a browser. You are responsible for applying the necessary security patches to the Web browser and the operating system.

The typical configuration of RIB runs on the following server:

- Oracle WebLogic Server 11g Release 2 (10.3.6) that hosts the rib application (rib-<app>.ear).
- Oracle Database 11g Release 2 (11.2.0.2).

You are responsible for applying any critical patch updates releases for the server hardware, application server, and the database.

Dependent Applications

Security Guides for dependent applications can be found at the following links.

- Oracle Database 11g Release 2 (11.2.0.2): http://docs.oracle.com/cd/E11882_ 01/server.112/e10575.pdf.
- Oracle WebLogic Server 11g Release 1 (10.3.6): http://docs.oracle.com/cd/E21764_01/web.1111/e14529/security.htm.

Oracle Retail Integration Bus Administration User Interface

Each RIB application PAK ear i.e. rib-<app>.ear deployed in application server has a Web based user interface application which can be accessed via HTTP or HTTPS. If the HTTP protocol is disabled, and accessing this application over HTTP is not possible, a valid SSL certificate needs to be installed to access the administration GUI over HTTPS. To install a valid SSL Certificate on the application server, see the documentation for your installed application server. The use of the default SSL certificate shipped with the application server is not recommended because it renders the application prone to intrusion attacks.

General Security Principles

Security is fundamentally about protecting assets. It is important to recognize that security is a path, not a destination. As you analyze your infrastructure and applications, you identify potential threats and understand that each threat presents a degree of risk. Security is about risk management and implementing effective countermeasures. One of the most important concepts in security is that effective security is a combination of people, process, and technology.

The Foundations of Security

Security relies on the following elements:

Authentication

Authentication addresses the question: who are you? It is the process of uniquely identifying the clients of your applications and services. These might be end users, other services, processes, or computers. In security parlance, authenticated clients are referred to as principals.

Authorization

Authorization addresses the question: what can you do? It is the process that governs the resources and operations that the authenticated client is permitted to access. Resources include files, databases, tables, rows, and so on, together with

system-level resources such as registry keys and configuration data. Operations include performing transactions such as purchasing a product, transferring money from one account to another, or increasing a customer's credit rating.

Auditing

Effective auditing and logging is the key to non-repudiation. Non-repudiation guarantees that a user cannot deny performing an operation or initiating a transaction.

Confidentiality

Confidentiality, also referred to as privacy, is the process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users or eavesdroppers who monitor the flow of traffic across a network. Encryption is frequently used to enforce confidentiality. Access control lists (ACLs) are another means of enforcing confidentiality.

Integrity

Integrity is the guarantee that data is protected from accidental or deliberate (malicious) modification. Like privacy, integrity is a key concern, particularly for data passed across networks. Integrity for data in transit is typically provided by using hashing techniques and message authentication codes.

Oracle Credential Store Framework API Principles

A credential store is used for secure storage of credentials. The Credential Store Framework (CSF) API is used to access and perform operations on the credential store. The Credential Store Framework:

- Enables you to manage credentials securely.
- Provides an API for storage, retrieval, and maintenance of credentials in different back-end repositories.
- Supports file-based (Oracle wallet) and LDAP-based credential management.

Critical (create, update, delete) functions provided by the CSF API include:

- Verifying if a credential map, or a credential with a given key, exists in the store.
- Returning credentials associated with <mapname, key>.
- Assigning credentials to <mapname, key>.
- D.eleting credentials associated with a given map name, or a given map name and key.
- Resetting credentials for a specified <mapname, key>.

Oracle Retail Recommended Security Approach

This section discusses the two security approaches that Oracle Retail recommends.

Oracle Software Security Assurance (OSSA)

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products. Oracle's goal is to ensure that Oracle's products, as well as the customer systems that leverage those products, remain as secure as possible.

OSSA compliance

To be OSSA compliant, it is required to use the CSF API to store the passwords in Oracle wallet based files. RIB and other products use the CSF API through a Credential Store Manager utility. This utility provides methods that can store and retrieve credentials from a wallet based file. Internally this utility is using CSF API to manage the credentials.

RIB Secure Installation and Configuration

This chapter explains how to securely configure Oracle Retail Integration Bus applications and related tools. For installation instructions, see the Installation Guide that accompanies each product.

Security in RIB Application Builder

RIB Application Builder is a tool for building and deploying RIB applications on the WebLogic server. The rib-deployment-env-info.xml file is the single source of all values used in the RIB App Builder tools. It is the only (or should be the only) file that requires editing. The RIB installer gathers the appropriate values from you, constructs the file, and invokes the appropriate tools.

```
<aq-jms-server jms-server-id="jms1">
<jms-server-home>linux1@linux1:/home/oracle/oracle/product/10.2.0/db_
1</jms-server-home>
<jms-url>jdbc:oracle:thin:@linux1:1521:ora10g</jms-url>
<jms-port>1521</jms-port>
<jms-user-alias>jms1_user-name-alias</jms-user-alias>
</aq-jms-server>
```

This file does not contain the username and password for connecting to the application server or the databases. Rather, it contains the alias for each user name/password combination. This alias refers to the user name/password stored in a secured wallet file. The wallet file is created when the user runs the application assembly tool during the RIB application building process.

The syntax for the application assembly command is as follows:

rib-app-compiler.sh setup-security-credential

The argument, *setup-security-credential*, must be used when running the rib-app-compiler for the first time. It prompts the user to enter all usernames and passwords required to install RIB components. It stores details as credentials in a wallet file inside the *rib-home/deployment-home/conf/security/* directory. The credentials are retrieved and used by the deployer script when installing RIB components.

Only the operating system user who created the wallet file with the RIB application assembly tool has read and write access to the file. Other users do not have permission to access the file. The file permissions are set up during the post-deployment phase for RIB applications.

For more information about RIB Application Builder, see the *Oracle Retail Integration Bus Operations Guide*.

Note: You can also change usernames and passwords for the RIB applications after deploying them. Refer to the section "setup-security-credential," under "RIB App Builder Tools" in the "Application Builder" chapter in Oracle Retail Integration Bus Operations Guide for information on changing RIB usernames and passwords after deployment.

Security in RIB Deployment Configuration File Editor

The RIB Deployment Configuration File Editor is an application used to configure the rib-deployment-env-info.xml file, following installation. It provides a user interface for adding, removing, and rearranging the elements of the RIB configuration.

This tool has fields for entering usernames and passwords required for connecting to application server and databases. Values entered in the password field in the tool are displayed as a series of asterisks (one for each character). The values entered in this field are stored in the secured wallet file in the

rib-home/deployment-home/conf/security/ directory.

For information about the RIB Deployment Configuration File Editor, see the section "RIB Deployment Configuration File Editor," in the "Application Builder" chapter in the *Oracle Retail Integration Bus Operations Guide*.

Security During RIB Deployment Process

You can run the RIB application assembly tool to build RIB application ear files. The generated .ear files contain deployment descriptors for data sources used by RIB runtime to connect to the application database and the error hospital database. The deployment descriptors contain the username for accessing the database, but the passwords are not stored there. During the deployment process for the RIB application, the passwords are read from the wallet file and encrypted using a WebLogic utility. The encrypted passwords are added in a WebLogic deployment plan that is uploaded on the server along with the .ear file.

Security During RIB Runtime

During the runtime process, the RIB application must make calls to the JMX server. WebLogic instance username and password are required to make connections to the JMX server. This information is stored in a secured wallet file, the path to which is stored in the rib-system.properties file.

For information about the properties in rib-system.properties file, see the "rib-system.properties" section in the "Backend System Administration and Logging" chapter of the *Oracle Retail Integration Bus Operations Guide*.

Only the operating system user who created them has read and write access to the properties files created during the RIB application deployment process. Other users do not have permission to access the files. Permissions are granted during the post deployment phase for RIB applications.

RIB Administration Security

For more information on RIB administration security, see the *Oracle Retail Integration Bus Implementation Guide*.

Security in RIHA

Oracle Retail Integration Bus Hospital Administration or RIB Hospital Administration (RIHA) is a tool to manage RIB messages in the RIB error hospital tables. It is a Web application that is deployable on the WebLogic server.

For more information on setting up security for RIHA, see the "Installation and Setup" section in the *Oracle Retail Integration Bus Hospital Administration Guide*.

Security in RDMT

The RIB Diagnostic and Monitoring Toolkit (RDMT) is a collection of command line tools for controlling and monitoring RIB applications. When used from within rib-home, RDMT loads configuration information from the rib-deployment-env-info.xml file. For username and password information, it reads

the wallet file created during the RIB application assembly process.

For information about RDMT, see the "Diagnostic and Monitoring Tools" chapter in the *Oracle Retail Integration Bus Operations Guide*.

Security in PL/SQL Application API Stubs

The plsql-api-stub is an API simulator designed to act as though the RIB is connected to the application, but it can process specific status and other parameters from a "stubbed" application. This set of tools is designed to emulate those applications exposing PL/SQL APIs to RIB, such as RMS and RWMS. The tool reads and writes the username and password for connecting to the database in a secured wallet file.

Security in Integration Gateway Services

The RIB Integration Gateway Services (IGS) component is a set of standard Simple Object Access Protocol (SOAP) based Web services that provide access to the RIB infrastructure. These Web services are generated using the Oracle Retail Service Enabler Tool. They should be secured after being deployed.

For more information, see Chapter 3 - Secure IGS Web Services Using the Administration Console in this guide.

Secure Sockets Layer Configuration

Secure Sockets Layer (SSL) provides secure connections by allowing two applications connecting over a network to authenticate each other's identity and encrypting the data exchanged between the applications. Configuring SSL in WebLogic servers in production environments is recommended.

For more information, see the WebLogic documentation on configuring SSL in WebLogic 11g server at http://download.oracle.com/docs/cd/E15523_01/web.1111/e13707/ssl.htm#SECMG384

Deployment of RIB applications over SSL protocol are supported by entering protocol values as https in deployment info xml file. After the applications are deployed, they run on the SSL protocol.

The following are high level steps for running the RIB in SSL environment:

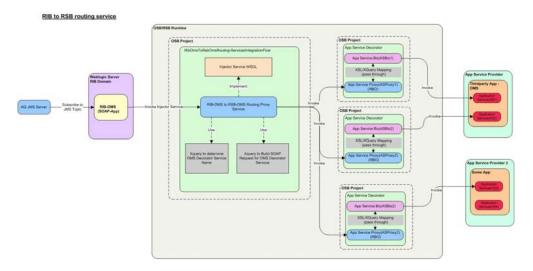
1. Configure SSL in the WebLogic server. (See WebLogic documentation for detailed steps.)

- 2. Keep the SSL ports of the WebLogic server instances open for RIB deployment. Verify that the SSL port is open: In the WebLogic administration console, go to the Configuration > General page of the server instance. Verify that the SSL Listen Port Enabled checkbox is checked and provide a unique listen address to each managed server and the admin server.
- **3.** Make sure that the rib-deployment-env-info.xml file has protocol specified as https and port numbers are https port numbers for WebLogic server instances.
- **4.** Start the managed server with SSL port enabled. For example, startManagedServer.sh rib-oms-server <AdminServerUrl>.
- **5.** Deploy the RIB applications.
- 6. If required, non-SSL ports can be disabled as follows. In the WebLogic administration console, go to the **Configuration** > **General page** of the server instance. Uncheck the Listen Port Enabled checkbox and check the SSL Listen Port Enabled checkbox. This is an optional step and must be done only when all communications with the server are over HTTPS protocol.

Security in Injector Service

The RIB integrates with the Web service providers (example: OMS) using an injector service. This section contains details about the security configuration required on RIB side.

End application (OMS) Web services can be secured with policyA or policyB. For more details on application service security, see the *Oracle Retail Service Backbone Security Guide*.





RIB-OMS Security Configuration

Provide the RibOmsToRsbOmsRoutingService URL, user-alias, and ws-policy-name information in rib-deployment-env-info.xml file present under rib-home/deployment-home/conf. The endpoint URL should be the secured injector service URL and user alias should be in <rib-app>_ws_security_user-name-alias format i.e. rib-oms_ws_security_user-name-alias. The ws-policy name should be either policyA or policyB depending on the OMS application Web service configuration.

Figure 2–2 RIB-OMS Security Configuration



For more information on installing the RIB-OMS application, see the *Oracle Retail Integration Bus Installation Guide*.

RIB-OMS to RSB-OMS Routing Service Security Configuration

Security policies needs to be applied on each layer listed below:

- Application Web services secured with policyA or policyB.
- Decorators, which are proxy to actual application service, will also have security policies applied.
- Injector service which is a bridge between the RIB and the RSB will also have security policies applied.

For more information on applying security policies to decorator services, see *Oracle Retail Service Backbone Security Guide*.

Take the following steps to apply security policies in a routing service:

1. Click the routing service proxy *RibOmsToRsbOmsRoutingService*. The following window appears. Click **Edit** as shown in red rectangular box.

Figure 2–3 Edit a Proxy Service - Summary

눌 Edit a Proxy Service - Summa	$\label{eq:construction} ry~(RibOmsToRsbOmsRouting-ServicesIntegrationFlow/ProxyService/RibOmsToRsbOmsRoutingService)$
General Configuration	
Service Name	RibOmsTaRsbOmsRouttingService
Description	
Service Type	Web Service - SOAP 1.1 (WSDL:RibOmsToRsbOmsRouting-ServicesIntegrationFlow/ProxyService/wsdl/InjectorService, port = "InjectorPort")
Transport Configuration	
Protocol	http
Endpoint URI	/RibOmsToRsbOmsRoutting-ServicesIntegrationFlow/ProxyService/RibOmsToRsbOmsRouttingService
Get All Headers	No
Headers	
HTTP Transport Configuration	
HTTPS required	No
Authentication	None
Operation Selection Configuration	
Enforce WS-I Compliance	No
Selection Algorithm	SOAP Body Type
Message Handling Configuration	
Transaction Required	Disabled

2. Select the HTTPS required option.

Figure 2–4	Edit a Proxy Service
------------	----------------------

HTTP Transport Config	uration	
HTTPS required		
Authentication	None Basic Client Certificate Custom Authentication (See Advanced Settings)	
Dispatch Policy	default	
Request Encoding		
Response Encoding		
Advanced Settings		8

3. Click on Last>>.

Figure 2–5 HTTP Transport Configuration

HTTP Transport Configuration	
HTTPS required	Yes
Authentication	None
Operation Selection Configuration	
Enforce WS-I Compliance	No
Selection Algorithm	SOAP Body Type
Message Handling Configuration	
Transaction Required	Disabled
Content Streaming	Disabled
XOP/MTOM Support	Disabled
	No

- 4. Click Save.
- **5.** Click the routing service proxy *RibOmsToRsbOmsRoutingService* again. The following window appears. Apply the policy by selecting the **Policies** tab. Choose the **OWSM Policies** radio button and click **Add**.

Figure 2–6 Service Policy Configuration - Policies Tab

Configuration Details	Operational Settings	SLA Alert Rules		Policies	Security	
a Service Policy Configuration	ı					
OWSM Policies						
From OWSM Policy Store						
WLS 9 Policies						
O From WSDL						
O From Pre-defined Policy or	WS-Policy Resource					
📄 🍃 RibOmsToRsbOmsRoutin	gService					
Service Level Policies						
Name		Category	Status	Description		A
		No OWSM Polic	ies to display.			
Add						8

6. Choose *oracle/wss_username_token_over_ssl_service_policy* and click **Submit**.

Figure 2–7 Select OWSM Policy

2	Search Name: Category	r: All	×	Search	View All
	Pag	je <u>3</u> of 3	Items	31-35 of 35 🛛 🔍	1 2 3 🕨 🕅
	Name 🛆	Category	<u>Status</u>	Description	
0	oracle/wss_saml_or_username_token_service_policy	Security	Enabled	This policy authenticat	tes users using cr
0	oracle/wss_saml_token_bearer_over_ssl_service_policy	Security	Enabled	This policy authenticat	tes users using cr
0	oracle/wss_saml_token_over_ssl_service_policy	Security	Enabled	This policy authenticat	tes users using cr
۲	oracle/wss_username_token_over_ssl_service_policy	Security	Enabled	This policy uses the cr	edentials in the ⁶
0	oracle/wss_username_token_service_policy	Security	Enabled	This policy uses the cr	edentials in the ⁶
	Pac	e 3 of 3	Items	31-35 of 35 🛛 🔌	1 2 3 🕨 🕅

7. Click Update.

Figure 2–8 Service Policy Configuration

Configuration Details	Operational Settings	SLA Alert Rules		Policies	Security
Service Policy Configuration	n				
WSM Policies					
From OWSM Policy Store					
WLS 9 Policies					
From WSDL					
O From Pre-defined Policy or	WS-Policy Resource				
🚽 눌 RibOmsToRsbOmsRoutin	gService				
The second se					
Service Level Policies					
Service Level Policies		Category	Status	Description	
	n_over_ssl_service_policy	Category Security	Status Enabled	10 NO	credentials in the ⁸

8. Click the **Security** tab.

Figure 2–9 General Configuration - Security Tab

Configuration Details	Operational Settings	SLA Alert Rules	Policies	Security	
General Configuration					
Service Key Provider			Browse		
Policy Overrides					
Override Values	Policy Name		Property	Default Value	Override Va
	oracle/wss_username_token_	over_ssl_servi	reference.priority	[No Policy Default]	
Web Services Security Confi	guration				
Process WS-Security Header	🔘 Yes 💿 No				
Access Control					
Transport Access Control	**************************************	iervice			

9. Select No (Pass-through option) as the Process WS-Security Header option.

Note: Both decorators and injector service proxy services are pass-through. This means that they will not authenticate the user but instead will pass the credentials to the application Web service; the application Web service will authenticate the user.

10. Click **Activate** and **Submit** to save the session.

The above steps complete securing the injector service using the OSB Console.

Secure IGS Web Services Using Administration Console

IGS Web services can be secured in two ways. One approach is to use a simple username and password authentication method. The second approach is to use passwords that are encrypted with certificates.

The following describes both approaches for server-side and client-side setup.

Note: The various policy files that can be used to secure Web services are listed in the WS-Policy tab of the Web service in the WebLogic Server Administration Console.

Server-side Setup for Username and Password Authentication

This section describes the two-step process required for securing Web services on the server side. These steps are performed using the Oracle WebLogic Server Administration Console.

Attach the Policy File to the Web Service

The usernametoken.xml contains the policy used by the web service and is found in the META_INF/policies folder in the .ear file.

Complete the following steps to attach the policy file to a Web service:

1. In the Summary of Deployments screen, click on the application. In the illustration below, the application is igs-service.

hange Center	2 Ho	one Log Out Preferences 🔛 Record Help			W	Alcome, weblogic Connected to: rib_domai
iew changes and restarts	Home	-Summary of Deployments				
o pending changes exist. Click the Release onfiguration button to allow others to edit the		vary of Deployments				
onain.	Contr	rel Montoring				
Lock & Edr	1.22					
Release Configuration	dom	page displays a list of Jawa EE applications and stand alone application modules t ain by first selecting the application name and using the controls on this page.	hat have been installed to this domain. Installed a	pplications and	nodules can be started, stopped,	updated (redeployed), or deleted from the
amain Structure	To in	nstall a new application or module for deployment to targets in this domain, click if	e Install button.			
doman Environment Deployments	- Curr	tensize this table				
Services Security Realms	Depl	loyments				
Interoperability	In	stal Update Delete Stat+ Stop+				Showing I to 10 of 15 Previous Next
E Deposito		Name in	State	Health	Туре	Deployment Order
		* C ¹ JARRENT	Active	¢ск	Enterprise Application	100
		(R Ditarase strates	Active	€ок	Enterprise Application	100
w do L		E mintal financial integration-ear 1.0 SWISH01.ear	Prepared	≪ ok	Enterprise Application	100
Instal an Enterprise application		🗷 🚆 retal-func-att/lat-gen-ga	Active	¢ск	Web Application	100
Configure an Enterprise application Update (redeploy) an Enterprise application		E gretal-sos-enable-gu	Active	₫ок	Web Application	100
Start and stop a depkyed Enterprise		R Disposition	New		Enterprise Application	100
application Monitor the modules of an Enterprise		E grb-config-agent.war	Active	∉ ок	Web Application	100
application		8 grb func-attfact.mar	Active	✓ OK	Web Application	100
Deploy E3B modules		I The out out	Tarres		Enterprise Application	100
Deploy EIII modules Instal a Web application		8 parb-fin.ear	Tape		Enterprise Application	100

Figure 3–1 Summary of Deployments

2. An overview page is displayed, including a list of modules and components installed as part of the application.

Figure 3–2 Modules and Components

tem Status	8 Modules and Components	Restored a feature from
ith of Running Servers		Showing 1 to 1 of 1 Previous Next
Faled (0) Critical (0)	Name 🐵	Туре
Overloaded (0)	8 ip-service	Enterprise Application
Warning (0) OK (4)	⊟ £36s	
	C ASIdnPublishingtean	6.0
	C ASNO utrubishingbean	C3
	CurRatehubishingtean	6.0
	Ofritfernifublishingtean	E30
	0Fulliordhubishingtean	63
	0 (4.COM/ublishingBean	E30
	3pth/rashutureManagerBean	E20
	0 InvAduatPublishingtean	EXI.
	0 Indephalehingtoan	E20
	PayTemPublishingBean	E38
	ReceivingPublishingBean	E38
	CRTVPublishingBean	E38
	VendorPublishingBean	E.36
	C XAlochubishingBean	E38
	C XCostChgPublishingBean	E38
	C)/Drent.ocPublishingTean	6.06
	C XDeenPublishingBean	E38
	C XOrderPublishingTean	E38
	CXRoreAddshingBean	638
	C XTdPublishingtivan	E38
	E Modules	
	Tigs service e(b.)ar	E28 Module

3. In the Web service list, click the service for which you want to enable security. The following screen is displayed to provide an overview of the Web service.

Change Center	A Home Log Out Preferences 🔤 Record Help	Q	Welcome, weblogic Connected to: rib_domain
iew changes and restarts	Home >Summary of Coplayments >igs-service >PayTermPublic		······································
to pending changes exist. Click the Release	Settings for PayTermPublishingBean		
Configuration button to allow others to edit the domain.	Overview Configuration Security Control Testin	g Monitoring	
Lock & Edt			
Release Configuration	Use this page to view basic information about the selected	Enterprise Java Bean (E38).	
omain Structure	Application Name:	igs-service	The name of this application deployment. More Info
b_domain E-Environment Deployments	E30 Module Name:	igs-service-efb.jar	The name of this module. More aris
B Services Security Realms	Bean Names	PayTemPublishingBean	The name of this bean. More Info
Security Realms Interoperability			
the Diagnostics			
€ Clagnostics			
tow do LIII			
tow do LR Configure EBits Deploy CBI modules			
tow do LR Configure EBits Deploy CBI modules			
R-Disprotio			
it: Cisponits invido L. III : Configure EBit Configure EBit Configure Ebit Dadi an Octoprime application inplaner Status III			
ter do 1 Configure Elles Deslay Elles Deslay Elle obdets Instal an Diterprise aglication			
the Gapanetes Configure EDe Configure EDe Configure EDe Dotal an Diference exploration yestern Status False(0) Configure Serves False(0) Configure (0) Confi			
itor do L. IIII Conformation Carlos Conforma Ellas Despire Ella nocidades Instala in Chempsina application Instala in Chempsina application Instala in Chempsina application Instala in Chempsina application Instala in Chempsina application Constalado (Chempsina application)			
te Gapanatia Confugar Ella Detail an Otenpiae aglication Install an Otenpiae aglication Sector Serves Falled (0) Otota (0)			

Figure 3–3 Settings

4. On this overview screen, click the **Configuration** tab. Click the **WS-Policy** tab. The Web service port is shown under **Service Endpoints and Operations**.

Figure 3–4 Settings - Configuration Tab

Settings for PayTernPublishingService + rb	*		
🗲 🕲 birðritt Aði: oraða.com 7001/conscie/co	nick port#_yfpt=truel_gageLabel=WebServoethold/eConfigurationWebServoethols/Hagethandle=com.bea.consile.handlesHudderlandle("com.beah" 🖺	- C 🕅 • Google 🔎 🗍	
ORACLE WebLogic Server®	Administration Console	Q	
Change Center	A Hone Log Out. Preferences 🖅 Record Help	Welcome, weblogic Connected to: rib_domain	
New changes and restarts	Hone sölammer of Deployments signmervice silles TemPublishingbean sölammer of Deployments signoervice silles TemPublishingbearvice		
No pending changes exist. Click the Release Configuration button to allow others to edit the	Settings for PayTermPublishingService		
toman.	Overview Configuration Security Testing Monitoring		
Lock & Edit	General Handlers WS-Policy Ports		
Release Configuration			
Domain Structure	This page lats the policy files that are attached to the endpoints and operations of this Web service. The operations are lated below the endpoint; click of	in the + sign to view them. Click on the endpoint or operation name to attach	
b_domain	a policy file. For example, you can specify that the policy file applies only for inbound (request) SOAP messages, and so on.		
8 Environment Deployments	WS-Policy Files Associated With This Web Service		
f Services		Showing 1 to 1 of 1 Previous Next	
Security Realms Intercoperability	Service Endpoints and Operations 🕫	Policies	
R Diagnostica	III Pay Tem Publishing Purt		
	Showing to t of 1 Previous Next		
teer do I			
Statt and stop a Web service			
Install a Web service Start and stop a Web service Attach a WS-Policy file to a Web service			
Initial a Web service Start and stop a Web service Attach a WG-Policy file to a Web service Configure Web services View the 50AP nessage handlers of a Web			
Install a Webservice Start and stop a Webservice Attach a WS-Policy file to a Webservice Configure Webservices Verwithe SOAP message handlers of a Web service			
Shafa A Web service Start and stop a Web service Attach a WS-Policy / Ra to a Web service Configure Web service Configure Web service Wee the VCDL of a Web service			
Sottal a Web service Start and stop a Web service Attach a Web-Reby: (Ne to a Web service Configure Web service Web the SOLP message handlers of a Web service Web the WCRL of a Web service Test a Web service			
Initial a Web service Start and stop is Web service Attach a WS-Policy file to a Web service Configure Web service Ourgings Web service Service Web the WSCk of a Web service Test a Web service Notice Web services			
Nee do L			

5. Click the plus sign next to the port name. The Web service operations are displayed.

Se Edit Yeer Higtory Boolmarks Book	(Hp			
Settings for PayTerniPublishingService - rb	+			
🗧 🕙 birdvitt Jác orada.com 7001/conscie/os	nick portal "page, abel- WebSer vozModuleConfigurator WebSer vozMak "Hageb "vipbtruets WebSer-vozConfigurator	etőer-szefolces/untetespandte 🎲 = C 🔀 + Google 🔎 🐥		
ORACLE WebLogic Server®	Administration Console			
Change Center	1 Hone LogOut Preferences 🖾 Record Help	Welcome, weblogic Connected to: rib_dom		
New changes and restarts	Hone +Summery of Deployments vigroenvice vPayTemPublishingBean vSummery of Deployments vigorenvice vPayTem	aPublishingService		
No pending changes exist. Click the Release Configuration button to allow others to edit the	Settings for PayTerm#ubilishingService			
configuration button to allow others to edit the lonan.	Overview Configuration Security Testing Monitoring			
Luck & Edit	General Handlers WS-Policy Ports			
Release Configuration				
Domain Structure rb_domain B Environment Deployments	a policy file. For example, you can specify that the policy file agales only for inbound (request) SOAP messages, and WS-Policy Files Associated With This Web Service	Showing 1 to 1 of 1. Previous Hent		
F Services Security Realms F Interoperability	Service Endpoints and Operations 🕫	Policies		
R Diagnostics	8 PaytemPublishingPurt			
	ping			
	publich PayTermCreated.kingPayTermDesc			
	publishPayTermDNCreateUsingPayTermDesc			
	publich PayTermCRModPyUsingPayTermDesc			
Hoer do L	publichPayTernModIyUshgPayTernDesc			
toer do I 🗵		Showing 1 to 1 of 1 Previous Next		
Install and web service Statt and stop a Web service Attach and stop a Web service Attach and WID-Relice (Re to a Web service Configure web service) Wesh the SOAP nessage handless of a Web service Wesh the WCSL of a Web service Montan Web service Montan Web service Montan Web service Montan Web service dents				
Start and stop a Web service Attach a WS-Policy file to a Web service Configure Web service Wee the SOAP nessage handlers of a Web service View the WSEL of a Web service Toot a Web service Notar Web service				

Figure 3–5 Settings - Configuration Tab

6. You can secure all the Web service operations at once or select only the operations you want to secure. Click the name of the port. On the Configure a Web Service Policy screen, you can attach the policy file to the Web service.

Figure 3–6 Configure a WS-Policy for a Web Service Endpoint

Configure a WebService policy - rib_de	main - WLS Console - Mozilla Firefox			
Ble Edit View Higtory Bookmarks Ipols	1940			
Configure a WebService policy - rb_doman	+			
(+) B birdvitt Adr. or ade.com.7001/conecie/cone	ole.portal?ConfigureWebServoolPolicyFortlet_actionOverride=Jcon/bea/console/actio	ns/vebiev/ce/vebiev/cepolicy/gitPolicyType	☆ = C S + Goode	P 🕹 🏦
donian. Lock & Edl Release Configuration	Back. Time Frank Cancel. Configure a WS-Policy File for a Web Service Endpoint			
Demain Structure r6_donain IP Environment Copplyments IF Services	Use this page to configure the WS-Polcy file that is associated with this Web Ser The Available Endport Polces window lats the WS-Polcy files that are available sectors.		moves to move a file to the Chosen Endpoint Policies table,	then click. OK to activate your
Security Realms	Service Endpoint Policies:			
R Diagnostica	Available Endpoint Policies:	Chosen Endpoint Policies:		
	policyDefaultRelability.uml policyDefaultRelability.1.aml policyDefaultRelability.1.aml policyLogEfaultRelability.aml policyLogEfaultRelability.aml policyLogEfaultRelability.aml policyDefaultRelability.aml	1		
Hew do. El > Solidal & Web service	plcycholaydr J_D_LLawi plcycholaydr J_D_LLawi plcycholaydr J_D_LLawi plcycholaydr J_L_Sequence STRawi plcychola	2 2 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4		
System Status 🛛 🗎 Health of Furning Servers	Back, New Frish, Cancel			
Paled (0) Critical (0) Overhaded (0) Warring (0) Warring (0) Critical (0) Critic				

7. From the **Available Endpoint Policies** list, select policy:usernametoken.xml. Click the right arrow to move it to the drop down list below Chosen Endpoint Policies. Click **Finish**.

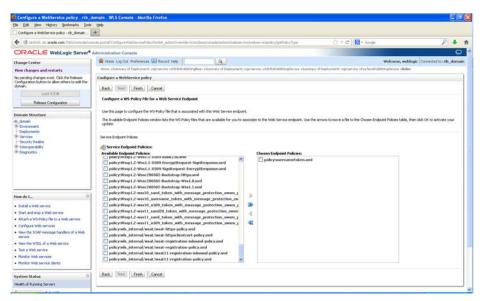


Figure 3–7 Configure a WS-Policy for a Web Service Endpoint

8. The following screen is displayed, including status messages near the top.

Figure 3–8 Settings - Configuration Tab

Settings for PayTerniPublishingService - rb	+		
Constant State Constant Consta	nevie portal?rfpb=-brush_jtageLabel=-webServceHoduleConfigurationWebServceHolcyPage	(2) = C [*] R + Goode	P + 1
ORACLE WebLogic Server*	Administration Console		0
Change Center	Hone Log Out Preferences - Record Help	Wekome, webio	igic Connected to: rila_domain
View changes and restarts	None vSummery of Deployments vigoraevice vASNIDPublishingBeen vSummery of Deployments vigoraevice vigoraevice vASNIDPublishingBeen vSummery of Deployments vigoraevice	IthingService volumnary of Deployments signatives vPayTemPublishingService vRales	
No pending changes exist. Click the Release Configuration button to allow others to edit the doman.	Messages @ Deployment plan has been successfully updated. @ Remember to update your disployment to reflect the new plan when you are firsthed with your changes.		
Lock & Edit	Settings for PayTermPublishingService		
Release Configuration	Overview Configuration Security Testing Monitoring		
Domain Structure	General Handers WS-Pallary Ports		
Environment Deployments Services Security Realms	This page lists the policy files that are attached to the endpoints and operations of this Web service. The operation a policy file. For example, you can specify that the policy file applies only for inbound (request) SOAP messages, an		or operation name to attach
	WS-Policy Files Associated With This Web Service		
P Interoperability P Diagnostics	W5-Policy Files Associated With This Web Service	Showing	1 to 1 of 1 Previous Next
	WS-Policy Files Associated With This Web Service Service Endpoints and Operations in	Soving Policies	1 to 1 of 1 Previous Next
		Television-	1 to 1 of 1 Previous Next
	Service Indpoints and Operations ++	Publices policy usernametralien, uni	1 to 1 of 1 Previous Next
R Dagnotice	Service Indpoints and Operations ++	Publices policy usernametralien, uni	
Records L. If the second secon	Service Indpoints and Operations ++	Publices policy usernametralien, uni	
No de L. III III IIII IIII IIIII IIIII IIIIIIII	Service Indpoints and Operations ++	Publices policy usernametralien, uni	
Records a la construcción de la	Service Indpoints and Operations ++	Publices policy usernametralien, uni	

9. Now update the application to reflect the new deployment plan. Go to Deployments and select igs-service. The following screen is displayed.

Summary of Deployments - rb. domain - WL	tteb +					
		rfot-truck, providel-AppDeckowertsControlPage			(7 = C N + Goode	₽ ♦
					in a line onte	
						Welcome, weblogic Connected to: rib_doma
ange Center iew changes and restarts		er ong our communities and menter many	s vigotarvica vPayTemPublishingServica vRoles	Policie Memo		records, accords, from the total
pending changes exist. Click the Release	Summi	ry of Deployments				
nfiguration button to allow others to edit the main.	Contr	al Monitoring				
Lock & Edit						
Release Configuration	This	age displays a list of Java EE applications and stand-alone application modules that in by first selecting the application name and using the controls on this page.	t have been installed to this domain. Installed	applications and	modules can be started, stopped,	, updated (redeployed), or deleted from the
main Structure		tal a new application or module for deployment to targets in this domain, dick the !	Instal button.			
dowain Environment Deployments Services Security Realms		omize this table syments				
Interoperability	Install Update Debte State Sta					
P Dispositor						
- Lagreoux		Name 🙃	State	Health	Туре	Deployment Order
- Magnetoka		Name ->	State Active	Health V ^{ar} CK	Type Enterprise Application	Deployment Order
- sagetoot	2		10000			
	8	(E) Distribution	Active	₹ cx	Enterprise Application	100
eer do I	800	18 Lightnesser	Active Active	₹ cx ₹ cx	Enterprise Application Enterprise Application	100
eer de 1	000	B (Tylessenke B Tylenee as state B (Tyleseke handelstag storee 1.0.9449401.es	Active Active Prepared	vrox vrox vrox	Enterprise Application Enterprise Application Enterprise Application	100 100 100
ee do L	800000	SE ggyapanose SE ggyanase-garstalos SE ggyanale/hanoidertagedon ear 1.0.994/9401.ear SE ggyatal/hanoidertagedon ear	Active Active Prepared Active	Vox Vox Vox	Enterprise Application Enterprise Application Enterprise Application Web Application	100 100 100 100
eer de 1	8000000	El gyaponica El gyanom-gestato El gyanom-gestato El gyatal francia etagedon ner 1.0.9449401 ner El gyatal-franciation gen gal El gyatal-franciation ga	Active Active Prepared Active Active	Vox Vox Vox	Enterprise Application Enterprise Application Enterprise Application Enterprise Application Web Application	900 900 900 900 900 900
ee do T. III Statul ao Deterprise application Configure en Deterprise application State and edge a designed Driesprese application	8000000	El Types proces El Types proces El Types and francial etcay alone are 1.0.99495401 aur El Typetal Anciel etcay alone are 1.0.99495401 aur El Typetal Anciel etcay along a El Type-so au	Active Active Prepared Active Active Active New	4 ax 4 ax 4 ax 4 ax 4 ax	Enterprise Application Enterprise Application Enterprise Application Web Application Web Application Enterprise Application	100 100 100 100 100 100 100
ee do L. IIII Suida to Exterprise application Under Simologi In Discopera application Section Necto the another of an Discopera application	800000000	జి గ్రాధ్యుకు కాగరు జి గ్రాధిగాజా ధూరిక జి ద్వాగకి గినాపరి కిరణ్ భూరు బా 1.0 5947507 aar జి ద్వాగకి విగు వారికి వర్తించాలు జి ద్వారించు కాజి జి ద్వారించుగి వర్తించాలు	Active Active Prepared Active Active Rem Active	Фок Фок Фок Фок Фок Фок	Diterprise Application Diterprise Application Enterprise Application Web Application Enterprise Application Web Application Web Application	100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100
ee do L. III Datal an Exterpris application (College an Exterprise application) (Lobele operation) and Exterprise application Advance the module of an Exterprise application (Deby CEII module)		B Cyclosenece B Tylenece optimizet B Tylenece optimizet	Active Active Active Active Active Reve Active Active Active Active	Фок Фок Фок Фок Фок Фок	Chempine Application Enterprise Application Enterprise Application Web Application Enterprise Application Web Application Web Application	100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100

Figure 3–9 Summary of Deployments

10. Click **Update** and then **Finish**.

Figure 3–10 Update Application Assistant

Se Edit Yeer Higtory Bookmarks Bo			
Update Application Assistant - nb_domain	*		
🗲 🕘 birdvitt Jäc.orada.com 7001/conscie/	una de portal?AppApploator/apdatePortiat_action?verride=/com/beak/oncode/actions/app/.pdate/beforeReview	😭 🗢 😋 🔣 - Google	P + 1
	Administration Console		0
hange Center	A Hone Log Out Preferences 🕢 Record Help		Welcome, weblogic Connected to: nb_domain
new changes and restarts	Hone signatrice siles TemPublishingService viloles silb_dosten sSummary of Deployments signatrice siles TemPublishingService	cx violes «Polces »Summary of Depleyments	
No pandag darugan sait. Cak'the Malaan Cargara daro Jathan Saka dhar ta sa dar Karaka dar ya dar ya dar ya dar Relasan Candigaatan Benala Sharutara O chanan Be Candigaatan Be Candigaatan Be Candigaatan Be Sakatan Be Sakatan Be Sakatan Be Sakatan	Update: Application: Answired Bits: Damil Locate: new deployment files Damil Distaine: Application in place with new deployment plan changes. (A deployment plan must be specified Deployment plan must be specified Deployment plan path: _ADD(do-10)A(0:sich/Holdbource). Adde-10A(0:sich/Holdbource). © Rodeploy this application using the following deployment files: Source path: _ADD(do-10)A(0:sich/Holdbource).	ver/upload/Plan.cml_Change Path	
eer da 1	Deployment planpatic(20(do-01)eb-103(0-ski)%Silewarqlare_protect((dowarqlet_dowarq	verjupload/Him.xwi_Dange Path_	
approation Confequee an Enterprise application			
Create a deployment plan			
Target an Enterprise application to a server Test the modules in an Enterprise application			
rstem Status B			
ealth of Furning Servers			
Paled (0) Critical (0) Overkaaded (0) Warrang (0)			

11. Click Activate Changes.

Ble Edit Yew Higtory Bookmarks Tools	t theb						
Summary of Deployments - rb_domain - WL	+						
🗲 🗟 birdvöt Adr. orada.com 7001/conacie/con	uniule putality (fpb=buels_pageLabel=AppDeploymentsControlPage					f 🔝 + Google	P 🕹
ORACLE WebLogic Server®	Administr	ration Console				A CONTRACTOR	c
Change Center	😰 Hone Log Cut. Preferences 🖾 Record Help.					Welcor	me, weblogic Connected to: nb_dom
New changes and restarts Pending changes exist. They must be activated to tale effect.	Messag	-signtanvics sillay TemPublishingServics viloles silb-doma ges dected Deployments were updated.	n «Summery of Depletements vigoraervic	a vPayTemPublishingSarvica vRoles vPolicie	-Summary of D	-glepsent:	
Activate Changes	ar 10	aumust also activate the pending changes to consult this	, and other updates, to the active syst	an.			
Undo All Changes	Samma	ary of Deployments					
Domain Structure	Contr	Nonitoring					
Deployments B: Services - Security Realms	The page display is let of useful type/conserved share application models but have been installed to the down. Shalled applications and non-down applications are been to the page. The notal a new application or models for displayment to targets in the downer, dot the "beatal" button. Constrained the table Deployments						
® Stancorstality ® Chagnostics	Deph			N			Showing 1 to 10 of 15 Previous Next
	Depl	kyments		State	Health	Туре	Showing 1 to 10 of 15 Previous Next Deployment Order
f Dageotics	Deph	oyments ad. (Dolar) (Dole) (Dole) (Story)			Health #OK	010/03	
R Chagnostics Seen do Lu.	Deph	oyments tal Dodae Owine Starr- Stop- Name vi		Rate	110,2190	Туре	Deployment Order
le Chagnolica Isee de L	Deph	toynonts tal, [Ubdate] [Onine] [Statie] [Statie] Name # Rgosternes		State deploy installeng	≠cx	Type Enterprise Application	Deployment Order
Rongrobics Ison do T		ayments Lat, Doctor Dente Storr Storr Name vir H Tylersen sprindet		State disloy bitalong Active	≠ox ≠ox	Type Enterprise Application Enterprise Application	Deployment Order 100 100
Readerates		symmets ad. [Date: [Date:]Stor:]Stor: Name vi 8 Tglaseries 8 Tglaseries al-tube 8 Tgletal-francial-stor atomer: 1.0 Staff2001 as		State disky bitaling Active Properd	dax dax dax	Type Enterprise Application Enterprise Application Enterprise Application	Deployment Order 100 100 100 100
Readerates		egeneration ed. [Database] [Database] Memory ve Mit Types and the second		Skate display brokeling Active Propend Active	Фак Фак Фак Фак	Type Enterprise Application Enterprise Application Enterprise Application Web Application	Deployment Order 100 100 100 100 100
Readerates		egymetriks ed. [Danier: Danier: [Danier:] Name riv 8 gyster metrik 8 gyster francestrate 8 gyster francestrate omga 8 gyster francestrate omga 8 gyster francestrate omga		Skate depky bindeng Actree Actree Actree Actree	Фак Фак Фак Фак	Type Enterprise Application Enterprise Application Enterprise Application Enterprise Application Web Application Web Application	Deployment Order 100 100 100 100 100 100 100 100
In Capacities		egymetriks ad. [Datase: Online: Datase: Stores: Name eis di ggloperante: di ggloperant		State disky bratery Active hreawd Active Active Active Active Active	4 ax 4 ax 4 ax 4 ax 4 ax	Type Enterprise Application Enterprise Application Enterprise Application Web Application Web Application Enterprise Application	Deployment Order 100 100 100 100 100 100 100 100 100 100
Capacity Compares Discrete application South of Discrete application Configure to Discrete application South of Discrete application South of Discrete application Configure to Discrete South of Discrete		Anners Anners Toporense Angere		Ride dejiv johdeng Actre Actre Actre Actre Actre Actre Actre	Фах Фах Фах Фах Фах Фах	Type Enterprise Application Enterprise Application Enterprise Application Web Application Enterprise Application Unterprise Application Web Application	Deployment Order 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100

Figure 3–11 Summary of Deployments

12. After activating changes following screen is displayed.

Figure 3–12 Summary of Deployments

Summary of Depkyments - rb_domain - WL	+					
Call birdstitt Alt orade.com.7001/conacie/con	Note portal	or the design abel-http://tird-01.4k. or scie.com/001/canade/carecie.po//	rhall_shpb=hrunb_pageLabel=AppCepkymere	Controllinge	🕎 🖛 😋 🔛 • Google	P 🔸
ORACLE WebLogic Server*	Administ	vation Console				Q
Change Center	1 Ho	ne Log Out. Preferences 🖼 Rocard Help			W	Aelcome, weblogic Connected to: rib_domai
New changes and restarts		signaryos sileyTemPublishingService sitoles with_domain sSummary of Deployment	is vigotarvice vPertemPublishingService vRoles	»Policies vitement	sary of Deployments	
Skk the Lock & Edit button to modify, add or felete items in this domain.	Messag and Al	yes I changes have been activated. However 3 items must be restarted for the change	s to take effect.			
Lock & Edit	Summ	ary of Deployments				
Paisase Configuration		al Montoring				
Iomain Structure						
b_donan B Environment — Deployments B Services — Secuty Dealans # Services addres	done To in	page diging a list of Jave IE applications and stand-alone application models th on by first selecting the application name and using the controls on this page. Ital a new application or module for displayment to targets in this domain, click the		applications and	modules can be started, stopped,	updated (redeployed), or deleted from the
		romize this table				
	Depk	nomize this table oyments tal Update: Dente Start- Stop =				Showing 1 to 10 of 15 Previous Next
	Depk	oyments	State	Health	Туре	Showing 1 to 10 of 15 Previous Next Deployment Order
	Deph	opports 1 Lindar (Dense) State (State)	State Active	Health of OK	Type Enterprise Application	
ê Çaşrotis	Deph	opments Inf. [Doder: (Dener) Starie: [Boxee] Name #				Deployment Order
F Chargeoutics new dia LE Jostal as Diferense application		nyments Inf Dotter Dome Starte Starte Name & 8 gyspeance	Active	Фок	Enterprise Application	Deployment Order
P Chapmatics		nyments Ind Spater Denne Stare Stare Name ri 28 gyap over	Active Active	√ox √ox	Enterprise Application	Deployment Order 100 100
Remotos Isee de J		angenetak ali [beakar] [beakar] [beakar] Nemerak ali gaga-an-sakar ali gagata Annoval-1.5-594/5907.esr ali ganta Annoval-1.5-594/5907.esr	Active Active Prepared	vrox vrox vrox	Enterprise Application Enterprise Application Enterprise Application	Deployment Order
P Capacitie Dear do L. El Social en Driespine application Configure and transpine application - Configure and transpine application - Space and transpine application - Space and the space application of the space application		agments المالية (المعند) (المعند) المعند بله المعند بلم المعند بو المعند بالمعند بلم الممن بالمم المعند بلم المعند بل	Active Active Proposed Active Active	Vox Vox Vox	Enterprise Application Enterprise Application Enterprise Application Web Application Web Application	Drepksymmethl (örder 100 100 100 100 100 100 100 100
Propuesto Companyation Statul and Elempton application Configure on Elempton application Under Configure on Elempton Application de Configure Application Application de Configure Application Configure on Elempton Application Configure on Elempton Application Configure on Elempton		ngments Internet Denser (Denser) Nome de Rogione expendé Rogione expendé Rogione expendé Rogione de Angelor est - Lo Stat/Stationes Rogione de Angelor est - Lo Stat/Stationes Rogiones - Lo Stationes Rogiones - Lo Rogiones Rogiones - Lo Rogiones	Active Active Property Active Active Netw	Фок Фок Фок Фок Фок	Enterprise Application Enterprise Application Enterprise Application Web Application Web Application Enterprise Application	Deskymmet ürder 100 100 100 100 100 100 100 100
en do L. El Jondia en Censoria equivario Conforce en Censoria equivario Conforce en Censoria equivario Under Conforce en Censoria equivario Altorito de modulo e do Enforme equivarion Debrito de modulo e do Enforme equivarion			Active Active Proposed Active Active New Active	Фок Фок Фок Фок Фок	Enterprise Application Enterprise Application Enterprise Application Web Application Enterprise Application Enterprise Application Web Application	Dealsymmet/Lbdw 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100
Programske Den de J. E Stadi en Efersjone agelektion Conferen en Erenspone agelektion Undere Underspone agelektion Stadt et de skale af elefteret forstynne agelektion Hontsch et mendade of an Dieterpine agelektion Deskiel Standami Jonal a Web agelektion		In Debain Denne Store Store Nome vis 21 Type-re-points 21 Type-re-points 22 Type-re-points 23 Type-re-points 24 Type-re-points 25 Type-re-points 25 Type-re-points 26 Type-re-points 27 Type-re-points 26 Type-re-points 27 Type-re-points 26 Type-re-points 27 Type-re-points 27 Type-re-points 27 Type-re-points 27 Type-re-points 28 Type-re-points 29 Type-re-points 29 Type-re-points 20 Type-re-p	Active Active Property Active Active New	Фок Фок Фок Фок Фок	Enterprise Application Enterprise Application Enterprise Application Web Application Web Application Enterprise Application	Deskymmet ürder 100 100 100 100 100 100 100 100
R Opposition Oppositio Opposition Opposition Oppositio Opposition Opposition Opposition			Active Active Proposed Active Active New Active	Фок Фок Фок Фок Фок	Enterprise Application Enterprise Application Enterprise Application Web Application Enterprise Application Enterprise Application Web Application	Dealsymmet/Lbdw 100 100 100 100 100 100 100 100 100 100 100 100 100 100 100

13. Under the **Testing** tab, on the Web Service page, click the WSDL to view the details of the policy just added to the Web service. The WSDL contains information similar to the following:

```
<?xml version='1.0' encoding='UTF-8'?>
<definitions
xmlns:tns="http://www.oracle.com/retail/igs/integration/services/PayTermPublish
ingService/v1"
xmlns:ns1="http://www.oracle.com/retail/integration/bus/gateway/services/Busine
ssObjectId/v1"
xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ns2="http://www.oracle.com/retail/integration/services/exception/v1"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"</pre>
```

xmlns="http://schemas.xmlsoap.org/wsdl/" name="PayTermPublishingService" targetNamespace="http://www.oracle.com/retail/igs/integration/services/PayTermP ublishingService/v1" xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wssutil="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecuri ty-utility-1.0.xsd"> <wsp:UsingPolicy wssutil:Required="true" /> <wsp:Policy wssutil:Id="usernametoken"> <ns0:SupportingTokens xmlns:ns0="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512"> <wsp:Policy> <ns0:UsernameToken ns0:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512/Inc ludeToken/AlwaysToRecipient"> <wsp:Policy> <ns0:WssUsernameToken10/> </wsp:Policy> </ns0:UsernameToken> </wsp:Policy> </ns0:SupportingTokens> </wsp:Policy>

Create Roles and Users

This section describes steps to add roles and users who can access the Web services. The first step is to add users to the security realm.

1. In the Domain Structure window of the Oracle WebLogic Services Administration Console, click the **Security Realms** link. The Summary of Security Realms screen is displayed, including the name of the default realm.

Figure 3–13 Summary of Security Realms

Summary of Security Realms - rib_de	omain - WLS Console - Nozilla Firefox			E @ 🔀
Ble Edt Yew Higtory Boolmarks Joci	k Heb			
Summary of Security Realms - rib_domain	+			
🗲 🖲 birdiritt Jác. orada.com 7001/conacie/o	unside portal?_r/pb=hush_jogeLabel=SecurityRashiRaahi1ableh	NQE .		P 🕹 🏦
ORACLE WebLogic Server	Administration Console			0
Change Center	1 Hone Log Out Preferences 🖾 Recard Help	9		Welcome, weblogic Corrected to: rik_domain
View changes and restarts	Hone seb_domain stiummery of Deployments signoenvice sP	eyTemPublishingService sillales sPolicies sSumm	ary of Diployments signarries sPayTemPublishingService s Sense ary of Se	curity Realme
Citck the Lock & Edit button to modify, add or delete items in this domain.	Summary of Security Realms			
Lock & Edit	A new pite reads in a container for the mechanismic probability	na sere an en en etcades serents rabie	es, and security providers—that are used to protect WebLogic resources. Yo	u nan hawa ni dirila nan altu na dan in a Mahi nan
Palease Configuration	Server domain, but only one can be set as the default (act	tve) realm.	of an actual frame, not as one of board second s	
Domain Structure	This Security Realms page lists each security realm that has	s been configured in this WebLogic Server doni	an. Old: the name of the realm to explore and configure that realm.	
rb_domain				
Environment Deployments	© Customize this table			
B Services	Realms (Filtered - More Columns Exist)			
Security Realms	Click the Lock & Edit button in the Change Center to activ	ate all the buttons on this page.		
E Ciagnostica	News Dalata			Showing 1 to 1 of 1 Previous Next
	Name 🙃	Default Re	calm -	
	ingreader .	true		
	New Debte			Showing 1 to 1 of 1 Previous [Next
-	In the second se			
How do I				
· Configure new security realms				
 Delete security realms Change the default security realm 				
Change the default security ream]			
System Status				
Health of Furning Servers				
Paled (0)				
Critical (0) Overloaded (0)				
Warning (0)				
GK (4)				
WebLoge Server Verson: \$5.5.6.0 Copyright © 1796, 2011, Cruck and/or in affiliate.	the state way and			
Oracle is a registered balance's of Oracle Organist	on and/or to allians. Other name may be tradenaries of their regards	n Inclurit.		

2. Click the name of the default realm. The settings for the realm are displayed.

Settings for myrealm - nb_domain - WLS Con	+				
🗲 📵 birdvöt idt. orade.com. 7001/conacie/cor	vide portal" _r/pb=truels_logeLabel=Realingeres af	abPagel (ex.ext) Real of ealer Genera	Portiethande-combea.console.ha	rdes Securitationaritande("s ☆ = C 🛃 + Google	P + 1
DRACLE WebLogic Server*	Administration Console				0
hange Center	🔒 Hone Log Out Preferences 🔙 Recard H			Welcome, weblo	gic Connected to: rib_domain
ies changes and restarts	Hone sSummery of Deployments signaryics sP	ay TermPublishingService villales viPola	iet +Summwy of Deployments +ignow	vice of systemPublishingService vSummery of Security Revins S ecurity Revins	
Ick the Lock & Edit button to modify, add or elete items in this domain.	Settings for myrealm				
Lock & Edit	Configuration Users and Groups Roles a	and Policies Credential Mappings	Providers Migration		
Parlinase Configuration	General RDBMS Security Store User Lod	kout Performance			
amain Structure	Gick the Lock & Edit button in the Change Co	inter to modify the settings on this p	age.		
, doman Environment	Seve				
F Services -Security Realms F Interoperability F Diagnostics	Note: If you are inglementing security using functions for Web applications and ED	3AOC (Java Authorization Contract) Bi in the Administration Console are i	for Containers as defined in JSR 115 disabled.), you must use the DD Only security model. Other WebLogic Server models are not	I available and the security
	Name:	nyreain		The name of this security realm. More Info	
	🕂 Security Model Default:	DD Owly	8	Specifies the default security model for Web applications or E3 security reals. You can override this default during deployment	is that are secured by the z. Hore Info
ion de 1	Combined Role Mapping Enabled			Determines how the rule mappings in the Ditterprise Application containers interact. This setting is valid only for Web application Advanced security model and that initialize roles from deptoms Info	ns and £36s that use the
EXBs Set the default security nodel Delegate Milean authorization to the realm	💭 🚓 Use Authorization Providers to Pr	otect JMX Access		Configures the WebLogic Server Milean servers to use the set providers to determine whether a 340 client has permission to or mode an Milean operation. More 246	urty realin's Authoritation access an Milean attribute
	- 9 Advanced				
rstem Status 🛛 🔅	Save				
Palled (0) Critical (0) Critical (0) Overloaded (0) Warning (0)	Gick the Lock & Edit button in the Change Co	when to modify the settings on this p	69F.		

Figure 3–14 Settings

3. On the Setting screen, click the Users and Groups tab.

Figure 3–15 Settings

Settings for myrealm - nb_domain - WLS Con.	1.1			
C Birdvitt Jdc.orade.com/7001/conscie/	conside portal? _rfqb=bruebbageLabel=itealeiC	seManagementTabPage5Eande=com.bes.console.handes.5eourtyHtbearHande("	Security%SMiane%SDn 😳 🗢 😋 🔣 • Google	₽ ♦
DRACLE WebLogic Server	Administration Console			0
hange Center	A Hone Log Out Preferences 💹 Pre	and Help	Welcome, weblogic Connected b	: rib_domair
new changes and restarts	Horse signarytice silling TemPublishingSer	vice sitilate sitilates sSummary of Displayments signatives sitesTemPublishingService	s Summary of Security Realms simplealm siltness and Gewape	
Dick the Lock & Edit button to modify, add or felete items in this domain.	Settings for myrealm			
Lock & Edit	Configuration Users and Groups	Roles and Policies Credential Mappings Providers Higration		
Palease Corligization	Users Groups			
omain Structure	The same design of the state of the	ch user that has been configured in this security reads.		
b, donan # Environment - Oxployments # Services - Secuty Realms	© Customize this table Users			
F Interoperability F Diagnostica	New		Showing I to 10 of 13 Prev	ous Next
	Name 💀	Description	Provider	
	Tagadhan		DefaultAuthenticator	
	igsednin	igsadhin	DefaultAuthenticator	
	gai,ser	kgc user	DefaultAuthenticator	
eer de L	CracleSystemLiser	Cracle application software system user.	Default/luthenticator	
	🔲 rfiednan	rhadnin	CellouthAthenticator	
Manage users and groups	D ribadhin	R30 Admin user.	DefaultAuthenticator	
Create users ModPy users	C rémisednin	RIB Admin user.	Defaultiuthenticator	
Delete users	insadnin .	R3B Admin user,	Default/uthenticator	
	stuar	rsbuser	Defaulthatherticator	_
rstem Status	a raevaer		Defailt/uthenticator	
rath of Fluring Servers Field (3)	New Delete		Showing 1 to 10 of 13 Free	ious Next
Critical (0) Overloaded (0) Warning (0) Oct (4)				

4. In the **Users and Groups** tab, click the **Users** tab. At the bottom of the Users tab, click **New**. The Create a New User screen is displayed.

Figure 3–16 Create a New User

le Edit Yew History Bookmarks Too			
Create a New User + rb_domain - WLS Cons.	+		
🗲 🕘 birdvitt Jär. orada.com 7001/conscie/	uniole.portal?SecurityUsiesiCinateUsePortlebatu	n To-Realition Hanagement tablaget Security Realistic sinction Hanagement Overstor Liett and e-combes. 🍸 🛎 😋 🛛 🛃 • Goo	de 🖉 🖡 🕇
	Administration Console		<u> </u>
Thange Center	A Hone Log Out Preferences 💹 Room	d Neb	Welcome, weblogic Connected to: rib_domain
ies changes and restarts	Horse signaryice silleyTemPublishingServi	a vitoles sPolices sSummary of Diployments signamics sPayTemPublishingService sSummary of Security Radius servicedim vitoers and	Graupt
Ski the Lock & Edit button to modify, add or felete items in this domain.	Create a New User		
Lock & Edit	DK. Cancel		
Palease Configuration	User Properties		
Domain Structure Bydoman	The following properties will be used to id * bridicates required fields	while your new User.	
7 Environment Deployments 7 Services	What would you like to name your new Use	et .	
Security Realms El Interoperability	*Name:	igsuser	
2 Diagnostics	How would you like to describe the new Us	er?	
	Description:	IGS service user	
	Please choose a provider for the user.		
	Provider:	DetsutAuthenticator 😕	
toer do I	The password is associated with the login r	ame for the new User.	
Create users	* Password		
 Modify users 	Password		
Delete users	* Confirm Passmort		
Create groups Manage users and groups			
Manage users and groups	OK Cancel		
ystem Status			
lealth of Punning Servers			
Paled (0) Critical (0) Overloaded (0)			
Warning (0)			

5. In the Create a New User screen, enter a username and password. Leave the default value for Provider. Click **OK** to save the information. The new user is added to the list of users.

Figure 3–17 Settings

Settings for myrealm - rb_domain - WLS Con.	1			
🕒 🕘 birdvitt Adr. orade.com: 7001/conscie/c	uncole portal?_rfgt=bruels_pageLabel=RealmUse	Maxagement/UserTabPage	(2) ≠ (2) (3) ★ Google	P 🔶
DRACLE WebLogic Server	Administration Console			Ó
hange Center	Hone Log Out Preferences 🔛 Proce	-: Heb Q	Welcome, weblogic	Connected to: rib_domain
iew changes and restarts		a sholes sholes s Summary of Diployments signatives sheethern Publishe	gService assumery of Security Realms anyreals allower and Generge	
ick the Lock & Edit button to modify, add or elete items in this domain.	Mensages			
Lock & Edit	Settings for myrealm			
Palease Configuration		oles and Policies Credential Mappings Providers Migration		
omain Structure	Users Groups			
b, dowan B: Environment — Cospoyments B: Services — Security Realms B: Otercopenability B: Otercopenability B: Diagnostics	This page displays information about each © Customize this table Users	user that has been configured in this security reals.		
	New [Oslints]		Showing 1 to	10 of 14 Previous Next
	🔲 Name 🙃	Description	Provider	
	🗈 fagadhin		DefaultAuthenticator	
en de L	igradnin i	igsadhin	DefaultAuthenticator	
eer do J	igiusier	igs user	DefaultAuthenticator	
Manage users and groups	gauser1	355 service user	DefaultAuthenticator	
Create users	CracleSystemLaar	Cracle application software system user.	DefaultAuthenticator	
ModPy users Delete users	🗋 rhadnan	rfiadhin	DefaultAuthenticator	
Leete users	i rbadnin	RIB Admin user.	DefaultAuthenticator	
stem Status 2	C rémisadrier	R2B Admin user.	DefaultAuthenticator	
abli of Running Servers	🖸 msadnin	HIB Adren user.	Def oult Authenticator	
Failed (0)	C rstuser	rsbuser	DefaultAuthenticator	
Critical (0) Overloaded (0) Warring (0)	New/ Delete		Showing L to	10 of 14 Previous Next

Note: You can add roles from the Roles and Policies tab of the security realm or through the Security tab of the Web service. The following instructions are for creating a role through the Security tab of the Web service.

6. Navigate to the **Security** tab of the Web service. Click the **Roles** tab.

Settings for PayTensPublishingService - rb	+				
🗧 🗟 birdvitt Jdc. orada.com 7001/conacie/o	uncole.portal?_rfpt=-truets_paget.abel=-WebServiceHodule	SecurityRoles fablePaget/handle+com.bes.co	oole hardes Modulariande("con.beat%34Name%3 😭 = 😋	🚼 • Google	P 🕹 1
	Administration Console				9
hange Center	🔒 Hone Log Out Preferences 🔛 Facant Help	Q		Welcome, weblogic	Connected to: rils_does
New changes and restarts	Hone sSummery of Deployments signaervice sPayTe	PublishingService xSummery of Security Real	is inversion induces and Groups inSummary of Deployments of sylfe	mPublishingService sPolicies siReles	
Ick the Lock & Edit button to modify, add or eleteritems in this domain.	Settings for PayTermPublishingService				
Lock & Edt	Overview Configuration Security Testing	Monitoring			
Palease Configuration	Roles Policies				
banuain Structure b, dowan 17 Environment 1 Services 11 Services 1 Services 11 Services 11 Services	This page summarizes the security roles that can b © Customize this table Web Service Module Scaped Roles	used only in the policy for this Web service	eodule,		
E Clagnostica	New Deline	1/2		Showing 0 to	0 of 0 Previous Next
	🗆 Name 🙃	Pro	vider Name		
			There are no items to display		
	New Oslata			Showing 0 to	0 of 0 Previous Next.
tow do I]				
Oracle scoped security roles Delete security roles Use roles and policies to secure resources					
ystem Status 🛛					
lealth of Running Servers	1				
Pailed (0) Critical (0) Overloaded (0) Warring (0) Crit (4)					

Figure 3–18 Settings for Web Service > Security > Roles Tab

7. In the **Roles** tab, click **New**. The Create a Web Service Module Role screen is displayed.

Figure 3–19 Create a Web Service Module Role

Be Edit View History Boolmarks Tool	ib_domain - WLS Console - Nozilla Firefox	
Create a Web Service Module Role - rb_dom		
Carade.com 7001/conscie/o	nich patal Witzenezhoù JeOnizel elenation num 10-witzenezhoù elenatio	P + 1
ORACLE WebLogic Server®	Administration Console	
Change Center	🔹 Hone Log Out Preferences 🖾 Rocard Help	ne, weblogic Corrected to: rik_dom
View changes and restarts	Hone stammer of Diploments vignamics silestambulatingServes stammer of Security Relation served in states and Goops stammer of Diploments vignambulatingServes violation silest	n .
Click the Lock & Edit button to modify, add or delete items in this domain.	Create a Web Service Module Role	
Lock & Edit	Dr. Carcel	
Parlease Configuration	Role Properties	
Domain Structure rb. doman	The following properties will be used to identify your new role. * Industries required fields	
Environment Cepkoyments Services	What would you like to name your new role?	
Security Realms	*Name: igsrcle	
E Diagnostics	Which role mapper would you like to use with this role?	
	Provider Names XACMLFioleMapper 👻	
	OK. Cecct	
Heer de 1		
Oreate scoped security roles Use roles and policies to secure resources		
System Status 🖂		
Health of Punning Servers		
Pailed (0) Critical (0) Overloaded (0) Warring (0) CK (6)		
WebLogs Service Version: 19.3.4.4 CopurgP4 © 1994, 2012, Oracle and Int Malein. 1	for philos to an Allen. Other sames may be budness bir of their regardine moment.	

8. In the Create a Web Service Module Role screen, enter the role name in the Name field (for example, rmsrole). Leave the default value in the **Provider Name** field. Click **OK**. The new role is displayed in the **Roles** tab of the Web service.

hange Center	🍘 Home Log Out Preferences 🐼 Record Help	Q		Welcome, weblogic Connected to: rib_doms	
lew changes and restarts	Home xSummary of Deployments xigs-service xPayTerrol	PublishingService >Summary of Security Reals	s xnyrealm xUters and Groups xSummary of Deployments xPayTemPublishingService	»Policies »Roles	
Sick the Lock & Edit button to modify, add or lelete items in this domain. Lock & Edit Release Configuration	Settings for PayTermPublishingService Overview Configuration Security Testing Roles Polices	Monitoring			
Domain Structure de, Januar - Daghanata -	The page numerous the security relies that can be used only in the palcy for this Web service module. © Constraints: this table: Web Service Priodels Rouged Rates				
	New Delete		der Name Roleftagger	Showing 1 to 1 of 1 Previous Next	
	New Delete	1000	cons abhan	Showing 1 to 1 of 1 Previous Next	
low do L					
Greate scoped security roles Delete security roles Use roles and policies to secure resources					
ystem Status 🖂					
ealth of Running Servers					
Paled (0) Critical (0) Overloaded (0) Warning (0) OK (4)					

Figure 3–20 Settings

9. To add the user to the role, click the name of the new role in the **Roles** tab. The Edit Web Service Module Scoped Roles screen is displayed.

Figure 3–21 Edit Web Service Module Scoped Roles

le Edit View Higtory Boolmarks Too Edit Web Service Module Scoped Roles - nb		
	** ustal Jonaile potali ritob-trusk, postabel-webServetikoldelisiesTablagebiebServetikoldelisiesTurkshande-con bea onsole handes Senathobactes 🖙 = 🖱 🔯 • Googe	• افر
ORACLE WebLogic Server		0
Change Center		ome, weblogic Connected to: rib_domain
View changes and restarts	Hone signatures was ferrabiliting Service vSummery of Security Helms many elements victors and Groups vSummery of Deployments whether Publishing Service whiches whether wheth	Medale Scoped Roles
Click the Lock & Edit button to modify, add or	Edit Web Service Module Scoped Roles	
delete items in this domain. Lock & Edit	Sam	
Palease Configuration	Web Service Rule Conditions	
Domain Structure	Use this page to edit the conditions of a security role scoped to this Web service module.	
burnain Structure budonain T Environment Ceptoyments	Contra a page to take the databases to a structury ran known of the take the models. This is the name role that is allowed to involve this Web Service.	
B Services Security Reality B Scheroperability B Chapponitics	Name: garde The following conditions determine exercises/by in the rate. Rate Conditions of	
	Add Conditions Contrine Uncontaine Mone Up, Mone Down, Remove Regards Ne Rolin Sportfall	
	See	
How do I		
Oreate scoped security roles		
Delete security roles		
Use roles and policies to secure resources Combine Conditions		
lystem Status II Health of Furning Servers		
Paled (0) Gitsul (0) Overloaded (0) Warning (0) Ok (4)		

10. In the Edit Web Service Module Scoped Roles screen, click **Add Conditions**. The **Choose a Predicate** option is displayed.

le Edit Yew Higtory Bookmarks Tools			
Edt Web Service Module Scoped Holes - rb	The set of WebGeworthod. Before/Furthet, actionCoverdee-Sconsbeaktonisbeaktonisbeau hotobies/addicordition/pseudo. Begin		P + 1
		The C LEAS coope	0
Anape Contex Mesh copic Server [®] Anape Contex Manape Contex Starte Lock 1 Cd Lock 1 Cd	Administration Consets		alogic Connected to: rib_domain
ee de L Croste rooped security roles Delete security roles Late role and polices to secure resources Combre Conditions			
yetens \$2 alus 30 inable of Running Servers Galaci (0) Garissal (0) Warning (0) Core (4)			

Figure 3–22 Choose a Predicate

11. From the Predicate List, select **User**. Click **Next**. The **Edit Arguments** option is displayed.

Figure 3–23 Edit Web Service Module Scoped Roles

	es - rib_domain - WLS Console - Mozilla Firefox			E 🖻 🛛
Ele Edit View Higtory Bookmarks Epsi Edit Web Service Module Scoped Roles - nb				
	entei neole partathintsien oothoduleitaleithurtiirt_actionOvienden/co		<pre>c[*] ≠ C[*] N • Goode</pre>	₽ ♣ ♠
ORACLE WebLogic Server		And completion that a Life shall be constructed	II - C III - with	0
	Administration Console			
Change Center	The second se	ecurity Revins workelin subject and Groups vSummery of Englishments when		slogic Connected to: rib_domain
View changes and restarts Cick the Lock b. Edit button to modify, add or	Edit Web Service Module Scoped Roles	ectual senses and another symmetry and point and	and the provide section of the sector secto	taped Kaner
delete items in this domain.	interest interest interested interests			
Lock & Edit	Back Next Finish Cancel			
Parlease Configuration	Edit Arguments			
Domain Structure	On this page you will fill in the arguments that pertain to th	e predicate you have chosen.		
rb_domain	User Argument Description			
Environment Deployments	User Argument Name:	Add		
H Services	1755.047 (BALIC SHERE CT)	(Addition		
Security Realms		igsuser		
Ciagnostics		Remove		
	Back, Next, Fresh, Cancel			
How do L.	1			
Onate scoped security roles				
Delete security roles				
Use roles and policies to secure resources				
Combine Conditions				
System Status	i			
Health of Fluming Servers				
Faled (0)				
Gritcal (0)				
Overloaded (0) Warring (0)				
CK (4)				
WebLopp Server Verson 30.3.4.0	e constantes			_
Copuright @ 2096, 2011, Oracle and/or #1 affiliates.	48 og Hernowened.			

12. In the **User Argument Name** field, enter the username created in the security realm. Click **Add**. The name will move down to the box below the Add button. Click **Finish**. The following screen is displayed.

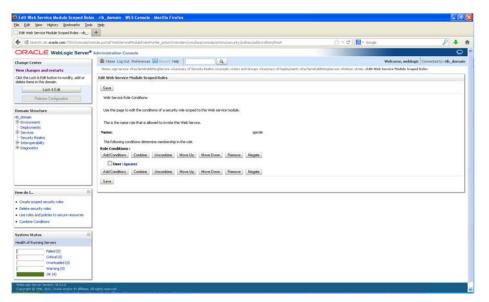


Figure 3–24 Edit Web Service Module Scoped Roles

13. Click **Save**. The same screen is displayed with this message near the top: *Changes saved successfully.*

Figure 3–25 Edit Web Service Module Scoped Roles

Edt Web Service Module Scoped Roles - rb	<u>*</u>			
🗲 🕙 birdvitt Adr. orada.com 7001/conacie/kar	node portal?WebService/NoduleFolesPurtiet_actionOvernde=j:conjSea/console/actions/vebcervice/roles/edUnodule/persuit	🗇 🕫 🕅 🖬 • Google	P 🕹 1	
ORACLE WebLogic Server®	Administration Console		Q	
Change Center West changes and restarts Dick the Lock & Edit button to eodify, add or delete Zems in this doman.	Know Log OL Preferences (20 Stort) Help Log Symmetric High Tender Help Tenses gravers with temperature of tenders fields: simple in stores of tenders and tenders and tenders Pressages Processing Processing		Corrected to: nb_domain Roles	
Lock & Edat Parlinane Configuration	Ridt Web Service Hodde Scopel Bales			
Jonnale Stockure Jonnal Polanomat Polanom	Und Service Rule Conditions Und Terrors Rule Conditions Und the conditions of a security rule scoped to the Web service module. This is the rune rule that is advand to involve the Web Service. The Rule-org conditions determine nearborhilp in the rule. Table Conditions Conditions Conditions (Conditions) More Down) Reserve Res			
teer de L. El	Januard (Langer, Langer, Lange			
Critical (0) Overloaded (0) Warning (0) OK (4)				

14. Return the **Security** tab of the Web service and click the **Policies** tab.

acide Performances (E. Parcant Help Innace «Sammer of Displayments comit-biblishingService aparticit (Security Testing Instages the security policy for th	Silver TemPLobbrog Service Werkomg Monitoring Monitoring Monitoring the Web service module. The Web service module.	Q na siPokoag siPok	anada Nardes Notderlande,"san a state web service Module Snaped I to web service operations. If the op	tales claumery of Exployments alle constances are implemented by Same	Winko w Tensk-JohdnergService strate: st n dissee, this policy also protects	is the Java inglementation. If the	rite_domain
acide Preferences 20 Decision Help Preferences of Decisioned particle Security Testing particle Security Testing particle Security Decision for H preference by an E&, this parksy thorization providers an admenti	Silver TemPLobbrog Service Werkomg Monitoring Monitoring Monitoring the Web service module. The Web service module.	Q na siPokoag siPok	s stårt Web Service Module Scoped ti stratet web service operations. 17 the op	tales claumery of Exployments alle constances are implemented by Same	Winko w Tensk-JohdnergService strate: st n dissee, this policy also protects	onne, webliegie Connected to: e indicise	C ritr_domain
acide Preferences 20 Decision Help Preferences of Decisioned particle Security Testing particle Security Testing particle Security Decision for H preference Dry on E&, this parksy thorization providers an admenti	Silver TemPLobbrog Service Werkomg Monitoring Monitoring Monitoring the Web service module. The Web service module.	Q na siPokoag siPok	s stårt Web Service Module Scoped ti stratet web service operations. 17 the op	tales claumery of Exployments alle constances are implemented by Same	Winko w Tensk-JohdnergService strate: st n dissee, this policy also protects	onne, webliegie Connected to: e indicise	rite_domain
Performances I Include Help Inners of Destruction International International International International International International International International International International International International International International International International Internat	n -Pry TemPublishing Servi g Manitoring this Web service module. I y protects the E38 method	na siPoksej siłok	ts Web service operations. If the o	perators are inclimiented by Java	when the second secon	Polities Is the Java exclementation. If the	rit domain
maps visionery of toplayments com/hubble/ing/Service paration Security Testing manage the security policy for it assume to security policy for it assume test by an E.R. this policy horization providers an achieved	n -Pry TemPublishing Servi g Manitoring this Web service module. I y protects the E38 method	na siPoksej siłok	ts Web service operations. If the o	perators are inclimiented by Java	when the second secon	Polities Is the Java exclementation. If the	
annihubblebingService puration Security Instru- nanage the security policy for th beneficied by an E.R., this policy horization providers an achieved	g Monitoring the Web service module. I y protects the E38 method	his policy protec	ts Web service operations. If the o	perators are inclimiented by Java	a classes, this policy also protects	is the Java inglementation. If the	
paration Security Testing	this Web service module. I y protects the EJB method	his policy protec	ts Web service operations. If the op from Web service dients; it does n	sentions are inglemented by Java of protect the LB when accessed	r classes, this policy also protects from E30 claents using RHS and 3	is the Java inclementation. 3' the JBCL	
nanage the security policy for the elemented by an EXIL, this policy thorization providers an administ	this Web service module. I y protects the EJB method	his policy protec Is when accesse	ts Web service operations. If the op of from Web service clerits; it does n	serations are inglemented by Java of protect the EBI when accessed	r classes, this policy also protects from LBD clients using RPM and 3	is the Java inglementation, 3' the 2001	
demented by an E30, this policy	y protects the E30 method	This policy protect is when accesse	ts Web service operations. If the op of from Web service clients; it does n	serations are implemented by Java of protect the EIB when accessed i	classes, this policy also protects from EJB clients using FMI and 3	is the Java inglementation, if the JACL	
demented by an E30, this policy	y protects the E30 method	his policy protec to when accesse	ts Web service operations. If the op of from Web service clients; it does n	serations are inglemented by Java of protect the EBI when accessed	classes, this policy also protects from IL3D clients using FMI and 3	is the Java inglementation, 3 ^o the JACL	
demented by an E30, this policy	y protects the E30 method	his policy protec Is when accesse	ts Web service operations. If the op f from Web service clents; it does n	serations are implemented by Java of protect the E38 when accessed	classes, this policy also protects from E30 clients using FMI and 3	is the Java inglementation. If the JACL	
ds in this Web service that you a have defined such a pokcy).	want to secure. You can e	ither secure ALL	XACMLAuthorizer	ie method. Any method that you di	Io not secure will be protected by	ry the policy for the Web Service's	parent
unders,			ALL M				
			Negate				
Conbine Unconbine	Move Up Move Dow	n Renove	Negate				
d wit na							
dtoo G	ontine Uncontine ontine Uncontine of	nis determine who is allowed to access this Web serv antime. Uncontaine, Move Up. Move Day antime. Uncontaine, Move Up. Move Day	ors determine who is allowed to actions the Web service. anteres (Monethine) More Up) (More Down) (Remove) anteres (Monethine) (More Up) (More Down) (Remove) at	und defensere who is allowed to access the Web serves. antere: [Schembers, [More Up); [More Down, [Remove, [Megate, antere: [Schembers, More Up]; [More Down, [Remove,]Megate, at	na deferenze who a dowed to actess the Web serves. antere Uskonstine More Up: More Down Remove Magne antere Uskonstine More Up: More Down Remove Magne A	reak mi ni deferme wie is diewel to konst bit Web service. antere Ustantiene Mans big Mons Dam, Remons, Negate, ak	res defermente velo la discondi la scresa flas Varde Laroneo. Indereza Educandeza Monestalio Mones Dona, Remova, Nagatar, Indereza Educandeza Monestalo Monestalo Remova, Nagatar,

Figure 3–26 Settings

15. On the **Policies** tab, click **Add Conditions**. The **Choose a Predicate** option is displayed.

Figure 3–27 Settings

	e - rib_domain - WIS Comole - Nozilla Firefox					
Elle Edit Year Higtory Bookmarks Book						
Settings for PayTemPublishingService + rb	*					
🗲 🕙 birdvitt Józ orada.com 7001/conacie/oz	nick portal WebServiceNodukSecurAuRolomPortiet_actionOveride=/com/bealconicke/actional=ebiervice/policies/led/incoduk/addCordition	∰ ≈ C Karte	₽ ♦ ♠			
ORACLE WebLogic Server®	Administration Console		0			
Change Center	A Hone Log Out. Preferences 🖾 Rocard Help	Welcome, we	eblogic Connected to: nlb_doenain			
View changes and restarts	Hane sitters and Groups Stammary of Deployments silvy TemPublishingService silvate sitchs staff Web Service Module Scoped Roles assummery of	Exployments vPayTemPublishingService vitales vPallecies				
Click the Lock & Edit button to modify, add or delete items in this domain.	Settings for PayTemiPublishingService					
Lock & Edit	Overview Configuration Security Testing Monitoring					
Pielease Configuration	Roles Policies					
Domain Structure	East Next Frish Carcel					
Ht., dawn Ht., dawn H. Characteristic H. Santa R. Salak Here de J	Oxnee e Producte Oxnee the products bit is a bit of enables products within can be used to inder up a security poly: condition Periodicate bit is Pole Items: Read:					
Use roles and policies to secure resources						
Contine Conditions						
System Status						
Health of Running Servers						
Pailed (0) Critical (0) Critical (0) Critical (0) Warning (0) Critical						
WebLoge Server Versey, 2018.0 Conseque & 196, 2018, Oracle and the Intelligence Oracle is a registered bademark of Gracie Corporati	ding for easi read. In a ships in a dilation. Other names may be historically of their expensive instruct.					

16. From the Predicate List, select **Role**. Click **Next**. The **Edit Arguments** option is displayed.

Figure 3–28 Settings

Settings for PayTermPublishingService - rb	*					
🗲 🕘 birdvitt kát orada.com .7001/conasie/o	ani de portel Nikóse-rochtoduk Securby folder Portier, jector Override-/com/bea/console/actional recurby/poloen/addoordoor/plap t	🗇 🕫 🕅 - Google	P + 1			
ORACLE WebLogic Server	Administration Console					
Change Center	Brites Lag Out. Preferences @ Rocall Help A House states and Groups statements of Deployments stray temPublishingService strates study with Service Module Scrapel Keles statement		logic Connected to: rils_doesa			
View changes and restarts Cick the Lock & Edit button to modify, add or						
delete items in this domain.	Settings for hyd TermiholliningService Denréem Carégation Security Tettag Mantang					
Lock & Edit						
Palease Configuration	Roles Policies					
Domain Structure	Back Need Cancel					
rb_donan ⊕ Environment Cestvouents	Edit Arguments On this page you will film the arguments that pertain to the predicate you have chosen.					
Services Security Realms	Add one or more roles to this condition, If you add nulliple roles, the condition evaluates as true if the user is in ANY of the roles.					
E Soberoperability E Diagnostics	Role Argument Name: Add					
	rgstole Remove					
teer de L	Back Ner Frish Canoel					
Onate policies for resource instances	-memory increase Instantion Instantion					
Use roles and policies to secure resources Combine Conditions						
System Status						
lealth of Running Servers						
Pailed (0) Critical (0) Overloaded (0) Warning (0) Cot (4)						

17. In the **Role Argument Name** field, enter the role name created earlier. Click **Add**. The role name will move down to the box below the **Add** button. Click **Finish** to return to the **Policy Conditions** screen.

Figure 3–29 Settings

Settras for Paylend/AddingService + rb +					
🗲) 🖲 birdivît Xir. orade.com 7001/conscie/o	niske portal Niebbennot NodulebeourbyPolicies/Portiet_justomOvernde=/com/bea/comole/actionaliseourby/policies/addoord/toah	😭 🕾 😋 🛃 • Google	P 🔶 1		
ORACLE WebLogic Server	Administration Console		- C		
Change Center	😰 Hone Log Out, Preferences 🐷 Proved Help	Welcome, w	eblogic Connected to: elb_doesa		
New changes and restarts	Hone within and Groups Stammery of Deployments sPayTemPlubittingService sPokset sPoles sUdit Web Service Module Scoped Roles sSumm	ary of Deployments silveyTemPublishingService silvales sPalleties			
Skk the Lock & Edit button to modify, add or felete items in this domain.	Sottops lar knyterneh Ablandspervice Overview Configuration Security Institut Nutritions Inster Marken				
Lock & Edt					
Palease Configuration					
Iomain Structure	Sam				
P: On-Account. Co-palyoneris P: Services F-Source Paales P: Storgonabley P: Congrestice	Las foi aports analysis free analysis of the trial design and analysis of the constant of the provide set of the provide set of a port of the port o	he EXE when accessed from EXE clerits using FPH and XAEC.			
tow do L	Web Service Methods: ALL				
	- Policy Conditions				
Create policies for resource instances Use roles and policies to secure resources	The following conditions determine who is allowed to access this Web service.				
Contine Conditions	Add Conditions Combine Uncombine Move Up, Move Down Remove Negate				
ystem Status 🛛 🗄	Add Conditions Combine Uncombine Move Up Move Down Remove Negate				
tealth of Running Servers	Save				
Pailed (0) Crexial (0) Creativated (0) Warning (0) Cik (4)	Decenden Policy Group I everyone				

18. Click **Save**. The Policy Conditions screen is displayed with this message near the top: *Changes saved successfully*.

le Edit View Higtory Bookmarks Took	1 Ma		Control Procession		
Settings for PayTernsPublishingService + rb	+				
🗧 🕘 birdvitt ids: orade.com 7001/conscie/os	node partal WebServiceRodukSecurityRokowRodski, unternOverride-jrom/ben/corride/actions/vebiervice/pokiers/veb/moduk/persist	☆ ≠ C [*]	P 🕹 1		
ORACLE WebLogic Server®	Administration Console	A CONTRACTOR OF A CONTRACTOR O	0		
hange Center	A Hone Log Out. Preferences 🖾 Second Help	Welcome, web	alogic Connected to: rib_domain		
New changes and restarts Ski the Lock & Edit button to modify, add or lelete items in this donian.	tens staar od droga stamov d bajonen strebabbrojevos stokas stala kali teks fores feak israel teks stamov d bajonen strebabbrojevos stala s ba kas Messages 🛫 Orangi sind azcelulaj				
Lock & Edit	Settings for PayTermPublishingService				
Release Configuration	Overview Configuration Security Testing Monitoring				
Domain Structure	Roles Policies				
€_down I "Californess". 1" Californess". 5" Concerns 5" Colongen ables 5" Colongen ables	Same Use the page to exempt the security poly/ for the Web server module. The poly portexts Web server operations. If the operation are is demented by an EX, the poly portexts the EX methods when accessed from Web server density. If due not portext the — Providers — These are the authorization providers in identification can select from. Methorization Providers: VACUM_Authorizer - Yethods	E 28 when accessed from E30 clients using FMI and 3401.			
tow do I 🗏	Select the methods in this Web service that you want to secure. You can either secure ALL methods (recommended) or only one method. An parent application (if you have defined such a policy).	w method that you do not secure will be protected by the p	olicy for the Web Service's		
Owate policies for resource instances	Web Service Methods: ALL				
Use roles and policies to secure resources Contine Conditions	- Policy Conditions The following conditions determine who is allowed to access this Web service.				
iystem Status 🛛	Add Conditions Combine Uncombine Move Up Move Down Remove Negate				
tealth of Running Servers	Role : igsrole				
Paled (0) Critical (0) Overloaded (0) Warring (0)	AddConditions Combine Discontine Non-Lip Mone Down Remove Negate Same Som Overmidde Index Gog: reworde				

Figure 3–30 Settings

Client-side Setup for Username and Password Authentication

The following is sample code for calling a secure IGS Web service.

Note: The following is sample code for invoking the *PayTermPublishingService* service. When you generate Java consumer for a Web service, the generated jar file contains classes specific to that Web service. Use the appropriate classes in the client code. Service namespace and WSDL location also should be changed accordingly.

```
package com.oracle.retail.rms.client;
import java.net.URL;
import java.util.ArrayList;
import java.util.List;
import java.util.Map;
import javax.xml.namespace.QName;
import javax.xml.ws.BindingProvider;
import
com.oracle.retail.igs.integration.services.paytermpublishingservice.v1.PayTermPubl
ishingPortType;
import
com.oracle.retail.igs.integration.services.paytermpublishingservice.v1.PayTermPubl
ishingService;
import
com.oracle.retail.iqs.integration.services.paytermpublishingservice.v1.PublishPayT
ermCreateUsingPayTermDesc;
import
com.oracle.retail.igs.integration.services.paytermpublishingservice.v1.PublishPayT
ermCreateUsingPayTermDescResponse;
import com.oracle.retail.integration.base.bo.paytermdesc.v1.PayTermDesc;
import weblogic.wsee.security.unt.ClientUNTCredentialProvider;
import weblogic.xml.crypto.wss.WSSecurityContext;
import weblogic.xml.crypto.wss.provider.CredentialProvider;
import junit.framework.TestCase;
```

```
public class PayTermPublishingClient extends TestCase {
public void testCreatePayTermDesc() {
trv {
// gName is namespace of the service
QName qName = new
QName("http://www.oracle.com/retail/igs/integration/services/PayTermPublishingServ
ice/v1", " PayTermPublishingService");
// url is the URL of the WSDL of the web service
URL url = new
URL("http://10.141.29.190:18030/PayTermPublishingBean/PayTermPublishingService?WSD
L");
// Create an instance of the web service
PayTermPublishingServiceservice = new PayTermPublishingService (url,qName);
PayTermPublishingPortType = service.getPayTermPublishingPort ();
// Set the security credentials in the service context
List credProviders = new ArrayList();
CredentialProvider cp = new ClientUNTCredentialProvider("<rms user>","<rms
password>");
credProviders.add(cp);
Map<String, Object> rc =
                                    ((BindingProvider)port).getRequestContext();
rc.put(WSSecurityContext.CREDENTIAL_PROVIDER_LIST, credProviders);
// Populate the service method input object
PayTermDesc payTermDesc = new PayTermDesc();
payTermDesc.setTerms("terms");
PublishPayTermCreateUsingPayTermDesc payTermCreateDesc = new P
PublishPayTermCreateUsingPayTermDesc();
payTermCreateDesc.setPayTermDesc(payTermDesc);
// Call the web service
PublishPayTermCreateUsingPayTermDescResponse response =
port.publishPayTermCreateUsingPayTermDesc(payTermCreateDesc,"1");
System.out.println("response="+response);
}catch(Exception e) {
  e.printStackTrace();
}
}
```

Server-side Setup for Encrypted Username and Password Token Authentication

WebLogic provides predefined policy files for securing Web services. This section describes the process required to secure a Web service where username and password are encrypted and signed.

Take the following steps to secure the Web service:

 Follow the steps to attach the policy file to the Web service described in the section, *Attach Policy File to the Web Service*, with this exception: In Step 7, select *policy:Wssp1.2-2007-Wss1.1-UsernameToken-Plain-X509-Basic256.xml* (instead of *policy:usernametoken.xml*). Follow the remaining steps as described.

After attaching the policy file, the header for the WSDL of the Web service contains the following:

}

```
<wsp:UsingPolicy wssutil:Required="true"/>
<wsp:Policy
wssutil:Id="Wssp1.2-2007-Wss1.0-UsernameToken-Plain-X509-Basic256.xml">
<ns1:AsymmetricBinding
xmlns:ns1="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
<wsp:Policv>
<ns1:InitiatorToken>
<wsp:Policy>
<ns1:X509Token
ns1:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/Inc
ludeToken/AlwaysToRecipient">
<wsp:Policy>
<ns1:WssX509V3Token10/>
</wsp:Policy>
</nsl:X509Token>
</wsp:Policy>
</nsl:InitiatorToken>
<ns1:RecipientToken>
<wsp:Policy>
<ns1:X509Token
ns1:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/Inc
ludeToken/Never">
<wsp:Policy>
<ns1:WssX509V3Token10/>
</wsp:Policy>
</nsl:X509Token>
</wsp:Policy>
</nsl:RecipientToken>
<ns1:AlgorithmSuite>
<wsp:Policy>
<ns1:Basic256/>
</wsp:Policy>
</ns1:AlgorithmSuite>
<ns1:Layout>
<wsp:Policy>
<ns1:Lax/>
</wsp:Policy>
</nsl:Layout>
<ns1:IncludeTimestamp/>
<ns1:ProtectTokens/>
<ns1:OnlySignEntireHeadersAndBody/>
</wsp:Policy>
</ns1:AsymmetricBinding>
<ns2:SignedEncryptedSupportingTokens
xmlns:ns2="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
<wsp:Policy>
<ns2:UsernameToken
ns2:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/Inc
ludeToken/AlwaysToRecipient">
<wsp:Policy>
<ns2:WssUsernameToken10/>
</wsp:Policy>
</ns2:UsernameToken>
</wsp:Policy>
</ns2:SignedEncryptedSupportingTokens>
<ns3:Wss10
xmlns:ns3="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">
<wsp:Policy>
<ns3:MustSupportRefKeyIdentifier/>
<ns3:MustSupportRefIssuerSerial/>
```

```
</wsp:Policy>
</ns3:Wss10>
</wsp:Policy>
```

- **2.** The key combination used by the client to sign the message is a valid one for the server. The client certificate must be signed with a certificate authority that is trusted by the server.
- **3.** WebLogic instances include a demo CA. The certificate and key for it is in *\$WL_HOME/Middleware/wlserver_10.3/server/lib/CertGenCA.der* and *CertGenCAKey.der*. The key does not appear to change between WebLogic installations and is trusted by the default *DemoTrust* store. For this reason, the DemoTrust store must never be enabled in a production environment. Otherwise anybody can become "trusted" fairly easily.
- **4.** WebLogic CertGen command can be used for generating keys of the correct key length and signing them with the demo CA noted above. A client certification/key pair is required to sign the outgoing message and server certificate to encrypt the critical information.

```
java -classpath $WL_HOME/Middleware/wlserver_10.3/server/lib/weblogic.jar
utils.CertGen -certfile ClientCert -keyfile ClientKey -keyfilepass ClientKey
-cn <rms user>
```

The above command generates the following files:

- 1. ClientCert.der
- 2. ClientCert.pem
- 3. ClientKey.der
- 4. ClientKey.pem

In the above example of a command, the username is <rms user>. Replace <rms user> with the username of the user who will access the Web service.

5. The command below generates the four files that follow it:

```
java -classpath $WL_HOME/Middleware/wlserver_10.3/server/lib/weblogic.jar
utils.CertGen -certfile ServerCert -keyfile ServerKey -keyfilepass ServerKey
-cn <rms user>
```

- 1. ServerCert.der
- 2. ServerCert.pem
- 3. ServerKey.der
- 4. ServerKey.pem

In the above example of a command, the username is <rms user>. Replace <rms user> with the username of the user who will access the Web service.

6. Using the following commands, import the files into key stores:

```
java -classpath $WL_HOME/Middleware/wlserver_10.3/server/lib/weblogic.jar
utils.ImportPrivateKey -certfile ClientCert.der -keyfile ClientKey.der
-keyfilepass ClientKey -keystore ClientIdentity.jks -storepass ClientKey -alias
identity - keypass ClientKey
```

```
java -classpath $WL_HOME/Middleware/wlserver_10.3/server/lib/weblogic.jar
utils.ImportPrivateKey -certfile ServerCert.der -keyfile ServerKey.der
-keyfilepass ServerKey -keystore ServerIdentity.jks -storepass ServerKey -alias
identity - keypass ServerKey
```

7. Using the script in Appendix: configWss.py, configure the WebLogic server to use the key. Copy the script and save it in the location from which it will run.

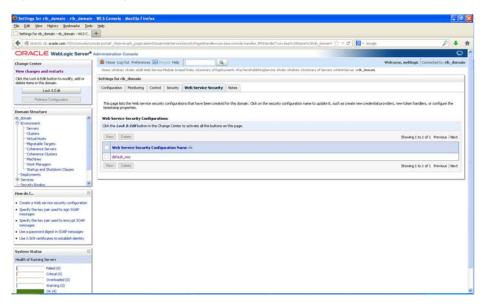
java -classpath \$WL_HOME/Middleware/wlserver_10.3/server/lib/weblogic.jar weblogic.WLST configWss.py <weblogicuser> <WebLogic Password> <weblogichost> <weblogic admin port> ServerIdentity.jks ServerKey identity ServerKey

For example:

java -classpath \$WL_HOME/Middleware/wlserver_10.3/server/lib/weblogic.jar weblogic.WLST configWss.py weblogic <*WebLogic Password>* localhost 7001/home/wls/ServerIdentity.jks ServerKey identity ServerKey

8. In the WebLogic logic console, check the **Web Service Security** tab to verify that the command ran properly. Note that the default_www configuration is used for all Web services unless otherwise indicated.

Figure 3–31 Settings



- **9.** After the certificate setup is completed for the Web service, follow the steps in the "Create Roles and Users" section to create a user in WebLogic to access the Web service.
- **10.** Restart the server. Create a client to invoke the Web service.

Client-side Setup for Encrypted Username and Password Token Authentication

The following is sample code for calling a Web service that is secured using the policy file, policy:Wssp1.2-2007-Wss1.1-UsernameToken-Plain-X509-Basic256.xml:

```
package com.test;
import java.net.URL;
import java.security.cert.X509Certificate;
import java.util.ArrayList;
import java.util.List;
import java.util.Map;
import java.xml.namespace.QName;
import javax.xml.ws.BindingProvider;
```

```
import javax.xml.ws.WebServiceRef;
import
com.oracle.retail.igs.integration.services.paytermpublishingservice.v1.PayTermPubl
ishingPortType;
import
com.oracle.retail.igs.integration.services.paytermpublishingservice.v1.PayTermPubl
ishingService;
import
com.oracle.retail.igs.integration.services.paytermpublishingservice.v1.PublishPayT
ermCreateUsingPayTermDesc;
import.
com.oracle.retail.igs.integration.services.paytermpublishingservice.v1.PublishPayT
ermCreateUsingPayTermDescResponse;
import com.oracle.retail.integration.base.bo.paytermdesc.v1.PayTermDesc;
import weblogic.security.SSL.TrustManager;
import weblogic.wsee.security.bst.ClientBSTCredentialProvider;
import weblogic.wsee.security.unt.ClientUNTCredentialProvider;
import weblogic.wsee.security.util.CertUtils;
import weblogic.xml.crypto.wss.WSSecurityContext;
import weblogic.xml.crypto.wss.provider.CredentialProvider;
public class Client {
public static void main(String args[]) {
try {
//qName is namespace of the service
QName qName = new
QName("http://www.oracle.com/retail/igs/integration/services/PayTermPublishingServ
ice/v1", " PayTermPublishingService");
// url is the URL of the WSDL of the web service
URL url = new
URL("http://10.141.29.190:18030/PayTermPublishingBean/PayTermPublishingService?WSD
L":
// Create an instance of the web service
PayTermPublishingServiceservice = new PayTermPublishingService(url,qName);
PayTermPublishingPortType = service.getPayTermPublishingPort ();
PayTermDesc payTermDesc = new PayTermDesc();
payTermDesc.setTerms("terms");
PublishPayTermCreateUsingPayTermDesc payTermCreateDesc = new
PublishPayTermCreateUsingPayTermDesc();
payTermCreateDesc.setPayTermDesc(payTermDesc);
String serverCertFile = "D:/head/retail-soa-enabler/dist/client/ServerCert.der";
String clientKeyStore =
"D:/head/retail-soa-enabler/dist/client/ClientIdentity.jks";
String clientKeyStorePass = "ClientKey";
String clientKeyAlias = "identity";
String clientKeyPass = "ClientKey";
List credProviders = new ArrayList();
ClientUNTCredentialProvider unt = new ClientUNTCredentialProvider("<rms
user>","<rms password>");
credProviders.add(unt);
final X509Certificate serverCert =
(X509Certificate)CertUtils.getCertificate(serverCertFile);
serverCert.checkValidity();
CredentialProvider cp = new ClientBSTCredentialProvider(clientKeyStore,
clientKeyStorePass,clientKeyAlias, clientKeyPass, "JKS", serverCert);
credProviders.add(cp);
```

```
Map requestContext = ((BindingProvider)port).getRequestContext();
requestContext.put(WSSecurityContext.CREDENTIAL_PROVIDER_LIST, credProviders);
requestContext.put(WSSecurityContext.TRUST_MANAGER,new TrustManager() {
public boolean certificateCallback(X509Certificate[] chain,int validateErr) {
boolean result = chain[0].equals(serverCert);
return result;
}
});
PublishPayTermCreateUsingPayTermDescResponse response =
port.publishPayTermCreateUsingPayTermDesc(payTermCreateDesc,"1");
System.out.println("response="+response);
} catch(Exception e){
e.printStackTrace();
}
}
}
```

Security Feature Overview

Caution: Oracle is not responsible for the security compliance of any product customization performed by a retailer, system integrator, or reseller.

The relevant security features fall into one or more of the following categories. For information on these categories, see the following sections:

- Securing Sensitive Data
- Securing the Application
- Securing the Application Environment and Configuration

Securing Sensitive Data

The protection of sensitive data during transit, processing, and storage is paramount. Sensitive data includes personally identifiable information such as credit card number, Social Security number, checking account number, and positive ID such as driver's license number. The Oracle Retail Integration Bus focuses on protecting sensitive data.

Cardholder Data

RIB, being an integration application, does not store credit card data. The applications getting integrated through RIB handle all access to cardholder data and supply tokens to use in place of actual cardholder data.

Communication with web service Application

An additional layer of communication security is provided for web application (example: OMS). These applications require the use of a Secure Socket Layer (SSL) to access them.SSL provides an additional layer of encryption and security of the information sent to and received from these applications.

Securing the Application

Securing access to the application against malicious attacks and auditing secure events are accomplished with passwords, additional testing of Web applications, and additional examination of source code.

Passwords

The RIB administration user interface username and password for accessing the user interface are created and stored inside the WebLogic Server security realm, and are protected by your WebLogic security configuration. For more information, see the *Oracle Retail Integration Bus Installation Guide*.

Default Accounts and Passwords

RIB applications do not contain any default accounts, user IDs, or passwords. An application username and password are entered by the user during the installation process.

Tools

RIB uses the Fortify 360 tool to scan for security issues. As with any tool, the output of this tool should be analyzed in detail since the output may contain false positive warnings. You can use any tools that you choose. No recommendation of the following tool is intended or implied. Fortify 360 is a tool that analyzes software for vulnerabilities. The static analysis component examines an application's source code for potentially exploitable vulnerabilities. The dynamic analysis component identifies vulnerabilities that can be found only when an application is running. All vulnerabilities can be ranked according to their relevance. Fortify can be found at the following website: http://www.fortify.com

Securing the Application Environment and Configuration

Securing the application environment and configuration covers the following areas:

Database

Database

If sensitive data is stored in a database, that data must be protected from unauthorized access. Oracle Retail provides the following recommendations protecting data:

- Access to the stored procedures used in the data purge scripts should be restricted.
- Authentication to the database should be done with a different user ID than authentication to the applications.

RIB does not populate the database with any pre-defined users. An administrative user is created during installation.

Credential Store Framework

A credential store is used for the secure storage of credentials. The credential store framework (CSF) API is used to access and perform operations on the credential store.

CSF provides the following capabilities:

- Enables the secure management of credentials.
- Provides an API for the storage, retrieval, and maintenance of credentials.
- Supports file-based, such as Oracle wallet, and LDAP-based credential management.

Oracle Retail RIB CSF Implementation

Oracle Retail Integration Bus protects authentication passwords using CSF and Oracle wallet. The credentials are stored and retrieved from the Oracle wallet store using APIs. Credential Store Manager is the utility which provides methods that can store and retrieve credentials from a wallet based file. Internally, this utility uses CSF API to manage the credentials.

Keytool Utility

The keytool utility is included with the JRE. It is used to create new keys, import digital certificates, export existing keys, and interact with the key management system.

Creating a Self-Signed Certificate

To create a self-signed certificate, use the following command. It creates a private key and a self-signed certificate that contains the corresponding public key:

keytool -genkey -keystore <keystore_location> -alias <your_alias> -keyalg RSA

Creating a Certificate Signing Request

To obtain a certificate signed by a real Certificate Authority, create a Certificate Signing Request:

1. Use the following command to generate the request:

```
keytool -certreq -keystore <keystore_location> -alias <your_alias> -file <your_
file.cer>
```

- 2. Once the Certificate Signing Request is saved in a file, send it to the Certificate Authority of your choice. To get a trial certificate, see the following Web site: https://www.thawte.com
- **3.** When the response from the Certificate Authority is received, save the certificate in a file from which it can be imported. In order to import the certificate, the root certificate must be in your list of trusted certificate authorities, or you must accept the root certificate selected by the keytool utility.
- 4. To import the certificate, use the following command:

```
keytool -import -keystore <your_keystore_name> -file <your_certificate_
file.cer> -alias <your_alias> -trustcacerts
```

For development or testing purposes, it should not be necessary to get a trial certificate or have your certificate signed.

Exporting and Importing Certificates

The server in an SSL conversation must have a private key and a certificate that verifies its identity.

- The private key is used by the server as a part of the key exchange algorithm.
- The certificate is sent to the client to identify the server. This information is obtained from the Key Store.

• The truststore is used by the client to verify the certificate that is sent by the server.

To populate the truststore with the public certificate of a server:

1. Export the RSA certificate (without the private key) from the server Key Store. For information on creating the certificate, see "Creating a Certificate Signing Request".

```
keytool -export -keystore <your_keystore> -alias <your_alias> -file <your_
file.cer>
```

2. Import the RSA certificate into the truststore.

```
keytool -import -alias <your_alias> -keystore <your_truststore> -file <your_
file.cer>
```

The certificate can be imported into any of the following files:

- cacerts, which is the default java truststore.
- jssecacerts, java truststore

Secure Web Services

Oracle Retail Integration Bus uses Web services for its integrations with Oracle Retail Management System. This appendix discusses security for the Web services.

WS-Security

The OASIS WS-Security specification is the open standard for Web services security. Its goal is to enable applications to secure SOAP message exchanges by providing encryption, integrity, and authentication support. WS-Security offers a general-purpose mechanism for associating security tokens with message content. The specification defines these approved token types:

- Username Token Profile
- X.509 Certificate Token Profile
- Security Assertion Markup Language (SAML) Token Profile

Web Service Security Implementation

Oracle Retail Management System Web services are protected using the WS-Security user authentication mechanism. Clients who want to access these Web services have to provide a valid user ID and password using a WS-Security Username Token.

Oracle Retail Management System Web Service

Oracle Retail Integration Bus can communicate with both secured and unsecured Oracle Retail Management System Web services. If the Web service is secured, the Oracle Retail Integration Bus adds the Username Token to the request.

Glossary

Glossary Term Element Structure is GlossEntry Followed by GlossTerm

The definition follows in a GlossDef element and a child Para or other appropriate element. The GlossDef element can contain informal examples, lists, and so on.

A LINE_OF_SYNTAX

Or you might have a line of code as part of your definition.